Модель визначення актуальних загроз безпеки конфіденційних даних в розподіленій інформаційній системі

Сергій Лєнков[1], Володимир Джулій[2], Ігор Муляр[3], Максим Димбовський[4]

[1] Військовий інститут Київського національного університету імені Тараса Шевченка
Юлії Здановської, 81, Київ, Україна, 03189
[1] lenkov_s@ukr.net, https://orcid.org/0000-0001-7689-239X
[2,3,4] Хмельницький національний університет
вул. Інститутська, 11, Хмельницький, Україна, 29000
[2,4] dzhuliivm@khmnu.edu.ua, http://orcid.org/0000-0003-1878-4301
[3] muliariv@khmnu.edu.ua, 0000-0002-6659-605X

Received 15.11.2023, accepted 20.12.2023
https://doi.org/10.32347/uwt.2023.13.1205

Анотація. В роботі запропоновано модель визначення актуальних загроз інформаційній безпеці розподілених інформаційних систем, заснована 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 інформаційній безпеці розподілених систем на 5%, знижує витрати на закупівлю засобів захисту інформації від 15 до 30%. Враховує наступні фактори: ІТ-інфраструктуру розподіленої інформаційної системи, можливості зловмисників та їх рівень мотивації у розподіленій інформаційній системи, перелік існуючих засобів захисту в розподіленій інформаційній системі.

Запропонований підхід відрізняється від існуючих, в наступному: відсутність залучення висококваліфікованих фахівців в області безпеки інформації; процес автоматизований, має низьку обчислювальну складність; відсутність недоліків експертних оцінок; дозволяє визначати перелік актуальних загроз безпеки інформації в інформаційних системах різних класів та типів.

Задача забезпечення безпеки конфіденційної інформації стає найактуальнішею, 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 моделювання актуальних загроз інформаційної безпеки та оцінки ефективності системи захисту інформації не можуть бути задіяні на всіх етапах життєвого циклу розподілених інформаційних систем - не враховують в комплексі наступні показники: ІТ-інфраструктуру розподілених інформаційних систем, актуальні загрози інформаційної безпеки, вимоги безпеки конфіденційної інформації, перелік засобів захисту конфіденційної інформації та їх вартість як важливих показників при вирішенні даних задач

Для досягнення цілей забезпечення безпеки конфіденційної інформації необхідно: організувати ефективне створення системи захисту інформації (системи безпеки інформації), ефективне моделювання (визначення переліку) актуальних загроз інформаційної безпеки, визначення актуального порушника, а також надати можливість проводити якісну оцінку ефективності системи безпеки (захисту) інформації.

Однією з найважливіших задач забезпечення безпеки конфіденційної інформації є оцінка ефективності системи захисту (безпеки). У зв'язку з цим мета роботи (дослідження) - підвищення якості оцінки ефективності систем захисту (безпеки) розподілених інформаційних систем за рахунок визначення достатніх та необхідних показників оцінки з використанням сучасних (перспективних) інформаційних технологій, що дозволяють найбільш ефективно вирішувати наступні задачі: визначення параметрів роботи адаптивних продукційних нечітких нейронних систем, що найбільш підходять для вирішення поставлених задач, застосування технологій Data Science при обробці даних, алгоритмів нечіткого виведення.

Ключові слова: модель, 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, в свою чергу, до порушення територіальної цілісності та підриву суверенітету інших держав. Засоби масової інформації збільшують об’єми матеріалів та поширують їх в мережі Інтернет, які містять упереджену оцінку державної політики [2]. Значно зростають масштаби комп'ютерної злочинності, в першу чергу, у кредитно-фінансовій сфері суспільства. У сфері оборони держави, в економічній сфері, в області суспільної та державної безпеки, в галузі науки, освіти та технологій, в області рівноправного стратегічного партнерства та стратегічної стабільності спостерігаються визначені державою стратегічні цілі для забезпечення конфіденційній інформації ефективного стану безпеки [2].

Одночасно, з розвитком та зростанням інформаційних технологій зростає і кількість засобів та методів порушень стану безпеки конфіденційної інформації. Протягом останніх років спостерігається різке зростання кількості витоків конфіденційної інформації, зі звіту експертно-аналітичного центру групи компаній SafeNet. Змінити ситуацію, до забезпечення інформаційної безпеки, можливо шляхом розробки нових методів, підходів які можуть надати від сучасних загроз безпеки інформації надійний захист [3-5].

Задача забезпечення безпеки конфіденційної інформації стає найактуальнішею, що обумовлено, зростанням комп'ютерних атак та витоків інформації, що відображаються у статистичних даних скоєння злочинів у сфері високих технологій [7,8], 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 [10,11]. Серед усіх скоєних у 2021 році комп'ютерних злочинів лідирують злочини, які передбачають розповсюдження, використання, створення комп'ютерних «вірусів», а також відповідальність за неправомірний доступ до комп'ютерної конфіденційної інформації. Друге місце в незаконній електронній діяльності, займає шахрайство з використанням сервісів онлайн-платежів [8]. 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 (кіберзлочинами) 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 чи грошей.

Існуючі методи моделювання (визначення) актуальних загроз інформаційної безпеки та оцінки ефективності системи захисту інформації не можуть бути задіяні на всіх етапах життєвого циклу розподілених інформаційних систем - не враховують в комплексі наступні показники: IT-інфраструктуру розподілених інформаційних систем, актуальні загрози інформаційної безпеки, вимог безпеки конфіденційної інформації, перелік засобів захисту конфіденційної інформації та їх вартість як важливих показників при вирішенні даних задач [9, 10]. Одночасно з цим, для розглянутих методів моделювання загроз інформаційної безпеки та проведення оцінки ефективності системи

захисту розподілених інформаційних систем залишається мета - підвищення ефективності, з огляду визначення кількості актуальних загроз інформаційної безпеки, виконання закладених вимог до безпеки інформації, зниження вартості витрат на проектування та створення системи захисту розподілених інформаційних систем, а також мінімізація (виключення) помилок експертів. Для існуючих методів залишається актуальною задача зменшення помилки середньоквадратичної роботи продукційних адаптивних нечітких нейронних систем.

На підставі проведеного аналізу можна зробити висновок про необхідність удосконалення методів оцінки ефективності системи захисту розподілених інформаційних систем.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ ТА ПОСТАНОВКА ЗАДАЧІ

Моделювання інформаційних систем є одним з основних методів дослідження в областях знань, науково обґрунтованим підходом оцінок характеристик інформаційних складних систем. Моделювання інформаційних систем - заміщення існуючої інформаційної системи іншою з метою отримання необхідної інформації реальної системи з використанням об'єкта-моделі інформаційної системи, аналогічно для проведення моделювання загроз та атак безпеки даних [5,9].

На теперішній час існує класифікація типів моделювання інформаційних систем, яка наведена на рис. 1.

Рис. 1. Класифікація типів моделювання інформаційних систем

Відповідно класифікаційним ознакам, моделі поділяються на: неповні, наближені повні. Залежно від характеристик у процесах, моделі поділяться на: стохастичні, детерміновані, динамічні, статичні, дискретні, дискретно-безперервні, безперервні. Статичне моделювання визначає, у будь-який момент, поведінку інформаційної системи. Детерміноване - відображає процеси, у яких відсутні випадкові дії. Динамічне моделювання відображає поведінку інформаційної системи у часі. Стохастичне - відображає імовірнісні події та процеси. Безперервне моделювання відображає безперервні процеси, дискретне - описує дискретні процеси

в інформаційній системі. Моделювання дискретно -безперервне використовується при описі безперервних та дискретних процесів. Уявне використовується при моделюванні об'єктів, які існують поза умовами, їх створення або нереалізовані в визначеному інтервалі часу [13 - 15].

При наочному моделюванні формуються моделі інформаційної системи, що відображають процеси та явища, які протікають в системі. При гіпотетичному моделюванні використовується гіпотеза про закономірності процесів у реальній інформаційній системі, яка базується на причинно-наслідкових зв'язках між виходом і входом і відображає рівень знань експерта досліджуваної інформаційної системи. Гіпотетичне моделювання використовується, коли недостатні знання про інформаційну систему для побудови формальних моделей. Макетування застосовується в реальній інформаційній системі, коли процеси не піддаються фізичному моделюванню. В основі макетів лежать аналоги інформаційної системи, що базуються на причинно-наслідкових зв'язках між процесами та явищами системи. При математичному моделюванні має бути проведена формалізація цього процесу, побудовано математичну модель. Математичне моделювання – процес встановлення відповідності деякого математичного об'єкта реальної інформаційної системи– математичної моделі [13,14].

На сучасному етапі засобом моделювання інформаційних систем є засоби обчислювальної техніки. При побудові математичної моделі кожна система *S* характеризується відповідним набором властивостей, які враховують умови взаємодії системи із зовнішнім середовищем *E* та відображають поведінку досліджуваної моделі системи. Модель системи *S* можна представити у вигляді множини величин, що описують процеси функціонування реальної інформаційної системи та утворюють наступні підмножини:

1. Сукупність внутрішніх параметрів системи: $□_k \in H, k = \overline{1, n_H}$.
2. Сукупність вихідних характеристик: $y_j \in Y, j = \overline{1, n_Y}$.
3. Сукупність вхідних впливів на систему: $x_i \in X, i = \overline{1, n_X}$.
4. Сукупність впливів зовнішнього середовища: $v_l \in V, l = \overline{1, n_V}$.

Змінні $x_i, y_j, □_k, v_l$ - елементи підмножин, містять стохастичні і детерміновані складові, не перетинаються.

При моделюванні системи внутрішні параметри системи, впливи зовнішнього середовища, вхідні впливи є незалежними змінними, які у векторній формі мають наступний вид:

$$\vec{x}(t) = \left(x_1(t), x_2(t), \ldots, x_{n_X}(t)\right);$$
$$\vec{v}(t) = \left(v_1(t), v_2(t), \ldots, v_{n_V}(t)\right);$$
$$\vec{□}(t) = \left(□_1(t), □_2(t), \ldots, □_{n_H}(t)\right).$$

Вихідні характеристики інформаційної системи є залежними змінними, векторною формою мають наступний вид:

$$\vec{y}(t) = \left(y_1(t), y_2(t), \ldots, y_{n_Y}(t)\right).$$

Функціонування інформаційної системи *S* описується оператором F_S:

$$\vec{y}(t) = F_S\left(\vec{x}, \vec{v}, \vec{□}, t\right) \qquad (1)$$

Залежність (1) є законом функціонування інформаційної системи. Алгоритм функціонування системи A_S - метод отримання вихідних характеристик системи з урахуванням впливів внутрішніх параметрів системи $\vec{□}(t)$, зовнішнього середовища $\vec{v}(t)$, вхідних впливів $\vec{x}(t)$. Закон функціонування F_S інформаційної системи *S* може бути реалізований множиною різних алгоритмів функціонування A_S, різними способами.

Відношення (1) є математичним описом інформаційної системи моделювання *S* протягом часу *t*, математичні моделі такого типу є динамічними.

Відношення (1) може бути реалізовано різними способами: таблично, аналітично, графічно.

Математична модель системи - кінцева підмножина змінних $\left\{\vec{x}(t), \vec{v}(t), \vec{h}(t)\right\}$ з

математичними зв'язками між ними та характеристиками $\vec{y}(t)$ [9].

Дискретно детерміновані моделі системи *F*-схеми. В основі, яких лежить теорія автоматів, математична модель автомата. Автомат задається *F*- схемою

$$F = \langle Z, X, Y, \varphi, \psi, z_0 \rangle,$$

яка функціонує в дискретному автоматному часі, де Z - множина внутрішніх станів системи, *Y*-вихідні сигнали, *X*-вхідні сигнали, z_0 - початковий стан, $z_0 \in Z$, функція виходу $\psi(z, x)$, функція переходу $\varphi(z, x)$.

Мережеві моделі (*N* -схеми) - мережі Петрі. Для вирішення задач, пов'язаних з аналізом причинно-наслідкових зв'язків та з формалізованим описом у складних системах.

Найпоширенішим формалізмом, що описує взаємодію та структуру процесів та паралельних систем використовуються мережі Петрі.

Мережа Петрі (*N*-схема) задається наступним чином:

$$N = \langle B, D, I, O \rangle,$$

де, B – позиції, D – переходи, I – вхідна функція, O – вихідна функція.

Для кожного переходу $d_j \in D$ можна визначити для переходу множину вхідних позицій $I(d_j)$ і для переходу множину вихідних позицій $O(d_j)$.

Класифікація методів побудови моделей системи наведено на рис. 2.

Роглянуті методи та моделі мають свої недоліки та переваги.

Основні недоліки перерахованих моделей: будь-яка модель мінімізує пояснення можливих явищ; під час моделювання не завжди існує можливість виявлення якісних нових характеристик; як правило, необхідних даних не вистачає для налаштування моделей; статистичні моделі системи можуть бути об'єктивними в межах емпіричної множини побудови моделі.

Рис. 2. Класифікація методів побудови моделей атак

На основі проведеного дослідження, можна зробити висновок - існуючі підходи побудови моделей системи мають низку недоліків, що, своєю чергою, доводить необхідність удосконалення розглянутих моделей.

Для досягнення цілей забезпечення безпеки конфіденційної інформації необхідно: організувати ефективне створення системи захисту інформації (системи безпеки інформації), ефективне моделювання (визначення переліку) актуальних загроз інформаційної безпеки, визначення актуального порушника, а також надати можливість проводити якісну оцінку ефективності системи безпеки (захисту) інформації. Однією з найважливіших задач забезпечення безпеки конфіденційної інформації є оцінка ефективності системи захисту (безпеки). У зв'язку з цим мета роботи (дослідження) - підвищення якості оцінки ефективності систем захисту (безпеки) розподілених інформаційних систем за рахунок визначення достатніх та необхідних показників оцінки з використанням сучасних (перспективних) інформаційних технологій, що дозволяють найбільш ефективно вирішувати наступні задачі: визначення параметрів роботи адаптивних продукційних нечітких нейронних систем, що найбільш підходять для вирішення поставлених задач, застосування технологій Data Science при обробці даних, алгоритмів нечіткого виведення.

МОДЕЛЮВАННЯ ЗЛОВМИСНИКА ТА ЗАГРОЗ БЕЗПЕКИ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

Аналіз можливостей, які може мати зловмисник, проводиться у рамках розробки моделі зловмисника. Виходячи з актуальності порушників інформаційної безпеки, визначено внутрішні та ймовірні зовнішні порушники безпеки даних, що обробляються у розподілених системах. До можливих внутрішніх зловмисників інформаційної безпеки відносяться: особи, які мають санкціонований доступ до контрольованої зони розподілених систем, але не мають доступу до інформації, що обробляється в системі; зареєстровані користувачі розподіленої інформаційної системи - здійснюють обмежений доступ з робочого місця до ресурсів системи; зареєстровані користувачі розподіленої інформаційної системи - здійснюють віддалений доступ до інформації. До ймовірних зовнішніх зловмисників інформаційної безпеки даних відносяться: атакуючі інформаційну систему, колишні працівники розподіленої інформаційної системи.

Для виділених типів можливих зловмисників визначаються наступні методи реалізації загроз інформаційної безпеки [16,17]:

1. Загрози витоку даних з технічних каналів можуть бути реалізовані за допомогою: перегляду інформації, з використанням оптикоелектронних (оптичних) засобів відображення, екранів дисплеїв, інформаційно-обчислювальних комплексів, технічних засобів обробки буквенно-цифрової, графічної, відеоінформації; перехоплення випромінюваних чистот при обробці інформації у розподілених інформаційних системах, спеціальними технічними засобами радіотехнічної розвідки, розміщеними як на території контролюємої зони, так і за її межами.
2. Загрози несанкціонованого доступу до інформації можуть бути реалізовані за допомогою: впливу на технічні засоби в ході завантаження операційної системи; прямого доступу до технічних засобів чи програмного забезпечення після завантаження операційної системи; віддаленого доступу до технічних засобів чи програмного забезпечення; віддаленого або прямого впливу на об'єкти віртуального середовища системи і інформацію, яка зберігається у віртуальному просторі розподіленої системи.
3. Загрози спеціальних впливів на розподілену систему можуть бути реалізовані з використанням: хімічного впливу; механічного впливу; акустичного впливу; радіаційного впливу; біологічного впливу; електромагнітного впливу; термічного впливу; магнітного поля;

електромагнітного випромінювання.

При визначенні способу реалізації загроз інформаційній безпеці передбачалося, що загрози можуть бути реалізовані за рахунок доступу до інформації, компонентів розподіленої інформаційнох системи, за рахунок створення засобів, умов які забезпечують необхідний доступ.

При визначенні можливих способів реалізації загроз інформаційній безпеці враховано наступні умови: існує можливість змови зловмисників (зовнішніх та внутрішніх); загроз інформаційній безпеці можуть бути реалізовані в будь-якій точці та в будь-який час інформаційної системи (на будь-якому хості, вузлі); для досягнення мети зловмисник обирає найслабшу ланку інформаційної системи.

Модель ймовірного зловмисника розподіленої інформаційної системи містить систему поглядів на потенційних зловмисників безпеки інформації, що обробляється в системі, мотивацію та причини їх дій, цілі, які вони переслідують, загальний характер дій у процесі підготовки до реалізації загроз інформаційній безпеці та здійснення впливу на дані, що обробляються в розподіленій системі.

Модель ймовірного порушника інформаційної системи відбиває теоретичні та практичні можливості ймовірного зловмисника, його апріорні знання, місце та час дії. За наявності права разового чи постійного доступу до контрольваної зони зловмисники поділяються на: особи, які не мають прав доступу до контрольваної зони системи; особи, які мають право разового або постійного доступу до контрольваної зони системи. Факторами, які знижують ймовірність змови зловмисників, є: створення умов мінімальної фінансової зацікавленості юридичних та фізичних осіб, що входять до числа ймовірних зловмисників безпеки інформації розподілених систем, у реалізації загроз інформаційної безпеки, щодо розподілених систем; укладення угоди про конфіденційність даних між власником ситсеми та фізичними, юридичними особами, що входять до числа ймовірних зловмисників безпеки інформації системи; підтримання та забезпечення високого рівня підготовки користувачів розподіленої інформаційної системи у сфері забезпечення безпеки інформації; створення умов настання негативних наслідків для потенційного зловмисника у разі реалізації загрози інформаційної безпеки: втрата прибутку та ділової репутації, розрив цивільно-правових відношень; визначення відповідальності, що покладається на користувача розподіленої інформаційної системи, при порушенні вимог безпеки даних у розподіленій інформаційній системі.

На підставі зазначених категорій порушників з урахуванням умов експлуатації, характеру оброблюваної інформації, суб'єктів доступу до інформаційної системи, об'єктів захисту пропонується використовувати класифікацію внутрішніх порушників, за наступними категоріями: особи, які не мають доступу до даних, що обробляється в інформаційній системі, але мають санкціонований доступ до системи; зареєстровані користувачі, які здійснюють обмежений доступ до ресурсів системи з робочого місця; зареєстровані користувачі інформаційної системи, які здійснюють віддалений доступ до даних, які обробляються в системі; зареєстровані користувачі з повноваженнями адміністратора інформаційної безпеки сегмента системи; зареєстровані користувачі інформаційної системи з повноваженнями системного адміністратора; зареєстровані користувачі системи з повноваженнями адміністратора безпеки даних інформаційної системи; постачальники (програмісти-розробники) програмного забезпечення та особи, які забезпечують супровід прикладних програм на об'єкті, що захищається; особи та розробники, які забезпечують ремонт, постачання, супровід технічних засобів розподіленої інформаційної системи. Типи потенційних зловмисників інформаційної безпеки встановлюються на підставі відповідного потенціалу, що визначає наявні можливості реалізації загрози безпеки даних: порушники з низьким потенціалом - мають можливість використовувати дані, отриманих із загальнодоступних джерел для реалізації загрози інформаційній безпеці; порушники з середнім потенціалом - мають можливість здійс-

нювати аналіз прикладного програмного забезпечення, знаходити в ньому вразливості та використовувати їх для реалізації загроз інформаційній безпеці; порушники з високим потенціалом - мають можливість вносити закладки в програмне забезпечення інформаційної системи, застосовувати спеціалізовані засоби проникнення, проводити спеціальні дослідження та добування інформації для реалізації зазгрози інформаційній безпеці.

Для кожної категорії порушників визначення актуальності інформаційної безпеки інформації використовуються наступні критерії: рівень небезпеки; рівень мотивації. Перелік потенційних зловмисників інформаційної безпеки, що обробляються в розподіленій інформаційній системі, та рівень мотивації наведені в таблиці 1.

Для визначення рівня небезпеки зловмисника інформаційній безпеці використовуються наступні характеристики: ступінь поінформованості про розподілену інформаційну систему; рівень знань в області безпеки даних.

Таблиця 1. Перелік потенційних порушників інформаційної безпеки та рівень їх мотивації

Порушник	Мотив	Рівень мотивації
Зовнішній порушник		
Розвідувальні служби держав	Відсутній	Мінімальний
Кримінальні структури	Корисні інтереси: досягнення безпосередньої матеріальної вигоди, підрив репутації фірми	Високий
Конкуренти (конкуруючі організації)	Відсутній	Мінімальний
Недобросовісні партнери	Корисливі інтереси: досягнення безпосередньої матеріальної вигоди, підрив репутації організації	Високий
Зломщики інформаційних систем та мереж	Хуліганство (вандалізм); професійне самоствердження	Високий

МОДЕЛЬ ВИЗНАЧЕННЯ АКТУАЛЬНИХ ЗАГРОЗ БЕЗПЕКИ КОНФІДЕНЦІЙНИМ ДАНИМ

Проведено дослідження адаптивних нейронних нечітких систем ANFIS із використанням алгоритмів нечіткого виведення Такагі-Сугено-Канга, Сугено-Такагі, Мамдані, Ванга-Менделя. Залежність похибки на тестовій вибірці від кількості правил під час перевірки менша у мережі ANFIS з алгоритмом Такагі-Сугено-Канга. Для визначення актуальних загроз інформаційної безпеки обрана нейронна продукційна адаптивна система ANFIS, заснована на нечіткій системі Такагі-Сугено-Канга. Алгоритм роботи полягає в реалізації нечіткої моделі, заснованої на правилах типу (2):

$$R_i: IFx_iISA_{i1}AND \dots AND_{x_j}ISA_{ij}AND \dots AND_{x_{im}}ISA_{im}, THEN \quad y = c_{i0} + \sum_{j=1}^{m} c_{ij}x_j, j = 1, \dots, n \qquad (2)$$

Сформовано базу правил визначення актуальних загроз інформаційної безпеки. Приклад заповнення бази знань правил, виходячи з сформованого набору даних наведено в таблиці 2.

Правила представлені в таблиці 2, фактично представляють множину правил, що складаються окремо за типом системи захисту інформації, типом зловмисника, (Dallas Lock, SecretNet) та впливом.

Нейронна продукційна адаптивна система ANFIS базується на наступних положеннях:

- вхідні змінні є чіткими;
- функції приналежності визначені функцією Гауса: $\mu_{A_{ij}}(x_j) = exp\left(-\frac{1}{2}\left(\frac{x_j - a_{ij}}{b_{ij}}\right)^2\right)$ де x - вхідні дані мережі, a_{ij}, b_{ij} - параметри функції приналежності, що налаштовуються;
- нечітка імплікація Ларсена нечіткий добуток;
- T-норма – нечіткий добуток; композиція не здійснюється;
- метод дефазифікації
- метод центроїду.

Таблиця 2. Фрагмент бази знань правил визначення актуальних загроз інформаційній безпеці

№ п/п	IF (ЯКЩО)			THEN (ТО)
	Тип порушника (джерело впливу)	IT-інфраструктура (об'єкт впливу)	Версія ПЗ	
1	Зовнішній порушник із низьким потенціалом. Внутрішній порушник з низьким потенціалом	Віртуальна машина VMWare	6.5 (VMWare Workstation), від 7.0.0 до 7.1.4 включно (VMWare Workstation)	Загроза несанкціонованого доступу до захищених віртуальних машин з боку інших віртуальних машин
2	Зовнішній порушник з високим потенціалом	Мобільний пристрій на базі iOS	(Android), до 10.3.3 включно (iOS)	Загроза контролю шкідливою програмою списку додатків, запущених на пристрої
…				
N	Зовнішній порушник із середнім потенціалом, Внутрішній порушник з середнім потенціалом	Засіб захисту інформації	12.4 (Cisco IOS), 12.4 (Cisco IOS), 15.0 (Cisco IOS), 15.0 (Cisco IOS), 15.2 (Cisco IOS), 15.1 (Cisco IOS)	Загроза несанкціонованого впливу на засіб захисту інформації

Функціональна залежність після дефазифікації для отримання вихідної змінної має вид (3):

$$y' = \frac{\sum_i^n \left(\left(c_{i0} + \sum_{j=1}^m c_{ij} x_j\right) \prod_j^m \mu_{A_{ij}}(x_j') \right)}{\sum_{i=1}^n \prod_j^m \mu_{A_{ij}}(x_j')} = \frac{\sum_i^n \left(\left(c_{i0} + \sum_{j=1}^m c_{ij} x_j\right) \prod_j^m exp\left[-\left(\frac{x_j' - a_{ij}}{b_{ij}}\right)^2 \right] \right)}{\sum_{i=1}^n \prod_j^m exp\left[-\left(\frac{x_j' - a_{ij}}{b_{ij}}\right)^2 \right]} \quad (3)$$

Вираз 3 лежить в основі нейронної мережі ANFIS із використанням алгоритму TSK, включає п'ять шарів:

1. Виконує фазифікацію чітких вхідних змінних: $x_j'(j = 1, \ldots, n)$.
2. Обчислює значення ступенів функції приналежності $\mu_{A_{ij}}[x_j']$, заданих функціями Гаусса з параметрами a_{ij}, b_{ij}.
3. Генерує значення функцій $\left(c_{j0} + \sum_{j=1}^m c_{ij} x_j'\right)$, які перемножуються на результати обчислень елементами другого шару.

4. Перший елемент четвертого шару необхідний для активізації виводів правил відповідно до значень, в третьому шарі, ступенів належності передумов правил. Другий елемент четвертого шару проводить додаткові обчислення для подальшої дефазифікації.
5. Даний шар складається з одного елемента нормалізуючого та робить дефаззифікацію результатів роботи нейронної мережі.

Нейронна мережа ANFIS містить два параметричні шари (1 і 3). Параметрами, які налаштовуються в процесі навчання нейронної мережі є: в першому шарі - нелінійні параметри a_{ij}, b_{ij}функції приналежності фазифікатора; в третьому шарі - параметри c_{i0} і c_{ij}лінійних функцій $\left(c_{j0} + \sum_{j=1}^{m} c_{ij} x_j^{'}\right)$ з висновків бази правил.

На наступному кроці розраховуються параметри c_{i0} і c_{ij}лінійних функцій за умови фіксованих значень параметрів a_{ij}, b_{ij}. Параметри c_{i0} і c_{ij} знаходяться шляхом розв'язання системи лінійних рівнянь. Вихідну змінну з виразу (3) представимо в наступному виді (4):

$$y^{'}y^{'} = \sum_{i=1}^{n} w_i^{'}\left(c_{i0} + \sum_{j=1}^{m} c_{ij} x_j\right), \tag{4}$$

де $w_i^{'} = \frac{\prod_j^m \mu_{A_{ij}}\left(x_j^{'}\right)}{\sum_{i=1}^n \prod_j^m \mu_{A_{ij}}\left(x_j^{'}\right)} = \frac{\prod_j^m exp\left[-\left(\frac{x_j^{'} - a_{ij}}{b_{ij}}\right)^2\right]}{\sum_{i=1}^n \prod_j^m exp\left[-\left(\frac{x_j^{'} - a_{ij}}{b_{ij}}\right)^2\right]} = const$

Алгоритм навчання нейроної продукційної адаптивної система ANFIS із застосуванням алгоритму TSK.

При k навчальних прикладах $x_1^{(k)}, x_2^{(k)}, \ldots, x_m^{(k)}, y^{(k)}$, де $k = 1, \ldots, K$ і заміна значень вихідних змінних $y'^{(k)}$ значеннями еталонних змінних $y^{(k)}$, отримаємо систему з k лінійних рівнянь (5):

$$\begin{bmatrix} w_1^{`(1)} w_1^{`(1)} x_1^{(1)} \ldots w_1^{`(1)} x_m^{(1)} \ldots w_n^{`(1)} w_n^{`(1)} x_1^{(1)} \ldots w_n^{`(1)} x_m^{(1)} \\ w_1^{`(2)} w_1^{`(2)} x_1^{(2)} \ldots w_1^{`(2)} x_m^{(2)} \ldots w_n^{`(2)} w_n^{`(2)} x_1^{(2)} \ldots w_n^{`(2)} x_m^{(2)} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ w_1^{`(k)} w_1^{`(k)} x_1^{(k)} \ldots w_1^{`(k)} x_m^{(k)} \ldots w_n^{`(k)} w_n^{`(k)} x_1^{(k)} \ldots w_n^{`(k)} x_m^{(k)} \end{bmatrix} \times \begin{bmatrix} c_{10} \\ \ldots \\ c_{1m} \\ \ldots \\ c_{n0} \\ \ldots \\ c_{nm} \end{bmatrix} = \begin{bmatrix} y^{(1)} \\ y^{(2)} \\ \ldots \\ y^{(k)} \end{bmatrix} \tag{5}$$

де $w_1^{`(k)}$- агрегований ступінь істинності передумов за і-им правилом при пред'явленні k-го вхідного вектора $\left(x_1^{(k)}, x_2^{(k)}, \ldots, x_m^{(k)}\right)$. Вираз (5) у скороченому виді: $W \cdot c = y$. Вирішення даної системи рівнянь можна провести за один крок за допомогою псевдоінверсії матриці W: $c = W^{+} y = (W^T W)^{-1} W^T y$. Після визначення лінійних параметрів ij розраховуємо та фіксуємо фактичні вихідні сигнали системи, для чого використовуємо лінійну залежність (6):

$$y^{`} = \begin{bmatrix} y^{(1)} \\ y^{(2)} \\ \ldots \\ y^{(k)} \end{bmatrix} = W \cdot c \tag{6}$$

Визначаємо вектор помилок: $e = y^{`} - y$. Виконуємо уточнення параметрів (7):

$$b_{ij}^{(k)}(t+1) = b_{ij}^{(k)}(t) - C \frac{\partial E^{(k)}(t)}{\partial b_{ij}^{(k)}} \qquad 7)$$

Для визначення актуальних загроз інформаційній безпеці із переліку потенційних можливих загроз необхідно визначити ймовірність реалізації.

Визначаємо коефіцієнти Y_2 експертним шляхом для кожної загрози інформаційної безпеки: 0 - малоймовірна загроза; 2 – низька ймовірність загрози; 5 – середня ймовірність загрози; 10 –висока ймовірність загрози.

З урахуванням визначених коефіцієнтів ймовірність реалізації загроз інформаційній безпеці Y визначається співвідношенням: $Y = (Y_1 + Y_2)$, де Y_1 - ступінь початкової захищеності розподіленої інформаційної системи, що визначається відповідно до методичних даних Кваліфікаційного центру інформаційних технологій та кібербезпеки України.

Структура нечіткої нейронної продукційної мережі ANFIS із застосуванням алгоритму TSK представлена на рис. 3.

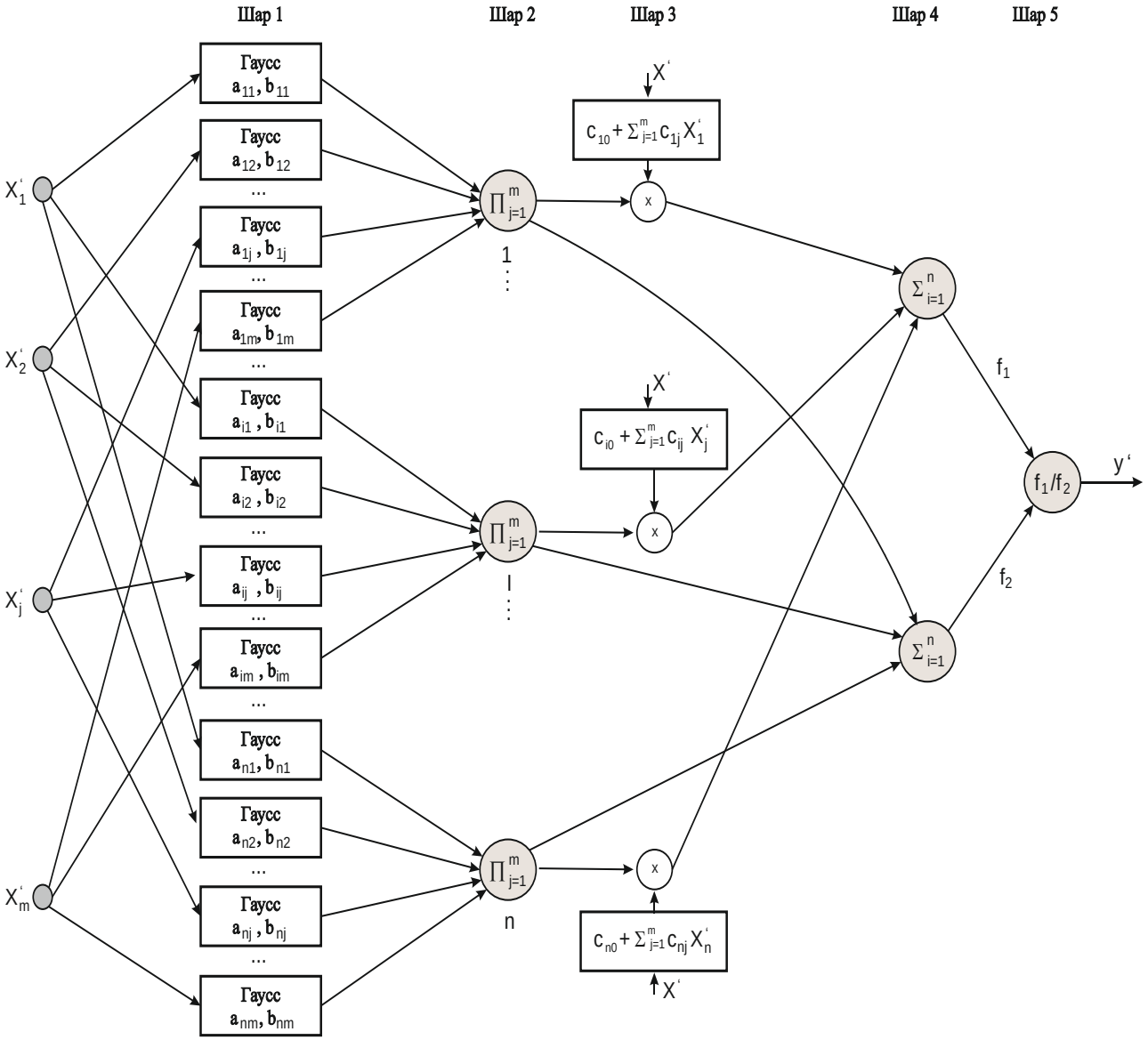

Рис. 3. Нейронна мережа ANFIS із застосуванням алгоритму TSK

Аналіз оцінки ефективності запропонованого підходу визначення актуальних загроз інформаційній безпеці наведені у табл. 3.

Таблиця 3 – Аналіз оцінки ефективності запропонованого підходу визначення актуальних актуальних загроз інформаційній безпеці

Таблиця 3. Аналіз оцінки ефективності запропонованого підходу визначення актуальних актуальних загроз інформаційній безпеці

Показник	Існуючі підходи	Запропонований підхід
RMSE	0,018-0,069	0,011-0,022
Визначення кількості актуальних загроз	понад 30%	більше 35%
Вартість системи захисту	зниження до 15%	зниження до 30%

Середньоквадратична помилка запропонованого підходу, що обчислюється за формулі (8):

$$RMSE = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(y_i - \hat{y}_i)^2}, \qquad (8)$$

де $y_i, \hat{y}_i$ - набори даних (перевірки, навчання).

Графіки порівняння *RMSE* запропонованого та існуючих підходів на заданому інтервалі представлені на рис. 4.

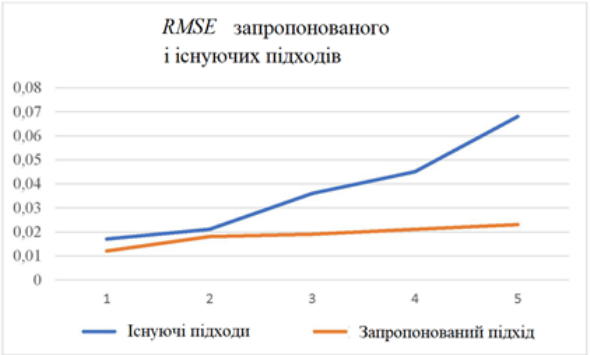

Рис. 4. Графік порівняння RMSE запропонованого та існуючих підходів на заданому інтервалі

ВИСНОВКИ

Запропоновано модель визначення актуальних загроз інформаційній безпеці, заснована на алгоритмах нечіткого виводу та теорії нечітких нейронних систем, на відміну від відомих, використовує певні достатні та необхідні показники, виключає помилки експертів. Збільшує виявлення кількість актуальних загроз інформаційній безпеці розподілених систем 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 у розподіленій інформаційній системи, перелік існуючих засобів захисту в розподіленій інформаційній системі. Запропонований підхід відрізняється від існуючих, в наступному: відсутність залучення висококваліфікованих фахівців у області безпеки інформації; процес автоматизований, має низьку обчислювальну складність; відсутність недоліків експертних оцінок; дозволяє визначати перелік актуальних загроз безпеки інформації в інформаційних системах різних класів та типів.

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.** 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.
4. **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.
5. **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.
6. **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, стр. 81–87.
7. Соціальні мережі – реальні загрози віртуального світу. [Електронний ресурс]. – Режим доступу : http://ogo.ua/ articles/view/011–02–23/26490.htm.
8. **Остапов С.Е.** Технології захисту інформації: навчальний посібник / С.Е. Остапов, С.П. Євсеєв, О.Г. Король – Харків : Вид-во ХНЕУ, 2016. – 476 с.
9. **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.
10. **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.
11. **Рибальченко Л.В., Косиченко О.О.** Проблеми безпеки персональних даних в Україні / Регіональна економіка / Запоріжжя. 2019. – с.57-62.
12. **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.
13. **Лавров Є.А**. Математичні методи дослідження операцій: підручник / Є. А. Лавров, Л. П. Перхун, В. В. Шендрик – Суми: Сумський державний університет, 2017. – 212 с.
14. **Гончар С.Ф.** Оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури: монографія. / С. Ф. Гончар. – Київ, 2019. – 175 с.
15. **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.
16. Сигнатура атаки. Wikipedia [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Сигнатура_атаки .
17. OPWNAI: Cybercriminals Starting to Use ChatGPT, January 6, 2023 [Електронний ресурс] – Режим доступу до ресурсу: https://research.checkpoint.com/2023/opwnai-cybercriminals-starting-to-usechatgpt.

REFERENCES

1. Doktryna informatsiinoi bezpeky Ukrainy, zatverdzhenoi Ukazom Prezydenta Ukrainy vid 25 liutoho 2017 roku № №47/2017, 15s.
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). Metod prohnozuvannia vrazlyvostei informatsiinoi bezpeky na osnovi analizu danykh tematychnykh internet-resursiv / S.V. Lienkov, V.M. Dzhulii, A.M. Bernaz, I.V. Muliar, I.V. Pampukha // Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. – K.: VIKNU -. №78. – C. 123-134.
4. **Lenkov S.V.** (2022). Metod protydii poshyrenniu ta vyiavlennia shkidlyvoi informatsii v sotsialnykh merezhakh/ S.V. Lenkov, V.M. Dzhulii, L.V. Solodieieva // Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. – K.: VIKNU. – Vyp. №77. – C. 103-117.
5. **Lenkov S.V.** (2020). Model bezpeky poshyrennia zaboronenoi informatsii v informatsiino-telekomunikatsiinykh merezhakh / S.V. Lenkov, V.M. Dzhulii, V.S. ORLENKO, O.V. Sieliukov, A.V. Atamaniuk // Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni

Tarasa Shevchenka. – K.: VIKNU. – №68. – pp. 53-64.
6. **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, стр. 81–87.
7. Cotsialni merezhi – realni zahrozy virtualnoho svitu. [Elektronnyi resurs]. – Rezhym dostupu: http://ogo.ua/ articles/view/011– 02– 23/26490.htm
8. **Ostapov S. E.** (2016). Tekhnolohii zakhystu informatsii: navchalnyi posibnyk / S.E. Ostapov, S.P. Yevseiev, O.H. Korol–Kharkiv: Vyd-vo KhNEU. – 476 s.
9. **Lenkov S.V.** (2017). AnalIz Isnuyuchih metodiv ta algoritmiv viyavlennya atak v bezdrotovih merezhah peredachI danih / S.V. Lenkov, V.M. Dzhuliy, N.M. Bernaz, S.O. Bozhuk // Zbirnik naukovih prats Viyskovogo Institutu Kiyivskogo natsionalnogo universitetu imeni Tarasa Shevchenka. – K.: VIKNU. – Vip. No 56. – p.124-132
10. **Buriachok, V. L.** (2016). Informatsiinyi ta kiberprostory: problemy bezpeky, metody ta zasoby borotby : posibnyk / V. L. Buriachok, S. V. Toliupa, V. V. Semko – K. : DUT-KNU – 178 s.
11. **Rybalchenko L.V., Kosychenko O.O.** (2019). Problemy bezpeky personalnykh danykh v Ukraini / Rehionalna ekonomika / Zaporizhzhia – s.57-62
12. **Dzhulii V.M.** (2022). Metod klasyfikatsii dodatkiv trafika kompiuternykh merezh na osnovi mashynnoho navchannia v umovakh nevyznachenosti / V.M. Dzhulii, O.V. Miroshnichenko, L.V. Solodieieva // Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. – K.: VIKNU. – Vyp. №74. – pp. 73-82.
13. **Lavrov Ye. A**. (2017.). Matematychni metody doslidzhennia operatsii: pidruchnyk / Ye. A. Lavrov, L. P. Perkhun, V. V. Shendryk – Sumy: Sumskyi derzhavnyi universytet – 212 p
14. **Honchar S. F.** (2019). Otsiniuvannia ryzykiv kiberbezpeky informatsiinykh system obiektiv krytychnoi infrastruktury: monohrafiia. / S. F. Honchar. – Kyiv – 175 s.
15. **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.
16. Syhnatura ataky. Wikipedia [Elektronnyi resurs] – Rezhym dostupu do resursu: https://uk.wikipedia.org/wiki/Syhnatura_ataky.
17. OPWNAI: Cybercriminals Starting to Use ChatGPT, January 6, 2023 [Elektronnyi resurs] – Rezhym dostupu do resursu: https://research.checkpoint.com/2023/opwnai-cybercriminals-starting-to-usechatgpt.

Model of current threats to security of confidential data in divisional information systems

Volodymyr Dzhuliy, Ihor Muliar, Maksym Dymbovsky

Abstract. The paper proposes a model for determining actual threats to the information security of distributed information systems, based on algorithms of fuzzy inference and the theory of fuzzy neural systems, unlike known ones, uses sufficient and necessary indicators, excludes expert errors, increases the detection of the number of actual threats to information security of distributed systems by 5 %, reduces the cost of purchasing information protection equipment 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 distributed information system, the list of existing protection tools in the distributed information system.

The proposed approach differs from existing ones in the following: lack of involvement of highly qualified specialists in the field of information security; the process is automated, has a 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 information becomes the most 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.

Existing methods of modeling current threats to information security and assessing the effectiveness of the information protection system 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 information systems, current threats to information security, security requirements for confidential information, a list of means

of protecting confidential information and their value as important indicators when solving these problems.

In order to achieve the goals of ensuring the security of confidential information, it is necessary to: organize the effective creation of an information protection system (information security system), effective modeling (identification of the list) of current threats to information security, identification of the current violator, and also provide the opportunity to conduct a qualitative assessment of the effectiveness of the information security (protection) system.

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

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