УДК 004.052:004.738.2 (045)

Толстікова О.В., к.т.н.

ІМІТАЦІЙНА НЕЙРОМЕРЕЖЕВА МОДЕЛЬ ІДЕНТИФІКАЦІЇ АНОМАЛЬНИХ СТАНІВ ТРАФІКА КОМП'ЮТЕРНОЇ МЕРЕЖІ

Національний авіаційний університет

Запропонована нейромережева технологія ідентифікації атак на комп'ютерні мережі з використанням програмного забезпечення в системі MATLAB/SIMULINK/NEURAL NET. Задача ідентифікації атак на комп'ютерні мережі розглянута як задача класифікації.

Вступ

Проблема виявлення аномалій очолює списки й рейтинги найбільш актуальних проблем у різних програмах в області захисту інформації. Методи виявлення аномалій в комп'ютерних мережах (КМ) спрямовані на виявлення невідомих атак і вторгнень.

Виявлення мережних атак, зв'язаних з одержанням неавторизованого доступу до вилучених ресурсів, можливо на різних етапах їхнього здійснення: на етапі проникнення зловмисника і на етапі подальшого використання захопленого ресурсу. Це вимагає ретельного аналізу мережних потоків даних, особливо, полів даних мережних пакетів.

Для підвищення ефективності виявлення мережних атак необхідний аналіз на рівні прикладних протоколів, тобто необхідно оцінювати поля даних пакетів.

Наявність слідів атаки на прикладному рівні (рівні додатків) запропоноване виявляти шляхом оцінювання типу протоколу прикладного рівня (за вмістом полів даних пакетів) і зіставлення цієї інформації з параметрами використовуваного протоколу транспортного рівня. Оцінка типу протоколу прикладного рівня можлива після структуризації і збереження полів даних мережних пакетів.

Для системи, що підлягає захисту, на основі сукупності параметрів оцінки формується «образ» нормального функціонування. У сучасних системах виділяють кілька способів побудови «образа», тобто:

– накопичення найбільш характерної статистичної інформації для кожного параметра оцінки;

– навчання нейронних мереж значеннями параметрів оцінки;

– представлення на підставі подій.

Легко помітити, що у виявленні дуже значну роль грає множина параметрів оцінки. Тому у виявленні аномалій однією з головних задач є вибір оптимальної множини параметрів оцінки. Іншою, не менш важливою задачею, є визначення загального показника аномальності. Складність полягає в тому, що ця величина повинна характеризувати загальний стан «аномальності» у системі, що захищається.

Одним із способів представлення «образа» нормального функціонування системи є *застосування нейронної мережі* та її навчання значенням параметрів оцінки. Навчання нейронної мережі здійснюється послідовністю інформаційних одиниць (далі команд), кожна з який може знаходитися на більш абстрактному рівні в порівнянні з використовуваними параметрами оцінки. Вхідні дані мережі складаються з поточних команд і минулих **W** команд, що обробляються нейронною мережею з метою прогнозування наступних команд; **W** також називають розміром вікна. Після того як нейронна мережа навчена множиною послідовних команд системи, що захищається, чи однієї з її підсистем, мережа являє собою «образ» нормального поводження. Процес виявлення аномалій являє собою визначення показника неправильно передбачених команд, тобто фактично виявляється відмінність у поводження об'єкта.

Вхідний параметр задає кілька значень чи рівнів, кожний з який унікально визначає команду. Вихідний реагуючий шар складається з одну багаторівневого, котрий прогнозує наступну можливу команду користувача.

Недоліки:

– топологія мережі і ваги вузлів визначаються тільки після досить великого числа спроб і помилок;

– розмір вікна – ще одна величина, що має принципове значення при розробці; якщо зробити вікно маленьким, то мережа буде не досить продуктивною, занадто великим – буде страждати від небажаних даних.

Переваги застосування даного способу:

– успіх даного підходу не залежить від природи вихідних даних;

– автоматично враховуються зв'язки між різними вимірами, що, безсумнівно, впливають на результат оцінки.

Представлення «образа» у даному випадку ґрунтується на припущенні про те, що поточні значення параметрів оцінки можна зв'язати з поточним станом системи. Після цього функціонування представляється у вигляді послідовності подій чи станів.

Існує система правил, що характеризують сукупності значень параметрів оцінки (далі патерна) нормальної роботи. Ці правила формуються індуктивно і заміняються більш «працездатними» правилами динамічно під час навчання. Під «працездатними правилами» розуміються правила з більшою імовірністю їхньої появи і з великим рівнем унікальності для системи, що захищається.

Саме сукупність правил, створюваних індуктивно під час спостереження роботи користувача, складає «образ». Аномалія реєструється в тому випадку, якщо послідовність подій, що спостерігається, відповідає лівій частини правила виведеного раніше, а події, що мали місце в системі після цього, значно відрізняються від тих, котрі повинні були наступити за правилом.

Основний недолік даного підходу полягає в тім, що нерозпізнані патерни поводження можуть бути не прийняті за аномальні через те, що вони не відповідають ні одній з лівих частин усіх правил. Даний метод досить ефективно визначає вторгнення, тому що приймаються в увагу: залежності між подіями; та послідовність появи подій.

До переваг методу слід віднести:

– кращу обробку користувачів з великим коливанням поводження, але з чіткою послідовністю патернів;

– можливість звернути увагу на деякі важливі події безпеки, а не на всю сесію, що позначена як підозріла;

– краща чутливість до виявлення порушень: правила містять у собі семантику процесів, що дозволяє набагато простіше помітити зловмисників, що намагаються навчити систему у своїх цілях.

Запропонований підхід до структуризації трафіку базується на такому. Якщо визнано, що існуючих засобів (методологічних, програмних та ін.) не вистачає для ідентифікації трафіку або часовий ряд, то слід звернути увагу на пошук нових засобів, а не на модифікацію існуючих, зокрема, статистичних методів. По-перше, слід визнати, що за допомогою тільки чисел (раціональних і дійсних) описати трафік принципово неможливо. Звідси випливає рішення – застосувати новий вид чисел – *p*-адичні числа та матриці. По-друге, потрібно використати не тільки Архімедові метрику, але і інші. По-третє, на підставі визначених парадигм сформулювати нові підходи аналізу.

Можна виділити наступні достоїнства застосування нейромереж:

– вони мають здатність вивчати характеристики умисних атак;

– мають нагоду ідентифікувати раніше невідомі дії і надалі класифікувати їх;

– мають нагоду проводити моніторинг мережі на наявність вірусів.

– мають нагоду динамічно реагувати на різні дії, зокрема раніше невідомі;

– мають нагоду аналізувати неповні і спотворені дані, фільтрувати інформацію;

– мають нагоду паралельної (мультипроцесової) обробки. Коли у реальному часі аналізуються відразу декілька процесів, запущених на сервері;

– забезпечують прогноз характеру і наслідків зловживань.

Постановка задачі

Визначення аномального трафіка, під яким розуміють трафік, що є атакою або її попередником, як відзначають більшість фахівців з захисту комп'ютерних мереж від несанкціонованого доступу [1], є надзвичайно складною проблемою, бо на даний час не існує загально прийнятого визначення аномального трафіку. Визначення, які існують, торкаються окремих сторін або властивостей трафіку. Але, як показують досліди і практика, завжди апостеріорно можна визначити параметри трафіку, який в минулому класифікувався як аномальний або нормальний. Якщо припустити, що трафік описується множиною параметрів $X^{(T)} = \{x_i\}, i = \overline{1,n}$; і ці множини апостеріорно відомі для аномальних та нормальних станів – ${}^{A}X^{(T)}$, ${}^{N}X^{(T)}$ відповідно, то завжди можна (з певним запасом) визначити кордони, у яких змінювались параметри трафіка у кожному з станів, ${}^{A}X^{(T)} = \{[{}^{A}x_i^{min}, {}^{A}x_i^{max}]\}$,

${}^{N}X^{(T)} = \{[{}^{N}x_i^{min}, {}^{N}x_i^{max}]\}$, де індексами *min, max* позначені мінімальне та максимальне значення інтервалів, у яких визначено параметр, трафік згідно [2] доцільно аналізувати у такий спосіб.

Невизначеність поняття «аномальний стан» змушує вводити певні уточнення і обмеження на характер і склад задачі, що розглядаються. Аномальні дії обмежені розглядом наступних ситуацій:

- непомітний вплив, відсутність відповіді;
- шкідливий вплив, фатальна реакція;
- вплив відсутній, реагують всі;
- нестандартний вплив, ідентифікуюча відповідь.

Не вдаючись до детального аналізу підходу, зазначимо його певну умовність. Намагання уникнути нечітких визначень призводить до того, що з нечіткими поняттями виконуються дії з використанням стандартного математичного апарату, який є абсолютно неадекватним визначенням. Це, природно, впливає на достовірність отриманих висновків.

Аналіз трафіку базується на вмісті пакетів, розгляд ведеться для стандартного та прихованого запитів, дослідження пакетів ведеться на підставі і з допомогою *TCPdump*. Досліджується:

- *IP* заголовок, зокрема, визначається місце, де він закінчується;
- інші поля з вказівкою довжини, зокрема довжина *IP*- дейтаграми, довжина заголовка *TCP*-сегмента, збільшення фіксованої довжини або досліджується весь пакет.

Зазначимо в цьому зв'язку наступне.

Власне трафік комп'ютерної мережі вважається як семантичне поняття цілком дослідженим, хоча автори, використовують достатньо різний набір компонентів трафіку. При цьому зовсім не визначаються причини, з яких такий набір визначається, дуже часто ці причини є техніко-економічними і природно не дають відповіді на питання наскільки повний (необхідний та достатній) набір параметрів з точки зору ефективності виявлення аномального стану. Відповідно до такого підходу дослідження полів *IP*- заголовка орієнтоване на виявлення атак зі вставкою та прихованих атак.

Аналіз трафіку широко використовує поняття «нестандартного» (незвичного) трафіку, під яким розуміють загальну картину того, що відбулося, власне трафік, незвичайне сканування, хости-відправники та хости-приймачі, розташування конкретних хостів, значення полів *TTL*, розмір вікна, параметри *TCP*, повторні запити і та ін.

Продемонструвати всі можливі варіанти нормального трафіка досить складно, але можна представити різні стандартні ситуації і зразки трафіка, котрий передається частіше за все. Звернемо увагу на зразки. Особливу увагу слід звернути відповідній реакції хостів і маршрутизаторів при отриманні різної інформації при різних обставинах її отримання і при різних протоколах. Пояснити, що означає «нормальний трафік» неможливо, неможливо розглянути всі безкінечні варіанти нормального трафіку. Напевне, можна вражати, що найкращою характеристикою нормальності слід визнати відсутність нормальності, що передбачає розгляд можливо найбільшої кількості прикладів трафіка, який відрізняється від норми.

Шляхи вирішення задачі

Проблема виявлення аномалій в роботі КМ, в т.ч. на підставі аналізу трафіка, відноситься до важкоформалізованих проблем [3] розв'язання яких сучасна наука бачить у використанні *інтелектуальних технологій.*

Інтелектуальні технології (системи) представляють собою такі нформаційні технології, у яких передбачені:

- наявність баз знань, що відбивають досвід конкретних людей, груп, суспільств, людства в цілому, у рішенні творчих задач у виділених сферах діяльності, що традиційно вважалися прерогативою інтелекту людини (наприклад, такі недостатньо формалізовані задачі, як прийняття рішень, проектування, витягнення змісту, пояснення, навчання і т.ін.);
- наявність моделей мислення на основі баз знань: правил і логічних висновків; аргументації і міркування; розпізнавання і класифікації ситуацій; узагальнення і розуміння і т.ін.;
- здатність формувати цілком чіткі рішення на основі нечітких, несуворих, неповних, недовизначених даних;
- здатність пояснювати висновки і рішення, тобто наявність механізму пояснень;
- здатність до навчання, перенавчанню і, отже, до розвитку.

Вони ґрунтуються на ідеології штучного інтелекту.

Параметри трафіка (для визначення патернів) у загальному вигляді визначені: $\boldsymbol{x}=\{x_i\}, i=1,9$.

Сучасні системи виявлення атак (*Intrusion Detecting System, IDS*) працюють на двох рівнях у залежності від того, до якої інформації існує доступ. Загальним у цих підходах є пошук відповідних ознак (сигнатур), комбінації цих ознак (шаблонів), що вказують на ворожі чи дії на їхню підозру. Якщо пошук цих сигнатур і шаблонів виконується на рівні мережного трафіка, то *IDS* працюють на мережному рівні, якщо пошук ведеться в системному журналі чи в журналі додатків (мова йде про системний рівень). Звичайно найбільш ефективної буде технологія, що працює, з огляду на обидва рівні.

Однією із сучасних технологій *ISD*, від якої чекають визначених досягнень, є нейромережева технологія.

Запропоновано нейромережеву технологію ідентифікації атак на комп'ютерні мережі з використанням програмного забезпечення в системі *MATLAB/SIMULINK/NEURAL NET.*

Постановку задачі ідентифікації атак на КМ будемо розглядати як задачу класифікації, реалізація якої передбачена за допомогою

одне (чи багато-) кульового персептрона. Припустимо, що ми маємо тренувальні набори $(x_1, z_1), (x_2, z_2), \ldots, (x_n, c_n)$, що містять множину $X_t=\{x_1, x_2, \ldots, x_{Nt}\}$ і N_t тренувальних спостережень у n- мірному просторі $(x_j \in R^n, n\geq 2)$ і їхній зв'язаний клас-індикатор – вектор c_j, $j=1,2\ldots N_t$..... Обмежуємося розглядом двокласової проблеми ("атака на КМ", "відсутність атаки"), хоча в реальних умовах це обмеження може бути критичним, тому що в залежності від типу даних (наприклад, розходження між даними складає величину $10^8 \div 10^{10}$!) вибір ваг матриці зв'язків може бути дуже утрудненим і кількість класів прийдеться збільшувати. Саме така ситуація має місце при спробах аналізу трафіку. Прийнята постановка задачі вимагає, щоб індикатор c_j був би двовимірним вектором $(c_j=(c_1, c_2)^T)$, що вказує, що x_j може належати одному з двох класів – ω_1 чи ω_2.

Компоненти c_{1j}, c_{2j} визначені як "нуль" чи "одиниця" відповідно класу належності x_j, тобто:

$c_{1j}=1$ & $c_{2j}=0$ if $x_j \in \omega_1$ і $c_{1j}=0$ & $c_{2j}=1$ if $x_j \in \omega_2$.

Клас-індикатор вектор c_j передбачає декомпозицію множин X_t на підмножини, відповідно окремим класам. Позначимо через N_{ti} – кількість тренувальних спостережень у класі ω_i.

Позначимо через $y(x; w)$ функції відтворення багатошарового персептрона *(MLP)* нейронной мережі для класифікації з вектором w, що містить регульовані ваги нейромережі. Тренування мережі виконується шляхом мінімізації середньо-квадратичної (*MS*) похибки:

$$E^{mlp}(w)=\frac{1}{N_t}\sum_{j=1}^{N_t}[y(x_j;w)-(c_{1j}-c_{2j})]^2.$$

При цьому маємо, що приймач $(c_{1j}-c_{2j})=1$ для тренувальних векторів $x_j \in \omega_1$ і $(c_{1j}-c_{2j})=-1$ (чи нуль) для $x_j \in \omega_2$, подальше поліпшення вираження для $E^{MLP}(\,)$ можливо шляхом регулярізації цього вираження для зменшення узагальнюючих властивостей нейромережі.

Похибка $E^{MLP}(w)$ нейромережі з нелінійною активаційною функцією на схованому шарі моделі є істотно нелінійна функція. Послідовна мінімізація $E^{MLP}(\,)$ може бути проведеної з використанням ітераційних оптимізаційних алгоритмів, що доступні в середовищі *MatLab*. Головна мета – пошук глобального мінімуму $E^{MLP}(w)$. Найпростіше використання тренувального алгоритму – локальна мінімізація $E^{MLP}(w)$, обчислена величина спостереженого мінімуму може бути чистим локальним мінімумом. Рішення w^* строго залежить від стартових (початкових) значень локального оптимізатора. У представленій програмі використовуються рекурсивні (евристичні) методи для пошуку декількох невеликих (у визначеному розумінні, наприклад, досягнення величини 10^{-6}) локальних мінімумів, з яких вибирається один. Саме на цьому мінімумі фіксується матриця ваг нейромережі, що потім використовується як класифікатор.

Специфіка постановки задачі полягає у необхідності урахування таких обставин. Задано два вектори $x^{(1)}=\{x_j^{(1)}\}$, $x^{(2)}=\{x_j^{(2)}\}$, $j=1, 9$, компоненти яких характеризують трафік, $x^{(1)} \in \omega_1$, $x^{(2)} \in \omega_2$, де ω_1, ω_2 – класи ситуації, що відповідають наявності атаки (100 % гарантія) і відсутності атаки. З огляду на те, що наявності двох ідеалізованих векторів недостатньо для реалізації гарантованого результату, сформовані тестові вибірки $x^{(1t)}$ і $x^{(2t)}$ відповідно $x^{(1)}$ і $x^{(2)}$. Кожен компонент (крім бінарних) тестових вибірок $x_j^{(1t)} \in x^{(1t)}$ і $x_j^{(2t)} \in x^{(2t)}$ сформована за принципом:

$x_j^{1t}=x_j \pm 0.15*x_j rand()$,

де *rand()* –фунция *Matlab*, що генерує випадкові числа в інтервалі [0, 1].

Загальна схема моделювання ідентифікації атак з використанням засобів *Matlab/Simulink/NeuralNet* містить нейромережу, модель вхідних наборів і деякі інші допоміжні пристрої. У процесі експериментальних досліджень використовувались конкретні значення параметрів трафіку, на підставі яких навчалась мережа, і було реалізовано його моделювання. Навчання нейромережі вважалося виконаним правильно, якщо для набору $\mathbf{x}^{(1t)}$ одержували (0.95 і 0.05) і для $\mathbf{x}^{(2t)}$ відповідно (0.05 і 0.95), що звичайно приводить до виникнення певної зони невизначеності $(5 \div 10\ \%)$. Додаткове підвищення точності класифікації можливо за рахунок використання нових ознак. Однак потрібно при цьому ретельно підрахувати економічну доцільність. Вкажемо також, що умови вибору можна зробити більш толерантними, а саме – відносити вихід до одному із класів за умови одержання величини $y>>0.5$.

Слід зазначити, що правильно навчена мережа може досить чітко класифікувати ситуації при умовах, що деякі дані (значення вхідного вектора) можуть бути відсутніми (схованими), чи визначатися на рівні «м'яких» вимірів, тобто відображуваних у виді нечітких чи чисел змінних. У табл. 1 наведено фрагмент бази даних, який був використаний при експериментальних дослідженнях.

Таблиця 1.

Фрагмент бази даних трафіку

0	2098.40	73.28	1516035423.08	1385603780.84	1.00	1.00	385.17	3333.18
0	1992.35	71.86	1556094748.99	1563724918.41	1.00	1.00	400.28	3629.95
0	2274.75	70.25	1359246543.06	1543406223.70	1.00	1.00	393.65	3328.08
0	2004.67	74.14	1339328278.80	1491973541.58	1.00	1.00	369.04	3655.79
0	2266.38	73.74	1362329505.92	1357065158.14	1.00	1.00	380.84	3511.46
0	2306.19	76.85	1546135115.27	1564045191.37	1.00	1.00	349.70	3656.35
0	2039.16	78.17	1377005519.43	1534993222.75	1.00	1.00	362.56	3380.88
0	2180.58	76.27	1533856186.95	1367908610.34	1.00	1.00	381.59	3344.25
0	2010.17	69.98	1495012358.74	1371688201.84	1.00	1.00	372.15	3441.87
x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9

Базові патерни ("атака присутня" – "атака відсутня"), які використовувалися у експериментальних дослідженнях наведені у абсолютних величинах у табл. 2.

Трафік комп'ютерної мережі розглядається *нормованим*, згідно до стандантних методів та моделей нормування. Множини нормальних та аномальних станів приймаються у вигляді:

$$X^{(n)} = \{(\forall i)\ x_i^n \ \underline{\underline{\text{def}}}\ x_i^n \pm 0.15 \cdot \text{rand}() \cdot x_i^n\},$$

i=2,..,9; та відповідно

$$X^{(a)} = \{(\forall i)\ x_i^a \ \underline{\underline{\text{def}}}\ x_i^a \pm 0.15 \cdot \text{rand}() \cdot x_i^a\},$$

i=2,..,9; параметри представленого у вигляді таблиці бази даних (системний журнал).

Графічна ілюстрація патернів для навчання нейромережі надана на рис. 1.

Досліди показали, що навчена на приведених наборах мережа, по-перше, має відносно невеликий час навчання (секунди), що дозволяє використовувати технологію в реальному часі і, по-друге, усі тестові набори, утворені з наборів першого і другого типів (коливання параметрів у границях ±15-20%) і які експертами діагностувалися як «відсутність атаки» і «присутність атаки», нейронною мережею ідентифікувалися абсолютно безпомилково. участі в тестуванні) класу «атака присутня» дає на виході – **{1,0}**; відповідно «атака відсутня» – **{0,1}**.

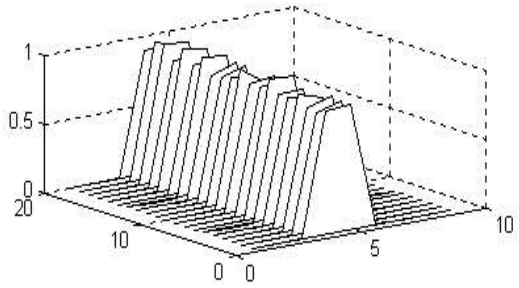
Дана програма дозволяє проаналізувати роботу запропонованої нейромережевої технології для ідентифікації атак. Автоматично генеруються випадкові вхідні набори, що відносяться до одного з класів, на екран одночасно виводиться згенерований набір і рішення, що приймає нейромережа, відносячи його до одному з класів.

Приклад імітації нормального і аномального трафіку наведено у табл. 3.

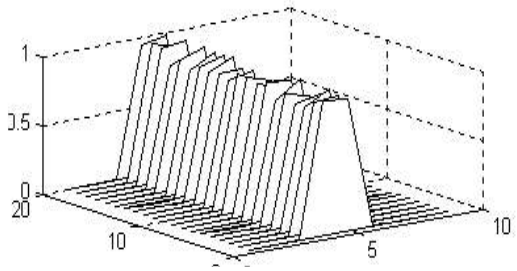
Таблиця 2.

Базові патерни

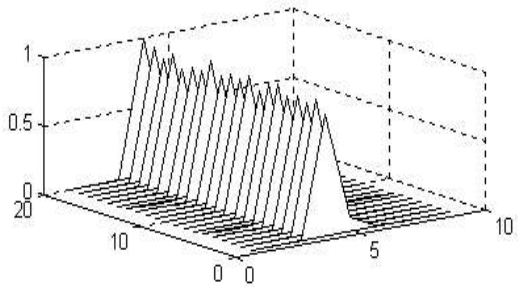
x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	y
0	2314	80	1573638018	-1580478590	1	1	401	3758	0, 1
0	1611	6101	8801886082	-926176166	1	1	0	2633	1, 0



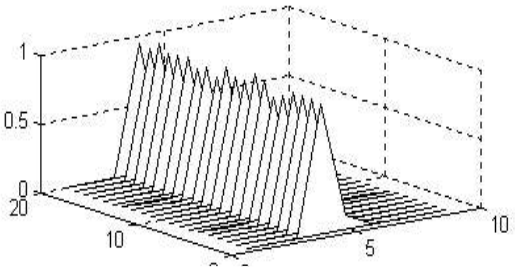
а) Normal mode 1



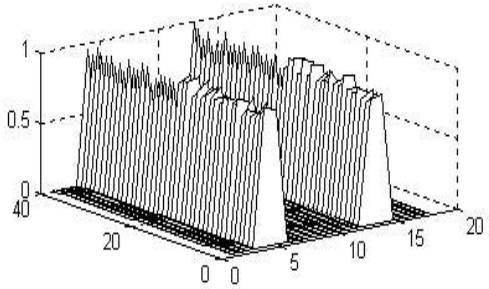
б) Normal mode 2



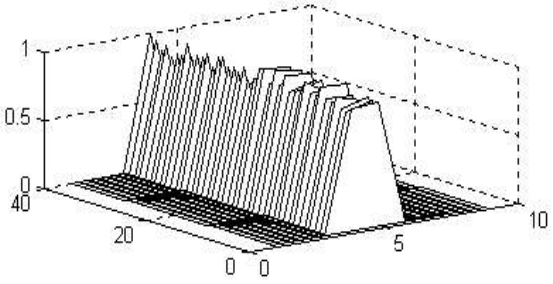
в) Abormal mode 1



г) Abormal mode 2



д) Normal mode 1 U Normal mode 2 .vs. Abnormal mode 1 U Abnormal mode



є) Normal mode 1 vs Abnormal mode 1

Рис. 1. Графічна ілюстрація патернів для навчання нейромережі
а), б) – нормальний стан трафіка з коливаннями параметрів ± 15 % від середнього;
в), г) – аномальний стан трафіка з коливаннями параметрів ± 15 % від середнього;
д) поєднання нормального та аномального станів (а ⋃ б ⋂ в ⋃
г), є) поєднання нормального та аномального станів (а ⋂ в)

Таблиця 3.

Приклад імітації нормального і аномального трафіку

Protocol ID	x1	0	0
Source Port	x2	2314	1611
Source Address	x3	80	6101
Destination Port	x4	1573638018	801886082
Destination Address	x5	-1580478590	-926167166
ICMP Type ID	x6	1	1
ICMP Code ID	x7	1	1
Raw Data	x8	401	0
Length Data	x9	3758	2633
ID Attack		0	1

Висновки

Виявлення зловживань, зокрема, є важкою проблемою через велику кількість вразливостей в комп'ютерних мережах. Застосування нейронних мереж дає багато переваг у виявленні атак. Як показали дослідження наведені в даній роботі, нейронні мережі визначають зловживання там де існуючі методи виявляються безсильними. Це не значить що потрібно відмовлятися від запропонованих на даний момент систем захисту і повністю перейти на нейромережеві технології. Кращим рішенням буде їхнє сполучення, що стане досить корисним і ефективним методом виявлення зловживань.

Аномальний стан трафіку як загальне семантичне поняття на даний час практично не визначено, прикладні рекомендації відносно цього здебільшого ґрунтуються на тому, що аномальним є стан, характеристики якого відрізняються від тих, які існують у базі даних. Недоліком даного підоду є те, що апріорі не враховуються нові стани з новими характеристиками, які не мають відповідних аналогів. Застосування стандартних нейромережевих методів для розв'язку задач класифікації обжено розглядом двокласової проблеми («аномальний стан КМ», «нормальний стан КМ»), хоча в реальних умовах це обмеження може бути критичним, бо залежно від типу даних (наприклад, різниця між числовими даними складає величину $10^8 \div 10^{10}$!) вибір ваг матриці зв'язків може бути достатньо утрудненим і кількість класів потрібно збільшувати, що змінює характер задачі.

Список літератури

1. Норткат С., Новак Дж. Обнаружение нарушений безопасности в сетях, 3-е изд.: Пер. с англ. – М.: Изд. Дом „Вильямс", 2003. – 448 с.

2. Кеннеди Дж. Нейросетевые технологии в диагностике аномальной сетевой активности. – http://www.beda.stup.ae.ru/lib/neuro /content/id/ neuro-net/htm.

3. Крон Г. Тензорный анализ сетей. – М.: Советское Радио. – 1978. – 720 с.