DOI: https://doi.org/10.33216/2222-3428-2023-25-3
УДК 004.023

**Рязанцев О.І., Кардашук В.С., Сафонова С.О. Кравцов С.В.**

# ЗАСТОСУВАННЯ НЕЙРОННОЇ МЕРЕЖІ ДЛЯ ЗАХИСТУ WEB-ДОДАТКІВ

*У статті розглянуті сучасні проблеми захисту інформації та рекомендації щодо особливостей функціонування Web-додатків у безпечному середовищі. Найбільш важливим рівнем щодо захисту інформації є програмно-технічні засоби, що містять у собі цілий комплекс апаратних, програмних і апаратно-програмних засобів захисту інформації. Розробники сучасних брандмауерів пропонують рішення, які працюють на всіх рівнях моделі OSI. Однак робота більшості "класичних" брандмауерів акцентується на мережевому й сеансовому рівнях. Нерідко функціональні можливості роботи брандмауера на рівні додатків забезпечуються окремим модулем, робота якого, як правило, носить загальний характер і не враховує особливостей функціонування додатків. Для реалізації дослідження відбиття атака на WEB-додатки проаналізована та досліджена нейронна мережа адаптивної-резонансної теорії (АРТ), що порівнює вхідне зображення до одного зі сформованих класів у процесі навчання, якщо воно відповідає заданому критерію подібності й у достатньому ступені подібно із прототипом цього класу. В процесі співставлення відбувається модифікація вхідного зображення для більшої відповідності із пропонованим зображенням – корегуються ваги зв'язків. Якщо вхідне зображення в недостатньому ступені подібно із пропонованим зображенням, у цьому випадку виділяється додатковий нейрон і формується новий клас зображень. Виділення додаткового нейрона під новий клас зображень відбувається завдяки наявності вільних, незадіяних нейронів у шарі, що розпізнає. Дана* операція *запобігає дублюванню існуючих зображення, що вже знаходяться у пам'яті.* З*апропонована модифікована структура мережі та рішення щодо усунення недоліків роботи нейронної мережі. В результаті дослідження намічені подальші шляхи удосконалення алгоритму навчання нейронної мережі, що направлені на збільшення кількості операцій відбиття атак на WEB-додатки за допомогою евристичного методу.*
***Ключові слова:*** *WEB-додаток, нейронна мережа, відбиття атак, система виявлення вторгнень.*

**Актуальність дослідження**. Розвиток сучасних інформаційних технологій характеризується ростом числа комп'ютерних злочинів і пов'язаних з ними розкрадань інформації [1].

Сьогодні неможливо назвати точну цифру сумарних втрат від комп'ютерних злочинів, пов'язаних з доступом до особистої інформації. Це пояснюється, насамперед, небажанням постраждалих компаній інформувати відповідні структури про свої втрати [2], а також тим, що не завжди втрати від розкрадання інформації можна точно оцінити в грошовому еквіваленті.

Найбільш істотними причинами активізації комп'ютерних злочинів і пов'язаних з ними фінансових втрат є перехід на електронний документообіг; наявність «шпаринок» у технологіях захисту інформації; об'єднання комп'ютерних систем; створення глобальних мереж і розширення доступу до інформаційних ресурсів; збільшення складності програмних засобів і пов'язане з цим зменшення їхньої надійності й збільшення комп'ютерних загроз.

**Постановка проблеми.** Надійність будь-якої системи захисту визначається самою слабкою ланкою.. Сьогодні на ринку технологій захисту комп'ютерної інформації існує велике різноманіття як програмних реалізацій систем захисту, так і концептуальних ідей побудови таких систем. Деякі з них пройшли перевірку часом, а деякі навпаки не витримали цієї перевірки. Політика безпеки визначається як сукупність документованих управлінських рішень, спрямованих на захист інформації й асоційованих з нею ресурсів. Надійність захисту інформації, насамперед, буде визначатися повнотою рішення цілого комплексу завдань щодо посилення кожної ланки комп'ютерної системи.

**Метою статті** є розроблення та дослідження евристичної системи захисту WEB-додатків [3], що має істотні переваги порівняно з існуючими на сьогоднішній день методами детектування і відбиття атак.

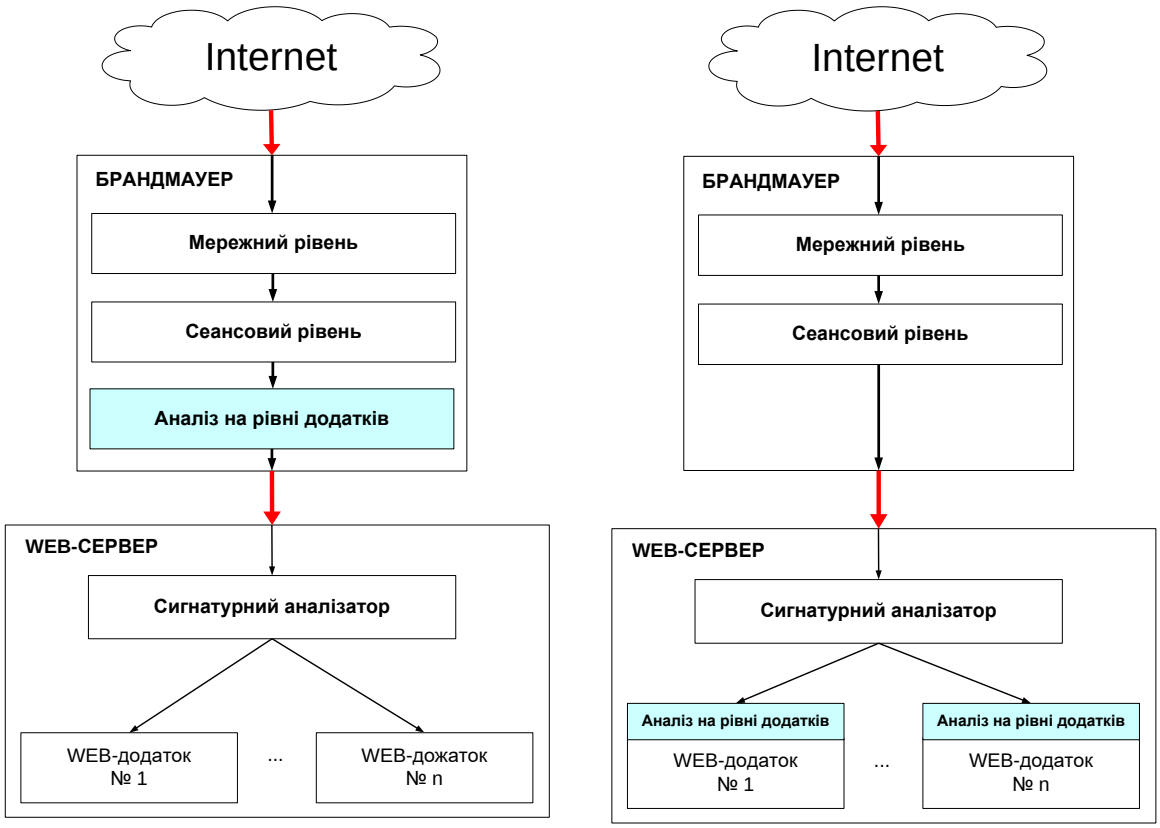
**Аналіз останніх досліджень і публікацій** показав, що боротися з загрозами, властиві мережному середовищу, засобами універсальних операційних систем не представляється можливим. Універсальна операційна система – це велика програма, що, очевидно, крім явних помилок, містить деякі особливості, які можуть бути використані для одержання нелегальних привілеїв доступу. Сучасна технологія програмування не дозволяє робити без помилок об'ємне програмне забезпечення. Крім того, адміністратор, що має справу зі складною системою, далеко не завжди може врахувати всі наслідки зроблених ним змін. Нарешті, в універсальній системі з багатьма користувачами, потенційно небезпечні ситуації постійно створюються самими користувачами (слабкі й/або тривалі паролі, невдало встановлені права доступу, залишений без догляду термінал тощо).

Існує єдиний перспективний шлях пов'язаний з розробкою спеціалізованих методів, які в силу своєї простоти допускають формальну або неформальну верифікацію. Брандмауер і є таким засобом, що допускає подальшу декомпозицію, пов'язану з обслуговуванням мережевих протоколів.

**Вирішення проблеми.** Системи виявлення вторгнень (СЗВ) [4], як вже було відзначено вище, не в змозі створити безпечне середовище роботи WEB-додатку. СЗВ мають великий потенціал, однак точність і ефективність їх роботи на сучасному етапі розвитку технологій інформаційної безпеки викликає безліч дорікань, а значить ці додатки вимагають подальшої вдосконалення й потребують внесення корінних змін.

Удосконалення СЗВ може бути здійснено у напрямку вдосконалення сигнатурного аналізатора та вдосконалення аналізатора аномалій (евристичний аналіз). Метод сигнатурного аналізу добре реалізований та випробуваний на антивірусному програмному забезпеченні й зараз активно впроваджується у СЗВ, де показує відмінні результати по відбиттю відомих атак. Метод аналізу аномалій поведінки користувача WEB-додатка заслуговує більше пильного вивчення. За результатами досліджень визначено, що виявити атаки на WEB-додатки можна тільки на сьомому рівні моделі OSI (рівень додатків).

На рис. 1а зображена схема захисту WEB-додатку у рамках брандмауера.




а) б)

Рисунок 1 – Схеми системи захисту WEB-додатку а) класична; б) що пропонується

Однак брандмауер не враховує й не може враховувати всіх особливостей функціонування WEB-додатка, який він захищає, і, як наслідок, дуже часто не може відрізнити дії зловмисного користувача від дій легітимного користувача [5].

З такої ситуації можливі два виходи: "навчити" брандмауер всім особливостям поведінки користувачів кожного WEB-додатку, що знаходиться на захищеному WEB-сервері, або ж винести контроль на рівні додатків з рамок брандмауера в рамки самого WEB-додатку (рис. 1б). Другий варіант представляється найбільш логічним і зручним. Для потенційного атакуючого відкриваються можливості аналізу в рамки самого WEB-додатку.

У запропонованій схемі (див. рис. 1б) аналіз на рівні додатків здійснюється сигнатурним аналізатором. Система "давачів" збирає інформацію в декількох розрізах: POST-параметри, GET-параметри, COOKIE-параметри, операції з базою даних, операції з файловою системою, помилки й попередження в процесі роботи користувача тощо. Інформація від "давачів" й деяка інша додаткова інформація про користувача (така як IP адреса, час початку сесії та ін.) є вхідною для евристичного аналізатора.

Ядром евристичного аналізатора є мережа адаптивної-резонансної теорії (АРТ) [6]. Для розв'язуваного класу завдань, як вже було зазначено вище, найбільше всього підходить мережа АРТ-1. Нейронна мережа виявляє атаки, які не зміг виявити сигнатурний аналіз.

Потрібно особливо відзначити, що немає необхідності навчати нейронну мережу всім відомим на сьогоднішній день видам атак. "Знати" існуючі атаки повинен сигнатурний аналізатор (перша ланка оборони), а евристичний аналізатор повинен "вміти відрізняти" поведінку легітимного користувача від поведінки зловмисного користувача (друга ланка оборони). Іншими словами, сигнатурний аналізатор повинен "вміти бачити" аномалії поведінки, щоб завчасно послати сигнал реагування.

Однак дуже важливо, щоб евристичний аналізатор не був занадто "жорстким" у визначенні відхилення поведінки користувача від нормального шаблону й у той же час він не повинен бути занадто "м'яким". Цю проблему можна вирішити двома способами: підбором оптимального коефіцієнта подоби; використання різних коефіцієнтів подоби для різних категорій користувачів.

Перший варіант недостатньо гнучкий для нашого завдання. У деяких системах підібрати єдиний коефіцієнт подоби може бути просто неможливо, тому звернемося до другого варіанта.

Виділимо чотири базові категорії користувачів WEB-додатка з погляду безпеки.

До першої категорії віднесемо так званих перевірених користувачів. Це користувачі яких адміністратор власноруч прописав у списки довірі. Цим користувачам дозволені будь-які дії без перевірки евристичним аналізатором. До цієї категорії рекомендовано включати суворо обмежене коло осіб. Частіше всього статус перевіреного користувача має адміністратор та один або декілька операторів системи.

До другої категорії віднесемо користувачів, дії яких не викликають підозри (яких, звісно, більшість). Таких користувачів евристичний аналізатор перевіряє у звичайному режимі, коли коефіцієнт подоби встановлено на середньому рівні.

До третьої категорії віднесемо "підозрілих" користувачів. Це такі користувачі, за якими була помічена деяка підозріла активність у попередні періоди часу (не обов'язково в межах поточної сесії), однак зібраних даних недостатньо, щоб визначити користувача як зловмисника. К цієї категорії користувач може попасти як в категорію користувачів, дії яких не викликають підозри, так і в категорію зловмисників.

До четвертої категорії віднесемо користувачів, яких було класифіковано як зловмисників. Для таких користувачів доступ до системи блокується повністю. Вилучити ідентифікатор користувача з цієї категорій (тим самим розблокувавши доступ до системи) може тільки адміністратор через панель адміністрування.

Для реалізації поставлених перед ним завдань евристичний аналізатор повинен складатися з декількох нейронних мереж АРТ-1. Кількість нейронних мереж повинна дорівнювати кількості WEB-додатків і ще однієї нейронної мережі, що відповідає за віднесення користувача до тієї або іншої категорії. Перед тим як WEB-додаток буде відкрито для доступу з Internet, адміністратор проводить навчання нейронних мереж, що захищають сторінки (кожна мережа свою сторінку). Адміністратор активізує режим навчання й починає роботу з додатком, намагаючись ініціювати "крайні ситуації", тобто такі ситуації, коли значення параметра (наприклад, розмір переданого файлу, кількість GET параметрів в одному запиті та ін.) досягають спочатку дозволеного мінімуму, а потім дозволеного максимуму. Такий режим роботи з додатком навчає нейронну мережу поняттю "нормальної поведінки" користувача. Поняття "нормальної поведінки" для різних сторінок сайту може сильно відрізнятися, тому для кожної сторінки сайту, що захищається, передбачена своя окрема нейронна мережа.

Нейронна мережа, яка пройшла навчання, може виявляти аномалії поведінки користувачів і відносити останніх до однієї із трьох категорій: "звичайні" користувачі (відповідності серед збережених раніше векторів не знайдено), "підозрілі" користувачі (знайдено відповідність вектору в рамках коефіцієнту подоби) або зловмисники (знайдено точну відповідність до вектору, що було раніше запам'ятовано). Після закінчення навчання адміністратор переводить мережу в робочий режим і відкриває доступ до WEB-додатку з Internet.

Система "давачів" збирає й віддає у вигляді двійкового вектору на вхід нейронної мережі деяку інформацію:

- кількість і сумарний обсяг GET-параметрів, що передаються у вигляді URL;
- кількість і сумарний обсяг POST-параметрів, що передаються у тілі HTTP пакету;
- кількість і сумарний обсяг COOKIE-параметрів, що збережені під час сеансу в сесії;
- MIME типи переданих файлів, якщо такі було передано;
- номер відповіді із заголовка HTTP, яка показує чи вірно був сформований запит до сторінки сайту;
- імена таблиць при генерації сторінки;
- дії проведені з таблицями в базі даних (вибірка, вставлення, оновлення, видалення, об'єднання та ін.);
- номери помилок, які виникли при роботі скриптів, або нуль, якщо таких не виникло.

Нейронна мережа порівнює наданий на вхід вектор з векторами, що були збережені в процесі навчання, і робить висновок чи нормальна поведінка користувача, що призвела до створення такого вектору, чи ні. Якщо мережа не може точно визначити, що відбувається атака, однак ступінь відхилення від моделі нормальної поведінки досить велика, то дані про потенційного зловмисника запам'ятовуються окремою мережею, яка відповідає за віднесення користувачів до тієї або іншої категорії. Наступного разу, коли користувач повернеться на сайт і буде проводити деякі дії, що викликають підозру, нейронна мережа класифікує його як "підозрілого" користувача й посилить "жорсткість" евристичного аналізу шляхом корекції коефіцієнта подоби. Якщо підозри підтвердяться, то користувач буде переведений у категорію зловмисників, і тоді всі його наступні дії будуть заблоковані.

Незважаючи на те, що нейронна мережа, яка реалізує віднесення користувача до тієї або іншої категорії, і нейронна мережа, що відповідає за захист конкретної сторінки сайту, мають різні функціональні призначення, робота їх заснована на одному й тому ж принципі. Відмінність цих мереж складається лише в тих даних, які вони

запам'ятовують. Перша мережа запам'ятовує дані про підозрілого користувача (IP адреса, країна, найменування й версія браузера, найменування й версія операційної системи, мова системи, чи є підтримка Flash, чи є підтримка Java, кількість точок на екрані, глибина кольорів, стартова сторінка браузера тощо), а друга – дані про нормальну поведінку користувачів системи. Аналізуючи вихід першої нейронної мережі, ми робимо висновок про необхідність підвищення коефіцієнта подоби при перевірці за допомогою другої нейронної мережі. Аналізуючи вихід другої нейронної мережі, ми робимо висновок про те нормальна поведінка користувача, або ж вона відхиляється від шаблона нормальної поведінки.

Нейроні мережі, що захищають сторінки WEB-додатку, і нейронна мережа, що відповідає за класифікацію користувачів, працюють на одному й тому ж самому принципу.

Показано, що ця нейронна мережа здатна розпізнати зловмисника, який раніше проявляв активність, навіть якщо він вжив заходів, що ускладнюють його ідентифікацію евристичною системою.

У реальній нейронній мережі вхідний вектор, який відповідає за ідентифікацію користувача, досить великий, тому в дослідженнях обмежились вектором довжиною в п'ять бітів.

Перші два біти нашого вектору визначають найменування клієнту користувача (00 – Internet Explorer, 01 – FireFox, 10 – Opera, 11 – інший), третій біт визначає чи встановлений на комп'ютері Flash програвач (0 – не встановлений, 1 – встановлений), четвертий біт визначає мова системи(0 – українська, 1 – інша) і нарешті останній біт визначає тип операційної системи (0 – UNIX подібна, 1 ОС сімейства Windows).

Припустимо, що в нас є дані про трьох користувачів, до яких необхідно застосувати більше "жорсткий" евристичний аналіз: X1 = (00001)T, X2 = (00110)T, X3 = (01111)T. Також у нас є дані про користувача X3, що з метою маскування змінив свій браузер з FireFox на якийсь інший браузер і намагається провести деякі несанкціоновані дії. Вхідний вектор для цього користувача буде мати вигляд X = (11111)T.

На рис. 2 зображена спрощена схема мережі АРТ-1.

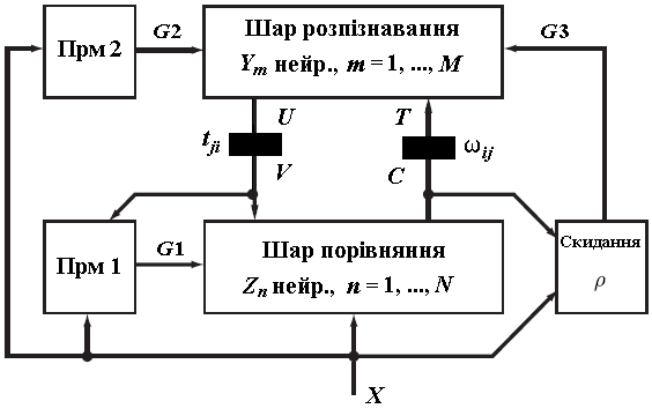



Рисунок 2 – Спрощена схема нейронної мережі АРТ-1

Вхідний вектор мережі X = (X1, ..., Xn, ..., XN) має N компонент. У шарі розпізнавання запам'ятовується M класів образів, по одному класу на кожний нейрон m = 1, ..., M. Основну роботу із класифікації робить шар порівняння й шар розпізнавання. Схеми приймачів (Прм 1, Прм 2) і схема скидання управляють режимом роботи мережі й генерують керуючі сигнали G1, G2 і сигнал скидання G3 відповідно. Матриця безперервних ваг і матриця двійкових ваг на рис. 2 позначені $\omega_{ij}$ й $t_{ji}$ відповідно.

Вхідний двійковий вектор X, при проходженні через мережу, проходить такі перетворення: X → C → T → U → V. Тут C – вихідний вектор шару порівняння, T – вхідний вектор шару розпізнавання, U – вихідний сигнал шару розпізнавання, V – вхідний вектор для шару розпізнавання й сигнал заборони для Прм 1.

Параметр подоби візьмемо ρ = 0,6. Матриці $\omega_{ij}$ й $t_{ji}$ ініціалізуються початковими значеннями згідно:

$$0 < \omega_{ij} < \frac{\lambda}{\lambda - 1 + N}; \qquad \frac{\beta - 1}{d} < t_{ji} \le 1,$$

де $\lambda \in (1, 2)$; β – константа; $d > 0$.

Розмірність вектору N = 5, параметр λ = 1,5. Одержимо матриці ваг:

$$\omega_{ij} = 0{,}2;\ t_{ji} = 1; \quad i = \overline{1,5};\ j = \overline{1,4}.$$

Проведемо навчання мережі першим трьом векторам. При надходженні на шар порівняння вектору X1 на виході шару порівняння одержуємо вектор C1 = X1. На всіх входах шару розпізнавання маємо сигнал:

$$T_m = \sum_{i=1}^{5} \omega_{1i} C_i = 0{,}2 \cdot 0 + 0{,}2 \cdot 0 + 0{,}2 \cdot 0 + 0{,}2 \cdot 0 + 0{,}2 \cdot 1 = 0{,}2,\ m = \overline{1,M}.$$

Нейроном-переможцем стає нейрон з найменшим індексом, тобто нейрон Y1. Ваги зв'язків приймають значення: (0, 0, 0, 0, 1). t1n ($n = \overline{1, N}$)

Обчислимо параметр подоби для вектору X1:

$$S = \frac{1\cdot 0+1\cdot 0+1\cdot 0+1\cdot 0+1\cdot 1}{0+0+0+0+1} = 1.$$

При S > ρ , то поданий на вхід вектор X1 створить перший збережений у пам'яті образ. Відповідно буде відкоректована матриця $\omega_{ij}$:

$$\omega_{1i} = \frac{1{,}5\cdot 0}{0{,}5+0+0+0+0+1} = 0, \qquad \omega_{15} = \frac{1{,}5\cdot 1}{0{,}5+0+0+0+0+1} = 1.$$

Далі на вхід будуть подані вектори X2 і X3, які також будуть збережені мережею.

В результаті навчання матриці $\omega_{ij}$ й $t_{ji}$ будуть мати вигляд:

$$\omega_{ij} = \begin{vmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0{,}6 & 0{,}6 & 0 \\ 0 & 0{,}33 & 0{,}33 & 0{,}33 & 0{,}33 \\ 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 & 0{,}2 \end{vmatrix}; \qquad t_{ji} = \begin{vmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{vmatrix}.$$

Атакуючий вектор X4 = (11111)T, змінивши свій браузер, намагається залишитися непоміченим мережею. У цьому випадку T1 = 1; T2 = 1,2; T3 = 1,32. Вибираємо нейрон Y3 з максимальним значенням T. Розрахуємо для нього S = 0,8 > ρ. У такий спосіб вектор X4 був правильно віднесений до третього класу, тобто зробивший спробу залишитися непоміченим атакуючий, все ж таки, був правильно класифікований.

Нейронні мережі, які захищають окремі WEB сторінки сайту, працюють по тому ж принципу, але результат їхньої роботи інтерпретується з точністю до навпаки: якщо була знайдена відповідність вхідного вектору в пам'яті мережі, то це нормальна ситуація, а якщо відповідності не було знайдено, то, можливо, ми маємо справу з атакою й необхідно більш пильно стежити за поточним користувачем.

**Результати досліджень**. Нейронні мережі, які захищають окремі WEB сторінки сайту, працюють по аналогічному принципу, але результат їхньої роботи інтерпретується з точністю до навпаки: якщо була знайдена відповідність вхідного вектору в пам'яті мережі, то це нормальна ситуація, а якщо відповідності не було знайдено, то, можливо, ми маємо справу з атакою й необхідно більш пильно стежити за поточним користувачем.

**Висновки.** Розроблений метод може застосовуватися як в якості додаткової ланки оборони у вже існуючих системах запобігання вторгнень [7], так і в якості самостійної системи виявлення та відбиття атак; дає можливість відслідковувати дії користувача, що неодноразово робить спроби проникнення.

Евристична система відповідно до концепції ешелонованої оборони [8] утворює третю ланку захисту. Данні потрапляють на вхід нейронних мереж евристичного аналізатора після фільтрації брандмауером та сигнатурним аналізатором (який може входити як в брандмауер так і у склад WEB-серверу).

Таким чином, евристична система виявлення і відбиття атак компенсує недоліки [9] притаманні сигнатурним методам аналізу: неможливість виявлення модифікованих та нових типів атак, особливості побудови WEB-додатку, що захищається.

**Література**


1. Карчевський М.В. Злочини в сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (тези лекцій) / М.В. Карчевський // Злочини в сфері використання ІТ [Електронний ресурс]. – Режим доступу: http://it-crime.at.ua/index/tezi_lekcij/0-31 (дата звернення 17.09.2023).
2. Дмитро Нікулеску. Кібербезпека: вразливі моменти. [Електронний ресурс]. – Режим доступу: https://yur-gazeta.com/publications/practice/inshe/kiberbezpeka-vrazlivi-momenti.html (дата звернення 23.09.2023).
3. Захист WEB-додатків. Чому це актуально? [Електронний ресурс]. – Режим доступу: https://octavacapital.ua/zahyst-web-dodatkiv-chomu-ce-aktualno/ (дата звернення 24.09.2023).
4. В. І. Мєшков, В. О. Віролайнен. Аналіз сучасних систем виявлення та запобігання вторгнень в інформаційно-телекомунікаційних системах. Державний ВНЗ «Національний гірничий університет», м. Дніпропетровськ. [Електронний ресурс]. – Режим доступу: https://ela.kpi.ua/bitstream/123456789/17609/1/meshkov.pdf (дата звернення 28.09.2023).
5. Что такое Брандмауэр, зачем нужна защита компьютера и как ее настроить. [Електронний ресурс]. – Режим доступу: https://club.dns-sh.op.ru/blog/t-326-internet/47175-chto-takoe-brandmauer-zachem-nujna-zaschita-komputera-i-kak-ee-nas/ (дата звернення 21.10.2023).

6. І. А. Терейковський, Д. А. Бушуєв, Л. О. Терейковська. Штучні нейронні мережі: Базові положення. Навчальний посібник. – Вид-во «Національний технічний університет України «КПІ», 2022 . – 123 с.
7. Web Application Firewall (ModSecurity). [Електронний ресурс]. Режим доступу: https://docs.plesk.com/en-US/obsidian/administrator-guide/server-administration/web-application-firewall-modsecurity.73383/ (дата звернення 24.10.2023).
8. Побудова мережевої та локальної системи безпеки. [Електронний ресурс]. Режим доступу: http://www.telesphera.net/blog/network-and-local-security-system.html (дата звернення 24.10.2023).
9. Демчук Л. Ю. Технології виявлення атак(аналіз сигнатур). [Електронний ресурс]. Режим доступу: https://int-konf.org/ru/2013/prostir-i-chas-suchasnoji-nauki-22-24-04-2013-r/258-demchuk-l-yu-tekhnologiji-viyavlennya-atak-analiz-signatur (дата звернення 24.10.2023).

**Reference**

1. Karchevs′kyy M.V. Zlochyny v sferi vykorystannya elektronno-obchyslyuval′nykh mashyn (komp″yuteriv), system ta komp″yuternykh merezh i merezh elektrozv'yazku (tezy lektsiy) / M.V. Karchevs′kyy // Zlochyny v sferi vykorystannya IT [Elektronnyy resurs]. – Rezhym dostupu: http://it-crime.at.ua/index/tezi_lekcij/0-31 (data zvernennya 17.09.2023).
2. Dmytro Nikulesku. Kiberbezpeka: vrazlyvi momenty. [Elektronnyy resurs]. – Rezhym dostupu: https://yur-gazeta.com/publications/practice/inshe/kiberbezpeka-vrazlivi-momenti.html (data zvernennya 23.09.2023).
3. Zakhyst WEB-dodatkiv. Chomu tse aktual′no? [Elektronnyy resurs]. – Rezhym dostupu: https://octavacapital.ua/zahyst-web-dodatkiv-chomu-ce-aktualno/ (data zvernennya 24.09.2023).
4. V. I. Myeshkov, V. O. Virolaynen. Analiz suchasnykh system vyyavlennya ta zapobihannya vtorhnen′ v informatsiyno-telekomunikatsiynykh systemakh. Derzhavnyy VNZ «Natsional′nyy hirnychyy universytet», m. Dnipropetrovs′k. [Elektronnyy resurs]. – Rezhym dostupu: https://ela.kpi.ua/bitstream/123456789/17609/1/meshkov.pdf (data zvernennya 28.09.2023).
5. Chto takoe Brandmauér, zachem nuzhna zashchyta komp′yutera y kak ee nastroyt′. [Elektronnyy resurs]. – Rezhym dostupu: https://club.dns-sh.op.ru/blog/t-326-internet/47175-chto-takoe-brandmauer-zachem-nujna-zaschita-komputera-i-kak-ee-nas/ (data zvernennya 21.10.2023).
6. I. A. Tereykovs′kyy, D. A. Bushuyev, L. O. Tereykovs′ka. Shtuchni neyronni merezhi: Bazovi polozhennya. Navchal′nyy posibnyk. – Vyd-vo «Natsional′nyy tekhnichnyy universytet Ukrayiny «KPI», 2022 . – 123 s.
7. Web Application Firewall (ModSecurity). https://docs.plesk.com/en-US/obsidian/administrator-guide/server-administration/web-application-firewall-modsecurity.73383/ [Elektronnyy resurs]. – Rezhym dostupu: (data zvernennya 24.10.2023).

*The article discusses modern information protection problems and recommendations on the features of the functioning of Web applications in a secure environment. The most important level in terms of information protection is software and technical means, which contain a whole complex of hardware, software, and hardware and software means of information protection. Developers of modern firewalls offer solutions that work at all levels of the OSI model. However, the work of most "classic" firewalls focuses on the network and session levels. Often, the functionality of the firewall at the application level is provided by a separate module, the work of which is, as a rule, of a general nature and does not take into account the peculiarities of the functioning of applications. To implement the study of the reflection of an attack on WEB applications, a neural network of the adaptive resonance theory (ART) was analyzed and investigated, which compares the input image to one of the classes formed in the learning process, if it meets the given criterion of similarity and is sufficiently similar to the prototype of this class . In the comparison process, the input image is modified for greater correspondence with the proposed image - the weights of the connections are adjusted. If the input image is not sufficiently similar to the proposed image, in this case, an additional neuron is allocated and a new class of images is formed. The allocation of an additional neuron for a new class of images occurs due to the presence of free, inactive neurons in the recognizing layer. This operation prevents duplication of existing images already in memory. A modified structure of the network and solutions to eliminate the shortcomings of the neural network are proposed. As a result of the research, further ways of improving the learning algorithm of the neural network are planned, aimed at increasing the number of operations to repel attacks on WEB applications using the heuristic method.*
***Keywords**: WEB application, neural network, attack repulsion, intrusion detection system.*

**Рязанцев О.І. –** професор, завідувач кафедри комп'ютерних наук та інженерії, Східноукраїнського національного університету ім. В. Даля, ryazancev@snu.edu.ua
**Кардашук В.С. –** доцент кафедри комп'ютерних наук та інженерії, Східноукраїнського національного університету ім. В. Даля, kardashuk@snu.edu.ua , kardashuk1@gmail.com
**Сафонова С.О. –** доцент кафедри комп'ютерних наук та інженерії, Східноукраїнського національного університету ім. В. Даля, safonova@snu.edu.ua
**Кравцов С.В.** – аспірант кафедри комп'ютерних наук та інженерії, Східноукраїнського національного університету ім. В. Даля