УДК 681.324

Куліков В.М., Іващенко О.В., Козлов О.О.

ВИЯВЛЕННЯ АНОМАЛЬНОЇ ПОВЕДІНКИ КОРИСТУВАЧІВ КОМП'ЮТЕРНИХ СИСТЕМ ЗА ДОПОМОГУЮ ШТУЧНИХ НЕЙРОННИХ МЕРЕЖ

Анотація:

У статті розглядається одне з можливих рішень задачі підвищення ефективності засобів захисту інформації шляхом виявлення аномальної мережевої активності у діях користувачів. Для рішення задачі застосовується апарат штучних нейронних мереж. Об'єктом дослідження є стан мережевих портів, який характеризує мережеву активність користувачів. Для визначення аномалій у діях користувачів за допомогою штучних нейронних мереж поточна мережева активність користувачів порівнюється з нормальною.

Аннотация:

В статье рассматривается одно из возможных решений задачи повышения эффективности средств защиты информации путем выявления аномальной сетевой активности в действиях пользователей. Для решения задачи применяется аппарат искусственных нейронных сетей. Объектом исследования является состояние сетевых портов, которое характеризует сетевую активность пользователей. Для определения аномалий в действиях пользователей с помощью искусственных нейронных сетей текущая сетевая активность пользователей сравнивается с нормальной.

Annotation:

The paper considers the solution of the efficiency of information security solutions by identifying anomalous network activity in the actions of users. For solution of problems the mathematical tools of artificial neural networks is used. The object of this study is the status of network ports, which characterizes the network activity of users. In order to determine of anomalies in the actions of users the current network activity of users compared with the normal actions.

Об'єднання комп'ютерів у єдину комунікаційну систему – комп'ютерну мережу – призводить до збільшення ризику втручань у роботу комп'ютерних систем з метою реалізації зловмисної діяльності Одним із засобів забезпечення безпеки є моніторинг дій користувачів під час роботи, коли увага приділяється самому користувачу. Знання того, які дії він виконує (або має виконувати), може використовуватися в системах безпеки.

Є доцільним застосування засобів виявлення аномальної поведінки користувачів у складі комплексної системи захисту інформації, а саме, відхилень від нормальної роботи мережевих сервісів, які використовуються користувачами. Перевагою даних систем є те, що вони здатні реагувати на несподівані відхилення поведінки користувачів (змін в роботі мережевих сервісів) від звичайної.

Існує багато різних за складністю, ефективністю та іншими характеристиками методів виявлення аномалій в роботі користувачів комп'ютерних систем. Останнім часом успішно використовуються штучні нейронні мережі. Їхньою основною задачею є класифікації та розпізнавання образів, в даному випадку користувачів.

Штучна нейронна мережа – це набір шарів з так званими штучними нейронами. Штучний нейрон (рис. 1) імітує властивості біологічного нейрона. На вхід штучного нейрона надходить деяка множина сигналів (координат): $x_1,x_2,\ldots,x_n$, кожний з яких є виходом іншого нейрона. Кожен вхід множиться на відповідну синаптичну вагу $w_1,w_2,\ldots,$ w_{1n}.

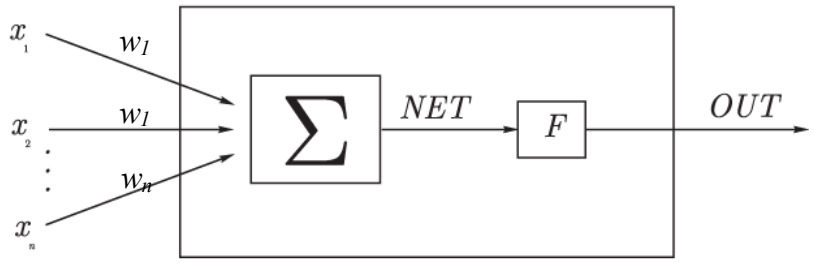

Рис. 1. Структура штучного нейрона

Усі добутки підсумовуються, визначаючи рівень активації нейрона *NET*. Далі сигнал *NET* перетворюється активаційною функцією *F* й дає вихідний нейронний сигнал *OUT*. Активаційна функція може бути лінійною функцією, логічною функцією або функцією гіперболічного тангенсу. Залежно від способу передачі результатів активаційній функції по нейронних шарах нейронні мережі діляться на різні класи.

Оскільки всі штучні нейронні мережі базуються на концепції нейронів, з'єднань та передатних функцій, існує подібність між різними структурами або архітектурами нейронних мереж. Більшість змін походить з різних правил навчання.

У цій статті використовується нейронна мережа, яка має назву “багатошаровий персептрон”. Ця нейронна мережа є мережею прямого розповсюдження, яка складається з вхідного, вихідного й одного або декількох прихованих шарів нейронів. Для навчання мережі було обрано навчання з “вчителем” – алгоритмом зворотного розповсюдження помилки.

Сутність алгоритму полягає у розповсюдженні сигналів помилки від виходів нейронної мережі до її входів у напрямку, зворотному прямому розповсюдженню сигналів у звичайному режимі.

Алгоритм зворотного розповсюдження помилки – це ітеративний градієнтний алгоритм навчання, який використовується з метою мінімізації середньоквадратичного відхилення поточних від необхідних виходів багатошарових нейронних мереж з послідовними зв'язками.

Згідно з методом найменших квадратів, функцією помилки нейронної мережі є величина:

$$E(w) = \frac{1}{2}\sum_{j,k}(y_{j,k}^{(Q)} - d_{j,k})^2,$$

де $y_{j,k}^{(Q)}$ - реальний вихідний стан нейрона *j* вихідного шару Q мережі при подачі на її вхід *k*-го набору сигналів;

$d_{j,k}$ – необхідний (еталонний) вихідний стан цього нейрона.

Підсумовування ведеться по всіх нейронах вихідного шару й по всіх наборах сигналів, що обробляються нейронною мережею. Мінімізація методом градієнтного спуску забезпечує підлаштування вагових коефіцієнтів $w_{ij}^{(q)}$ наступним чином:

$$w_{ij}^{(q)}(t) = w_{ij}^{(q)}(t-1) + \Delta w_{ij}^{(q)}(t),$$

$$\Delta w_{ij}^{(q)} = -\eta \frac{\partial E}{\partial w_{ij}},$$

де w_{ij} – ваговий коефіцієнт синаптичного зв'язку, що з'єднує *i*-й нейрон шару *(q-1)* з *j*-м нейроном шару *q*;

η – коефіцієнт швидкості навчання, $0 < \eta < 1$.

Відповідно до правила диференціювання складної функції:

$$\frac{\partial E}{\partial w_{ij}} = \frac{\partial E}{\partial y_j}\frac{\partial y_j}{\partial s_j}\frac{\partial s_j}{\partial w_{ij}},$$

де s_j - зважена сума вхідних сигналів нейрона *j*, тобто аргумент активаційної функції.

Другий множник – похідна активаційної функції. Для логічної (сигмоїдальної) функції активації:

$$y = f(s) = \frac{1}{1+e^{-\alpha s}},$$

$$f'(s) = \alpha f(s)[1 - f(s)].$$

Третій множник $\frac{\partial s_j}{\partial w_{ij}}$ дорівнює виходу нейрона минулого шару $y_j^{(q-1)}$.

Перший множник розкладається наступним чином:

$$\frac{\partial E}{\partial y_j} = \sum_r \frac{\partial E}{\partial y_r}\frac{\partial y_r}{\partial s_r}\frac{\partial s_r}{\partial y_j} = \sum_r \frac{\partial E}{\partial y_r}\frac{\partial y_r}{\partial s_r} w_{ir}^{(q+1)}.$$

Тут підсумовування по *r* виконується у нейроні шару *(q+1)*.

Вводячи нову змінну:

$$\delta_j^{(q)} = \frac{\partial E}{\partial y_j}\frac{\partial y_j}{\partial s_j},$$

отримаємо рекурсивну формулу для розрахунку $\delta_j^{(q)}$ шару *q* з величини $\delta_r^{(q+1)}$ старшого шару *(q+1)*:

$$\delta_j^{(q)} = \left[\sum_r \delta_r^{(q+1)} w_{jr}^{(q+1)}\right]\frac{\partial y_j}{\partial s_j}.$$

Для виходу шару:

$$\delta_j^{(Q)} = \left(y_j^{(Q)} - d_j\right)\frac{\partial y_j}{\partial s_j}.$$

Вираз для розрахунку величини коригування вагових коефіцієнтів можна записати в розгорнутому вигляді:

$$\Delta w_{ij}^{(q)} = -\eta \delta_j^{(q)} y_i^{(q-1)}.$$

Іноді, щоб надати процесу корекції ваг деякої інертності, що згладжує різкі зміни при переміщенні по поверхні цільової функції, останній вираз доповнюється значенням зміни ваги на попередній ітерації.

$$\Delta w_{ij}^{(q)}(t) = -\eta(\mu \Delta w_{ij}^{(q)}(t-1) + (1-\mu)\delta_j^{(q)} y_i^{(q-1)},$$

де μ – коефіцієнт інертності;

t – номер поточної ітерації.

Для кожного користувача комп'ютерної системи будується й навчається нейронна мережа таким чином, щоб прогнозувати наступну команду на основі попередніх. На основі кількості команд, які були правильно прогнозовані нейронною мережею, робиться висновок, чи відповідає поточна поведінка користувача раніше побудованій моделі. При цьому необхідно враховувати, що користувачам властиво змінювати поведінку із часом. Тому з метою забезпечення адаптації до їхньої поведінки нейронну мережу слід періодично навчати на нових вхідних наборах сигналів.

Нейронна мережа одержує на вхід вектор деяких значень, тобто набір координат. У загальному випадку вихід нейронної мережі також є вектором з безліччю координат. При розв'язанні поставленої задачі розмірність вихідного вектора встановимо рівним одиниці. При цьому очікуваний вихід багатошарового персептрона (рис. 2) може приймати значення в діапазоні [0;1]. 1 – для нормальної поведінки користувача й 0 – для аномальної.

Навчання нейронної мережі являє собою кінцевий набір ітерацій, кожна з яких полягає в одержанні навчального вектора й коригуванні коефіцієнтів нейронної мережі таким чином, щоб на навчальному векторі даної ітерації нейронна мережа видавала допустимий результат. При цьому обирається величина граничної помилки $E(w)$, яка враховується при оцінці завершення навчання нейронної мережі.

При навчанні мережі основне завдання полягає у виборі її характеристик і параметрів: чи буде мережа збігатися або розходитись, скільки нейронів повинен містити прихований шар, скільки ітерацій навчання слід провести тощо. Відсутні формальні вирази, що дають змогу обчислювати ці параметри. Існує лише набір рекомендацій, якими можна користуватися при виборі параметрів, однак при цьому не виключається використання емпіричного методу.

Для моделювання поведінки користувачів використовувалися реальні дані мережевої активності. Запропонований механізм виявлення аномалій за допомогою нейронних мереж має ряд переваг і недоліків. Перевагою є те, що побудувавши профіль поведінки користувача один раз, його можна використовувати постійно, лише періодично навчати на нових вхідних образах. Також із застосуванням деякої експертної оцінки для кожного користувача може бути підібраний свій набір координат, що враховує особливості його мережевої активності. Обробка вектора реальної поведінки користувача при сучасних обчислювальних потужностях проводитиметься майже миттєво. Тобто виявлення аномалії відбувається відразу ж після того, як вона відбулася.

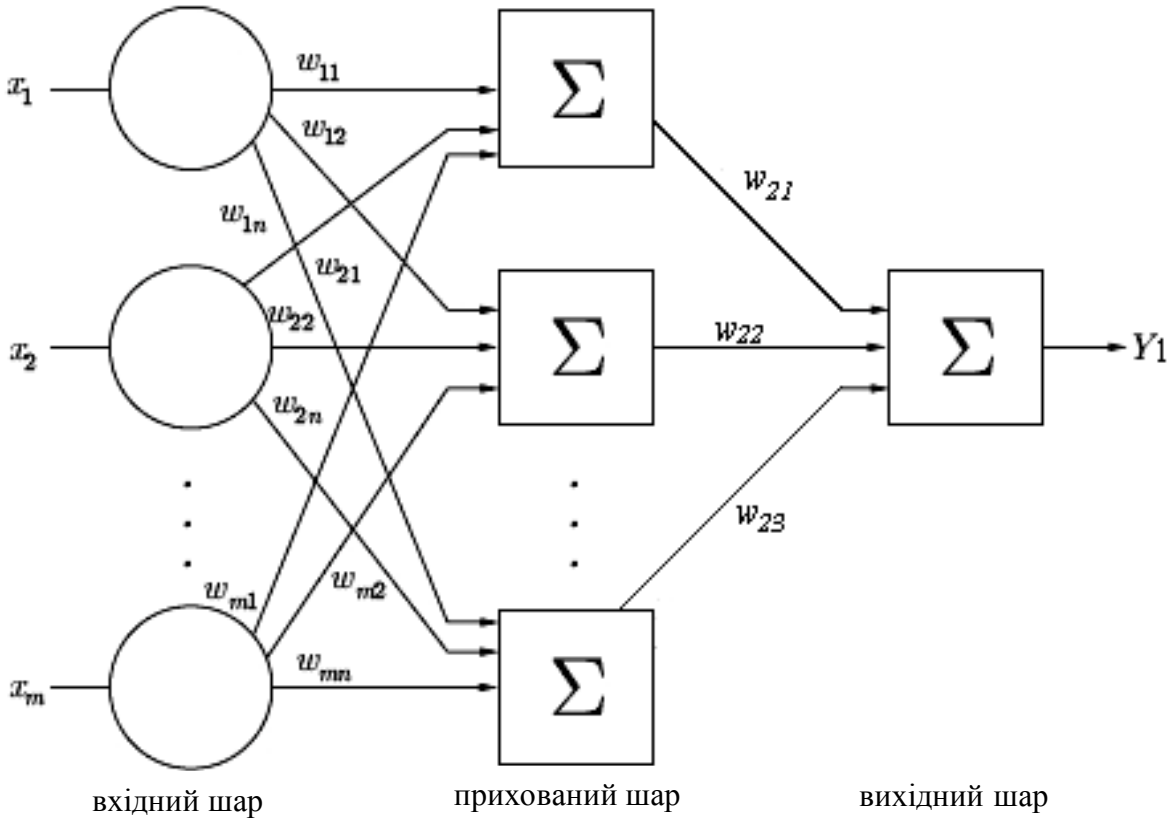

Рис. 2. Багатошаровий персептрон

Основним недоліком на цей момент є складність та тривалість процесу навчання, а також стадія збирання навчальних векторів. Навіть при невеликій розмірності вектора число навчальних векторів для нейронної мережі будь-якого роду значно зростає, але це число навчальних векторів можна значно зменшити шляхом виконання умови опису якнайбільш різних варіантів запуску, а не багаторазового запуску того самого варіанта. І все ж таки автоматизована побудова профілю поведінки користувача потребує деякого часу, а також експертної оцінки й бажано додаткових знань про мережеву активність користувача.

У ході експерименту досліджувалася мережева активність двох користувачів, які працювали із подібним набором програм, що використовують мережеві сервіси. Дослідження отриманих результатів проводилося шляхом аналізу значень виходу нейромережі. Обчислювалося середнє значення виходів всіх образів нейромережі. Це число і характеризувало аномальність вхідного вектора, тобто аномальність дій користувача. На вхід нейронної мережі, яка була навчена на певного користувача здійснювалася подача вхідного вектора іншого користувача, у нашому випадку він виступав зловмисником.

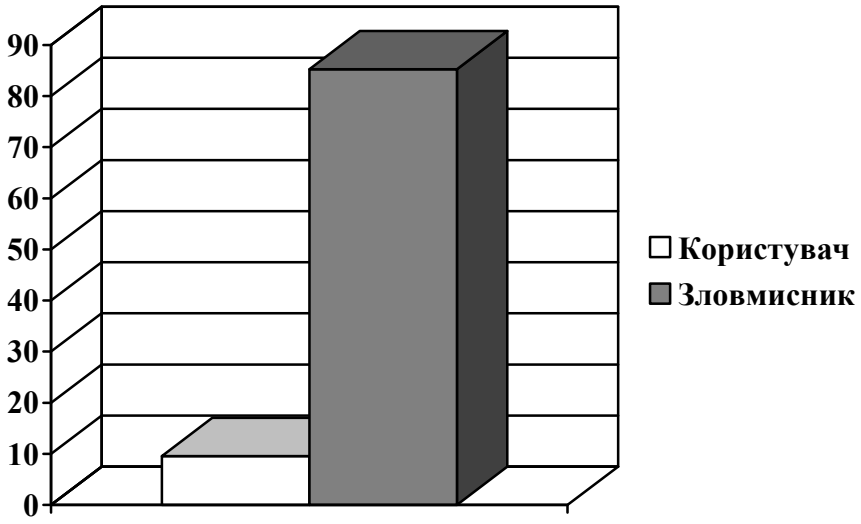

Рис. 3. Рівень аномальності користувача та зловмисника

При подачі на вхід нейронної мережі вхідного вектора того користувача, на якого вона була навчена, вихід мережі був рівним близько 0.9. При подачі вхідного вектора зловмисника вихід мережі був рівним близько 0.15.

Узявши за 100% те, що дії користувача повністю аномальні, а за 0% – те, що аномалій немає, можна побудувати діаграму, яка показує рівень аномальності користувача та зловмисника (рис. 3).

Отримані результати свідчать про перспективність використання штучних нейронних мереж у системах виявлення втручань у комп'ютерні системи.

Література:

1. *Хайкин,* Саймон. Нейронные сети: полный курс, 2-е издание. – М.: «Вильямс», 2006. – 1104 с.

2. *Куссуль Н.Н.* Скакун С.В. Нейросетевая модель пользователей компьютерных систем // Кибернетика и вычислительная техника. – 2004.

3. *С. Норткат, Дж. Новак.* Обнаружение нарушений безопасности в сетях. – 3-е изд. – М.: Вильямс, 2003. – 448 с.

4. *Лукацкий А.* Обнаружение атак. – 2-е изд. – СПб.: БХВ-Петербург,