Метод оцінки ефективності безпеки конфіденційних даних розподіленої інформаційної системи

Сергій Лєнков[1], Володимир Джулій[2], Ігор Муляр[3]

[1] Військовий інститут Київського національного університету імені Тараса Шевченка
Юлії Здановської, 81, Київ, Україна, 03189
[2,3] Хмельницький національний університет
вул. Інститутська, 11, Хмельницький, Україна, 29000
[1] lenkov_s@ukr.net, https://orcid.org/0000-0001-7689-239X
[2] dzhuliivm@khmnu.edu.ua, http://orcid.org/0000-0003-1878-4301
[3] muliariv@khmnu.edu.ua, http://orcid.org/0000-0002-6659-605X

Received 13.05.2024, accepted 20.05.2024
https://doi.org/10.32347/uwt.2024.14.1201

Анотація. В роботі запропоновано метод оцінки ефективності безпеки конфіденційних даних розподіленої інформаційної системи, заснований на моделі визначення актуальних загроз безпеки конфіденційних даних в інформаційній системі, на алгоритмах нечіткого виводу та теорії нечітких нейронних систем, на відміну від відомих, використовує достатні та необхідні показники, виключає помилки експертів, збільшує виявлення кількості актуальних загроз безпеці конфіденційних даних інформаційної системи на 5%, знижує витрати на закупівлю засобів захисту інформації від 15 до 30%. Враховує наступні фактори: IT-інфраструктуру розподіленої інформаційної системи, можливості зловмисників та їх рівень мотивації в інформаційній системи.

Запропонований підхід відрізняється від існуючих автоматизованим процесом, необхідністю залученням фахівців високої кваліфікації в області безпеки інформації, має низьку обчислювальну складність; відсутність недоліків експертних оцінок; дозволяє визначати перелік актуальних загроз безпеки даних в інформаційних системах різних класів та типів.

Задача забезпечення безпеки конфіденційних даних є актуальною, що обумовлено, зростанням комп'ютерних атак та витоків інформації, що відображаються у статистичних даних скоєння злочинів у сфері високих технологій, зростання кримінальної активності з використанням сучасних комунікаційних пристроїв та інтернет.

Існуючі методи виявлення загроз та оцінки ефективності безпеки конфіденційних даних не можуть бути задіяні на всіх етапах життєвого циклу інформаційних систем - не враховують в

комплексі наступні показники: IT-інфраструктуру розподілених систем, актуальні загрози інформаційної безпеки, вимоги безпеки конфіденційних даних, їх вартість як важливих показників при вирішенні даних задач

Однією з найважливіших задач забезпечення безпеки конфіденційних даних є оцінка ефективності системи захисту. У зв'язку з цим мета роботи - підвищення якості оцінки безпеки конфіденційних даних розподіленої інформаційної системи за рахунок визначення достатніх та необхідних показників з використанням сучасних інформаційних технологій, що дозволяють найбільш ефективно вирішувати наступні задачі: визначення параметрів роботи адап-

тивних продукційних нечітких нейронних систем, що найбільш підходять для вирішення поставлених задач, застосування технологій Data Science при обробці даних, алгоритмів нечіткого виведення.

Ключові слова: метод, інформаційна безпека, розподілені інформаційні системи, вразливості, атаки, конфіденційні дані.

ВСТУП

Інформаційна безпека стає все більш важливою та значущою сферою національної безпеки України, що відображено у Доктрині інформаційної безпеки України, затвердженої Указом Президента України від 25 лютого 2017 року № №47/2017 [1]. Відповідно до Доктрини, на теперішній час, інформаційні технології набули глобального характеру і стали невід'ємною частиною всіх сфер діяльності держави, суспільства та особистості. Розширення сфер застосування інформаційних технологій, на сучасному етапі, значно розширює перспективи розвитку нових інформаційних загроз та атак. Зарубіжні спеціальні служби розширюють інформаційно-психологічний вплив, спрямований на дестабілізацію соціальної та внутрішньо-політичної ситуації в різних регіонах світу, що призводить допорушення територіальної цілісності та підриву суверенітету інших держав. [2].

Значно зростають масштаби комп'ютерної злочинності: у кредитно-фінансовій сфері суспільства, у сфері оборони держави, в економічній сфері, в області державної та суспільної безпеки, в галузі науки, освіти та технологій, в області рівноправного стратегічного партнерства та стратегічної стабільності [2].

Одночасно, з розвитком та зростанням інформаційних технологій зростає і кількість засобів та методів порушень стану безпеки конфіденційних даних інформаційної системи. Протягом останніх років спостерігається різке зростання кількості витоків конфіденційних даних (зі звіту експертно-аналітичного центру групи компаній SafeNet). Змінити ситуацію можливо шляхом розробки нових методів, підходів які можуть надати надійний захист конфіденційних даних [4-6].

Задача забезпечення безпеки конфіденційних даних є актуальною, що обумовлено, зростанням комп'ютерних атак та витоків інформації, що відображаються у статистичних даних скоєння злочинів у сфері високих технологій [8,9], зростання кримінальної активності з використанням сучасних комунікаційних пристроїв та інтернет у 2021 році склало 39%. Кожен двадцятий злочин, відповідно до числа всіх зареєстрованих злочинів класифікується як кіберзлочин [11,12]. У 2021 році серед скоєних комп'ютерних злочинів лідирують злочини, які передбачають використання, розповсюдження, створення комп'ютерних «вірусів». Друге місце в незаконній електронній діяльності, займає шахрайство з використанням сервісів онлайн-платежів [9]. Кількість таких правопорушень у першому півріччі 2022 р. зросла у 8 разів. Іншим прикладом зростання витоків інформації є щорічні звіти міжнародної компанії Group-IB, в яких йдеться про активність проурядових організацій, які займаються проведенням атак на користь своїх держав. Відповідно до звіту "Hi-Tech Crime Trends 2021-2022", відзначається збільшення кібератак з використанням відповідного шпигунського програмного забезпечення, бекдорів, шифрувальників, зростання фінансового шахрайства з використанням соціальної інженерії та збільшення атак на банки, мотив кіберзлочинців - крадіжка інформації, за яку можна отримати винагороду.

Існуючі методи визначення актуальних загроз інформаційної безпеки та оцінки ефективності безпеки конфіденційних даних не можуть бути задіяні на всіх етапах життєвого циклу, не враховують в комплексі наступні показники: IT-інфраструктуру розподілених інформацій-них систем, актуальні загрози інформаційної безпеки, вимоги безпеки конфіденційних даних, перелік засобів захисту інформації та їх вартість, як важливих показників при вирішенні даних задач [10, 11]. Одночасно з цим, для розглянутих методів визначення загроз інформаційної безпеки та оцінки ефективності системи захисту залишається мета - підвищення ефективності, з огляду

визначення кількості актуальних загроз інформаційної безпеки, виконання закладених вимог до безпеки інформації, зниження вартості витрат на проектування системи захисту інформації, а також мінімізація помилок експертів.

На підставі проведеного аналізу можна зробити висновок про необхідність удосконалення методів оцінки ефективності безпеки конфіденційних даних розподілених інформаційних систем.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ ТА ПОСТАНОВКА ЗАДАЧІ

Ефективність системи захисту конфіденційних даних - ступінь відповідності результатів захисту інформації меті захисту інформації. Для проведення оцінки ефективності безпеки конфіденційних даних необхідно визначити метод та відповідні показники.

Основні методи оцінки ефективності захисту інформації розподілених систем наступні: імовірнісний; статистичний; експертний; частотний; інформаційно - ентропійний; формальний (матричний); метод мінімізації ризиків; нейромережний (багатокритеріальний); оптимізаційний (комбінаторний); багато-рівневий [9,11].

Статистичний метод - проводиться обробка потенційних атак, загроз та їх наслідків. Показник оцінки ефективності - загроза *i*-го типу виникає в середньому за період T_i.

Ймовірнісний метод - визначається можливість відмови інформаційної системи від обробки даних в результаті проведення успішної загрози. Сумарні втрати розраховуються за формулою (1):

$$R = \sum_{i=1}^{2^m} \sum_{j=1}^{2^m} P\left(\frac{\vec{\gamma}}{\vec{S}}\right) P\left(\vec{S}\right) \prod\left(\vec{\gamma}, \vec{S}\right) + m, \quad (1)$$

де $P\left(\frac{\vec{\gamma}}{\vec{S}}\right)$ - ймовірність усунення, $P\left(\vec{S}\right)$ - ймовірність стану об'єкта контролю, $\prod\left(\vec{\gamma}, \vec{S}\right)$ - втрати прийняття рішення при стані об'єкта *S*, *m*- кількість виявлених загроз безпеці даних.

Частотний метод - на підставі аналізу статичної інформації визначається значення *S*, величина *V* вибирається в діапазоні від 1 до максимальної можливої суми втрат, розраховується значення показника R_i, як функції параметрів *V* і *S*. Показник оцінки ефективності системи - очікувані втрати від *i*-ї загрози (2):

$$R_i = F\left(S, V\right), \quad (2)$$

де *S* показник частоти виникнення загрози безпеці даних, *V* - умовний показник шкоди.

Експертний метод - визначається кількість *n* параметрів, що характеризують систему захисту інформаційної системи. Задаються суб'єктивні значення коефіцієнтів важливості W_i, кожної з характеристик G_i призначені експертним шляхом. Розраховується значення параметра *SR*. Показник оцінки ефективності системи - ступінь забезпечення безпеки даних *SR* системи *S* розраховується за формулою (3):

$$SR_{(s,r)} = \frac{1}{n_{i-1}^{n}} W_i G_{i,} \quad (3)$$

Інформаційно-ентропійний метод - проводиться аналітичне обчислення ентропії інформаційної системи, використовуючи, при цьому, поняття згортки функції. У випадку лінійної залежності ефективність інтеграції систем вважають задовільною, інакше неефектив-ною. Показником оцінки ефективності є величина ентропії Шеннона (4):

$$\psi\left(t\right) = \left(\int_0^{\tau} S_n\left(t-\tau\right) ... \left(\int_0^{\tau} S_3 \left(\int_0^{\tau} S_1\left(\tau\right) S_2\left(t-\tau\right) dt \right) dt ... \right) dt \right), \quad (4)$$

де $S_1,...,S_n$ - значення ентропій інформаційних різних підсистем.

Нейромережевий метод (багатокритеріальна оцінка). Приналежність до певного рівня безпеки даних визначається в діапазоні [0,1], показники надійності є функцією прилежності: $\mu^A(x_i)$, x_i, елемент множини X - вимог щодо безпеки даних, A - множина значень, що визначають виконання вимог щодо безпеки даних.

Оцінка ефективності системи захисту інформаційної системи проводиться за чітко визначених показників. Нечіткі показники системи захисту розподіленої системи - лінгвістичні змінні, такі як «середній ступінь захищеності», «низький ступінь захищеності» «високий ступінь захищеності».

Метод мінімізації ризиків, реалізується за наступними кроками: фіксація ризиків безпеки даних; індекс ризику; проводиться класифікація ризиків; визначаються методи обробки ризиків безпеки даних; розраховуються показники, що характеризують ризики; розраховуються показники економічного ефекту управління ризиками безпеки даних. Показником оцінки ефективності - показник економічного ефекту захисту даних управління ризиками, розраховується за формулою (5)

$$E = \left(\sum_{i=1}^{N} M_{oi} - \sum_{i=1}^{N} M_i\right) - \left(\left(\sum_{i=1}^{N} I_{\phi i} + \sum_{i=1}^{N} H_{\phi i}\right) + \left(\sum_{j=1}^{K} I_{\phi ni} + \sum_{j=1}^{K} H_{\phi ni}\right)\right), \quad (5)$$

де M_o - сумарні ймовірні втрати без обробки ідентифікованих ризиків, M - сумарні ймовірні втрати після обробки ризиків, I_ϕ - сумарні фактичні втрати від прояву ризиків, $I_{\phi н}$ - сумарні фактичні втрати від прояву ризиків, $H_{\phi н}$ - сумарні фактичні витрати на обробку ризиків

Матричний метод (формальні моделі захисту) реалізується наступними кроками:
- визначаються параметри;
- складається матриця відношень;
- перетворення матриці на двовимірну матрицю;
- визначаються кількісні та якісні значення показників.

Показником оцінки ефективності системи є стан системи захисту, описаний параметрами: (*S, O, M*) - множини *S* - суб'єктів, *O* - об'єктів, *M* - прав доступу або (*O, H, M*), де *O* - складові та основи частини системи (технічна, нормативно-правова, організаційна), *H* - напрями захисту, *M* - етапи створення системи захисту.

Багаторівневий метод використовує модель Д. Деннінга та модель кінцевих станів Белла Ла-Падули. Стан системи захисту описується наборов категорій конфіденційності та сукупністю рівнів конфіденційності. Метод використовує алгоритми нечіткої логіки [9, 11].

Комбінаторний (оптимізаційний) - вирішується задача дискретного програмування типу: максимізувати $\sum_{j=1}^{n}\left(c_j x_j\right)$ за умов:

$$\sum_{j=1}^{n}\left(a_{ij} x_j\right) \le b_i;\ i=\overline{1,m},\ x_j \in \{0,1\}\ j=\overline{1,n}.$$

Недоліки та переваги методів [11] оцінки ефективності системи захисту наведені в Табл. 1.

Аналіз проведених досліджень показав, що існуючі методи оцінки ефективності системи захисту мають низку недоліків, що зумовлює необхідність підвищення якостей існуючих на теперішній час методів.

Визначення переліку актуальних загроз безпеці інформації, оцінка ефективності системи захисту є невід'ємною частиною життєвого циклу розподіленої інформаційної системи. Специфіка IT-інфраструктури, складність визначення зловмисника, актуальних загроз, вибору показників, недоліки методів оцінки ефективності систем захисту, як наслідок, недостатня ефективність безпеки конфіденційних даних розподілених інформаційних систем призводить до ризиків заподіяння шкоди активам власників систем.

Таблиця 1. Недоліки та переваги методів оцінки ефективності безпеки конфіденційних даних розподіленої інформаційної системи

Table 1. Disadvantages and advantages of methods for evaluating the effectiveness of the security of confidential data of a distributed information system

Метод оцінки системи захисту	Переваги	Недоліки
Статистичний	Дозволяє отримувати резуль-тати, коли не відомі параметри СЗ, дозволяє оцінювати систему будь-якої складності	Результати достовірні з певною ймовірністю, великий обсяг обробки статистичних даних
Імовірнісний	Аналізується повний спектр загроз, використання реаліс-тичного підходу, взаємозв'яз-ків міжелементами системи враховуються у явному виді	Складність обчислень, неможливо виявити зміну імовірнісних характеристик спостережень
Експертний	Використання у відсутності статистичних даних. Швидкість отримання результатів.	Достовірність результатів залежить від компетенцій експертів.
Багатокритеріальний ий (нейромережний)	Дозволяє враховувати велику кількість критеріїв оцінки системи. Дозволяє враховувати кількісні, якісні показники	Складність вибору оптимальної структури Відсутність формалізованих процедур
Матричний (формальний)	Універсальний для проведення оперативної оцінки системи захисту Вимагає мінімальних обчислювальних ресурсів	Не дозволяє проводити оцінку в умовах невизна-ченості, великої кількості показників оцінки
Комбінаторний (оптимізаційний)	Найбільш ефективний метод оцінки ефективності.	Складність проведення обчислень

МЕТА ДОСЛІДЖЕННЯ

Підвищення якості оцінки ефективності безпеки конфіденційних даних за рахунок визначення достатніх та необхідних показників.

ОСНОВНА ЧАСТИНА ДОСЛІДЖЕННЯ

В загальному вигляді задача дослідження може бути сформульована наступним чином: підвищити якість методів визначення актуальних загроз безпеці даних за рахунок визначення достатніх і необхідних показників, автоматизувати процес для виключення помилок експертів; підвищити якість методів оцінки ефективності системи захисту визначення найкращих параметрів роботи адаптивних нейронних нечітких продукційних систем, та застосування технологій Data Science при обробці великого обсягу даних; розробити рекомендації щодо оцінки ефективності системи захисту інформації; провести оцінку ефективності запропонованих методів.

Аналіз проведених досліджень оцінки ефективності систем захисту показав, що на теперішній час існують недоліки, пов'язані з вибором показників оцінки, складне обчислювальне навантаження, недостатня ефективність в частині достовірної оцінки системи захисту, необхідність залучення високо-кваліфікованих фахівців у галузі інформаційної безпеки, недоліки експертних оцінок.

Вирішення поставлених задач дозволить підвищити ефективність оцінки безпеки даних розподілених систем.

Для досягнення цілей забезпечення безпеки конфіденційної інформації необхідно: організувати ефективне створення системи безпеки інформації, ефективне визначення переліку актуальних загроз інформаційної безпеки, визначення актуального порушника, а також надати можливість проводити

якісну оцінку ефективності системи безпеки інформації.

Показники оцінки ефективності безпеки конфіденційних даних розподіленої інформаційної системи.

На підставі запропонованої моделі загроз інформаційній безпеці типових розподілених інформаційних систем та на підставі методичних документів Кваліфікаційного центру інформаційних технологій та кібербезпеки України сформовано перелік загроз безпеці конфіденційних даних [1-3,12]. Вирішена задача перетворення та очищення великого об'єму даних, сформовано набір даних для визначення актуальних загроз інформаційній безпеці конфіденційних даних з використанням технологій Data Science. На основі використання нечітких адаптивних продукційних нейронних мереж запропоновано модель визначення актуальних загроз інформаційній безпеці даних [3].

При формуванні необхідних вимог захисту даних в інформаційних системах на підставі даних Кваліфікаційного центру інформаційних технологій та кібербезпеки України сформовані вимоги для різних класів і типів інформаційних систем щодо захисту конфіденційної інформації. Під час розробки системи захисту для розподілених інформаційних систем враховувалися такі фактори, як використання, за вимогами безпеки інформації, сертифікованих засобів захисту [1,2,11,15].

Для проведення адекватної оцінки ефективності системи захисту необхідно визначити достатні та необхідні показники. Оцінка ефективності системи захисту даних досягається шляхом створення відповідної системи, здатної максимально нейтралізувати актуальні загрози конфіденційних даних, виконати вимоги захисту інформації, що пред'являються до розподіленої системи на підставі вимог в області інформаційної безпеки, а також дозволяє при розробці системи захисту максимально скоротити фінансові витрати. Таким чином, показники оцінки пропонуються наступні: перелік актуальних загроз інформаційній безпеці; ІТ-інфраструктура розподілених інформаційних систем з урахуванням їх специфіки; перелік вимог до безпеки інформації з урахуванням класифікації конкретної інформаційної системи; вартість засобів захисту інформації; перелік засобів захисту інформації, за результатами розробки системи захисту розподіленої інформаційної системи.

Виходячи з результатів аналізу проведених досліджень розподілених систем, визначень ефективності системи захисту в області інформаційної безпеки даних можна зробити наступний висновок: перераховані показники є достатніми та необхідними для достовірної та повноцінної оцінки ефективності безпеки конфіденційних даних розподіленої інформаційної системи.

На підставі результатів інформаційного обстеження розподілених систем, вхідних даних, у сфері забезпечення інформаційної безпеки у проведеному дослідженні пропонується визначити вимоги до безпеки інформації у сукупності. Вимоги, що пред'являються до досліджуваної розподіленої системи до безпеки конфіденційних даних, наведені в табл. 2.

Наведений у табл. 2 перелік вимог щодо захисту інформації та сформований для четвертого рівня захищеності персональних даних та третього класу захищеності держвної інформаційної системи. Для кожного класу та типу, категорії значущості розподіленої інформаційної системи, рівня захищеності, формуються переліки вимог щодо захисту конфіденційних даних.

На підставі сформованого переліку вимог інформаційної безпеки, переліку засобів захисту інформації, переліку актуальних загроз безпеки даних, підготовлено набір даних для оцінки ефективності системи. Використання технологій Data Science виконано наступні кроки: перетворення та очищення підготовленого набору даних; порівняння якості роботи моделей; вибір найбільш актуальних ознак, створення нових більш репрезентативних; перевірка моделі на тестовій вибірці; визначення параметрів у найкращій моделі; підсумкове представлення результатів виконання задачі; інтерпретація результатів.

Таблиця 2. Вимоги безпеки конфіденційних даних досліджуваної інформаційної системи

Table 2. Security requirements of confidential data of the researched information system

Умовне позначення	Найменування функції підсистеми	Відповідність функції системі	
		4 РЗ	3 -клас
Аутентифікація та ідентифікація суб'єктів до об'єктів доступу			
АІ.1	Аутентифікація та ідентифікація користувачів та процесів	+	+
АІ.2	Захист автентифікаційної інформації при передачі	+	+
АІ.3	Керування ідентифікаторами, створення, знищення.	+	+
АІ.4	Ідентифікація та аутентифікація користувачів	+	+
…			
Керування доступом суб'єктів до об'єктів доступу			
КД.1	Керування обліковими записами користувачів	+	+
КД.2	Дозвіл (заборона) дій користувачів, дозволених до ідентифікації та автентифікації	-	+
КД.3	Поділ повноважень (ролей) користувачів, адміністраторів, які забезпечують функціонування системи	+	+
…			
Обмеження програмного середовища			
ПС.1	Установка (інсталяція) дозволеного до використання програмного забезпечення та його компонентів	-	+
Захист машинних носіїв інформації			
МН.1	Облік машинних носіїв інформації	-	+
МН.2	Управління доступом до машинних носіїв інформації	-	+
…			
Реєстрація подій безпеки			
ПБ.1	Визначення змісту та складу інформації про події безпеки, що підлягають реєстрації	+	+
ПБ.2	Моніторинг (аналіз, перегляд) результатів реєстрації подій безпеки та реагування на них	-	+
…			
Захист інформаційної системи, її засобів, систем зв'язку та передачі даних			
ЗС.1	Захист бездротових з'єднань в системі	-	+
	Заборона несанкціонованої активації відеокамер, мікрофонів, периферійних пристроїв, які можуть активуватися віддалено, оповіщення користувачів	-	+
…			
Аналіз (контроль) захищеності інформації			
АК.1	Виявлення вразливостей системи та оперативне усунення вразливостей	-	+
АК.2	Контроль складу технічних засобів, ПЗ	-	+
АК.3	Контроль встановлення оновлень ПЗ	+	+

В процесі виконаного дослідження визначено ключові складові системи захисту інформації:

1. Список актуальних загроз інформаційної безпеки з ознаками нейтралізації/ не нейтралізації.
2. Перелік вимог до інформаційної безпеки конфіденційних даних з ознаками відповідності: загалом відповідає, відповідає, не відповідає, частково відповідає.
3. Найменування засобів захисту інформації, їх версія, патчів (версії оновлень).
4. Вартість засобів від виробника (специфікації вендорів).

На підставі проведеного визначення ключових складових системи захисту інформації проведена фільтрація надлишкової інформації з отриманого набору даних.

Наступним кроком є проводення попереднього аналізу отриманих даних, на підставі попереднього аналізу: визначаємо аномалії, закономірності, зв'язки між ознаками. Таким чином, необхідно визначити значення ознак та ознаки, що мають суттєвий вплив на цільову ознаку отриманих даних, оцінюємо вплив значень категоріальних ознак на цільовий – density plot.

Для оцінювання ознак ступеня їхнього впливу, у роботі використовується коефіцієнт кореляції Пірсона - міра позитивності та ступеня лінійних зв'язків між двома змінними. Значення коефіцієнта +1 означає ідеальну пропорційність між відповідними значеннями ознак, -1 аналогічно, але з відємним коефіцієнтом.

Вибір ознак інформації – вибір найбільш релевантних ознак. З dataframe видаляються ознаки даних, щоб модель відповідала більше признакам та ресурсів першорядним ознакам. Таким чином, проводиться фільтрація набору даних відповідної інформації, залишаються найважливіші для даної задачі.

Створення нових ознак – процес, у якому на основі наявних отриманих даних конструюються нові ознаки. Потім визначаються колінеарні ознаки.

Після виконання попереднього аналізу, фільтрації даних, залишаться найбільш важливі ознаки. Наступним кроком перед початком проведення навчання моделі ANFIS є отримання показника, на якому можна визначити, чи є позитивний результат від використання задіяного алгоритму.

До проведення розрахунку вищеописаного критерію, необхідно розділити вибірку на тестову та навчальну:

1. Тестова вибірка використовується для перевірки отриманої моделі ANFIS. Модель ANFIS не використовує цільової ознаки при обробці даних, має передбачити його величину, використовуючи значення інших ознак. Отримані прогнози порівнюються з реальними відповідями.
2. Навчальна вибірка - набір сформованих даних, який подається разом з відповідями на вхід моделі ANFIS в процесі навчання, з метою навчити модель виявляти зв'язок між сформованими ознаками і правильною відповіддю.

Сформований набір даних включає в себе перелік вимог до інформаційної безпеки, перелік засобів захисту, актуальних загроз інформаційної безпеки в розподіленій системі, зроблено його форматування та перетворення, що дозволило зібрати лише достатні та необхідні дані для оцінки ефективності системи захисту, що, зменшує кількість помилок експертних оцінок, складність обчислювального процесу, підвищуючи ефективність запропонованого підходу.

Метод оцінки оцінки ефективності безпеки конфіденційних даних інформаційної системи.

На теперішній час існує велика кількість нейро-нечітких гібридних моделей, що відрізняються можливостями та архітектурою. На основі отриманих результатів виконаного дослідження проведено аналіз моделей і визначено основні властивості: застосування різних підходів до навчання моделі; можливість автоматизованого формування набору правил; зміна структури моделі гібридних нейро-нечітких моделей наведені в Табл. 3.

На основі аналізу проведеного дослідження моделей зроблені висновки щодо використання типів моделей для спектра розв'язуваних задач. Результати проведеного аналізу наведені у Табл. 4. З отриманих результатів, можливо зробити висновок, що для вирішення задачі оцінки ефективності безпеки конфіденційних даних розподіленої інформаційної системи доцільно використовувати модель ANFIS.

Для розробки методу оцінки ефективності безпеки конфіденційних даних розподіленої інформаційної системи проведено аналіз моделі мережі ANFIS з алгоритмами нечіткого виведення Мамдані, Такагі-Сугено-Канга, Ванга-Менделя, Такагі-Канга. Мережі ANFIS призначені, зокрема, для вирішення задач оцінювання.

Таблиця 3. Область застосування гібридних нейро-нечітких моделей

Table 3. Scope of application of hybrid neuro-fuzzy models

№ п/п	Модель	Область застосування
1	ANFIS	- структура бази правил має бути відома заздалегідь; - параметри налаштовуються в першому і останньому шарі; - навчання в два етапи: параметри першого шару фіксовані, використовується оцінка параметрів другого шару; параметри другого шару фіксовані, параметри першого шару оцінюються алгоритмом RMSE (зворотного розповсюдження помилки).
2	NEFCON	- можливість індукування та оптимізації бази правил; - лінгвістичні нечіткі моделі.
3	NEFCLASS	- можливість оптимізації бази правил; - структура бази правил може змінюватися.
4	FALCON	- навчання у два етапи: навчання без вчителя; параметрична оптимізація (метод градієнтного спуску).
5	FUN	- алгоритм зміни параметрів та перебудови зв'язків, функція приналежності має випадковий характер

Таблиця 4. Спектр розв'язуваних задач в залежності від типу моделі

Table 4. Spectrum of solvable problems depending on the type of model

№ п/п	Модель	Спектр задач
1	NEFPROX, NEFCLASS	Інтелектуальна обробка та аналіз даних
2	NEFCLASS	Задачі класифікації, прийняття рішень
3	ANFIS, NEFPROX, FBF	Апроксимація нелінійних залежностей
4	NEFCON, FUN, GARIC, ANFIS	Інтелектуальне управління
5	NNDFR, ANFIS	Моделювання
6	FAM, NEFPROX	Прогнозування

Вивід системи відповідє набору нечітких правил if-then (якщо-то), які мають здатність до навчання апроксимування нелінійних функцій.

Алгоритм роботи мережі ANFIS з алгоритмом TSK (нечіткого виведення Такаги-Сугено-Канга) у запропонованому методі оцінки ефективності системи захисту даних полягає у реалізації нечіткої моделі, заснованої на правилах (6)

загроз інформаційної безпеки та ІТ-інфраструктури розподілених систем було сформовано базу правил, фрагмент бази наведено в табл. 5.

В табл. 5 наведено: терм-множинами змінних лінгвістичних є наступні: С - відповідає, ЧС - частково відповідає, ЦС – в цілому відповідає, Н - загроза нейтралізована, НН - загроза не нейтралізована, min - ціна системи захисту мінімальна, max - ціна системи захисту максимальна. Оцінка ефективності Д – досягається, НД – не досягається.

$$R_i : IFx_i ISA_{i1} AND...AND_{x_j} ISA_{ij} AND...AND_{x_{im}} ISA_{im}, THEN$$
$$y = c_{i0} + \sum_{j=1}^{m} c_{ij} x_j,\ j = 1,...,n \qquad (6)$$

На підставі вимог та показників щодо захисту даних, також на підставі актуальних

Таблиця 5. Фрагмент бази правил оцінки ефективності системи захисту

Table 5. Fragment of the base of rules for evaluating the effectiveness of the protection system

IF (ЯКЩО)			THEN (ТО)
Вимоги до системи захисту інформації	Загроза інформаційній безпеці	Вартість системи захисту	
AI.3 C	ЗІБ. 01 H	min	Ефективність СЗІ досягається
AI.4 HC	ЗІБ. 02 HH	max	Ефективність СЗІ не досягається
...			
КД.2 ЦС	ЗІБ. 0N HH	min	Ефективність СЗІ не досягається

База правил для реалізації методу оцінки ефективності системи захисту конфіденційних даних має наступний вигляд (7):

$$
\begin{aligned}
&R_1 : AI.1(C)\ AND ЗІБ.01(H)\ ANDCOST\ (MIN)\ THENEVALSZI\ (Д)\\
&R_2 : AI.1(C)\ AND ЗІБ.01(H)\ ANDCOST\ (MAX)\ THENEVALSZI\ (Д)\\
&R_3 : AI.1(C)\ AND ЗІБ.01(HH)\ ANDCOST\ (MIN)\ THENEVALSZI\ (НД)\\
&R_4 : AI.1(C)\ AND ЗІБ.01(HH)\ ANDCOST\ (MAX)\ THENEVALSZI\ (НД)\\
&R_5 : AI.1(ЦС)\ AND ЗІБ.01(H)\ ANDCOST\ (MIN)\ THENEVALSZI\ (Д)\\
&R_6 : AI.1(ЦС)\ AND ЗІБ.01(H)\ ANDCOST\ (MAX)\ THENEVALSZI\ (Д)\\
&R_7 : AI.1(ЦС)\ AND ЗІБ.01(HH)\ ANDCOST\ (MIN)\ THENEVALSZI\ (НД)\\
&R_8 : AI.1(ЦС)\ AND ЗІБ.01(HH)\ ANDCOST\ (MAX)\ THENEVALSZI\ (НД)\\
&R_9 : AI.1(ЧС)\ AND ЗІБ.01(H)\ ANDCOST\ (MIN)\ THENEVALSZI\ (Д)\\
&\ldots\\
&R_n : КД.2(ЦС)\ AND ЗІБ.03(HH)\ ANDCOST\ (MIN)\ THENEVALSZI\ (НД)
\end{aligned}
\tag{7}
$$

Мережа ANFIS у запропонованому методі базується на положеннях запропонованих в моделі визначення актуальних загроз безпеки конфіденційних даних в розподіленій інформаційній системі [3].

За результатами отриманих нелінійних параметрів та їх уточнення, процес адаптації нейрона запускається до тих пір, поки не досягне повторення результатів, алгоритм є гібридним.

Особливість роботи алгоритму полягає у розподілі етапів навчання. Такий алгоритм нечіткого виведення є найефективнішим, що дозволило в роботі досягти кращого результату у проведеному дослідженні. Структура нечіткої нейронної продукційної мережі ANFIS із застосуванням алгоритму нечіткого виведення Такагі-Сугено-Канга, наведено на Рис. 1. За рахунок адаптації параметрів нейронної мережі в роботі вдалося досягти найменшої середньоквадратичної помилка (RMSE) на відміну від відомих методів оцінки ефективності систем захисту інформації.

Метод оцінки ефективності безпеки конфіденційних даних розподіленої інформаційної системи.

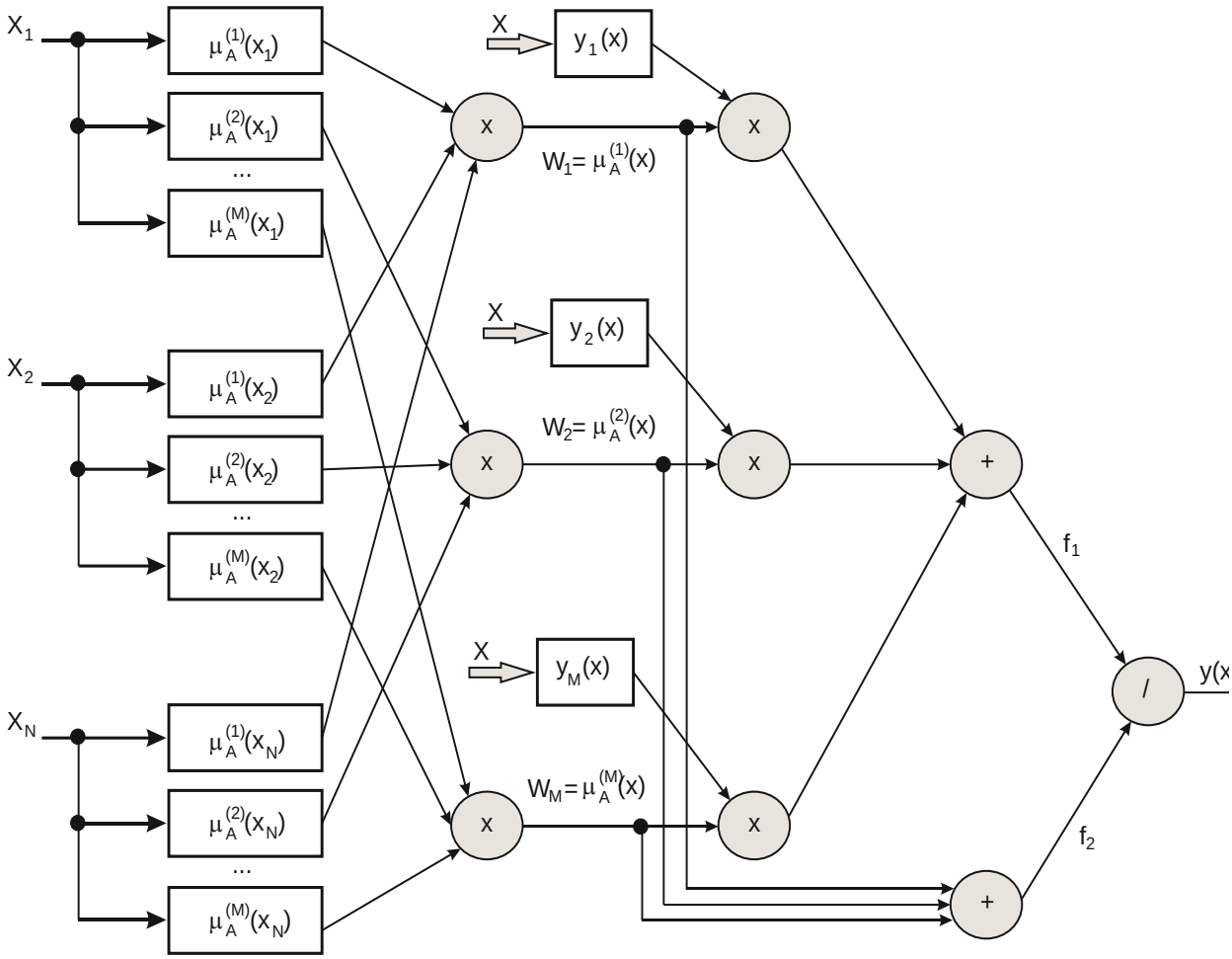

Рис. 1. Структура нечіткої нейронної продукційної мережі ANFIS із TSK

Fig. 1. Structure of fuzzy neural production network ANFIS with TSK

Для визначення ефективності запропонованого методу оцінки ефективності безпеки даних, необхідно розглянути аспекти продукційної нечіткої системи логічного висновку. Нечітка подукційна система логічного висновку представляє собою систему, яка певним чином відображає вхідні дані у вихідні за допомогою використання трьох основних етапів: фазифікація; логічний вивід; дефаззифікація. Розглянуто функції приналежності тільки фіксовані, які обрані довільно для моделювання оцінки ефективності системи захисту даних, структура правил яких визначена експертом інтерпретацією характеристик використовуваних змінних у моделі. У певних ситуаціях моделювання систем захисту неможливо розрізнити, як мають виглядати, маючи відповідний набір даних, функції приналежності. Адаптуючи та аналізуючи набір даних для проведення оцінки ефективності системи, неможливо визначити функції приналежності. Нейро-адаптивні продукційні методи навчання надають методи нечіткого адаптивного моделювання, що дозволяють провести аналіз інформації про набори даних. Метод обчислює відповідні параметри функції приналежності, що дозволяють системі продукційного нечіткого виводу відстежувати дані введення-виведення.

Структура адаптивної мережі подібної до нейронної продукційної мережі може використовуватися для інтерпретації входів-виходів, що дозволяє відображати вхідні дані з набору даних за допомогою викори-

стовуваних функцій приналежності та пов'язаних параметрів, і потім на основі пов'язаних параметрів та вихідних функцій приналежності для виведення. Параметри, що пов'язані з функціями приналежності, адаптуються у процесі проведення навчання системи. Адаптація та обчислення параметрів спрощується застосуванням вектора градієнта. Вектор градієнта забезпечує міру, наскільки добре система продукційного нечіткого виводу моделює вихідні та вхідні дані з набору даних параметрів. Після отримання вектора градієнта, надалі застосовується процедура оптимізації для налаштування параметрів функції приналежності. Зазначена процедура призначена зменшити значення середньоквадратичної помилки. RMSE визначається сумою квадратів різниці між бажаним та фактичним виходом. Таким чином, необхідність використан-ня мережі ANFIS, а також її ефективність для проведення оцінки системи захисту інформації стає очевидною.

Наступним кроком при обчисленні ефективності методу оцінки системи захисту кофіденційних даних, є визначення алгоритму нечіткого виводу. На підставі проведених експериментів, аналізу досліджень, можливо зробити висновок, що мережа ANFIS з алгоритмом нечіткого продукційного висновку TSK (Такагі-Сугено-Канга), для вирішення задач проведення оцінки ефективності безпеки конфіденційних даних розподілених інформаційних систем є найкращою.

Якість запропонованого методу оцінки ефективності системи захисту конфіденційних даних, порівняно з існуючими методами, досягається наступними показниками: фінансові витрати можуть досягти зменшення вартості розроблюваної системи захисту інформації до 25%, ефективність системи захисту досягає 97%.

Поставлену задачу, в проведеному дослідженні щодо підвищення якості оцінки ефективності системи захисту розподіленої інформаційної системи можна вирішувати з використанням методів класифікації, які використовують різні підходи реалізації та математичні апарати, проте, ефективність використовуваних методів залежить від конкретної задачі, що вирішується. У роботі проведено порівняльний аналіз методів розв'язання поставленої задачі, отримані результати наведено в Табл. 6.

В роботі проведені експерименти досліджень роботи існуючих методів та запропонованого. Отриманні результати наведені у Табл. 7. Як порівняльна характеристика, при проведенні експериментів, використовувалася точність визначення досяжності/не досяжності ефективності системи захисту розподіленої інформаційної системи (точність класифікації).

Таблиця 6. Порівняльний аналіз методів для вирішення поставленої задачі

Table 6. Comparative analysis of methods for solving the given problem

Метод	Переваги	Недоліки
Метод Байєса (Naive Bayes, NB)	Швидкодія методу. Підтримка інкрементного навчання.	Відносно низька якість класифікації;
Метод *k*-найближчих сусідів (*KNN*)	Простота реалізації. Опрацьована теоретична база. Адаптація під необхідну задачу.	Недостатня продуктивні-сть у реальних задачах. Труднощі в наборі ваг.
Метод опорних векторів	Еквівалентна двошарова нейронна мережа- простота реалізації	Неможливість калібрува-ння попадання у клас
Метод дерев рішень	Висока продуктивність навчання та прогнозування. Дозволяє працюва-ти з великим об’єом інформації	Проблема отримання оптимального дерева рішень

Таблиця 7. Результати порівняльного аналізу

Table 7. Results of comparative analysis

	Наївний Байєс	Метод *k*-найб-лижчих сусідів	Дерева рішень	Логістична регресія		Запропонований метод на основі ANFIS
Точність %	86,7	70,4	92,1	93,6		97,2

На Рис. 2 наведено графік порівняльного аналізу методів для вирішення поставленої задачі у роботі при проведенні дослідження.

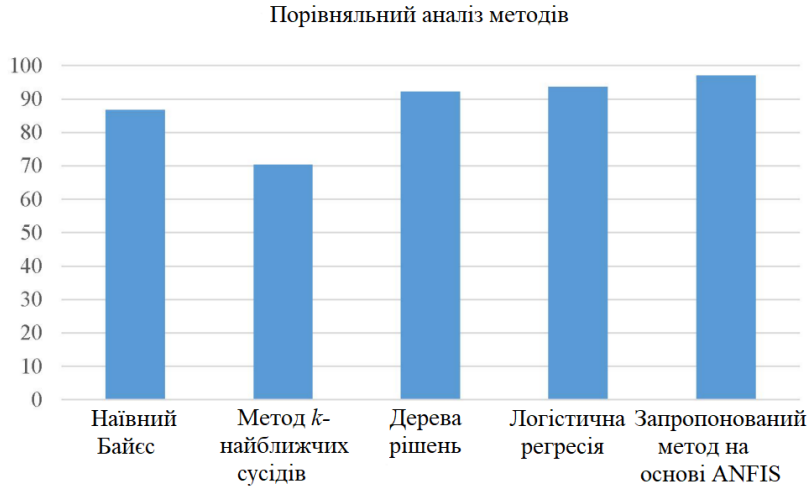

Рис. 2. Графік порівняльного аналізу методів

Fig. 2. Schedule of comparative analysis of methods

Таблиця 8. Аналіз оцінки ефективності запропонованого методу

Table 8. Analysis of the effectiveness of the proposed method

Показник	**Існуючі методи**	**Запропонований метод**
RMSE	0,022-0,214	0,012-0,017
Ефективність системи захисту	85,6%	97,2%
Вартість системи	зниження до 15%	зниження до 30%

Середньоквадратична помилка запропонованого методу, обчислюється за формулою: $RMSE = \sqrt{\frac{1}{N}\sum_{i=1}^{N}\left(y_i - y_i\right)^2}$, де y_i, y_i - набори даних (перевірки, навчання). Графіки порівняння RMSE відомих та запропонованого методу на заданому інтервалі представлені на Рис. 3.

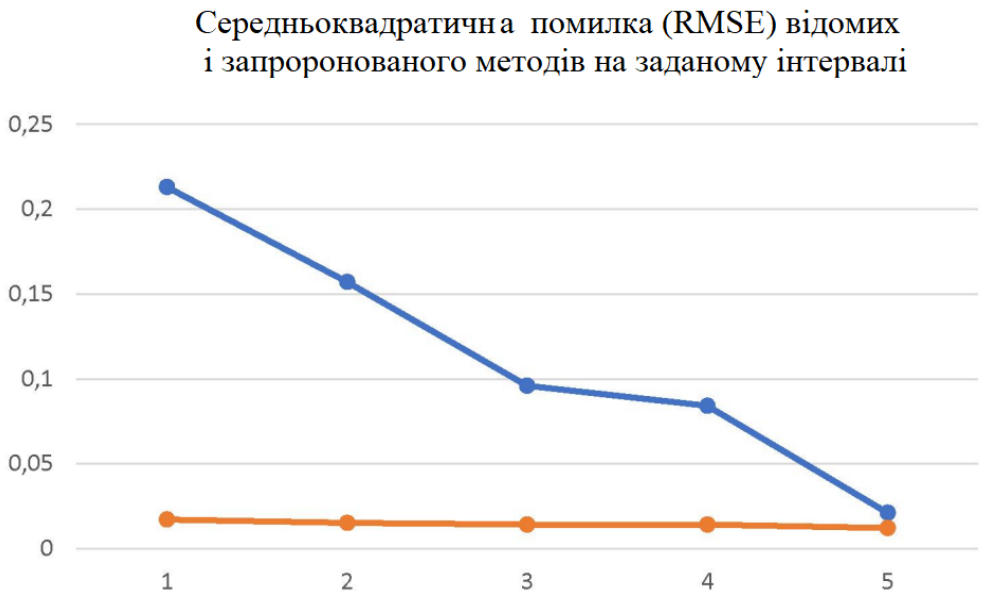

Рис. 3. Графік порівняння RMSE на заданому інтервалі

Fig. 3. Comparison chart of RMSE at the given interval

Середньоквадратична помилка RMSE досягає значення в діапазоні 0,012-0,017, є локальним мінімумом на заданому інтервалі та дозволяє довести виконання поставленої в роботі дослідженні задачі.

ВИСНОВКИ

У роботі визначено достатні та необхідні показники, запропоновано метод оцінки ефективності безпеки конфіденційних даних розподіленої інформаційної системи, заснований на продукційній, адаптивній нейронній нечіткій системі та алгоритмі нечіткого виведення *TSK* (Такагі-Сугено-Канга), на відміну від відомих, дозволяє досягати меншого значення RMSE -середньоквадратичної помилки роботи системи захисту, підвищує ефективність проведення оцінки системи до 97%, що на

15% вище порівняно з відомими, фінансові витрати на створення системи захисту даних дозволяють досягати зменшення вартості розробки системи до 30%.

Запропонований метод оцінки ефективності дозволяють власникам систем автоматично оцінювати ефективність системи захисту у режимі реального часу на всіх етапах проведення життєвого циклу системи, що дозволяє, при цьому, своєчасно внести коригування до проектних рішень системи захисту для нейтралізації актуальних загроз інформаційній безпеці та виконання вимог щодо захисту інформації, також враховуючи фінансову складову. Слід зазначити, що для запропонованого методу, показники оцінки ефективності можуть бути змінені залежно від потреб та цілей власника системи у проведенні оцінки ефективності системи захисту.

ЛІТЕРАТУРА

1. Доктрина інформаційної безпеки України, затвердженої Указом Президента України від 25 лютого 2017 року №47/2017, 15с.
2. Державний стандарт України Захист інформації. Технічний захист інформації. Основні положення. ДСТУ 3396.0-96 [Електронний ресурс]. – Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=38883&cat_id =38836.
3. **Ленков С. В.** Модель визначення актуальних загроз безпеки конфіденційних даних в розподіленій інформаційній системі/ С.В. Лєнков, В.М. Джулій, І.В. Муляр, І.В. Димбовський М. // UNDERWATER TECHNOLOGIES: Industrial and Civil Engineering, Iss.13 (2023),45-59
4. **Ленков С. В.** Метод прогнозування вразливостей інформаційної безпеки на основі аналізу даних тематичних інтернет-ресурсів / С.В. Лєнков, В.М. Джулій, А.М.

Берназ, І.В. Муляр, І.В. Пампуха // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2023. – Вип. №78. – С. 123-134.
5. **Ленков С. В.** Метод протидії поширенню та виявлення шкідливої інформації в соціальних мережах/ С.В. Ленков, В.М. Джулій, Л.В. Солодєєва // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2022. – Вип. №77. – С. 103-117.
6. **Ленков С. В.** Модель безпеки поширення забороненої інформації в інформаційно-телекомунікаційних мережах / С. В. Ленков, В. М. Джулій, В. С. Орленко, О. В. Сєлюков, А. В. Атаманюк // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2020. – Вип. №68. – С. 53-64.
7. **Lienkov S., Podlipaiev V., Tolok I., Lisitsky I., .Lytvynenko N., Kuznichenko S.** The Information and Analytical Using of Non-Structured Information Resources CEUR Workshop Proceedingsthis link is disabled, 2021, 3126, С. 81–87.
8. Соціальні мережі – реальні загрози віртуального світу. [Електронний ресурс]. – Режим доступу : http://ogo.ua/articles/view/011–02–23/26490.htm.
9. **Остапов С. Е.** Технології захисту інформації: навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король – Харків : Вид-во ХНЕУ, 2016. – 476 с.
10. **Лєнков С. В.** Аналіз існуючих методів та алгоритмів виявлення атак в бездротових мережах передачі даних / С. В. Лєнков, В. М. Джулій, Н. М. Берназ, С. О. Божук // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2017. – Вип. № 56. – С.124-132.
11. **Бурячок В. Л.** Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби: посібник / [В. Л. Бурячок, С. В. Толюпа, В. В. Семко та ін.]. – К.: ДУТ-КНУ, 2016. – 178 с.
12. **Рибальченко Л. В., Косиченко О. О.** Проблеми безпеки персональних даних в Україні / Регіональна економіка / Запоріжжя. 2019. – С. 57-62.
13. **Джулій В. М.** Метод класифікації додатків трафіка комп'ютерних мереж на основі машинного навчання в умовах невизначеності / В. М. Джулій, О. В. Мірошніченко, Л.В. Солодєєва // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2022. – Вип. №74. – С. 73-82.
14. **Лавров Є. А**. Математичні методи дослідження операцій: підручник / Є. А. Лавров, Л. П. Перхун, В. В. Шендрик – Суми: Сумський державний університет, 2017. – 212 с.
15. **Гончар С. Ф.** Оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури: монографія. / С. Ф. Гончар. – Київ, 2019. – 175 с.
16. **Yemchuk L.** Organizational Network Analysis as a Tool for Leadership Assessment in Software Development Team. Zhylinska O.; Chornyi A.; Dzhuliy V. – Institute of Electrical and Electronics Engineers (30 September 2020); INSPEC Accession Number: 20008165; DOI: 10.1109/ACIT49673.2020.
17. Сигнатура атаки. Wikipedia [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Сигнатура_атак.

REFERENCES

1. Doktryna informatsiinoi bezpeky Ukrainy, zatverdzhenoi Ukazom Prezydenta Ukrainy vid 25 liutoho 2017 roku No.47/2017, 15.
2. Derzhavnyi standart Ukrainy Zakhyst informatsii. Tekhnichnyi zakhyst informatsii. Osnovni polozhennia. DSTU 3396.0-96 [Elektronnyi resurs]. – Rezhym dostupu: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=38883&cat_id =38836
3. **Lenkov S. V.** (2023). Model vyznachennia aktualnykh zahroz bezpeky konfidentsiinykh danykh v rozpodilenii informatsiinii systemi/ S.V. Lienkov, V.M. Dzhulii, I.V. Muliar, I.V. Dymbovskyi M. // Underwater technologies: Industrial and Civil Engineering, Iss.13,45-59
4. **Lenkov S. V. Dzhulii V. M., Bernaz A. M., Muliar I. V., Pampukha I. V.** (2023). Metod prohnozuvannia vrazlyvostei informatsiinoi bezpeky na osnovi analizu danykh tematychnykh internet-resursiv. Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka, No.78, 123-134.
5. **Lenkov S. V., Dzhulii V. M., Solodieieva L. V.** (2022). Metod protydii poshyrenniu ta vyiavlennia shkidlyvoi informatsii v sotsialnykh merezhakh. Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka, No. 77,

103-117.
6. **Lenkov S. V., Dzhulii V. M., Orlenko V. S., Sieliukov O. V.**, **Atamaniuk A. V.** (2020). Model bezpeky poshyrennia zaboronenoi informatsii v informatsiino-telekomunikatsiinykh merezhakh. Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka, No.68, 53-64.
7. **Lienkov S., Podlipaiev V., Tolok I., Lisitsky I., Lytvynenko N., Kuznichenko S.** (2021). The Information and Analytical Using of Non-Structured Information Resources CEUR Workshop Proceedingsthis link is disabled, 2021, 3126, 81–87.
8. Cotsialni merezhi – realni zahrozy virtualnoho svitu. [Elektronnyi resurs]. – Rezhym dostupu: http://ogo.ua/ articles/view/011– 02– 23/26490.html.
9. **Ostapov S. E., Yevseiev S. P., Korol O. H.** (2016). Tekhnolohii zakhystu informatsii: navchalnyi posibnyk. Kharkiv, KhNEU, 476.
10. **Lenkov S. V., Dzhuliy V. M., Bernaz N. M., Bozhuk S. O.** (2017). Analiz Isnuyuchih metodiv ta algoritmiv viyavlennya atak v bezdrotovih merezhah peredachI danih. Zbirnik naukovih prats Viyskovogo Institutu Kiyivskogo natsionalnogo universitetu imeni Tarasa Shevchenka, No 56, 124-132.
11. **Buriachok V. L., Toliupa S. V., Semko V. V.** (2016). Informatsiinyi ta kiberprostory: problemy bezpeky, metody ta zasoby borotby: posibnyk. Kyiv, DUT-KNU, 178.
12. **Rybalchenko L. V., Kosychenko O. O.** (2019). Problemy bezpeky personalnykh danykh v Ukraini. Rehionalna ekonomika. Zaporizhzhia, 57-62.
13. **Dzhulii V. M., Miroshnichenko O. V., Solodieieva L.V.** (2022). Metod klasyfikatsii dodatkiv trafika kompiuternykh merezh na osnovi mashynnoho navchannia v umovakh nevyznachenosti. Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka, No. 74, 73-82.
14. **Lavrov Ye. A**., **Perkhun L. P., Shendryk V. V.** (2017). Matematychni metody doslidzhennia operatsii: pidruchnyk. Sumy: Sumskyi derzhavnyi universytet, 212.
15. **Honchar S. F.** (2019). Otsiniuvannia ryzykiv kiberbezpeky informatsiinykh system obiektiv krytychnoi infrastruktury: monohrafiia. Kyiv, 175.
16. **Yemchuk L., Zhylinska O., Chornyi A., Dzhuliy V.** (2020). Organizational Network Analysis as a Tool for Leadership Assessment in Software Development Team. Institute of Electrical and Electronics Engineers (30 September 2020), INSPEC Accession Number: 20008165; DOI: 10.1109/ACIT49673.2020.
17. Syhnatura ataky. Wikipedia [Elektronnyi resurs] – Rezhym dostupu do resursu: https://uk.wikipedia.org/wiki/Syhnatura_atak.

The method of assessing the effectiveness of the security of confidential data of the distributed information system

Serhii Lienkov, Volodymyr Dzhuliy, Ihor Muliar,

Abstract. The paper proposes a method of assessing the effectiveness of the security of confidential data of a distributed information system, based on a model for determining the current threats to the security of confidential data in the information system, on algorithms of fuzzy inference and the theory of fuzzy neural systems, unlike known ones, it uses sufficient and necessary indicators, excludes expert errors , increases the detection of actual threats to the security of confidential information system data by 5%, reduces the cost of purchasing information protection tools from 15 to 30%. It takes into account the following factors: the IT infrastructure of the distributed information system, the capabilities of attackers and their level of motivation in the information system.

The proposed approach differs from existing ones by an automated process, the need to involve highly qualified specialists in the field of information security, and low computational complexity; absence of deficiencies in expert assessments; allows you to determine the list of current information security threats in information systems of various classes and types.

The task of ensuring the security of confidential data is urgent, which is due to the growth of computer attacks and leaks of information, which are reflected in the statistical data on the commission of crimes in the field of high technologies, the growth of criminal activity using modern communication devices and the Internet.

The existing methods of identifying current threats to information security and assessing the effectiveness of the security of confidential data cannot be used at all stages of the life cycle of distributed information systems, they do not take into account the following indicators in the complex: IT infrastructure of distributed systems, current threats to information security, security requirements of confidential data, their cost as important indicators when solving these problems.

One of the most important tasks of ensuring the security of confidential data is the evaluation of the

effectiveness of the protection system. In this regard, the goal of the research is to improve the quality of the assessment of the effectiveness of the security of confidential data of a distributed information system by determining sufficient and necessary indicators using modern information technologies, which allow the most effective solution of the following tasks: determining the parameters of the adaptive production fuzzy neural systems, which most suitable for solving the tasks, the application of Data Science technologies in data processing, algorithms of fuzzy output.

Keywords: method, information security, distributed information systems, vulnerabilities, attacks, confidential data.