КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (27), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.27.750
УДК 004.056.5:004.911.4

Толюпа Сергій Васильович
д.т.н., професор, професор кафедри кібербезпеки та захисту інформації
Київський національний університет імені Тараса Шевченка, Київ, Україна
ORCID ID: 0000-0002-1919-9174
serhii.toliupa@knu.ua

Кулько Андрій Аркадієвич
аспірант кафедри кібербезпеки та захисту інформації
Київський національний університет імені Тараса Шевченка, Київ, Україна
ORCID ID: 0009-0006-1185-0774
kulko452@gmail.com

НЕЙРО-НЕЧІТКА СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ У ІНФОРМАЦІЙНУ МЕРЕЖУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація. У ситуації військової агресії росії проти України, безпека людей і країни значною мірою залежить від надійності роботи критично важливих об'єктів інфраструктури. Крім фізичних атак з використанням зброї, росія використовує кіберзброю для нападів на управлінські системи цих об'єктів через кіберпростір. Особливо тривожною є тенденція до того, що такі об'єкти, які використовують сучасні технології та функціонують у єдиному інформаційному середовищі, залишаються вразливими до нових видів кіберзагроз, навіть при великих зусиллях для їх захисту. Це суттєво ускладнює завдання забезпечення стійкості і безпеки в довгостроковій перспективі. Захист інформаційних систем на таких об'єктах є критично важливим для стабільного розвитку сучасного суспільства. В даній статті розглянуто завдання виявлення вторгнень у в інформаційні мережі критичної інфраструктури. Виокремлено основні компоненти системи виявлення вторгнень і описано їхні функції. Виконано аналіз різних підходів до виявлення порушень інформаційної безпеки. Дано характеристику основних методів виявлення вторгнень, виокремлено їхні переваги та недоліки. Показано, що для підвищення ефективності виявлення ситуацій, пов'язаних із можливим вторгненням, необхідно використовувати сучасні технології інтелектуального аналізу даних. Було досліджено особливості технологій для застосування в системах виявлення вторгнень, за результатами їх порівняльного аналізу запропоновано гібридні засоби для виявлення атак. Показано, що найперспективнішим для розглядуваного завдання є використання нейро-нечітких методів. Запропоновано архітектуру нейро-нечіткої системи для виявлення вторгнень у інформаційну мережу критичної інфраструктури.

Ключові слова: інформаційна безпека; вторгнення; інформаційна мережа; інтелектуальний аналіз даних; нейро-нечітка система; нейромережа; кібератака; критична інфраструктура; штучна нейронна мережа.

ВСТУП

В зв'язку з військовим станом в нашій державі питанню захисту критичної інфраструктури (КІ) приділяється дуже велика увага. За період з 2014 року було прийнято цілий ряд нормативних документів щодо покращення безпекової складової таких об'єктів. Так, згідно постанови Кабінету Міністрів України від 19 червня 2019 р. № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури», визначені організаційно-методологічні, технічні та технологічні умови кіберзахисту об'єктів критичної інфраструктури, що є обов'язковими до виконання

підприємствами, установами та організаціями, які відповідно до законодавства віднесені до об'єктів критичної інфраструктури [1].

Аналіз останніх досліджень і публікацій. Питанням захисту КІ приділяється велика увага науковцями. Так в [2] запропонована методологія синтезу моделей інтелектуальних систем управління та безпеки об'єктів критичної інфраструктури, принципово різних за своїми властивостями. В [3] розглянуті проблеми виявлення вторгнень та розроблення методологічних основ для аналізу та синтезу функціонально стійких розподілених інформаційних систем до кібернетичних загроз на основі мультиагентної технології, яка забезпечить вчасне виявлення та блокування кібернетичних впливів. В [4] розглядаються базові питання теорії і практики інтелектуального аналізу даних: алгоритми, моделі, задачі класифікації, кластерного аналізу, пошуку, глибинного аналізу даних, теорії складних мереж (Complex Networks), а також приводяться відомості, необхідні для математичного і комп'ютерного моделювання та аналізу складних систем і мереж в сфері кібербезпеки. У [5] на основі теорії керування та загального математичного підходу розглядається оцінювання створення і функціонування систем кіберзахищеності у сучасних умовах, а також методів синтезу, без чого неможлива побудова розвиненого та адекватного наукового базису кібербезпеки.

В [6] розглянуті сучасний стан та перспективи розвитку механізмів складових безпеки: кібербезпеки, інформаційної безпеки, безпеки інформації, та інформаційних технологій. Перелік може бути досить великим і це говорить про те, що дане питання є одним із ключових при захисті критичної інфраструктури.

Як показали наукові дослідження у сфері виявлення вторгнень тривають вже багато десятиліть, і за цей час було розроблено безліч методів для виявлення мережевих атак. До основних заходів захисту інформаційних систем належать: впровадження політики безпеки інформаційних мереж, використання міжмережевих екранів, захист на рівні маршрутизаторів, проведення мережевого аудиту, застосування систем виявлення вторгнень та розробка регламентів реагування на виявлені загрози.

На сьогодні вирішення питань забезпечення безпеки в ІС та управління станом їх захищеності висвітлені в роботах вітчизняних та закордонних дослідників, а саме: Бучика С.С., Бурячка В.Л., Дудикевича В.Б., Ланде Д.В., Горбенка І.Д., Гнатюка С.О., Корченко О.Г., Євсеєва С.П., Субача І.Ю., Кузнецова О.О., Biehl M., Bhuyan M., Albers P., Begni A. та інших.

Постановка проблеми. Сьогодні доступно велика кількість методів та засобів захисту інформації інформаційних систем критичної інфраструктури (КІ) від несанкціонованого доступу, дублювання, зміни, знищення та кібератак. Система виявлення вторгнень (IDS) — це програма, яка аналізує те, що відбувається чи сталося під час виконання і намагається знайти ознаки того, що інформаційна система функціонує неналежним чином.

Як відомо основним засобом захисту інформаційних систем та мереж (ІСМ) від інформаційно-руйнівних впливів (втручань) у вигляді кібервторгнень (КВ) є системи виявлення та/або запобігання вторгненням (СВВ/СЗВ), основна задача яких зводиться до оперативної їх ідентифікації та в ідеальному випадку ініціювання ефективного захисного сценарію щодо припинення факту порушення конфіденційності, доступності та цілісності інформаційних ресурсів, сервісів. Практика застосування СВВ сформувала два напрямки протидії кібервпливам: виявлення зловживань (Misuse detection) та виявлення аномалій (Anomaly detection) [7], [8]. Побудувати універсальну систему виявлення вторгнень, щоб вона ефективно протидіяла будь-якому типу кібератак, досить складно.

Тому постає завдання побудови таких систем на основі штучного інтелекту, щоб вини були адаптивні до різного типу кібератак.

Аналіз баз інцидентів. Перші кіберінциденти порушення інформаційної безпеки, офіційно зареєстровані в базах даних вразливостей, з'явилися в 1989 році [9] – [12]. З тих пір ведеться постійний пошук вразливостей та їх реєстрація як в рамках різних відкритих проектів, так і комерційними компаніями, дослідницькими інститутами та дослідниками. Серед лідерів детектування вразливостей можливо зазначити наступних розробників відповідних баз даних вразливостей: компанія MITRE та її база вразливосей Common Vulnerabilities and Exposures (CVE) [9]; National Institute of Standardsand Technology та база National Vulnerabilities Database (NVD) [10]; United State Computer Emergency Readiness Team та база Vulnerability Notes Database (VND) [11], компанія IBM та база вразливостей X-Force [12] та інші [13] – [15].

Розробники систем виявлення атак, а також організації, що їх застосовують, повинні детально розуміти та вивчати їхню класифікацію, щоб обрати найефективніші рішення для забезпечення інформаційної безпеки. Аналіз різних аспектів таксономії та використання різних методів дозволяє підвищити рівень захисту інформаційних систем [3].

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

На сьогоднішній день системи виявлення атак і вторгнень зазвичай представлені у вигляді програмного або апаратно-програмного комплексу, що автоматизує моніторинг подій в інформаційних системах і мережах. Вони аналізують отримані дані, визначаючи можливі загрози безпеці. З огляду на зростання кількості способів та типів несанкціонованих вторгнень у чужі мережі, системи виявлення атак (СВА) стали невіддільною частиною інфраструктури кібербезпеки більшості компаній та установ.

Для того щоб розуміти різноманіття систем виявлення вторгнень пропонуємо узагальнену класифікацію таких систем представлену на рис. 1.

Рис. 1. Узагальнений вигляд класифікації систем виявлення вторгнень та протидії кібератакам

Сценарій кібератаки можна уявити у вигляді графа переходів. Основні етапи проведення кібератаки можуть включати: сканування портів, визначення апаратного та програмного забезпечення, збір банерів, використання експлойтів, дестабілізацію роботи мережі через кібератаки на відмову в обслуговуванні, контроль через бекдори, пошук встановлених троянів, виявлення проксі-серверів, приховування слідів діяльності тощо. Рівень деталізації може змінюватися залежно від конкретного аналізу.

Процес виявлення вторгнень передбачає оцінку підозрілих дій, що відбуваються в інформаційній мережі критичної інфраструктури. Іншими словами, це процес ідентифікації та реагування на потенційні загрози, спрямовані на комп'ютерні або мережеві ресурси. Головна функція систем виявлення вторгнень (СВВ) — автоматизація заходів із забезпечення безпеки інформаційної мережі, а також створення доступного механізму контролю безпеки для користувачів, які не є фахівцями у сфері інформаційного захисту. Такі системи збирають дані з різних точок мережі, аналізують їх і виявляють не лише спроби атак, а й реальні порушення безпеки [15].

Нехай маємо множину ситуацій порушення інформаційної безпеки $X = \{x_1, ..., x_i\}$, кожна *i*-та подія описується вектором ознак $X_i = \{x_{1_i}, ..., x_{n_i}\}$, де l — кількість загроз ІБ; n — кількість ознак. За результатами аналізу цих ознак відбувається ідентифікація підозрілої діяльності й СВВ виконує певні захисні дії з безлічі можливих варіантів $Y = \{y_1, ..., y_m\}$, де m — кількість захисних заходів.

Найбільш загальна структура системи виявлення вторгнень, розроблена групою дослідників CIDF (Common Intrusion Detection Framework) [16], яка входить в систему кіберзахисту інформаційної системи критичної інфраструктури, представлена на рис. 2.

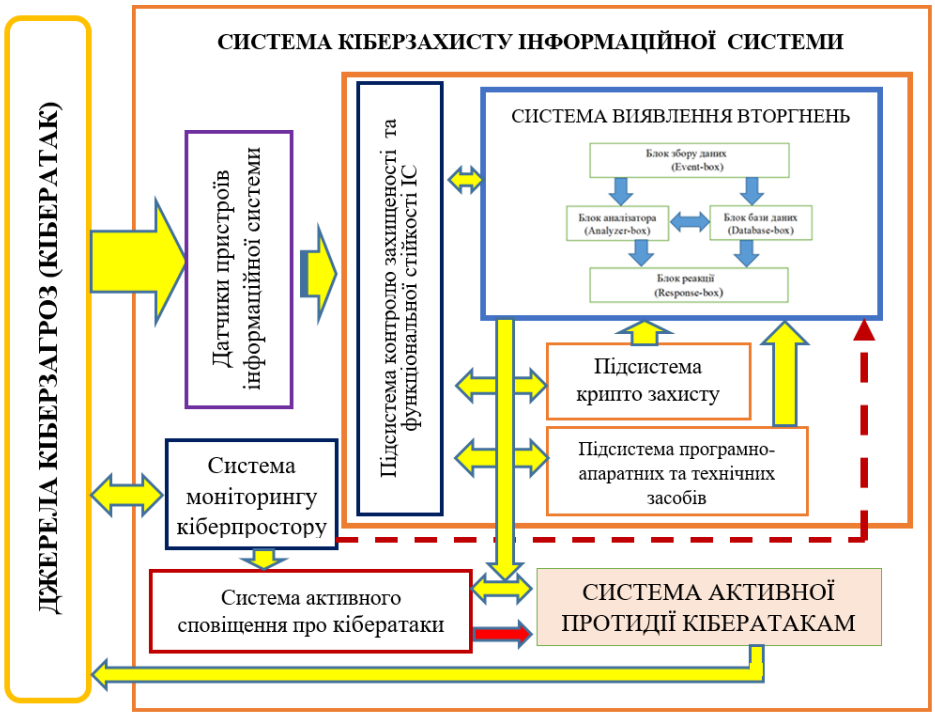

Рис. 2. Загальна структура кіберзахисту інформаційної системи критичної інфраструктури

Розглянемо основні компоненти системи виявлення вторгнень. Блок збору інформації (сенсор, Event–box) відповідає за отримання та первинну обробку даних, необхідних для прийняття рішень аналізатором. Отримані дані можуть містити параметри моніторингу, їх характеристики та значення. Сенсор також виконує перетворення інформації для приведення її до необхідного формату або зменшення обсягу переданої інформації.

Блок аналізу (Analyzer–box) оцінює отримані від сенсорів дані для виявлення можливих кібератак або аномалій. Під час аналізу система здійснює фільтрацію, нормалізацію, трансформацію та кореляцію даних. Якщо виявлено загрозу, система додає відповідний опис до вихідних даних. Аналізатор може мати багаторівневу архітектуру, що підвищує ефективність виявлення загроз.

Блок зберігання даних (Database–box) використовується для накопичення інформації, зокрема набору правил для прийняття рішень, опису кібератак та даних, отриманих від сенсорів. Інформація може зберігатися у вигляді текстових файлів, сигнатур, баз даних тощо.

Блок реагування (Response–box) відповідає за інформування служби безпеки про зафіксовані кібератаки. У випадку інтеграції з системами запобігання вторгнень цей блок забезпечує оперативне реагування на загрози в режимі реального часу.

Однією з найбільш критичних складових системи є підсистема аналізу, яка визначає наявність загроз на основі отриманих даних. Від її ефективності залежить рівень безпеки інформаційної інфраструктури. Оптимізація роботи цього блоку можлива завдяки використанню технологій штучного інтелекту для точнішого аналізу та оцінки загроз.

Застосування методів інтелектуального аналізу даних. Основними цілями методів інтелектуального аналізу даних є пошук функціональних і логічних закономірностей у накопиченій інформації, побудова моделей і правил, що пояснюють знайдені аномалії та/або прогнозують розвиток деяких процесів, а також виявлення прихованих знань у вигляді кореляцій, тенденцій і взаємозв'язків, які аналітик не в змозі виявити й узагальнити самостійно. Методи інтелектуального аналізу даних, на відміну від традиційних методів опрацювання даних, дають змогу більш ефективно виконувати оцінювання стану процесів, що спостерігаються, виявляти та ранжувати причини значущих змін, прогнозувати розвиток процесів і виробляти рекомендації з підготовки можливих варіантів рішень із прогнозом їхніх наслідків [4]. Якщо зробити висновки з аналізу досліджень в області виявлення мережевих атак, заснованих на методах інтелектуального аналізу даних, можна зробити висновок про широкі можливості вказаних методів для вирішення поставлених завдань по виявленню та протидії вторгненням в інформаційну систему (табл. 1).

Таблиця 1

Можливості методів інтелектуального аналізу даних для вирішення поставлених завдань по виявленню вторгнень

Метод інтелектуального аналізу даних	Показник розпізнавання (%)	Помилкові спрацьовування (%)
C4.5	95	1
Метод опорних векторів (SVM)	95,5	1
Багатошаровий персептрон	94,5	1
Машина лінійного програмування	94	1
Метод k–найближчих сусідів	92	1
Упорядкований дискримінантний аналіз	94	1
Дискримінантний аналіз Fisher	89	1

γ–алгоритм	80	1
k–means кластеризація	65	1
Single leakage кластеризація	69	1
Quarter–sphere SVM	65	1
Y–means кластеризація	89,89	1
Генетичне програмування	91	0,43
SVM + Генетичні алгоритми	99	–
SVM + Нечітка логіка	99,56	0,44
Нейронні мережі + МГК	92,22	–
C4.5 + МГК	92,16	–
Генетичні алгоритми	97,47	0,69
C4.5 + Гібридні нейронні мережі	93,28	0,2
Прихована марковська модель	79	–

Використання методів інтелектуального аналізу даних у системах виявлення вторгнень (СВВ) дозволяє інтегрувати професійний досвід спеціалістів у сфері кібербезпеки, ухвалювати рішення в умовах невизначеності та адаптуватися до нових загроз або їхніх модифікацій. Для досягнення цієї мети найчастіше застосовуються такі методи, як експертні системи, нечітка логіка та штучні нейронні мережі [18].

Розглянемо особливості методів інтелектуального аналізу даних для виявлення кібератак. Експертні системи (ЕС) відіграють важливу роль у процесі виявлення кібератак, оскільки дозволяють формалізувати знання фахівців у вигляді певного набору правил, що допомагає ухвалювати рішення в складних ситуаціях. Аналітик або інженер із знань здійснює структурування експертної інформації у вигляді бази знань.

Експертна система, побудована на основі правил, зазвичай складається з кількох основних компонентів: бази знань, яка містить правила та факти, необхідні для аналізу загроз; механізму логічного висновку, що використовує правила для ухвалення рішень; блоку пояснення результатів, який надає обґрунтування отриманих висновків; інтерфейсу користувача, який забезпечує взаємодію з аналітиками та адміністраторами безпеки.

Поєднання методів інтелектуального аналізу дозволяє значно підвищити ефективність виявлення атак, адаптуючи систему до динамічних умов кіберзагроз.

Розв’язання завдань реалізується за допомогою логічних висновків на підставі знань, що зберігаються в базі знань. Знання в ЕС організовані у вигляді системи правил вигляду:

IF (умова) *THEN* (наслідок).

Система логічного висновку здійснює порівняння даних про реальну подію і про еталонну ситуацію, що зберігається в базі знань і описує наявність вторгнень, і в разі збігу цих даних виконуються задані дії. Результати роботи ЕС доступні користувачеві через діалоговий інтерфейс, який дає змогу ознайомитися також із перебігом логічних «міркувань» системи, що призвели до отримання цього результату.

Одним із поширених підходів до виявлення атак є використання експертних систем (ЕС), у яких інформація про кібератаки представлена у вигляді набору правил. Ці правила можуть бути оформлені як певна послідовність дій або сигнатурні ознаки. При виконанні будь-якого з таких правил система приймає рішення про можливу несанкціоновану активність. Основною перевагою цього методу є мінімальна кількість хибних спрацювань.

Експертна система використовує базу даних (БД), яка повинна містити сценарії більшості відомих атак. Щоб залишатися ефективними, такі системи потребують регулярного оновлення, оскільки навіть незначна модифікація вже відомої кібератаки може стати серйозною перешкодою для її виявлення.

Альтернативним методом є застосування нечіткої логіки, яка дозволяє працювати з невизначеністю у процесі логічного висновку. Нечітка логіка є узагальненням класичної логіки та теорії множин. Замість чітких значень «істина» або «хиба» вона оперує функцією належності до нечітких множин, значення якої знаходяться в межах [0; 1]. На основі нечітких множин визначаються відповідні логічні операції, що дозволяють класифікувати аномальні події та співвідносити їх із відомими сценаріями кібератак [19].

Однією з ключових переваг цього підходу є можливість обробки суперечливих даних. У ситуаціях, коли у навчальній вибірці присутні однакові записи з різними мітками, нечітка логіка дозволяє оцінити ймовірність віднесення «сумнівних» мережевих пакетів до аномальних, що значно підвищує точність аналізу.

Нечітка логіка дає змогу описувати правила в незавершеному, «розмитому» режимі на основі знань і ваг подій, що дають змогу припустити ймовірність кібератаки. У результаті можна працювати не з конкретними значеннями параметрів, а з їхніми якісними описами.

Ступінь належності елемента $x \in X$ до нечіткої множини A описується його функцією належності $\mu_A(x): X \to [0,1]$. При цьому можна виділити три випадки:

1) $\mu_A(x) = 1$ означає повну приналежність елемента x до нечіткої множини A, тобто $x \in A$;
2) $0 < \mu_A(x) < 1$ означає відсутність належності елемента x до нечіткої множини A, тобто $x \notin A$;
3) означає часткову приналежність елемента x до нечіткої множини A.

Якщо повна множина X складається зі скінченного числа елементів, тобто $X = \{x_1, x_2 ...., x_n\}$, то нечітку множину A можна подати в такому вигляді:

$$A = \frac{\mu_A(x_1)}{x_1} + \frac{\mu_A(x_2)}{x_2} + ... + \frac{\mu_A(x_n)}{x_n} = \sum_{i=1}^{n} \frac{\mu_A(x_i)}{x_i} \ .$$

Наведений запис має символьний характер. Знак «+» означає $\frac{\mu_A(x_i)}{x_i}$, $i = 1,..., n$ є не додавання, а радше об'єднання. Запис $\frac{\mu_A(x_i)}{x_i}$, $i = 1,..., n$, означає, що $\mu_A(x_i)$ відноситься до елемента x_i, а не означає ділення.

Фактично запис $\frac{\mu_A(x_i)}{x_i}$, $i = 1,..., n$ означає пару $\{x_i, \mu_A(x_i)\}$, $i = 1,..., n$.

Для формалізації неточних тверджень, наприклад, «*x* майже дорівнює *y*» або «*x* значно більше, ніж *y*» застосовують нечіткі відношення. Нечітким відношенням R між двома непорожніми множинами (чіткими) X і Y називається нечітка підмножина прямого декартового добутку $X \times Y$, яка визначається так:

$$R \subseteq X \times Y = \sum_{X \times Y} \frac{\mu_R(x, y)}{x, y} \ .$$

Якщо знання подано за допомогою нечітких множин і нечітких відношень, то для реалізації логічних висновків у нечіткому середовищі необхідно застосовувати сукупність правил. Тому системи нечіткої логіки мають такі основні особливості:

– правила ухвалення рішень є умовними висловлюваннями типу «*IF*...,*THEN*...», що реалізуються за допомогою механізму логічного виведення;

– замість одного чіткого узагальненого правила нечітка логіка оперує з безліччю приватних правил для кожного локального набору даних, для кожної регульованої величини, для кожної мети управління;
– правила типу «*IF*...,*THEN*...» дають змогу розв'язувати задачі вибору рішення ітераційно, у режимі діалогу з користувачем, що сприяє підвищенню ефективності цього процесу.

Процес опрацювання нечітких правил виведення в системі складається з чотирьох етапів:

1) обчислення ступеня істинності лівих частин правил (між «*IF*» і «*THEN*») — визначення ступеня належності вхідних значень нечітким підмножинам, зазначеним у лівій частині правил виведення;
2) модифікація нечітких підмножин, зазначених у правій частині правил виведення (після «*THEN*»), відповідно до значень істинності, отриманих на першому етапі;
3) об'єднання (суперпозиція) модифікованих підмножин;
4) секуляризація результату суперпозиції - перехід від нечітких підмножин до скалярних значень.

До основних переваг нечіткої логіки належать: можливість оперування нечіткими вхідними даними; можливість нечіткої формалізації критеріїв оцінки та порівняння; можливість проведення якісних оцінок як вхідних даних, так і вихідних результатів; можливість проведення швидкого моделювання складних динамічних систем та їх порівняльний аналіз із заданим ступенем точності.

Недоліком нечітких систем є те, що зі збільшенням вхідних змінних складність обчислень збільшується експоненціально, у результаті збільшується база правил, що призводить до важкого її сприйняття.

Якщо структура області рішення заздалегідь невідома, а відомі тільки окремі точки області рішення, то доцільно для інтелектуальної обробки інформації застосувати нейронні мережі. Інтерес до штучних нейронних мереж викликаний тим фактом, що людський мозок виробляє обчислювальні операції принципово іншим чином, ніж звичайна цифрова обчислювальна машина. Нейронні мережі являють безліч інструментів для самих різних застосувань: кластеризація даних, витяг ознак, скорочення розмірності і т.д.

В деяких випадках застосовується модифікована версія навчання з підкріпленням для вивчення нових атак. При зустрічі нової атаки використовується зворотний зв'язок для оновлення сигнатур.

Також використовуються ієрархії нейронних мереж для виявлення аномалій. Нейронні мережі навчаються з використанням даних, які охоплюють нормальний простір і здатні розпізнавати невідомі атаки [18].

У функціональному відношенні елементарною складовою нейронних мереж є штучний нейрон. Його можна уявити або як спеціалізований процесорний елемент, або як нелінійний динамічний інформаційний елемент із пам'яттю. Кожен такий елемент (або вузол) пов'язаний з великою кількістю інших елементів. Особливість цих зв'язків полягає в тому, що на вхід елемента надходить кілька сигналів $U_{in}(i),\ i=1,...,N$, а на його виході формується тільки один U_{out} .

Сигнал U_{out} передається кільком іншим нейронам і так далі. Вхідні сигнали можуть мати синаптичні ваги ω_i , $i=1,...,N$. Математично такий нейропроцесор описується рівнянням

$$U_{out} = f\left[\sum_{i=1}^{N} \omega_i U_{in}(i) - Q\right]$$

де f — деяка функція активації, визначена для кожного типу нейрона; Q — поріг.

Функція активації визначає залежність вихідного сигналу нейрона від вхідних сигналів. Ця залежність може бути виражена за допомогою відомих функцій, наприклад, лінійної, кусковолінійної, сигмоїдальної або гаусової функції.

На практиці найчастіше застосовують сигмоїдальні функції активації. Стандартна сигмоїдальна функція визначається як

$$y(x) = \frac{1}{1 + e^{-\beta x}}$$

де β — параметр нахилу, який завжди позитивний.

Сигмоїдальна функція має властивість посилювати слабкі сигнали і запобігає насиченню від великих сигналів, оскільки вони відповідають тим областям аргументів, де сигмоїд має пологий нахил.

Нейроподібний функціональний елемент (нейропроцесор) є основним процесорним елементом штучної нейронної мережі (ШНМ). Фактично ШНМ являє собою адаптивну систему, життєвий цикл якої складається з двох незалежних фаз: фази навчання мережі та фази роботи мережі. Навчання вважається закінченим, коли мережа правильно виконує перетворення на тестових прикладах і подальше навчання не спричиняє значної зміни вагових коефіцієнтів, які налаштовуються. Далі мережа виконує перетворення раніше невідомих їй даних на основі сформованої нею в процесі навчання нелінійної моделі процесу. Застосування нейронних мереж у СВВ дає змогу максимально використовувати наявну інформацію за обмеженої кількості експериментальних даних [3].

Якщо ШНМ являє собою окрему систему виявлення кібератак, то вона обробляє трафік і аналізує інформацію на наявність у ньому зловживань. Будь-які випадки, які ідентифікуються із вказівкою на кібератаку, перенаправляються адміністратору ІБ або використовуються модулем автоматичного реагування на кібератаки.

Важливою перевагою ШНМ під час виявлення зловживань є їхня здатність «вивчати» характеристики навмисних атак та ідентифікувати елементи, які не схожі на ті, що спостерігалися в мережі раніше. Недоліком нейронних мереж є те, що вона не дає змоги дослідити процес формування класифікаційних висновків про кібератаки, є не цілком «прозоре» представлення знань в інформаційному полі ШНМ і неочевидність процесу формування результатів їхньої роботи.

Порівняльний аналіз підходів до інтелектуального аналізу даних показує, що в кожному з них є як сильні, так і слабкі сторони. Це відображено в табл. 2, де балами позначено: 1 — погано, 2 — задовільно, 3 — добре.

Порівняльна характеристика інтелектуальних методів аналізу вторгнень показана в табл. 2.

Таблиця 2

Порівняльна характеристика інтелектуальних методів аналізу вторгнень

Характеристики	Експертні системи	Нечіткі системи	Нейронні мережі
Представлення знань	2	3	1
Нечіткі виводи	1	3	3
Адаптивність	1	1	3
Здатність навчання	1	1	3
Опис результату	3	3	1
Простота обслуговування	1	2	3

З таблиці видно, що доцільно використовувати гібридні засоби, у яких поєднуються переваги окремих інтелектуальних методів. Порівняння експертних систем, нечітких систем і нейронних мереж дає змогу дійти висновку, що в підсистемі аналізу вторгнень краще поєднувати ШНМ або з експертними системами, або з підходом нечіткої логіки. Тому можна виокремити такі варіанти застосування ШНМ у системах виявлення атак:

– доповнення нейронною мережею наявних експертних систем для зниження числа помилкових спрацьовувань, властивих ЕС;
– нейро-нечіткі методи для виявлення вторгнень.

Нейромережева експертна система багато в чому організована аналогічно ЕС. Однак базу знань нейро-експертної системи організовано у вигляді нейронної мережі, знання в якій подано у формі нечіткого адаптивного розподіленого інформаційного поля. Оскільки ЕС отримує від ШНМ дані тільки про події, які розглядаються як підозрілі, чутливість системи зростає. Якщо навчена ШНМ отримала можливість ідентифікувати нові атаки, то експертну систему також слід оновити. В іншому разі нові атаки будуть ігноруватися ЕС, колишні правила якої не описують цю загрозу.

Використання нейромережевої бази знань дає змогу усунути один з основних недоліків експертних систем, заснованих на правилах: неможливість оперування з не цілком достовірною інформацією.

Більш перспективним підходом для виявлення атак є об’єднання можливостей нейронних мереж і нечіткої логіки [19], оскільки нечіткі ШНМ об’єднують переваги ШНМ і нечіткої логіки, що спирається на досвід експертів в області ІБ. Саме нечітка логіка якнайкраще доповнює нейронні мережі, компенсуючи дві основні «непрозорості» ШНМ: у поданні знань і пояснень результатів роботи інтелектуальної системи. Нечіткі ШНМ дають змогу розв’язувати не тільки окремо взяті завдання ідентифікації загроз, зіставлення поведінки користувачів із наявними в системі шаблонами, а й автоматично формувати нові правила в разі зміни загроз.

Нейро-нечітка система для виявлення вторгнень у мережу. Застосування нечітких нейронних мереж у СВВ забезпечує: функціональну стійкість; можливість класифікації загроз; опис відповідності «загрози — механізми захисту» у вигляді системи нечітких предикатних правил; адаптивність нейро-нечітких систем захисту інформації (системи нечітких правил).

Нехай існує невідома цільова залежність — відображення в $y^*: X \to Y$, значення якої відомі тільки на об’єктах навчальної вибірки $X^r = [(x_1, y_1), ..., (x_r, y_r)]$ розмірністю r. Застосування нейро-нечіткої системи дає змогу апроксимувати невідоме відображення у вигляді алгоритму $a: X \to Y$, здатного ідентифікувати подію ІБ за вектором її ознак і визначити захисні дії. Для цього використовують множину нечітких правил $R = \{R_1, ..., R_k\}$ виду:

$$R_1: \text{ якщо } x_1 \in A_1^1 \text{ і } ... \; x_n \in A_1^n, \text{ то } Y \in y_1,$$

$$R_2: \text{ якщо } x_1 \in A_2^1 \text{ і } ... \; x_n \in A_2^n, \text{ то } Y \in y_2,$$

$$.....$$

$$R_k: \text{ якщо } x_1 \in A_{k_1}^1 \text{ і } ... \; x_n \in A_{k_n}^n, \text{ то } Y \in y_m,$$

де A_1^1 — відповідні нечіткі множини, $k = k_1, ..., k_n$.

Структурна модель СВВ, що включає нейро-нечітку систему для ідентифікації події ІБ, показана на рис. 3.

Нейро-нечітка система являє собою штучну нейронну мережу (рис. 4), яка є адаптивним функціональним еквівалентом нечіткої моделі виведення. Знання кваліфікованих фахівців у галузі ІБ, представлені у формі нечітких змінних і нечітких правил, відображаються у структурі нейро-нечіткої мережі.

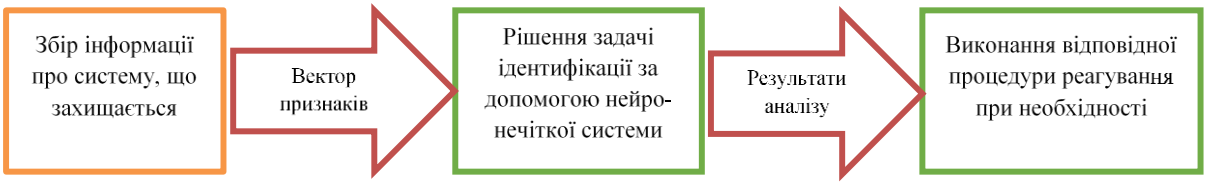

Рис. 3. Структурна модель СВВ, що включає нейро-нечітку систему для ідентифікації події ІБ

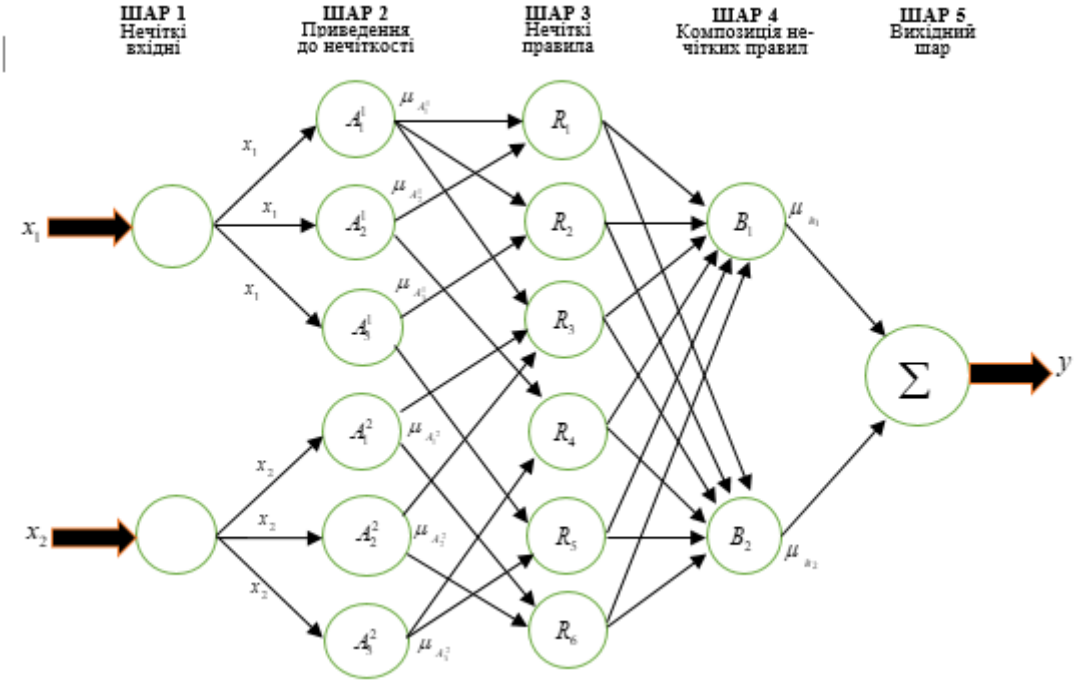

Рис. 4. Нейро-нечітка система являє собою штучну нейронну мережу

Основні етапи нечіткого логічного виведення розподілено за шарами ШНМ і реалізуються, наприклад, для мережі з двома входами x_1, x_2 і одним виходом y так:

– введення нечіткості виконується шаром вхідних функцій належності $\mu_{A_1^1} - \mu_{A_3^1}$, $\mu_{A_1^3} - \mu_{A_3^3}$ які здійснюють перетворення кожного з чітких вхідних значень x_1 і x_2 у ступінь істинності відповідної передумови для кожного правила;

– нечіткому логічному висновку відповідає шар нечітких правил $R_1 - R_6$, який за ступенем істинності передумов $\mu_{A_1^1}, \mu_{A_3^3}$, $i = 1,2,3$ формує висновки за кожним із правил;

– композиція висновків нечітких правил $R_1 - R_6$ проводиться шаром вихідних функцій приналежності μ_{B_1}, μ_{B_3} (output membership functions) з метою формування нечітких підмножин B_1, B_2;
– композиція нечітких підмножин B_1, B_2 і приведення до чіткості виконується у вихідному шарі та призводить до формування вихідного чіткого значення y.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Оскільки в архітектурі нейро-нечіткої системи використовуються нечіткі правила, що ґрунтуються на знанні експертів у сфері захисту інформації, то для навчання доцільно обрати метод навчання з учителем, наприклад, метод мінімізації середньоквадратичної помилки. Його переваги полягають у можливості широкого використання та математичній простоті. Як функції активації нейронів краще вибрати сигмоїдальні, а як функції належності можна вибрати, наприклад, Z-подібні та S-подібні функції.

Навчання нечіткої ШНМ дає змогу не тільки налаштувати ваги зв'язків (тобто відкоригувати достовірність окремих нечітких правил), а й усунути суперечливість системи нечітких правил загалом. У разі відсутності апріорної інформації з цієї предметної області, але за достатнього обсягу навчальної вибірки нейро-нечітка мережа автоматично перетворює приховані в даних навчальної вибірки закономірності на систему правил нечіткого логічного висновку.

Отже, застосування нейро-нечіткої системи є найкращим варіантом побудови одного з модулів СВВ, який проводитиме аналіз даних, отриманих від підсистеми збирання інформації, і повідомлятиме про виявлення несанкціонованих дій, підтверджуючи факт наявності вторгнення або атаки.

Таким чином в роботі виконано аналіз наявних підходів для вирішення завдання виявлення вторгнень у інформаційну мережу. Показано, що перспективним напрямком під час розроблення засобів виявлення атак є використання методів інтелектуального аналізу даних. Оскільки системи нечіткої логіки компенсують основні «непрозорості» ШНМ у поданні знань і поясненні результатів роботи інтелектуальної системи, то для побудови модуля аналізу інформації в СВВ запропоновано нейро-нечітку систему. Також, включення нечіткої логіки до складу нейромережевих засобів виявлення атак на інформаційну мережу дає змогу враховувати апріорний досвід експертів ІБ, реалізувати притаманне нейронним мережам нечітке представлення інформації, витягати знання із вхідних неповних і не цілком достовірних даних. Перспективними напрямками подальших досліджень є більш глибокий аналіз методів інтелектуального аналізу даних і створення на їх основі гібридних методів виявлення вторгнень в інформаційні системи та мережі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. On Approval of the General Requirements for the Cyber Defense of Critical Infrastructure, Resolution of the Cabinet of Ministers of Ukraine № 518 (2022) (Ukraine). https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text.
2. Yevseev, S. P., Zakovorotnyi, O. Y., Milov, O. V., Kuchuk, G. A., Galuza, O. A., Koval, M. V., Voitko, O. V., & Hryshchuk, R. V. (2024). *Methodology for synthesizing models of intelligent control and security systems for critical infrastructure facilities: monograph.* Kharkiv: Novyi Svit-2000 Publishing House.

3. Lukova-Chuyko, N. V, Toliupa, S. V., Nakonechnyi, V. S., & Brailovsky, M. M. (2021). *Intrusion Detection Systems and Functional Resilience of Distributed Information Systems to Cyber Threats: monograph.* K.: Format.
4. Lande, D. V., Subach, I. Y., & Boyarynova, Y. E. (2018). *Fundamentals of the theory and practice of data mining in the field of cybersecurity: a textbook*. K.: ISZZI KPI.
5. Brailovskyi, M. M., Zybin, S. V., Kobozeva, A. A., Khoroshko, V. O., & Khokhlachova, Y. E. (2021). *Analysis of cybersecurity of information systems: monograph.* K.: FOP Yamchynskyi O.V.
6. Abdalla, A., Aleshyn, G. V., Vdovychenko, I. N., et al. (2020). *Cybersecurity and Information Technology: a monograph.* Kh.: DISA PLUS LLC.
7. Toliupa, S. V., & Nakonechnyi, V. S. (2020). Problems of protection of critical infrastructure objects. *Security of Information Systems and Technologies, 1(2),* 57–65. https://doi.org/10.17721/10.17721/ISTS.2020.1.31-39
8. Toliupa, S., Lukova-Chuyko, N., Parkhomenko, I. (2021). Intrusion Detection Methods in Modern IDS Systems. *Security of information systems and technologies, 1(5),* 19–26. https://doi.org/10.17721/ISTS.2021.1.17-24
9. *Official website of the United States Computer Emergency Readiness Team*. (n. d.). http://www.us-cert.gov
10. *Official website of X-Force.* (n. d.). http://xforce.iss.net
11. *Official website of Secunia.* (n. d.). http://secunia.com
12. *Official website of BugTraq.* (n. d.). http://securityfocus.com
13. *Official website of the Open Source Vulnerabilities Data Base.* (n. d.). http://osvdb.org
14. *Official website of The MITRE Corporation.* (n. d.). http://attack.mitre.org
15. *Official website of KDD Cup 1999 Data.* (n. d.). http://kdd.ics.uci.edu/databases/kddcup99/kddcup99
16. Dovbeshko, S. V., Toliupa, S. V., & Shestak, Y. V. (2019). Application of data mining methods for building attack detection systems. *Modern Information Protection, 1,* 6–15.
17. Toliupa, S., Pliushch, O., & Parkhomenko, I. (2020). Construction of attack detection systems in information networks on neural network structures. *Electronic professional scientific publication "Cybersecurity: Education, Science, Technology". 2(10),* 169–183. https://doi.org/10.28925/2663-4023.2020.10.169183.
18. Subach, I. Y., Kubrak, V. O., Mykytiuk, A. V., Korotaiev, S. O. (2020). Zero-day polymorphic cyberattacks detection using fuzzy inference system. *Austrian Journal of Technical and Natural Sciences, 5–6,* 8–13.
19. Hulak, H. M., Zhiltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2024). *Information and cyber security of the enterprise. Textbook.* Lviv: Publisher Marchenko T. V.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (27), 2025
ISSN 2663 - 4023

Serhii Toliupa
Doctor of Technical Sciences, Professor
Professor of the Department of Cybersecurity and Information Protection
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
ORCID ID: 0000-0002-1919-9174
serhii.toliupa@knu.ua

Andrii Kulko
Postgraduate Student of the Department of Cybersecurity and Information Protection
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
ORCID ID: 0009-0006-1185-0774
kulko452@gmail.com

NEURO-FUZZY SYSTEM FOR DETECTING INTRUSIONS INTO THE INFORMATION NETWORK OF CRITICAL INFRASTRUCTURE

Abstract. In the situation of Russia's military aggression against Ukraine, the safety of people and the country largely depends on the reliability of critical infrastructure. In addition to physical attacks with weapons, Russia uses cyber weapons to attack the management systems of these facilities through cyberspace. Particularly alarming is the tendency for such facilities, which use modern technologies and operate in a single information environment, to remain vulnerable to new types of cyber threats, even with great efforts to protect them. This significantly complicates the task of ensuring long-term sustainability and security. Protecting information systems at such facilities is critical for the stable development of modern society. This article considers the task of detecting intrusions into critical infrastructure information networks. The main components of an intrusion detection system are identified and their functions are described. The article analyzes various approaches to detecting information security violations. The main methods of intrusion detection are characterized, their advantages and disadvantages are highlighted. It is shown that in order to increase the efficiency of detecting situations related to possible intrusion, it is necessary to use modern technologies of data mining. The features of technologies for use in intrusion detection systems were investigated, and based on the results of their comparative analysis, hybrid tools for detecting attacks were proposed. It is shown that the most promising for the task under consideration is the use of neuro-fuzzy methods. The architecture of a neuro-fuzzy system for detecting intrusions into the information network of critical infrastructure is proposed.

Keywords: information security; intrusion; information network; data mining; neuro-fuzzy system; neural network; cyberattack; critical infrastructure; artificial neural network.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. On Approval of the General Requirements for the Cyber Defense of Critical Infrastructure, Resolution of the Cabinet of Ministers of Ukraine № 518 (2022) (Ukraine). https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text.
2. Yevseev, S. P., Zakovorotnyi, O. Y., Milov, O. V., Kuchuk, G. A., Galuza, O. A., Koval, M. V., Voitko, O. V., & Hryshchuk, R. V. (2024). *Methodology for synthesizing models of intelligent control and security systems for critical infrastructure facilities: monograph.* Kharkiv: Novyi Svit-2000 Publishing House.
3. Lukova-Chuyko, N. V, Toliupa, S. V., Nakonechnyi, V. S., & Brailovsky, M. M. (2021). *Intrusion Detection Systems and Functional Resilience of Distributed Information Systems to Cyber Threats: monograph.* K.: Format.
4. Lande, D. V., Subach, I. Y., & Boyarynova, Y. E. (2018). *Fundamentals of the theory and practice of data mining in the field of cybersecurity: a textbook.* K.: ISZZI KPI.
5. Brailovskyi, M. M., Zybin, S. V., Kobozeva, A. A., Khoroshko, V. O., & Khokhlachova, Y. E. (2021). *Analysis of cybersecurity of information systems: monograph.* K.: FOP Yamchynskyi O.V.
6. Abdalla, A., Aleshyn, G. V., Vdovychenko, I. N., et al. (2020). *Cybersecurity and Information Technology: a monograph.* Kh.: DISA PLUS LLC.

7. Toliupa, S. V., & Nakonechnyi, V. S. (2020). Problems of protection of critical infrastructure objects. *Security of Information Systems and Technologies, 1(2),* 57–65. https://doi.org/10.17721/10.17721/ISTS.2020.1.31-39
8. Toliupa, S., Lukova-Chuyko, N., Parkhomenko, I. (2021). Intrusion Detection Methods in Modern IDS Systems. *Security of information systems and technologies, 1(5),* 19–26. https://doi.org/10.17721/ISTS.2021.1.17-24
9. *Official website of the United States Computer Emergency Readiness Team*. (n. d.). http://www.us-cert.gov
10. *Official website of X-Force.* (n. d.). http://xforce.iss.net
11. *Official website of Secunia.* (n. d.). http://secunia.com
12. *Official website of BugTraq.* (n. d.). http://securityfocus.com
13. *Official website of the Open Source Vulnerabilities Data Base.* (n. d.). http://osvdb.org
14. *Official website of The MITRE Corporation.* (n. d.). http://attack.mitre.org
15. *Official website of KDD Cup 1999 Data.* (n. d.). http://kdd.ics.uci.edu/databases/kddcup99/kddcup99
16. Dovbeshko, S. V., Toliupa, S. V., & Shestak, Y. V. (2019). Application of data mining methods for building attack detection systems. *Modern Information Protection*, *1*, 6–15.
17. Toliupa, S., Pliushch, O., & Parkhomenko, I. (2020). Construction of attack detection systems in information networks on neural network structures. *Electronic professional scientific publication "Cybersecurity: Education, Science, Technology". 2(10),* 169–183. https://doi.org/10.28925/2663-4023.2020.10.169183.
18. Subach, I. Y., Kubrak, V. O., Mykytiuk, A. V., Korotaiev, S. O. (2020). Zero-day polymorphic cyberattacks detection using fuzzy inference system. *Austrian Journal of Technical and Natural Sciences, 5–6,* 8–13.
19. Hulak, H. M., Zhiltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2024). *Information and cyber security of the enterprise. Textbook.* Lviv: Publisher Marchenko T. V.