УДК 004.056.53 : 004.492.3
Мельник К.В., Мельник В.М., Лотоцький І.М.
Луцький національний технічний університет

ВІДСТЕЖЕННЯ ВІРУСНИХ АТАК НА ОСНОВІ НЕЙРОННИХ МЕРЕЖ

Мельник К.В., Мельник В.М., Лотоцький І.М. Відстеження вірусних атак на основі нейронних мереж. Розроблено нейромережевий детектор вірусних атак, що базується на нейронній мережі векторного квантування LVQ з нейронними елементами Кохонена в прихованому шарі. Запропонований метод дозволив працювати з малим об'ємом навчальної вибірки, а структура нейронної мережі дозволила здійснити кластеризацію атак і нормальних з'єднань в прихованому шарі, що підвищило достовірність виявлення і класифікацію атак на комп'ютерну систему.
Ключові слова: мережа Кохонена, нейромережевий детектор, вірусна атака.

Мельник К.В., Мельник В.М., Лотоцкий И.М. Отслеживание вирусных атак на основе нейронных сетей. Разработан нейросетевой детектор вирусных атак, основанный на нейронной сети векторного квантования LVQ с нейронными элементами Кохонена в скрытом слое. Предложенный метод дает возможность работать с малым объемом обучающей выборки, а структура нейронной сети позволила осуществить кластеризацию атак и нормальных соединений в скрытом слое, что повышает достоверность обнаружения и классификации атак на компьютерную систему.
Ключевые слова: сеть Кохонена, нейросетевой детектор, вирусная атака.

Melnyk K.V., Melnyk V.M., Lototsky I.M. Tracking virus attacks based on neural networks. Neural network detector of virus attacks, was developed based on neural network LVQ vector quantization of Kohonen's neural elements in the hidden layer. The proposed method allowed us to work with a small amount of training set, and the structure of the neural network allowed to carry out attacks clustering and normal connections in the hidden layer, which increased the reliability of the detection and classification of attacks on computer system.
Keywords: Kohonen network, neural network detector, virus attacks.

Постановка проблеми. Сучасні методи антивірусного захисту з використанням сигнатурних методів, в даний час переживають серйозну кризу. На думку деяких експертів, сучасні антивірусні продукти не можуть захистити від 80% «небажаних» програм. Це особливо ясно показало наявність зараження троянськими програмами промислових додатків, які сучасні противірусні засоби не виявляли протягом 5-8 років [2].

Виявлення комп'ютерних атак в якості противірусних агентів, в основному, спрямовані на сигнатурні («пошук за шаблоном») методи, які безсилі проти нових класів атак. Однією з основних проблем, системи виявлення вторгнень на основі евристичного аналізу, є висока ймовірність помилкових спрацьовувань.

Наявні факти викрадення конфіденційної інформації та здійснення деструктивних дій в КС (комп'ютерних системах), в яких встановлене антивірусне програмне забезпечення, свідчать про недоліки відомих технологій діагностування КС на наявність вірусних програм. Сучасні інформаційні технології діагностування КС на наявність вірусних програм орієнтовані на виявлення відомого шкідливого програмного забезпечення, та не повністю адаптовані до розпізнавання нових вірусних програм.

Факти викрадення конфіденційної інформації і проведень деструктивних дій в КС (комп'ютерній системі), в яких встановлені антивірусні програми, показала недоліки відомих технологій для діагностики вірусних програм діагностування КС. Сучасні інформаційні технології для діагностики вірусних програм на КС, спрямовані на виявлення відомих шкідливих програм і не повністю адаптовані до виявлення нових вірусів.

Аналіз ситуації в області шкідливого програмного забезпечення показує інтенсивне зростання числа вірусних програм здатних виконувати в комп'ютерних системах деструктивні або шкідливі дії. Таким чином, слід зробити висновок про те, що існує необхідність у вивченні нових методів і технологій в області інформаційної безпеки. Один і перспективних напрямків в області інформаційних технологій вважаються штучні нейронні мережі.

Дослідженнями в цій сфері займаються Головко В.А. [1], Городецький В.І. [2], Котенко І.В. [3], Широчин В.П. [4], De Castro L. [5] та ін. Разом з тим, дані підходи характеризуються наявністю ряду вузьких місць, таких як складність створення або вибору необхідних детекторів атак, складність адаптації до невідомих атак, здатність коректно працювати тільки на невеликих наборах даних.

Мета роботи полягає в створенні нейромережевий детектора, що дозволить здійснити кластеризацію атак і нормальних з'єднань в комп'ютерній системі.

Виклад основного матеріалу роботи. Залежно від техніки, що використовується при здійсненні несанкціонованих дій на комп'ютерну систему, виділяють чотири основні класи

мережевих атак (denial of service, user-to-root, remote-to-local, probe), кожен з яких складається з декількох типів [6,7]. Розглянемо кожен з класів атак докладніше.

DOS (denial of service, відмова в обслуговуванні) атаки. Це мережеві атаки, направлені на виникнення ситуації, коли в системі, що атакується, відбувається відмова в обслуговуванні. Дані атаки характеризуються генерацією великого об'єму трафіку, що приводить до перевантаження і блокування сервера. Виділяють шість типів *DOS*-атак: *back, land, neptune, pod, smurf, teardrop* [7] .

U2R (user-to-root) атаки. Атаки даного класу передбачають отримання зареєстрованими користувачами привілеїв локального суперкористувача (адміністратора). Виділяють чотири типи *U2R*-атак: *bufferoverflow, loadmodule, perl, rootkit* [7].

R2L (remote-to-local) атаки. Такі атаки характеризуються отриманням доступу незареєстрованого користувача до комп'ютера з боку віддаленої машини. Виділяють вісім типів *R2L*-ата: *ftp_write, guess_passwd, imap, multihop, phf, spy, warezclient, warezmaster* [7].

Probe-атаки грунтуються на процесі сканування мережевих портів віддаленої машини з метою отримання конфіденційної інформації. Виділяють чотири типи *Probe*-атак: *ipsweep, nmap, portsweep, satan* [7].

Виявлення і класифікація мережевих атак на комп'ютерну систему відбувається за допомогою аналізу інформації в каналах обміну. Для розуміння даного процесу розглянемо параметри мережевого з'єднання, які аналізуються для забезпечення безпеки комп'ютерних систем.

Дані в інформаційних телекомунікаційних мережах передаються у вигляді мережевих пакетів. У структурі мережевого пакету виділяють три основні поля (рисунок 1): заголовок пакету, поле даних пакету, кінець пакету.

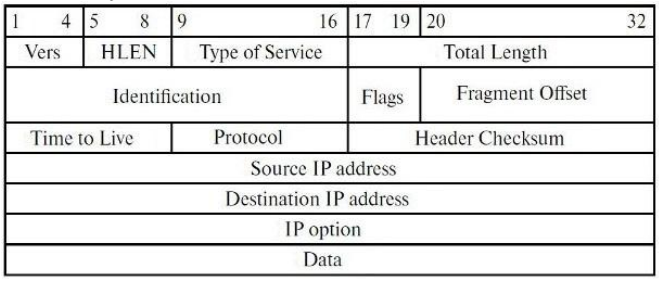

Рис. 1. Структура мережевого пакету

Виділяють 41 параметр мережевого з'єднання, які, у свою чергу, об'єднані у три групи [7]:

а) вбудовані параметри;

б) параметри контенту;

в) параметри трафіку.

З розвитком методів штучного інтелекту, з середини 90-х років відбувається перехід від ручних методів аналізу поведінки складних систем до автоматизованих методів аналізу. Методи штучного інтелекту відомі, перш за все, такими характеристиками, як здатність до адаптації і навчання на помилках, високі обчислювальні швидкості, робота із зашумленими даними.

Найбільш використовуваним підходом в області аналізу мережевого трафіку з метою виявлення аномалій є: штучні нейронні мережі, нечіткі системи, методи еволюційного програмування, штучні імунні системи.

У науково-дослідних роботах основною проблемою при спробі порівняння різних підходів до виявлення і класифікації атак є те, що практично немає двох різних досліджень, які використовують в якості даних для аналізу однакові вхідні дані. А якщо навіть і використовуються однакові набори даних, то навчання і тестування пропонованої системи все одно проводиться, найчастіше, на різних підмножинах із заявленого набору.

Оскільки, в дослідницьких роботах запропоновані підходи виявлення і класифікації мережевих атак, побудовані на основі наборів даних, то якість підготовки даних безпосередньо впливає на якість підготовки моделей. Як правило, набори тестових даних зібрані з трьох джерел: дані мережевих пакетів, дані поведінки користувачів або дані системних викликів (таблиця 1).

Першим поширеним набором даних став Internet Exploration Shootout Dataset (IES) , що представляв чотири колекції даних, що включали заголовки пакетів, отримані в реальній мережі: одна з нормального трафіку і три з аномаліями. У 1998 році була сформована база даних DARPA98, де даними є записи TCP-з'єднань реальної ЛОМ, які включають відомі і невідомі атаки. База даних KDD Cup1999 Data [7] була сформована в рамках проведення міжнародної

наукової конференції KDD-99, метою якої було стимулювання досліджень в області обробки даних і створення нових алгоритмів виявлення і класифікації мережевих атак. Цей набір даних підготовлений SJ Stolfo разом із співавторами і будується на основі даних, отриманих в DARPA98. DARPA98 включає близько 4 Гб стиснених TCP-даних мережевого трафіку, які формувалися впродовж 7 тижнів. В результаті отримано близько 5 мільйонів записів, кожен з яких розміром близько 100 байт.

База даних KDD-99 містить параметри, як нормальних мережевих з'єднань, так і 22 типів мережевих атак, що відносяться до чотирьох класів [7]. У таблиці 1 представлений розподіл по класах в 10% базі даних KDD-99 [7].

Таблиця 1. Розподіл по класах в базі даних KDD99

Клас	Кількість записів	Відсоток
Normal	97278	19.6911%
DOS	391458	79.2391%
U2R	52	0.0105%
R2L	1126	0. 2279%
Probe	4107	0. 8313%

Як вже наголошувалося, виявлення і класифікація мережевих атак на КС відбувається на основі аналізу інформації, що передається по каналах передачі даних. Узагальнену функціональну модель прийняття рішень можна представити у вигляді наступних етапів (рисунок 2).

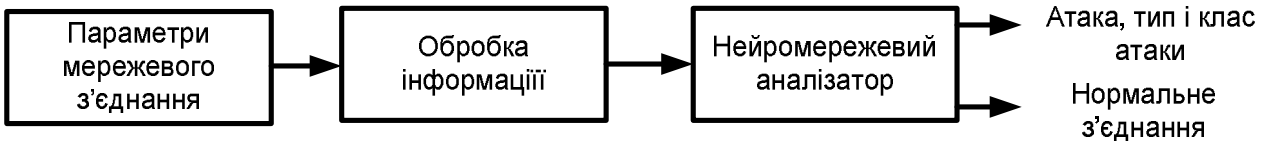

Рис. 2. Узагальнена функціональна модель прийняття рішень при виявленні і класифікації атак на КС

У зв'язку із здатністю ШНМ в процесі навчання виявляти складні залежності між вхідними і вихідними даними, які були відсутні в навчальній вибірці, і здатністю коректно класифікувати зашумлені образи, вони є привабливим інструментом для вирішення складних різноманітних задач захисту комп'ютерної інформації [4].

Так нейронні мережі Кохонена дозволяють в результаті навчання здійснювати типологічно безперервне відображення *F*- вхідного *n* - мірного простору у вихідний *m* - мірний простір. Структура такої нейронної мережі є мережею з прямим розповсюдженням сигналу. В якості методу навчання використовується конкурентне навчання. У міру надходження вхідних образів на таку мережу за допомогою навчання відбувається розбиття *n* - мірного вхідного простору на різні області рішень, кожній з яких відповідає окремий нейрон.

LVQ мережа є розширенням мережі Кохонена і містить, окрім конкурентного шару, лінійний шар, який здійснює класифікацію кластерів, виділених шаром Кохонена. Проектування нейромережевого детектора на базі нейронної мережі LVQ відбувається наступним чином.

Перший шар нейронних елементів є розподільним і призначений для розподілу вхідних сигналів на нейрони прихованого шару. Вхідними сигналами є параметри мережевого з'єднання [7], які характеризують мережевий трафік і містять інформацію про час з'єднання, тип протоколу, кількість переданих байт, кількість виникнення помилок під час з'єднання і т.д. Кількість нейронних елементів розподільного шару дорівнює кількості атрибутів мережевого з'єднання, тобто *n = 41*.

Другий шар нейронної мережі складається з нейронів Кохонена [8]. Шар Кохонена відіграє ключову роль в класифікації інформації і здійснює кластеризацію вхідного простору образів, внаслідок чого утворюються кластери різних образів, кожному з яких відповідає свій нейронний елемент. Для навчання нейронів прихованого шару використовується конкурентний принцип навчання відповідно до правила «переможець бере все» (winner-take-all) [8]. Кількість нейронів в шарі Кохонена дорівнює *m*, вони пов'язані з двома нейронами вихідного шару.

Третій шар складається з двох лінійних нейронних елементів, які використовують лінійну функцію активацію [8] і здійснюють відображення кластерів, сформованих шаром Кохонена, в два класи, які характеризують нормальне з'єднання або атаку.

Структура нейромережевого детектора [9] виявлення атак представлена на рисунку 3.

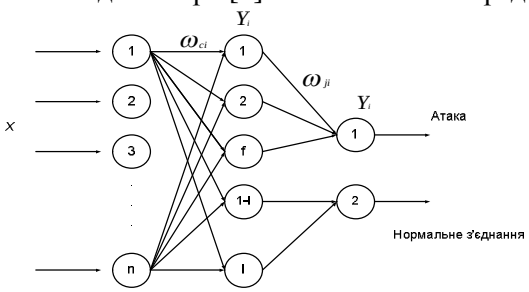

Рис.3. Структура нейромережевого детектора для виявлення атак

Таким чином, відмінною особливістю представленого детектора є те, що нейрони в прихованому шарі розділені на дві групи: перша група характеризує клас мережевих з'єднань, що відносяться до мережевих атак; друга група нейронів характеризує клас нормальних з'єднань [9]. В результаті, можна отримати більш точне розділення одного класу від іншого.

Характеристики для оцінки якості виявлення і класифікації атак на КС:

- TPR (True Positives Rate) – чутливість (Sensitivity, Se), ймовірність правильної класифікації атак.
- FNR (False Negative Rate) – помилка першого роду або рівень значущості, що характеризує ймовірність неправильної класифікації атак.
- TNR (True Negative Rate) – специфічність (потужність критерію) (Specificity, Sp), що характеризує ймовірність правильної класифікації нормальних з'єднань.
- FPR (False Positives Rate) – помилка другого роду, що характеризує ймовірність класифікації нормальних з'єднань, як атак (ймовірність помилкових спрацювань.

У таблиці 2 представлені результати виявлення Dos_back атаки нейромережевим детектором на базі MPL, в таблиці 3 представлені результати виявлення мережевої атаки нейромережевим детектором на базі LVQ з нейронами Кохонена в прихованому шарі, в таблиці 4 – нейромережевий детектор на базі RBF і в таблиці 5 представлені узагальнені результати роботи нейронних мереж.

Таблиця 2. Результати виявлення мережевої атаки на базі MPL

Dos_back (розмір тестової вибірки - 2139 атак)				
	TPR (Se), %	TNR (Sp), %	FNR, %	FPR, %
Детектор MLP1	99,05	98,27	0,95	0,73
Детектор MLP2	99,14	96,87	0,86	3,13
Детектор MLP3	99,05	97,62	0,95	2,38
Детектор MLP4	99,05	99,41	0,95	0,59
Детектор MLP5	100	87,32	0	12,68
Детектор MLP6	99,05	99,37	0,95	0,63
Детектор MLP7	99,18	90,54	0,82	9,46
Детектор MLP8	99,59	97,56	0,41	2,44
Детектор MLP9	99,05	98,79	0,95	1,21
Детектор MLP10	99,05	99,02	0,95	0,98

Таблиця 3. Результати виявлення мережевої атаки на базі LVQ

Dos_back (розмір тестової вибірки - 2139 атак)				
	TPR (Se), %	TNR (Sp), %	FNR, %	FPR, %
Детектор Koh1	99,05	97	0,95	3,01
Детектор Koh2	100	88,63	0	11,37
Детектор Koh3	99	99,8	1	0,2
Детектор Koh4	99,05	98,14	0,95	1,86
Детектор Koh5	99,37	90,46	0,63	9,54
Детектор Koh6	100	85,73	0	14,27

Детектор Koh7	100	94	0	6
Детектор Koh8	99,05	98,44	0,95	1,56
Детектор Koh9	99,05	91,41	0,95	8,59
Детектор Koh10	99,77	90,49	0,23	9,51

Таблиця 4. Результати виявлення мережевої атаки на базі RBF

Dos_back (розмір тестової вибірки - 2139 атак)				
	TPR (Se), %	TNR (Sp), %	FNR, %	FPR, %
Детектор RBF1	99,05	74,32	0,95	25,68
Детектор RBF2	100	84,91	0	15,09
Детектор RBF3	99,09	90,78	0,91	9,22
Детектор RBF4	100	89,85	0	10,15
Детектор RBF5	99,09	74,55	0,91	25,45
Детектор RBF6	100	89,41	0	10,59
Детектор RBF7	99,09	93,72	0,91	6,28
Детектор RBF8	100	89,48	0	10,52
Детектор RBF9	99,09	93,52	0,91	6,48
Детектор RBF10	100	87,62	0	12,38

Таблиця 5. Узагальнені результати виявлення мережевих атак

Dos_back (розмір тестової вибірки - 2139 атак)				
	TPR (Se), %	TNR (Sp), %	FNR, %	FPR, %
Детектор Koh3	99,434	96,477	0,779	3,423
Детектор MLP4	99,221	93,41	0,566	6,591
Детектор RBF7	99,541	86,816	0,459	13,184

Висновки.

Результати експериментальних досліджень дозволяють зробити висновок про те, що система виявлення аномалій з достатньо високою точністю здатна розпізнавати різноманітні мережеві атаки, маючи при цьому невелику частку помилкових спрацьовувань. Таким чином, запропонована ідея використанням нейромережевих детекторів в імунному алгоритмі для виявлення аномалій мережевого трафіку є ефективною і може бути успішно використана для виявлення нештатних ситуацій і можливих порушень функціонування комп'ютерної системи. Крім того, обрана нейронна мережа не вимагає для свого формування значних обчислювальних витрат і дозволяє результативно виявляти аномалії трафіку комп'ютерної системи .

1. Golovko V. Nerual Ntworks approaches for Intrusion Detection and Recognition / V. Golovko, L. Vaitsekhovich // Computing. – 2006. – Vol. 5, N.3. – P. 118-125
2. Kathleen A Jackson, David H DuBois, and Cathy A Stallings, «An +ert system application for network intrusion detection.» // Proceedings of the 14th National Computer Security Conference, pages 215–225,Washington, D.C., 1–4 October 1991.
3. Чечулин А.А. Обнаружение и противодействие сетевым атакам на основе комбинированных механизмов анализа трафика / А.А. Чечулин, И.В. Котенко // Материалы XVIII Общероссийской научно-технической конференции «Методы и технические средства обеспечения безопасности информации». СПб.: Издательство политехнического университета. – 2009. – С.69.
4. Широчин В.П. Обнаружение аномалий на основе неконтролируемой кластеризации / В.П. Широчин, Ху Чженбин, Д.Г. Гундарцев // Труди 6 - ой международной начно-практической конференции «Современные информационные и электронные технологии», Одесса (Украина), 2005. – С 116.
5. De Castro L. Artificial Immune Systems as a Novel soft Computing Paradigm / L. N. De Castro, J. Timmis // Soft Computing Journal. – 2003. – Vol. 7. Issue 7. – P. 268 – 284.
6. Лукацкий А.В. Обнаружение атак / А.В. Лукацкий. – СПб.: БХВ-Петербург, 2003. – 596 с.
7. KDD Cup 1999 Data [Електронний ресурс]. – Режим доступу: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html
8. Слеповичев И.И. Обнаружение DDoS-атак нечет-кой нейронной сетью / И.И. Слеповичев,П.В. Ирматов, М.С. Комарова, А.А. Бежин // Известия Саратовского университета. – 2009. – Т. 9,сер. Математика. Механика. Информатика, вып. 3.– С. 84-89.
9. Комар М.П. Нейросетевой подход к обнаружению сетевых атак на компьютерные системы / М.П. Комар, И.О. Палий, Р.П. Шевчук, Т.Б. Федысив // Інформатика та математичні методи в моделюванні – 2011. – Том 1, №2. – С. 156-160.