УДК 004

Д.Ященко, магістр гр. КІ-21М-1,4,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ФОРМУВАННЯ ПРОФІЛІВ ЗАХИСТУ ХМАРНИХ СЕРВІСІВ

У статті розроблено програмне забезпечення, яке призначено для системи формування профілів захисту хмарних сервісів. Метою розробки є дослідження та програмна реалізація системи формування профілів захисту хмарних сервісів. Об’єктом дослідження є процес формування профілів захисту хмарних сервісів. Предметом дослідження є методи формування профілів захисту хмарних сервісів. Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи формування профілів захисту хмарних сервісів. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.
комп’ютерна інженерія, профілі захисту, хмарні сервіси

Постановка проблеми. В останні роки в банківській діяльності загострилася проблема забезпечення безпеки даних. Вона містить у собі кілька аспектів. По-перше, це гнучка, багаторівнева й надійна регламентація повноважень користувачів – цінність банківської інформації висуває особливі вимоги до захисту даних від несанкціонованого доступу, у тому числі, до контролю керування процесами, що змінюють стан даних. По-друге, важливим аспектом є наявність засобів для підтримки цілісності й несуперечності даних; подібні засоби мають на увазі можливість здійснення контролю введення даних, підтримки й контролю зв'язків між даними, а також уведення й модифікації даних у режимі транзакцій – набір операцій, що забезпечують підтримку погодженості даних. По-третє, необхідна присутність у системі багатофункціональних процедур архівації, відновлення й моніторингу даних при програмних і апаратних збоях.

Забезпечення безпеки інформаційних банківських систем являє собою комплексну проблему, що вирішується в напрямках удосконалювання правового регулювання застосування інформаційних технологій, удосконалювання методів і засобів їхньої розробки, розвитку системи сертифікації, забезпечення відповідних організаційно-технічних умов експлуатації. Ключовим аспектом рішення проблеми безпеки є вироблення системи вимог, критеріїв і показників для оцінки рівня безпеки інформаційних технологій.

ДСТ ІСО/МЕК 15408 визначає критерії, за яких історично закріпилася назва "Загальні критерії" (ЗК). ЗК призначені для використання інформаційних технологій як основу при оцінці характеристик безпеки продуктів і систем. Установлюючи загальну базу критеріїв, ЗК роблять результати оцінки безпеки значимими для більше широкої аудиторії.

Сукупність вимог безпеки, узятих з ЗК або сформульованих у явному виді, представляється у вигляді профілю захисту, оцінка й обґрунтування якого виконується відповідно до критеріїв оцінки, що втримується в частині 3 ЗК. Метою такої оцінки є демонстрація того, що профіль повний, несуперечливий, технічно правильний і придатний для використання при викладі вимог до об'єкта оцінки, передбачуваному для оцінки.

Обґрунтування ж містить у собі наступне:

а) логічне обґрунтування цілей безпеки, що демонструє, що викладені цілі безпеки зіставлені з усіма аспектами середовища безпеки;

б) логічне обґрунтування вимог безпеки, що демонструє, що сукупність вимог безпеки придатна для досягнення цілей безпеки й порівнянна з ними.

Проте, відсутність методології економічного обґрунтування й оцінки профілю захисту в цей час приводить до відсутності прагнення до впровадження ЗК. Розробка моделі обґрунтування, що опирається на економічні показники діяльності, буде стимулювати впровадження ЗК у різні галузеві сфери, зокрема, у сферу банківських інформаційних технологій. Це дозволить значно підвищити рівень безпеки банківських інформаційних систем, збільшить довіру до них як з боку користувачів (банківських організацій), так і сторони кінцевих споживачів банківського продукту.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи формування профілів захисту хмарних сервісів.

Мета й завдання дослідження. роботи є дослідження та програмна реалізація системи формування профілів захисту хмарних сервісів.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем формування профілів захисту хмарних сервісів.
– Дослідження системи формування профілів захисту хмарних сервісів.
– Програмна реалізація системи формування профілів захисту хмарних сервісів.

Об'єктом дослідження є процес формування профілів захисту хмарних сервісів.

Предметом дослідження є методи формування профілів захисту хмарних сервісів.

Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Розглянемо основні принципи, методи формування й структуру профілю захисту, а також характеристику стану інформаційних систем банківської сфери

Представимо огляд сучасних інформаційних банківських систем, їхню структура. Основні функціональні модулі систем, що реалізують всі види банківських послуг:

– розрахунково-касове обслуговування юридичних осіб;
– обслуговування рахунків банків-кореспондентів;
– кредитні, депозитні й валютні операції;
– будь-які види внесків приватних осіб і операції по них;
– фондові операції; розрахунки за допомогою пластикових карток;
– бухгалтерські функції;
– аналіз, прийняття рішень, менеджмент, маркетинг і ін.

Освітимо найбільш перспективні напрямки розвитку банківських інформаційних технологій, такі як:

– інтернет-банкінг;
– системи дистанційного обслуговування: «Інтернет-банк», «Інтернет-клієнт», домашній банк, телебанк, мобільний банк або WAP-сервіс.

З їхньою допомогою задовольняються практично будь-які, крім касового обслуговування, вимоги клієнтів банку. Освоєння українськими кредитними організаціями нових напрямків розвитку брокерських послуг полягає в наданні фізичним особам доступу до українських і міжнародних валютних і фондових ринків (інтернет-трейдінг).

Розглянемо стандарти в області інформаційної безпеки:

– міжнародні й національні стандарти оцінки керування інформаційною безпекою;
– галузеві стандарти забезпечення безпеки в банківській сфері;
– стандарти й рекомендації в області стандартизації:

а) забезпечення інформаційної безпеки організацій банківської системи України. Загальні положення СТО БР ІББС-1.0-2006;

б) методика оцінки відповідності інформаційної безпеки організацій банківської системи України вимогам СТО БР ІББС-1.0-2006;

в) посібник із самооцінки відповідності інформаційної безпеки організацій банківської системи України вимогам СТО БР ІББС-1.0-2006;

– аудит інформаційної безпеки.

Розглянемо стандарти й методичні рекомендації, присвячені формуванню й оцінці профілів захисту й завдань по безпеці відповідно до ДСТ ІСО/МЕК 15408. Представлено існуючі на даному етапі способи формування профілів захисту й завдань по безпеці. Особлива увага приділена складеним об'єктам оцінки (складається із двох і більше компонентів), якими і є в деяких випадках автоматизовані банківські системи. На рисунку 1 представлені два види складених об'єктів оцінки (ОО), з єдиним і різним середовищем безпеки.

Запропонуємо конкурентну модель СЗІ автоматизованих банківських систем комерційних банків і метод обґрунтування профілю захисту на основі даної моделі.

Введемо поняття конкуренції стосовно до інформаційних систем. Інваріантність даного поняття дає підставу припускати можливість побудови деякої математичної моделі даного процесу. Конкуренція, одержавши широке поширення в теорії еволюції біологічних і економічних систем, а також інших сферах, таких як політика, історія науки, утворення, мистецтво, соціальна психологія й навіть фізика, дозволяє використовувати дане поняття й у сфері інформаційних технологій. Зокрема, в області інформаційної безпеки.

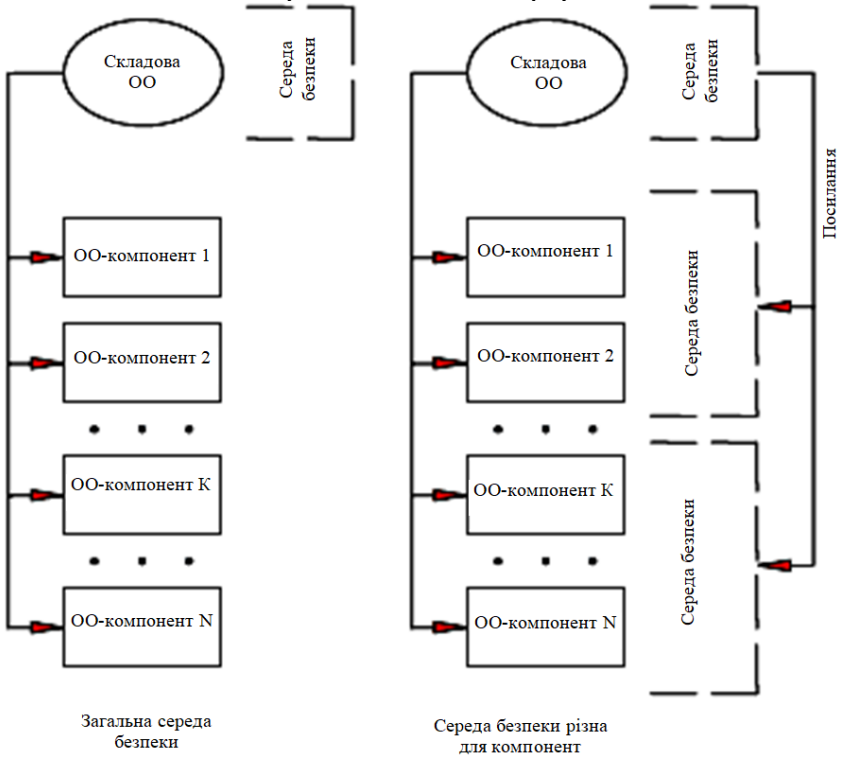

Рисунок 1 – Складені об'єкти оцінки ОО

Опишемо вимоги, запропоновані до моделі як до відбиття однієї зі сторін взаємодії, й не є повним функціональним аналогом реальної системи, а також вимоги до вибору економічного показника, що не повинен бути вузькоспеціалізованим параметром, характерним тільки для деяких систем, а повинен бути властивий всім учасникам взаємодії. Як такий показник запропонований використовувати чисті активи (нетто-активи), обумовлені як різниця між активами й пасивами:

$$A = AK - П, \quad (1)$$

де:

– A – чисті активи (грн.);
– AK – активи (грн.);
– $П$ – пасиви (грн.).

Для виключення впливу таких макроекономічних показників як середні доходи населення, середня заробітна плата, ціни, рівень інфляції, безробіття, зайнятість, продуктивність праці вводиться поняття нормалізованого активу:

$$AN_i = \frac{A_i}{\sum_{i=1}^{n} A_i}, \tag{2}$$

де:

– AN – нормалізований актив;
– A – чистий актив (грн.);
– n – число діючих кредитних організацій.

У графічному виді представлена й проаналізований взаємозв'язок між чистими й нормалізованими активами п'яти найбільших банків.

Введемо визначення конкурентоспроможності як суми показника захищеності ($З$) і показника росту активів ($Н$):

$$КС = З + Н, \tag{3}$$

де:

– $КС$ – нормалізований актив;
– $З$ – захищеність;
– $Н$ – приріст активу.

Формулювання конкурентної моделі взаємодії систем СЗІ автоматизованих банківських систем комерційних банків представлені на рисунку 2.

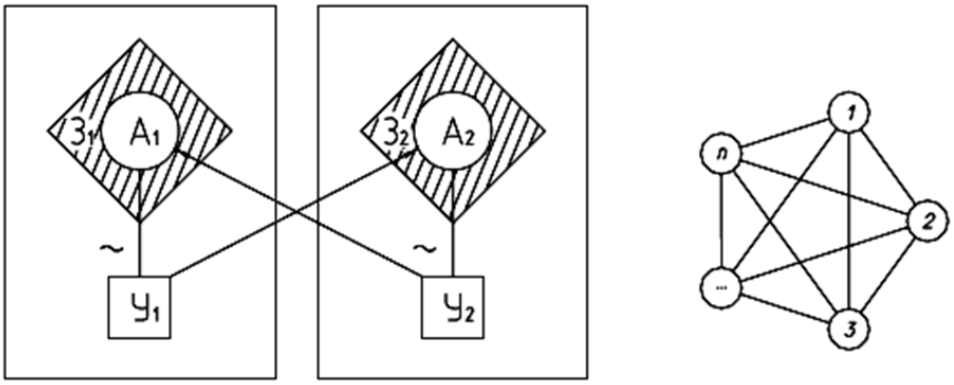

Рисунок 2 – Концептуальна схема конкурентної моделі СЗІ АБС КБ

Суб'єкт 1 має актив ($А_1$), що володіє тією або іншою захищеністю ($З_1$) від погроз, що виходять від другого ($В_2$). І, у той же час, сам формує погрозу ($В_1$), спрямовану на інший суб'єкт:

$$З_i(t) = \frac{\Delta AN_i(t)}{У_i}. \tag{4}$$

Захищеність суб'єкта ($З$) – це зміна нормалізованого активу AN від часу t-1 до часу t під впливом погрози ($В$):

$$\Delta AN_i(t) = AN_{i(t)} - AN_{i(t-1)}. \tag{5}$$

Погроза – імовірність втрати активу в одиницю часу. Як вихідне положення поле погроз для всіх суб'єктів системи єдино. Розходження погроз обумовлене як потужністю активу як з боку джерела, так і мети спрямованості погроз.

$$У_i = К_i \times \left(\sum_{i=1}^{n} К_i - К_i \right), \tag{6}$$

де:

– $У$ – погроза;
– $К$ – потужність активу.

Ріст своїх активів у результаті реалізації погроз, спрямованих на інші, у конкурентній моделі СЗІ автоматизованих банківських систем комерційних банків:

$$H = \frac{A_i^t - \sum_{i=1}^{n} A_i^t / \sum_{i=1}^{n} A_i^t \times A_i^{t-1}}{\sum_{i=1}^{n}\left(A_i^t - \sum_{i=1}^{n} A_i^t / \sum_{i=1}^{n} A_i^t \times A_i^{t-1} \right)}, \quad (7)$$

де:
H – приріст активу;
A – чистий актив (грн.).

У випадку, коли система не задовольняє вимозі конкурентоспроможності, за результатами експлуатації буде потрібно внесення розроблювачем виправлень в об'єкт оцінки, а також перевизначення вимог безпеки й/або припущень щодо середовища експлуатації, що спричинить перегляд профілю захисту.

Викладені вище положення не суперечать п.4.2.2 (Оцінка ОО) Державного стандарту України ДСТ ІСО/МЕК 15408-1-2002, у якому регламентоване, що процес оцінки може проводитися як паралельно з розробкою, так і слідом за нею.

Опишемо метод виконання оцінки на базі моделюючого комплексу. Метод містить у собі наступні етапи:

1. Одержання вихідних даних і прийняття ряду положень.

2. Розрахунок необхідних показників (нормалізований актив, захищеність, потужність активу, зміна активу за рахунок перерозподілу, конкурентоспроможність).

3. Ухвалення рішення про відповідність профілю захисту.

1-й етап: Збір статистичних даних, отриманих з відкритих джерел, за результатами діяльності банків і кредитних організацій.

Достатньою умовою є одержання даних по 500 самих великих організаціях. Вплив інших незначний, дані по них екстраполюються. Одержання свідчення про відповідність профілю захисту конкретної реалізації системи.

2-й етап: Обчислення нормалізованого активу за формулою (2): n – приймаємо рівним 1125, а потім і на часовому інтервалі від t-1 до t (5). Величина інтервалу приймається залежно від даних, отриманих на 1-му етапі (0,5 року). Визначаємо потужність активу кожного суб'єкта відповідно до його активу.

Ріст активів у результаті реалізації погроз, спрямованих на інші, являє собою відхилення від середнього приросту активів протягом часу від від t-1 до t. Обчислюється за формулою (7).

Обчислення захищеності виробляється за формулою (4), де B приймається за формулою (6). Таким чином, величина погрози B являє собою добуток потужності власного активу на суму потужностей активів інших організацій. Безпосереднє значення погрози, як імовірності втрати активу, не враховується, тому що є константою для всіх суб'єктів. При обчисленні значення захищеності вхідними параметрами виступають величина суб'єкта і його нормалізований актив.

Останнім значенням обчислюється параметр КС (конкурентоспроможність). Результатом є сума показників захищеності й показника росту активу.

3-й етап: Ухвалення рішення про відповідність профілю захисту на підставі показника КС. Для успішного розвитку в майбутньому показник КС повинен приймати, як мінімум, значення вище за середнє, тому що захищеність має тенденцію до зниження протягом часу, а разом з нею знизиться й показник КС .

Розробка структурної схеми

Структурна схема розробленої системи зображена на рисунку 3. В основному інтелектуальні засоби захисту інформації (СЗІ) знайшли своє застосування в системах

виявлення атак як інтелектуальний інструмент, у яких, як правило, використовуються нейронні мережі (НМ), системи нечіткої логіки (НЛ) і засновані на правилах експертні системи (ЕС) [1].

Схеми виявлення атак розділяють на дві категорії:

1) виявлення зловживань;

2) виявлення аномалій.

До першої відносять атаки, які використовують відомі уразливості інформаційної системи (ІС), а до других – невластиву користувачам ІС діяльність.

Для виявлення аномалій виявляється діяльність, що відрізняється від шаблонів, установлених для користувачів або груп користувачів. Виявлення аномалій, як правило, пов'язане зі створенням бази знань (БЗ), що містить профілі контрольованої діяльності [2], а виявлення зловживань – з порівнянням діяльності користувача з відомими шаблонами поводження хакера [3] і використовує методи на основі правил, що описують сценарії атак. Механізм виявлення ідентифікує потенційні атаки у випадку, якщо дії користувача не збігаються із установленими правилами.

Завдання класифікації в експертних системах

Експертні системи (рисунок 3) призначені для рішення класифікаційних завдань у вузькій предметній області виходячи з бази знань, сформованої шляхом опитування кваліфікованих фахівців і представленою системою класифікаційних правил *If-Then* (*Якщо – Тоді*) [4]. У системах забезпечення безпеки ІС експертні системи використовуються в інтелектуальних СЗІ на основі моделі [5] і містять у БЗ опис класифікаційних правил, що відповідають профілям легальних користувачів ІС, сценаріям атак на ІС [6].

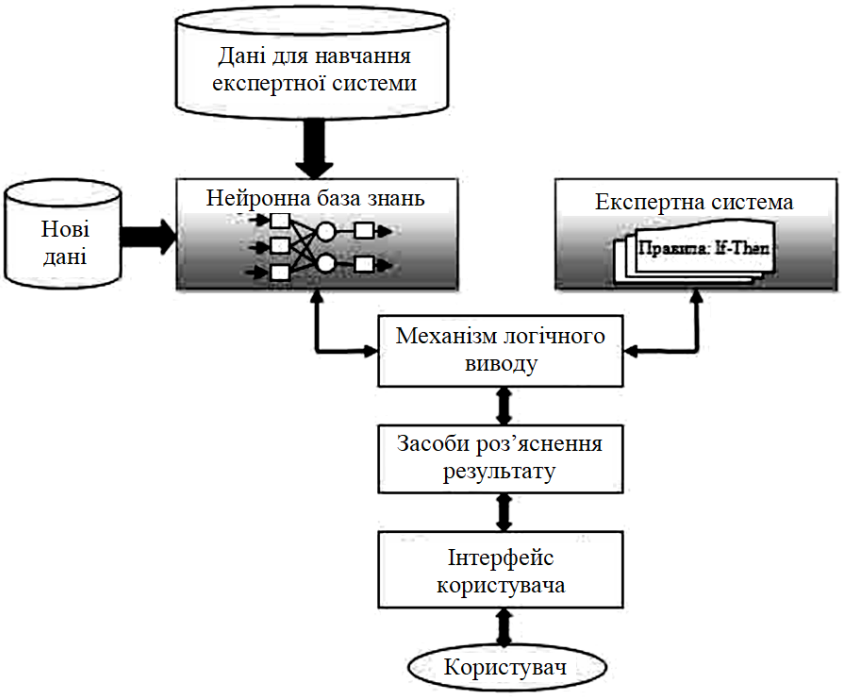

Рисунок 3 – Структурна схема системи

До недоліків ЕС, як засобів класифікації, відносять [7]:

– Непрозорість зв'язків між окремими правилами в базі знань. Хоча окремі правила відносно прості й логічно прозорі, наочність їхнього логічного взаємозв'язку в межах БЗ має бути досить низькою, тобто не просто визначити суперечливі правила в БЗ і їхню роль у рішенні завдання.

– Неефективна стратегія пошуку. ЕС із великою базою знань можуть виявитися недостатньо продуктивними для рішення оперативних завдань забезпечення безпеки ІС у реальному масштабі часу.

– Відсутність можливості адаптації. ЕС не мають здатність до автоматичного

навчання, тобто ЕС не може автоматично змінювати БЗ, коректувати існуючі правила або додавати нові правила *If-Then.*

Імовірнісні методи рішення завдання класифікації

Методи недостовірного керування й імовірнісних міркувань застосовуються в ЕС не тільки для формулювання класифікаційних висновків відповідно до правил *If-Then,* але й формування оцінок вірогідності проведеної класифікації у вигляді значень значення фактора впевненості або умовної ймовірності виникнення класифікуємої події.

Можливість оцінки вірогідності пророкування є достоїнством методу імовірнісних міркувань Байеса, тому що базується на математичному апараті теорії ймовірностей [4]. У вітчизняній практиці метод імовірнісних міркувань Байеса застосовують у ряді прикладних ЕС [8].

Практична значимість методу факторів упевненості для рішення завдання класифікації підтверджена розробкою ряду експертних систем [9]. Останній підхід до класифікації більше прийнятний з погляду обчислювальної ефективності, тому що не вимагає наявності більших обсягів статистичних даних і складних розрахунків умовних ймовірностей при великій розмірності простору вхідних посилок [7].

У всіх додатках забезпечення безпеки ІС на основі експертних систем може успішно застосовуватися підхід формування й підтримки класифікаційної бази знань відповідно до методів недостовірного керування й імовірнісних міркувань.

Чисельна оцінка класифікаційних висновків особливо важлива в умовах неповноти й низкою вірогідності вхідних ознак, використовуваних як посилки більшістю існуючих систем класифікації вторгнень у комп'ютерні системи.

Завдання нечіткої класифікації

Нечітка класифікація є подальшим розвитком підходу до рішення експертними системами завдань класифікації. Достоїнство нечіткої класифікації – можливість формулювати достовірні класифікаційні висновки виходячи з неповних і не цілком достовірних вхідних посилок [7].

При збереженні математичного апарата, розробленого для систем чіткої логіки, у нечітких логічних системах вирішене завдання перетворення чисельної і якісної інформації в ступінь приналежності значень конкретним нечітким безлічам [10]. Нечіткі безлічі описуються за допомогою функцій приналежності, що ставлять у відповідність безлічі значень із області визначення безперервної змінної безліч значень істинності з інтервалу [0, 1].

Етапи нечіткого логічного виводу безпосередньо пов'язані із процесом формування класифікаційних висновків [11]:

1) етап введення нечіткості (fuzzification) пов'язаний з перетворенням по засобом вхідних функцій приналежності (input membership functions) кожного із чітких вхідних значень x_i , $i = 1,\ldots,n$, де n – число вхідних значень класифікатора (crisp inputs) у ступінь істинності відповідної посилки μ_{xi}, $i= 1,\ldots,m$, де m-для кожного із класифікаційних правил (fuzzy rules);

2) етап нечіткого логічного виводу відповідає формуванню висновку (відповідні нечіткі підмножини) по кожному із правил μ_{Ri}, $i = 1,\ldots,m$, де m – кількість класифікаційних правил, виходячи зі ступеня істинності посилок μ_{xi}, $i= 1,\ldots,n$;

3) етап композиції нечітких підмножин по кожному із правил μ_{Ri}, $i = 1,\ldots,m$ за допомогою вихідних функцій приналежності (output membership functions) з метою формування нечітких підмножин класифікаційних висновків μ_{Ci}, $i = 1,\ldots,p$, де p – число виходів класифікатора;

4) етап об'єднання (aggregation) нечітких підмножин μ_{Ci}, $i = 1,\ldots,p$ і приведення до чіткості (defuzzification) приводить до формування вихідного чіткого значення $в$.

Нечіткі логічні системи зберігають у своєму составі базу знань кваліфікованих фахівців ІБ у вигляді системи правил *If-Then,* однак розширюють область застосування ЕС за рахунок рішення завдання класифікації виходячи з неповної й не цілком достовірної

інформації.

Системи НЛ мають обмежені можливості до адаптації, тому що можуть навчатися шляхом зміни параметрів функцій приналежності під реальні значення вхідних даних і бажаних класифікаційних висновків. Варто відзначити, що процес навчання функцій приналежності нечіткої ЕС із досить великою базою знань (понад 100 правил) трудомісткий і вимагає значних витрат часу [7].

Застосування НМ у завданнях класифікації й кластеризації

Нейронні мережі найбільше часто використовують для рішення завдань класифікації. Доведено, що НМ є універсальним аппроксіматором, тобто будь-яка функція може бути представлена у вигляді багатошарової НМ із формальних нейронів з нелінійною функцією активації. Формально підтверджена верхня границя складності НМ, що реалізує довільну безперервну функцію від декількох аргументів. Нейронною мережею з одним схованим шаром і прямими повними зв'язками можна представити будь-яку безперервну функцію, для чого досить у випадку n-мірного вхідного вектора $2n+1$ ФН схованого шару із заздалегідь застереженими обмеженими функціями активації [10].

Відомі численні застосування нейромережних засобів для забезпечення безпеки ІС, причому більшість випадків пов'язане з рішенням завдань класифікації й кластеризації [10].

Варто врахувати, що із всіх розглянутих раніше інтелектуальних засобів тільки НМ обдають властивістю самоорганізації, вирішує використовувати їх для рішення завдання кластеризації.

Можливість самоорганізації розглядається як одне з найбільш важливих якостей нейромережних СЗІ, вирішує адаптуватися до зміни вхідної інформації. Навчальним фактором виступають присутні в даних сховані закономірності й надмірність вхідної інформації. Інформаційна надмірність дозволяє фіксувати в інформаційному полі НМ вхідні дані, представляючи їх у більше компактній формі. Зменшення ступеня надмірності інформації в адаптивних СЗІ дозволяє виділяти істотні незалежні ознаки в даних.

Самоорганізація НМ реалізується за рахунок механізму кластеризації: подібні вхідні дані групуються нейронною мережею відповідно до взаємної кореляції й представляються конкретним ФН-прототипом. НМ, здійснюючи кластеризацію нечітких даних, знаходить такі усереднені по кластеру значення ваг ФН-прототипів, які мінімізують помилку подання згрупованих у кластер даних.

– Розглянуті механізми класифікації й кластеризації вхідних даних у СЗІ дозволяють не тільки відносити класифікуємий об'єкт (вектор вхідних даних) до одного з відомих класів, але й реалізувати еволюційні процеси самоорганізації, адаптації, розвитку в інтелектуальних засобах забезпечення інформаційної безпеки ІС. Причому кращі функціональні характеристики виходять при сполученні різних інтелектуальних засобів у гібридній системі захисту інформації.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів формування профілів захисту хмарних сервісів.

Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем формування профілів захисту хмарних сервісів; Досліджена система формування профілів захисту хмарних сервісів; На основі отриманих результатів досліджень створена програмна реалізація системи формування профілів захисту хмарних сервісів.

Розроблені під час виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання формування профілів захисту хмарних сервісів.

Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Kovalenko Oleksandr Qualitative risk analysis of software development / Oleksandr Kovalenko, Jamil Al-Azzeh, Oleksii Smirnov, Anna Kovalenko, Serhii Smirnov // Asian Journal of Information Technology. – Volume 17 Issue 3. – Medwell Journals. – 2018. – P. 218-230. ISSN: 1682-3915.
2. Kovalenko Oleksandr, The mathematical model of the testing technology for DOM XSS vulnerabilities / O. Kovalenko, O. Smirnov, A.Kovalenko, S. Smirnov, V. Vialkova // Scientific & practical cyber security journal (SPCSJ) Volume 2 Issue 1, P. 22-28. Georgia. Tbilisi. Scientific Cyber Security Association (SCSA), 2018 ISSN: 2587-4667.
3. Коваленко А.В. Методы качественного анализа и количественной оценки рисков разработки программного обеспечения / А.В. Коваленко, А.А. Смирнов // Информационные технологии в управлении, образовании, науке и промышленности: монография / Под редакцией профессора В.С. Пономаренко. – Х.: Видавець Рожко С.Г., 2016. – 566 с.
4. Smirnov, O., Neskorodieva, T., Fedorov, E., Rudakov, K., Neskorodieva, A. «Method Detection Audit Data Anomalies on Basis Restricted Cauchy Machine» CEUR Workshop Proceedings, Volume 3187, 2022, pp. 1-12..
5. Smirnov O., Smirnova T., Anas M. Al-Oraiqat, Drieiev O., Polishchuk L., Sheroz Khan, Yassin M. Y. Hasan, Aladdein M. Amro, Hazim S. AlRawashdeh «Method for Determining Treated Metal Surface Quality Using Computer Vision Technology». Sensors (Basel, Switzerland) Volume 22, Issue 16, 6223, 2022..
6. Smirnov, O., Lakhno, V., Akhmetov, B., Chubaievskyi, V., Khorolska, K., Bebeshko, B. «Selection of a Rational Composition of İnformation Protection Means Using a Genetic Algorithm». In: Rajakumar, G., Du, KL., Vuppalapati, C., Beligiannis, G.N. (eds) Intelligent Communication Technologies and Virtual Mobile Networks. Lecture Notes on Data Engineering and Communications Technologies, vol 131. 2023. Springer, Singapore. pp. 21-34..
7. Smirnov O.A., Al-Oraiqat A.M., Ulichev O.S., Meleshko Ye.V., Al-Rawashdeh H.S., Polishchuk L.I. «Modeling strategies for information influence dissemination in social networks». Journal of Ambient Intelligence and Humanized Computing Volume 13, Issue 5. Springer, Cham. 2022, pp. 2463-2477..
8. Smirnov O., Kuznetsov A., Kryvinska N., Kiian A., Kuznetsova K. «Full Non-Binary Constant-Weight Codes». SN Computer Science, Vol 2, 337, 2021. https://doi.org/10.1007/s42979-021-00739-w.
9. Smirnov O., Kovalenko O., Kovalenko A., Kavun S. «Quantitative Risk Assessment Method Development in the Context of the SDLC-model». 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T), 2021, pp. 203-208, doi: 10.1109/PICST54195.2021.9772143.
10. Smirnov O., Neskorodieva T., Fedorov E., Rymar P. «Neural Network Modeling Method of Transformations Data of Audit Production with Returnable Waste». CEUR Workshop Proceedings Volume 3101, 2021, Pages 192-207..
11. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova K. «Data hiding scheme based on spread sequence addressing». CEUR Workshop Proceedings Volume 2805, 2020, Pages 44-58..
12. Smirnov, O., Kuznetsov, A., Potii, O., Poluyanenko, N., Stelnyk, I., Mialkovsky, D. «Combining and filtering functions in the framework of nonlinear-feedback shift register». International Journal of Computing; 2020, Volume 19, Issue 2 – Research Institute for Intelligent Computer Systems – 2020. – P. 247-256..
13. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114..
14. Smirnov O.A., Alimseitova Zh., Adranova A., Akhmetov B., Lakhno V., Zhilkishbayeva G. «Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources». Journal of theoretical and applied information technology Vol.98. No 21, 2020, P. 3334-3346..
15. Smirnov O., Kuznetsov A., Arischenko A., Chepurko I., Onikiychuk A., Kuznetsova T. «Pseudorandom sequences for spread spectrum image steganography». CEUR Workshop Proceedings Volume 2654, 2020, Pages 122-131..
16. Smirnov O., Kuznetsov A., Kovalchuk D., Kuznetsova T. «New technique for data hiding in cover images using adaptively generated pseudorandom sequences». CEUR Workshop Proceedings Volume 2654, 2020, Pages 1-14..
17. Smirnov O., Lutsenko M., Kuznetsov A., Kiian A., Kuznetsova T., «Biometric cryptosystems: overview, state-of-the-art and perspective directions». Lecture Notes in Networks and Systems, vol 152. Springer, Cham. 2021, pp 66-84..
18. Smirnov O., Kuznetsov A., Pushkar'ov A., Serhiienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In: Radivilova T., Ageyev D., Kryvinska N. (eds) Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 48. Springer, Cham. 2021. pp 557-587..
19. Smirnov, O., Markovets, O. Vovk, N., Turchyn, Y., «Model of informational support for social network administrators' content creation». CEUR Workshop Proceedings Volume 2616, 2020, Pages 125-136..
20. Smirnov, O., Drieieva, H., Drieiev, O., Polishchuk, Y., Brzhanov, R., Aleksander, M. «Method of fractal traffic generation by a model of generator on the graph». CEUR Workshop Proceedings Volume 2616, 2020, Pages 366-379..