Міністерство освіти і науки, молоді та спорту України
Тернопільський національний економічний університет

КОМАР МИРОСЛАВ ПЕТРОВИЧ

УДК 004.056.53 : 004.492.3

ІНТЕЛЕКТУАЛЬНА ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ВИЯВЛЕННЯ І КЛАСИФІКАЦІЇ АТАК НА ІНФОРМАЦІЙНІ ТЕЛЕКОМУНІКАЦІЙНІ МЕРЕЖІ

05.13.06 – інформаційні технології

Автореферат дисертації на здобуття наукового ступеня
кандидата технічних наук

Тернопіль – 2012

Дисертацією є рукопис.

Робота виконана в Тернопільському національному економічному університеті Міністерства освіти і науки, молоді та спорту України.

Наукові керівники: заслужений винахідник України,
доктор технічних наук, професор
Саченко Анатолій Олексійович,
Тернопільський національний економічний університет,
завідувач кафедри інформаційно-обчислювальних систем та управління;

доктор технічних наук, професор
Головко Володимир Адамович,
Брестський державний технічний університет,
м. Брест, Республіка Білорусь,
завідувач кафедри інтелектуальних інформаційних технологій

Офіційні опоненти: доктор технічних наук, професор
Антощук Світлана Григорівна,
Одеський національний політехнічний університет,
директор інституту комп'ютерних систем,
завідувач кафедри інформаційних систем;

кандидат технічних наук, доцент
Савенко Олег Станіславович,
Хмельницький національний університет,
доцент кафедри системного програмування

Захист відбудеться «31» січня 2013 р. о 14 ^{00} годині на засіданні спеціалізованої вченої ради К 58.082.02 при Тернопільському національному економічному університеті за адресою: 46020, м. Тернопіль, вул. Львівська, 11а (корпус 11, зал засідань).

З дисертацією можна ознайомитись у бібліотеці Тернопільського національного економічного університету за адресою: 46020, м. Тернопіль, вул. Бережанська, 4.

Автореферат розісланий «28» грудня 2012 р.

Учений секретар
спеціалізованої вченої ради
кандидат технічних наук, доцент В.В. Яцків

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Останнім часом відбулося злиття комп'ютерних мереж, інформаційних і телекомунікаційних технологій, що дозволило утворити сучасні інформаційні телекомунікаційні мережі (ІТМ), які є складною розподіленою системою, що характеризується наявністю множини взаємодіючих ресурсів, системних та прикладних інформаційних і телекомунікаційних процесів. У таких умовах важливою науково-технічною задачею є забезпечення цілісності, достовірності та конфіденційності інформації. Інформаційні телекомунікаційні мережі піддаються різного роду загрозам, і користувач не може бути впевнений у захищеності важливої інформації, оскільки кіберзлочинці продовжують удосконалювати і розробляти методи і засоби організації мережевих атак. Наприклад, за даними «Лабораторії Касперського» щодня в світі з'являється близько 70 тисяч нових шкідливих програм, близько 200 мільйонів мережевих атак блокується щомісячно, а в 2011 році система IDS Kaspersky Internet Security відбила майже 3 мільярди мережевих атак.

Аналіз найбільш поширених інформаційних технологій виявлення мережевих атак, таких як сигнатурний і статистичний аналіз, показує їх нездатність виявляти нові або невідомі атаки, для яких характерна відсутність записів в системі про них. Інформаційні технології, які базуються на евристичних методах, мають високу ймовірність помилкових спрацювань. Ситуація, що склалася, стимулює пошук і розробку нових методів та інформаційних технологій, спрямованих на підвищення достовірності виявлення і класифікації атак на ІТМ.

Одним з перспективних напрямків є застосування методів штучного інтелекту. Дослідженнями у цій сфері займаються Головко В.А., Городецький В.І., Котенко І.В., Широчин В.П., Cannady J., Dasgupta D., De Castro L., Grediaga A., Ibrahim LM , Jing Xiao-Pei, Moradi M., Mukkamala S., Murad Abdo Rassam, Novosad T., Ramadas M., Sammany M., Sridevi R. та ін. Разом з тим, відомі підходи характеризуються наявністю ряду вузьких місць, таких як складність створення або вибору необхідних детекторів атак, громіздкість процедури адаптації до невідомих атак, здатність коректно працювати тільки на невеликих наборах даних.

Для усунення цих недоліків запропоновано використати інтеграцію методів штучних нейронних мереж і штучних імунних систем, оскільки вони поєднують високу достовірність виявлення і класифікації атак з властивістю до навчання, адаптації, самоорганізації і пам'яті.

Враховуючи вищесказане, можна зробити висновок про актуальність досліджень, спрямованих на розробку інформаційної технології на базі теорії штучних нейронних мереж та штучних імунних систем з метою підвищення достовірності виявлення та класифікації атак на ІТМ.

Зв'язок роботи з науковими програмами, планами, темами. Основний зміст дисертаційної роботи складають теоретичні і практичні результати досліджень, проведених автором при виконанні держбюджетної науково-дослідної роботи Тернопільського національного економічного університету «Методи та засоби виявлення вторгнень на комп'ютерні системи» (номер державної реєстрації – 0110U000786, термін виконання 06.2010 р. – 06.2012 р.), де автор був відповідальним виконавцем.

Мета і задачі дослідження. Метою дисертаційної роботи є створення нової інтелектуальної інформаційної технології на базі теорії штучних нейронних мереж і штучних імунних систем для підвищення достовірності виявлення і класифікації атак на ІТМ.

Для досягнення поставленої мети вирішуються наступні задачі:

1. Аналіз існуючих інформаційних технологій для визначення шляхів підвищення достовірності виявлення та класифікації атак на ІТМ.
2. Розробка узагальненої функціональної моделі прийняття рішень при виявленні і класифікації атак.
3. Вибір нейронної мережі для виявлення і класифікації атак на ІТМ.
4. Розробка методу побудови нейромережевого детектора атак на базі нейронної мережі, що характеризується малим обсягом навчальної вибірки.
5. Розробка методу побудови сукупного класифікатора для ієрархічної класифікації атак на основі багатоканальних нейромережевих детекторів.
6. Розробка комбінованого методу виявлення і класифікації атак на ІТМ на основі інтеграції нейромережевих детекторів в штучну імунну систему.
7. Створення інтелектуальної інформаційної технології для вирішення задачі підвищення достовірності виявлення та класифікації атак на ІТМ на основі запропонованих методів.
8. Проведення статистичної оцінки достовірності розробленої інформаційної технології з метою порівняння з відомими рішеннями.

Об'єкт дослідження – процес обробки інформації при виявленні і класифікації атак на інформаційні телекомунікаційні мережі.

Предмет дослідження – методи і засоби інтелектуальної інформаційної технології виявлення і класифікації атак на ІТМ.

Методи дослідження. Для вирішення поставлених задач використовуються методи системного аналізу, математичної статистики, теорії розпізнавання образів, теорії штучних нейронних мереж і штучних імунних систем.

Наукова новизна дослідження. В ході виконання дослідження були отримані наступні основні результати, що відображають наукову новизну роботи:

1. Вперше розроблено комбінований метод виявлення і класифікації атак на інформаційні телекомунікаційні мережі шляхом інтеграції нейромережевих детекторів в штучну імунну систему, що дозволило їм адаптуватися до невідомих атак за рахунок здійснення операцій клонування і мутації.
2. Вдосконалено метод побудови нейромережевого детектора атак на інформаційні телекомунікаційні мережі, в якому, на відміну від відомих, нейронні елементи в прихованому шарі розділені на два класи, які характеризують атаку або нормальне з'єднання, що дало можливість окремо здійснити кластеризацію атак і нормальних з'єднань в прихованому шарі і підвищити достовірність виявлення атак при малому об'ємі навчальної вибірки.
3. Вдосконалено метод побудови сукупного класифікатора для ієрархічної класифікації атак на інформаційні телекомунікаційні мережі на основі багатоканальних нейромережевих детекторів, який, на відміну від відомих, поєднує використання методу головних компонент, об'єднання і усунення конфліктів між навченими на певний тип атак нейромережевими детекторами, що дозволило зменшити розмір-

ність аналізованої інформації та класифікувати мережеві атаки.

4. Отримала подальший розвиток інтелектуальна інформаційна технологія виявлення і класифікації атак на інформаційні телекомунікаційні мережі на основі використання операцій навчання, відбору, клональної селекції, мутації та імунної пам'яті з метою формування якнайкращої популяції детекторів, яка, на відміну від відомих, характеризується генеруванням множини нейромережевих детекторів для кожного типу мережевої атаки, що дало можливість підвищити достовірність виявлення і класифікації як відомих, так і невідомих мережевих атак.

Практичне значення одержаних результатів. В результаті виконаного дисертаційного дослідження, на основі розроблених методів і засобів, реалізована та впроваджена нова нейромережева імунна система виявлення і класифікації як відомих, так і невідомих атак на ІТМ. Результати експериментальних досліджень підтверджують правильність наукових положень дисертаційної роботи, оскільки впровадження інтелектуальної інформаційної технології підвищує достовірність виявлення і класифікації атак на ІТМ на 0,27-8,5% у порівнянні з відомими рішеннями.

Теоретичні та практичні результати роботи використані:

– Приватним підприємством «МагнетікВан» (м. Тернопіль) (акт впровадження від 12.10.2012 р.);

– Товариством з обмеженою відповідальністю «СофтІнвест» (м. Брест, Республіка Білорусь) (акт впровадження від 25.09.2012 р.);

– Науково-дослідним інститутом інтелектуальних комп'ютерних систем (Тернопільський національний економічний університет, Інститут кібернетики ім. В.М. Глушкова НАН України) в рамках науково-дослідної роботи на тему: «Методи та засоби виявлення вторгнень на комп'ютерні системи» (акт впровадження від 18.10.2012 р.);

– в рамках двостороннього договору про партнерство, співпрацю і науковий обмін між Тернопільським національним економічним університетом і Брестським державним технічним університетом (акт впровадження від 19.09.2012 р.);

– у навчальному процесі Тернопільського національного економічного університету при викладанні дисциплін «Комп'ютерні мережі», «Телекомунікаційні системи», «Теорія нейронних мереж», «Методи і системи штучного інтелекту» (акт впровадження від 05.10.2012 р.).

Особистий внесок здобувача. Всі основні результати, що виносяться на захист, отримані здобувачем особисто. У роботах, опублікованих у співавторстві, здобувачеві належить: у [1] – вдосконалення і експериментальні дослідження методів і алгоритмів виявлення мережевих атак шляхом застосування нейромережевих детекторів на основі штучних нейронних мереж; у [7] – спосіб виявлення мережевих атак нейромережевою штучною імунною системою; у [8] – комбінована інформаційна технологія виявлення і класифікації мережевих атак на основі методу головних компонент і нейромережевого детектора і експериментальні дослідження; у [10] – метод побудови нейромережевого детектора і експериментальні дослідження застосування методу головних компонент для підвищення достовірності виявлення атак; у [11] – метод виявлення і класифікації атак на інформаційні телекомунікаційні мережі, заснований на інтеграції нейромережевих детекторів в штучну імунну систему і оцін-

ка достовірності запропонованого підходу на основі ROC-аналізу; у [12] – метод побудови сукупного класифікатора для ієрархічної класифікації атак на основі багатоканальних нейромережевих детекторів, який поєднує використання методу головних компонент, об'єднання і усунення конфліктів між нейромережевими детекторами; у [13] – структура штучної імунної системи виявлення і класифікації атак на інформаційні телекомунікаційні мережі; у [18] – експериментальні дослідження інтелектуальної системи виявлення шкідливих дій на комп'ютерні системи.

Апробація результатів дисертації. Основні положення і результати дисертаційної роботи були висвітлені і обговорені на міжнародних і національних конференціях: міжнародній конференції «Комп'ютерні системи і мережеві технології» (Київ, 2009); республіканській конференції молодих вчених і студентів «Сучасні проблеми математики і обчислювальної техніки» (Брест, Республіка Білорусь, 2009); міжнародній конференції «Modern Problems of Radio Engineering, Telecommunications and Computer Science» (Львів-Славське, 2010); міжнародній науково-технічній конференції «Internet–Education–Science» (Вінниця, 2010); міжнародній конференції молодих вчених і студентів «Актуальні задачі сучасних технологій» (Тернопіль, 2010); міжнародній конференції «Методи та засоби кодування, захисту й ущільнення інформації» (Вінниця, 2011); міжнародній конференції «Обчислювальний інтелект (результати, проблеми, перспективи)» (Черкаси, 2011); міжнародній конференції «Інформаційні технології та безпека в управлінні» (Севастополь, 2011); міжнародній конференції «Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications» (Прага, Чехія, 2011); загальноуніверситетській науковій конференції професорсько-викладацького складу, докторантів, аспірантів і здобувачів вченого ступеня ТНЕУ «Економічні, правові, інформаційні і гуманітарні проблеми розвитку України в умовах проведення системних реформ» (Тернопіль, 2012); міжнародній конференції «Захист інформації і безпека інформаційних систем» (Львів, 2012); міжнародній конференції «CAD in Machinery Design. Implementation and Educational Issues» (Львів, 2012).

Публікації. Основні результати дисертаційної роботи висвітлені у 20 друкованих працях, в т.ч. 6 статей (з них 5 одноосібні) у фахових виданнях України; один патент України; одна стаття у зарубіжному науковому журналі, одна стаття у вітчизняному науковому журналі, 11 робіт у збірниках міжнародних і всеукраїнських наукових конференцій.

Структура та обсяг роботи. Дисертаційна робота складається зі вступу, чотирьох розділів, висновків, списку використаних джерел і додатків. Загальний обсяг роботи становить 204 сторінки, з яких 132 сторінки основного тексту. Робота містить 47 рисунків, 36 таблиць і 10 додатків. Список використаних джерел включає 192 найменування на 22 сторінках.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі обґрунтовано актуальність теми і доцільність проведення дисертаційних досліджень, сформульовані мета і задачі дослідження, визначені наукова новизна і практична цінність отриманих результатів. Вказано зв'язок дисертації з нау-

ковими програмами, приведена кількість публікацій, показано особистий внесок здобувача.

У **першому розділі** зроблено огляд і виконано порівняльний аналіз відомих підходів існуючих інформаційних технологій виявлення і класифікації атак на ІТМ. Визнано доцільним створити нову інформаційну технологію на базі штучних нейронних мереж і штучних імунних систем з використанням, в якості тестових наборів, бази даних KDD (Knowledge Discovery and Data Mining), яка часто вживається на практиці. Проведений порівняльний аналіз відомих рішень підтвердив, що одним з основних критеріїв оцінки ефективності інформаційної технології виявлення і класифікації мережевих атак є достовірність результатів її функціонування, тому визнано доцільним використати ROC-аналіз в якості засобу оцінки достовірності результатів. На завершення обґрунтовано шляхи вдосконалення методів виявлення і класифікації атак на ІТМ та сформульовано задачі дослідження.

Другий розділ присвячений розробленим нейромережевим методам виявлення і класифікації атак на ІТМ.

Запропоновано узагальнену функціональну модель прийняття рішень при виявленні і класифікації атак на ІТМ (рисунок 1).

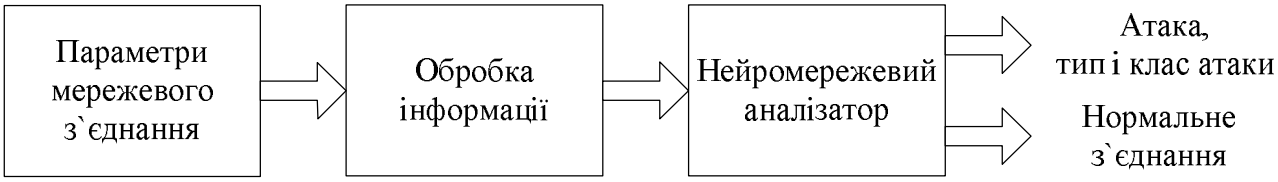


Рисунок 1 – Узагальнена функціональна модель прийняття рішень при виявленні і класифікації атак на ІТМ

На першому етапі з кожного мережевого пакету виділяється 41 параметр мережевого з'єднання. Оскільки значення параметрів різні, то для аналізу інформації за допомогою нейронних мереж, на другому етапі відбувається перетворення символьних значень в числові. Нейромережевий аналізатор може складатися з множини нейронних мереж, об'єднаних в єдину систему. Назвемо окрему нейронну мережу для виявлення і класифікації атак на ІТМ нейромережевим детектором.

Для вибору базової архітектури нейромережевого детектора проведено теоретичні та експериментальні дослідження на базі трьох нейромереж – MLP, RBF і LVQ. Теоретичні дослідження показали, що для навчання мережі MLP розмір навчальної вибірки повинен становити 4420 образів ($L \approx O(W/\varepsilon)$, $W=m(n+k+1)+k$), де L – розмір навчальної вибірки, W – загальна кількість параметрів, що налаштовуються (вагових коефіцієнтів і порогових значень), ε – допустима помилка класифікації, $O()$ – порядок величини, n – кількість вхідних нейронів, m – кількість нейронів прихованого шару, k – кількість нейронів вихідного шару. Для нейронної мережі RBF – кількість нейронів прихованого шару зростає пропорційно розміру навчальної вибірки ($L^{1/3}=<m<=L$), а для LVQ мережі з десятьма нейронами Кохонена в прихованому шарі необхідно мати навчальну вибірку розмірністю більшу *20* образів ($L>= 2m$).

В результаті проведення експериментальних досліджень, найкращі результати показала нейронна мережа LVQ. Ймовірність виявлення (чутливість нейромережевого детектора) атак типу *dos_back* для неї склала 99% при рівні помилок другого

роду 0,2%. Ця ж нейронна мережа показала результат виявлення атак типу *dos_neptune*, який рівний 100% при рівні помилок другого роду 0,1%.

Тому в якості основи нейромережевого детектора вибрано нейронну мережу векторного квантування (LVQ) з нейронами Кохонена в прихованому шарі, яка характеризується малим об'ємом навчальної вибірки, що дозволило навчати нейромережеві детектори на атаках, які характеризуються малою кількістю записів.

З врахуванням цього вдосконалено метод побудови нейромережевого детектора атак на ІТМ на базі нейронної мережі LVQ (рисунок 2).

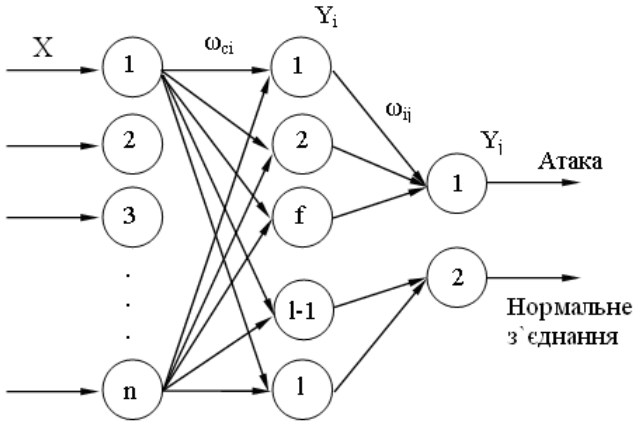


Рисунок 2 – Структура нейромережевого детектора атак

Перший шар нейронних елементів є розподільним і призначений для розподілу вхідних сигналів на нейрони прихованого шару. Вхідними сигналами є параметри мережевого з'єднання. Кількість нейронних елементів розподільного шару дорівнює кількості параметрів мережевого з'єднання, тобто $n = 41$.

Другий шар нейронної мережі складається з нейронів Кохонена. Шар Кохонена здійснює кластеризацію вхідного простору образів, внаслідок чого утворюються кластери різних образів, кожному з яких відповідає свій нейронний елемент. Кількість нейронів m в шарі Кохонена

$$m = f + l, \tag{1}$$

де f – кількість перших нейронів шару Кохонена, які відповідають класу мережевої атаки;

l – кількість останніх нейронів шару Кохонена, активність яких характеризує клас нормального, легітимного з'єднання.

Нейрони прихованого шару функціонують за принципом «переможець бере все». Відповідно до цього, під час поступлення вхідного образу обчислюється, для кожного нейрона, евклідова відстань між вхідним і ваговим вектором відповідного нейронного елементу

$$D_i = |X - \omega_i| = \sqrt{(X_1 - \omega_{1i})^2 + (X_2 - \omega_{2i})^2 + ... + (X_n - \omega_{ni})^2}, \tag{2}$$

де $i = 1, m$.

Потім визначається нейрон-переможець з номером k, який має максимальне значення евклідової відстані

$$D_k = \max_i D_i. \tag{3}$$

Вихідне значення нейрона-переможця дорівнює 1, а решти нейронних елементів – нулю, тобто:

$$Y_i = \begin{cases} 1, i = k \\ 0, \textit{інакше} \end{cases}. \tag{4}$$

Третій шар складається з двох лінійних нейронних елементів, які використовують лінійну функцію активації і здійснюють відображення кластерів, сформованих шаром Кохонена, в два класи. Активність вихідних нейронів характеризує атаку або нормальне, легітимне з'єднання:

$$Y_1 = \begin{cases} 1, & \textit{якщо атака} \\ 0, & \textit{інакше} \end{cases}$$
$$Y_2 = \begin{cases} 1, & \textit{якщо нормальне з`єднання} \\ 0, & \textit{інакше} \end{cases} . \quad (5)$$

У загальному випадку вихідне значення *j*-го нейрона третього шару

$$Y_j = \sum_{i=1}^{m} \omega_{ij} \cdot Y_i, \quad (6)$$

де ω_{ij} – ваговий коефіцієнт між *i*-м нейроном шару Кохонена і *j*-м нейроном лінійного шару. Всі вагові коефіцієнти мають одиничне значення.

Якщо нейрон-переможець в шарі Кохонена має номер *k*, то вихідне значення *j*-го нейрона третього шару

$$Y_j = \omega_{kj} \cdot Y_k. \quad (7)$$

Відмінною особливістю запропонованого 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, що дозволяє окремо здійснити кластеризацію атак і нормальних з'єднань в прихованому шарі.

Оскільки еталонні вихідні значення відомі, то для навчання нейромережевого детектора використано контрольоване конкурентне навчання відповідно до правила «переможець бере все». В рамках цього методу запропоновано алгоритм навчання нейромережевого детектора, який враховує особливості його структури і характеризується тим, що в процесі навчання коректна класифікація відбувається у тому випадку, коли при подачі на вхід нейронної мережі параметрів з'єднання, що відноситься до класу мережевої атаки, переможцем є один з *f* нейронів шару Кохонена, або, якщо при подачі на вхід нейронної мережі параметрів нормального з'єднання переможцем є один з *l* нейронів шару Кохонена. В даному випадку модифікація вагових коефіцієнтів проводиться згідно наступного виразу:

$$\omega_{ck}(t+1) = \omega_{ck}(t) + \gamma(X_c - \omega_{ck}(t)), \quad (8)$$

де γ – крок навчання.

У решті випадків відбувається некоректна класифікація. При цьому вагові коефіцієнти нейронів шару Кохонена модифікуються згідно виразу:

$$\omega_{ck}(t+1) = \omega_{ck}(t) - \gamma(X_c - \omega_{ck}(t)). \quad (9)$$

В процесі навчання при коректній класифікації вагові коефіцієнти нейрону-переможця посилюються, а при некоректній класифікації – послаблюються. Навчання проводиться до бажаного ступеня узгодження між вхідними і ваговими векторами, тобто до тих пір, поки значення сумарної квадратичної помилки мережі не стане мінімальним.

Для вибору структури нейронів прихованого шару і навчальної вибірки проведено експериментальні дослідження з різним співвідношенням кількості атак і кіль-

кості нормальних з'єднань в навчальній вибірці і, відповідно, різним співвідношенням кількості нейронів в шарі Кохонена. При цьому, найкращий результат показали ті детектори, для навчання яких використовувалася вибірка, що складається з 80% мережевих атак і 20% нормальних мережевих з'єднань, тобто співвідношення атак до нормальних з'єднань становить чотири до одного.

Вдосконалено метод побудови сукупного класифікатора для ієрархічної класифікації мережевих атак на основі багатоканальних нейромережевих детекторів, який базується на сумісному використанні методу головних компонент, об'єднанні та усуненні конфліктів між навченими на певний тип атаки нейромережевими детекторами. При цьому метод головних компонент – Principal Component Analysis (PCA) застосовано з метою скорочення кількості інформації при навчанні нейромережевих детекторів і аналізі мережевих з'єднань.

Для визначення числа головних компонент запропоновано використати критерій відносної інформативності

$$J = \frac{\lambda_1 + \lambda_2 + ... + \lambda_p}{\lambda_1 + \lambda_2 + ... + \lambda_n}, \qquad (10)$$

де λ_i – кількість інформації в *i*-й компоненті.

Аналізуючи за допомогою формули (10) розподіл кількості інформації, що міститься в кожній подальшій компоненті *n*, визначається число головних компонент *p*, які доцільно використовувати для подальшого аналізу без істотної втрати відносної інформативності *J*.

Проведено експериментальні дослідження, які показали, що одна головна компонента містить 52,4% інформації, дві головних компоненти - 71,7% інформації, три головних компоненти – 88,4% інформації, а 12 перших головних компонент містять 99,2% інформації про мережеві з'єднання.

Експериментально підтверджено, що для успішного навчання детекторів та аналізу мережевих з'єднань достатньо використати 12 головних компонент, а не 41 параметр. Це дозволило зменшити розмірність аналізованої інформації в 3,4 рази при втраті відносної інформативності 0,8%.

Сукупним нейромережевим детектором є такий детектор, який складається з множини нейромережевих детекторів, кожен з яких навчений на певному типі атак. Запропоновано узагальнений алгоритм функціонування сукупного нейромережевого детектора атак на ІТМ.

Оскільки виділяють 22 типи мережевих атак, які об'єднані в чотири класи (*DoS*, *U2R*, *R2L* і *Probe*), то розглянемо схему функціонування сукупного класифікатора для ієрархічної класифікації на базі 22 багатоканальних нейромережевих детекторів, які навчені на певний тип атак (рисунок 3). Стиснений набір вхідних даних розмірністю 12 поступає на нейромережеві детектори (НД), кожен з яких навчений на відповідний тип атак. Якщо детектор виявляє атаку, то вихідне значення його першого виходу встановлюється в одиничне значення. Для усунення конфліктів в роботі такого класифікатора, коли декілька детекторів встановлюються в одиничний стан, на другий вихід кожного детектора передається мінімальна евклідова відстань між вхідним образом і ваговими векторами відповідного детектора:

$$E_j = \min_j D_j = \min_i \sqrt{(x_1 - w_{1j})^2 + (x_2 - w_{2j})^2 + ... + (x_{12} - w_{12j})^2}\ . \qquad (11)$$

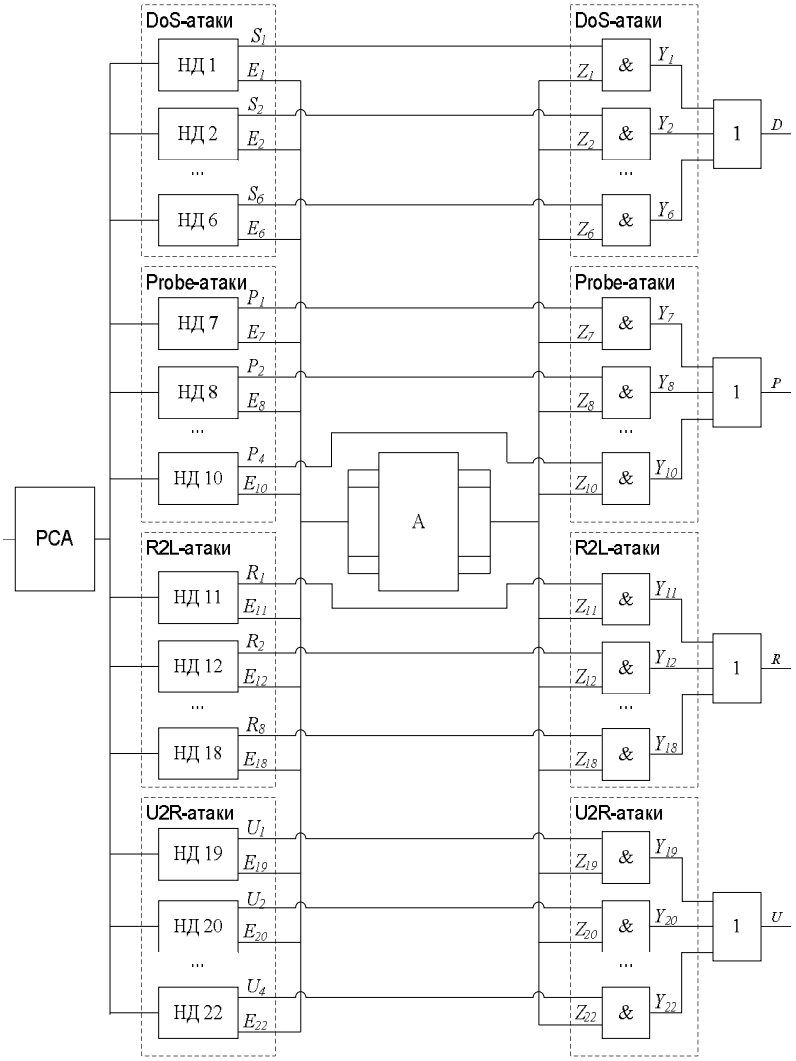


Рисунок 3 – Схема сукупного класифікатора для ієрархічної класифікації атак на ІТМ

Інформація про мінімальну евклідову відстань поступає з кожного детектора атак на арбітр *A*, який визначає детектор з номером *k*, що має мінімальну евклідову метрику:

$$E_k = \min E_j,\ j = \overline{1,22}. \quad (12)$$

В результаті *k*-й вихід арбітра встановлюється в одиничний стан, а решта виходів – в нульовий стан:

$$Z_i = \begin{cases} 1, & якщо\ i = k \\ 0, & інакше \end{cases}. \quad (13)$$

На виходах логічних елементів «І» визначається тип атаки:

$$Y_i = F_i Z_i, \quad (14)$$

$$\text{де } F_i = \begin{cases} S_i, & якщо\ i = \overline{1,6} \\ P_i, & якщо\ i = \overline{7,10} \\ R_i, & якщо\ i = \overline{11,18} \\ U_i, & якщо\ i = \overline{19,22} \end{cases}.$$

Виходи логічних елементів «АБО» визначають клас атаки:

$$D = \bigvee_{i=1}^{6} Y_i,\ \ P = \bigvee_{i=7}^{10} Y_i,\ R = \bigvee_{i=11}^{18} Y_i,\ U = \bigvee_{i=19}^{22} Y_i, \quad (15)$$

де *D – DoS*-атака, *P– Probe*-атака, *R– R2L*-атака, *U– U2R*-атака.

У **третьому розділі** запропоновано комбінований метод виявлення і класифікації атак на ІТМ, що базується на інтеграції нейромережевих детекторів у штучну імунну систему. В якості імунного детектора використано розроблений в другому розділі нейромережевий детектор, в основі якого лежить нейронна мережа LVQ, що дозволяє оперативно генерувати різноманітні імунні детектори атак різних типів. При цьому застосовано базові принципи функціонування штучної імунної системи.

Розроблений метод виявлення і класифікації атак на ІТМ можна представити сукупністю наступних кроків:

1. *Генерація імунних детекторів.* На даному кроці відбувається генерація чотирьох груп нейромережевих імунних детекторів відповідно до кількості класів атак з випадковою ініціалізацією вагових коефіцієнтів, де кожна група складається з множини детекторів:

$$D = \left\{ D_i,\ \ i = \overline{1, F_d} \right\},\ P = \left\{ P_i,\ \ i = \overline{1, F_p} \right\},\ R = \left\{ R_i,\ \ i = \overline{1, F_r} \right\},\ U = \left\{ U_i,\ \ i = \overline{1, F_u} \right\}, \quad (16)$$

де D_i, P_i, R_i, U_i – *i*-й нейромережевий імунний детектор для виявлення і класифікації *DoS*, *Probe, R2L* і *U2R*-атак відповідно;

F – загальна кількість детекторів відповідного типу.

2. *Навчання імунних детекторів.* На даному кроці згенеровані нейромережеві імунні детектори піддаються процесу навчання. Проте механізм навчання такого детектора дещо відрізняється від того, який був представлений раніше. В даному випадку для виявлення і класифікації атак певного типу може використовуватися не один навчений нейромережевий імунний детектор, а декілька, по-різному навчених детекторів, що дозволяє застосувати процедуру диверсифікації детекторів і відповідно підвищити достовірність виявлення і класифікації атак на ІТМ.

Для навчання нейромережевих імунних детекторів одного і того ж типу атаки використовуються різні навчальні вибірки, які генеруються випадковим чином з множини з'єднань, що складаються з певного типу мережевих атак і нормальних з'єднань. В результаті створюється множина різноманітних детекторів.

Нехай N – множина з'єднань, що відносяться до певного типу мережевих атак, а M – множина з'єднань, що відносяться до класу нормальних з'єднань. З них випадковим чином формується множина вхідних образів для навчання *i*-го детектора:

$$X_i = \begin{bmatrix} X_i^1 \\ X_i^2 \\ \dots \\ X_i^L \end{bmatrix} = \begin{bmatrix} X_{i1}^1 & X_{i2}^1 & \dots & X_{in}^1 \\ X_{i1}^2 & X_{i2}^2 & \dots & X_{in}^2 \\ \dots & & & \\ X_{i1}^L & X_{i2}^L & \dots & X_{in}^L \end{bmatrix}. \tag{17}$$

Відповідно, множина еталонних образів

$$e_i = \begin{bmatrix} e_i^1 \\ \mathrm{e}_i^2 \\ \dots \\ e_i^L \end{bmatrix} = \begin{bmatrix} e_{i1}^1 & e_{i2}^1 \\ e_{i1}^2 & e_{i2}^2 \\ \dots & \\ e_{i1}^L & e_{i2}^L \end{bmatrix}, \tag{18}$$

де L – розмірність навчальної вибірки.

Еталонні вихідні значення для *i*-го детектора формуються таким чином:

$$\begin{aligned} e_{i1}^k &= \begin{cases} 1, & \textit{якщо } X_i^k \in N \\ 0, & \textit{інакше} \end{cases} \\ e_{i2}^k &= \begin{cases} 1, & \textit{якщо } X_i^k \in M \\ 0, & \textit{інакше} \end{cases} \end{aligned}. \tag{19}$$

Спочатку навчання нейронної мережі проводиться до моменту мінімізації значення сумарної квадратичної помилки:

$$E_i = \frac{1}{2}\sum_{k=1}^{L}\sum_{j=1}^{2}(Y_j^k - e_j^k)^2, \tag{20}$$

де Y_j^k – *j*-е вихідне значення детектора для *k*-го вхідного образу;

e_j^k – *j*-е еталонне значення для *k*-го еталонного образу.

Потім навчання продовжується до тих пір, поки кількість навчених імунних детекторів не стане рівною заданому значенню F.

3. *Відбір імунних детекторів*. Тут для мінімізації виникнення помилкових спрацьовувань, коли нормальне з'єднання приймається за мережеву атаку, всі на-

вчені нейромережеві імунні детектори проходять перевірку на коректність. Для цього, на нейронну мережу подається заздалегідь створена тестова вибірка, що складається тільки з параметрів нормальних з'єднань. Якщо *i*-й детектор класифікує одне з тестових з'єднань, як атаку, то він знищується, а замість нього генерується і навчається новий детектор. Якщо *i*-й детектор не генерує помилкові спрацьовування на тестовій вибірці, то він вважається коректним і допускається до аналізу мережевих з'єднань. В результаті утворюється множина нейромережевих імунних детекторів для аналізу параметрів мережевих з'єднань, яка, як буде показано далі, може поповнюватися за рахунок детекторів імунної пам'яті та генерування нових детекторів після закінчення часу життя.

4. *Функціонування імунних детекторів*. На цьому кроці вся інформація, що отримується комп'ютером, спочатку аналізується сукупністю нейромережевих імунних детекторів, і, якщо жоден з детекторів не виявив аномалію, інформація обробляється операційною системою і відповідним програмним забезпеченням. Крім того, кожен детектор наділяється часом життя, впродовж якого він аналізує мережеві з'єднання. Якщо після закінчення виділеного часу детектор не виявив аномалію, він знищується, а на його місці створюється новий детектор. Механізм наділення детекторів часом життя дозволяє позбуватися від детекторів, які хоч і пройшли успішно стадії навчання і відбору, проте із-за своєї структурної особливості (набору вагових коефіцієнтів) є малопридатними.

Якщо мережеве з'єднання класифікується сукупністю нейромережевих імунних детекторів як мережева атака, то відбувається реагування на атаку (наприклад, блокування з'єднання, в результаті чого воно не допускається до обробки операційною системою і програмним забезпеченням). При цьому видається повідомлення користувачу про спробу атаки на комп'ютерну систему.

5. *Формування імунної пам'яті.* При виявленні і блокуванні мережевої атаки доцільно зберегти її параметри з метою подальшого детального аналізу. Справа в тому, що НІД навчаються на обмеженому наборі даних, які не можуть включати всі ймовірні мережеві атаки. Тому на цьому кроці для підвищення достовірності виявлення і класифікації атак та забезпечення гнучкості системи, параметри мережевого з'єднання, класифікованого як невідома атака, зберігаються і заносяться в навчальну вибірку, тим самим, поповнюючи її актуальними даними. Новостворені детектори вже навчатимуться, зокрема, і на нових даних. Крім цього, на основі детектора, який виявив атаку, створюється новий детектор (операція клонування), який навчається на даних, виділених з виявленої атаки (операція мутації), і вводиться в систему виявлення та класифікації атак на ІТМ. Це дозволяє точніше виділити дану атаку при повторній подібній атаці на комп'ютерну систему. Сукупність детекторів імунної пам'яті зберігає в собі інформацію про всі невідомі мережеві атаки, направлені в минулому на комп'ютерну систему, і забезпечує високий рівень реагування на повторні спроби атак.

Результати проведених експериментів по дослідженню узагальнюючої властивості нейромережевих імунних детекторів показали, що навчені детектори виявляють і класифікують не тільки атаки, на яких детектори навчалися, але і атаки інших типів. Достовірність виявлення і класифікації невідомих атак, в окремих випадках, може досягати 100% (таблиця 1).

Таблиця 1 – Результати узагальнюючої властивості нейромережевих імунних детекторів

Тип атаки	Детектор 1 (навчений на *DoS_back*), %	Детектор 2 (навчений на *Probe_portsweep*), %	Детектор 3 (навчений на *R2L_ftpwrite*), %
DoS-атаки			
Back	100,0	0,0	0,3
Land	0,0	100	23,8
Neptune	99,1	100	0,0
Probe-атаки			
Portsweep	2,1	100	0,1
Satan	13,3	92,2	2,1
R2L-атаки			
Spy	100,0	0,0	0,0
Ftp_write	0,0	0,0	100
U2R-атаки			
Loadmodule	88,9	0,0	0,0

Проведено експериментальні дослідження адаптації нейромережевих імунних детекторів до невідомих атак в результаті операції клонування та мутації. Для цього в якості батьківського детектора вибрано детектор 2, який навчався на атаці типу *DoS_land*. Даний детектор виявив невідомі для нього атаки – *R2L_imap* і *Probe_portsweep*. Припустивши, що в базі даних такі атаки відсутні, згенеруємо два нових детектори А1 і А2, додамо параметри виявлених атак в навчальні вибірки для цих детекторів і навчимо відповідні детектори-клони (таблиця 2).

Таблиця 2 – Адаптація нейромережевих імунних детекторів до невідомих атак

Тип атаки	Детектор 2, Sp(TNR)= 99,0%	Детектор А1, Sp(TNR)= 99,1%	Детектор А2, Sp(TNR)= 98,9%
	Se (TPR),%	*Se (TPR),%*	*Se (TPR),%*
DoS-атаки			
Land	100,0	100,0	100,0
Pod	2,3	0,0	31,8
Probe-атаки			
Ipsweep	7,22	0,2	33,9
Portsweep	15,9	2,6	55,3
Satan	11,0	31,3	11,0
R2L-атаки			
Imap	83,3	91,7	83,3
Multihop	0,0	0,0	14,3
U2R-атаки			
Perl	0,0	66,7	0,0
Rootkit	0,0	20,0	0,0

Із таблиці 2 видно, що детектор А1 почав краще виявляти атаки окремих класів, зокрема *Probe_satan* - в 2,8 раза, а *R2L_imap* на 8,4%, а також він почав виявляти атаки класів *U2R_perl* і *R2L_rootkit*. В свою чергу детектор А2 показав кращі результати на атаках класів *Probe_ipsweep, DoS_pod, Probe_portsweep, R2L_multihop*.

При проведені експериментальних досліджень розмір навчальної вибірки склав 80 векторів (64 – атака одного з типів і 16 – нормальні з’єднання), тестової вибірки – множина записів бази KDD в розрізі типів, структура мережі LVQ – 12-10-2.

Таким чином, експериментально підтверджено, що нейромережеві імунні детектори здатні виявляти та адаптуватися до невідомих типів атак, що дозволило підвищити достовірність виявлення і класифікації невідомих атак на ІТМ в 2–3 рази.

У **четвертому розділі** на основі запропонованих методів та засобів розроблено інтелектуальну інформаційну технологію виявлення і класифікації атак на ІТМ, яка характеризується генеруванням множини нейромережевих імунних детекторів для кожного типу мережевої атаки. Цю технологію реалізовано в рамках нейромережевої імунної системи виявлення і класифікації атак (рисунок 4), алгоритми функціонування якої описано в дисертаційній роботі.

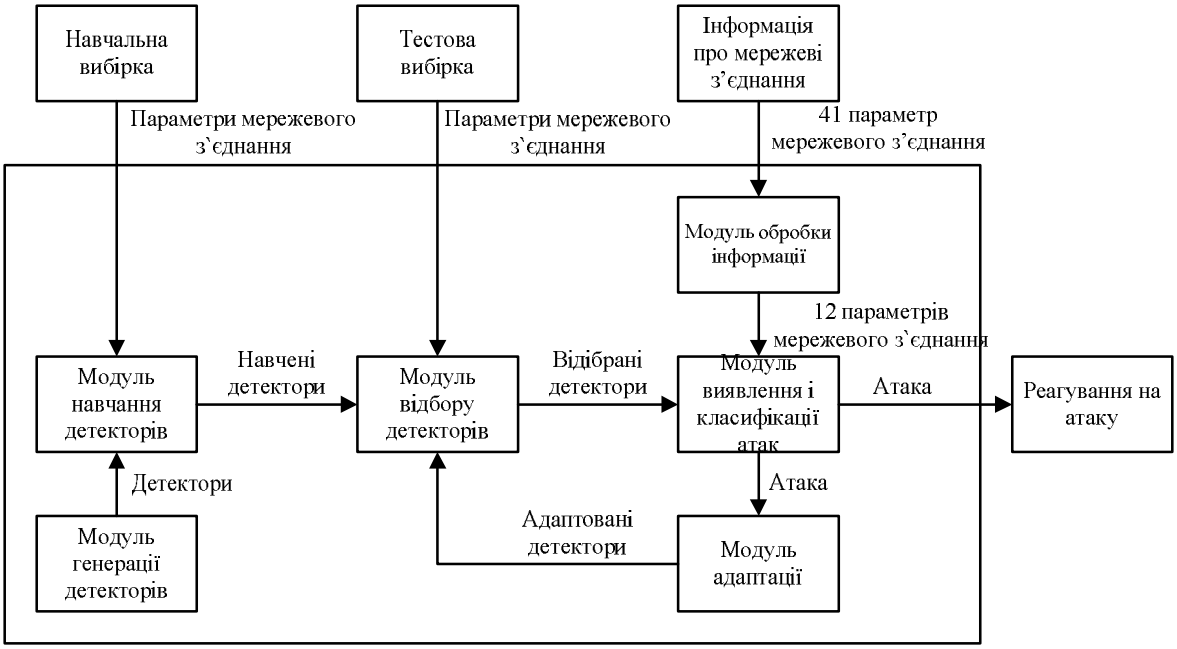


Рисунок 4 – Структура нейромережевої імунної системи виявлення і класифікації атак на ІТМ

Виконано статистичну оцінку достовірності запропонованої інтелектуальної інформаційної технології виявлення і класифікації атак на ІТМ на основі ROC-аналізу. Результати оцінки достовірності розглянуто на прикладі одного нейромережевого імунного детектора, навченого на атаці *DoS_neptune* (таблиця 3).

Таблиця 3 – Характеристики нейромережевого імунного детектора 1

Детектор 1 навчання на *DoS_neptune*. Sp (TNR) = 99,9%, FPR = 0,1%			
Тип атаки	*Se (TPR),%*	*FNR,%*	*Accu,%*
DoS-атаки			
Land	100,0	0,0	100,0
Neptune	100,0	0,0	100,0
Teardrop	3,7	96,3	51,8
Probe-атаки			
Ipsweep	6,5	93,5	53,2
Portsweep	98,9	1,1	99,4
Satan	90,0	10,0	95,0

ROC-криві, що відображають здатність детектора 1 виявляти і класифікувати мережеві атаки певних типів, приведені на рисунку 5.

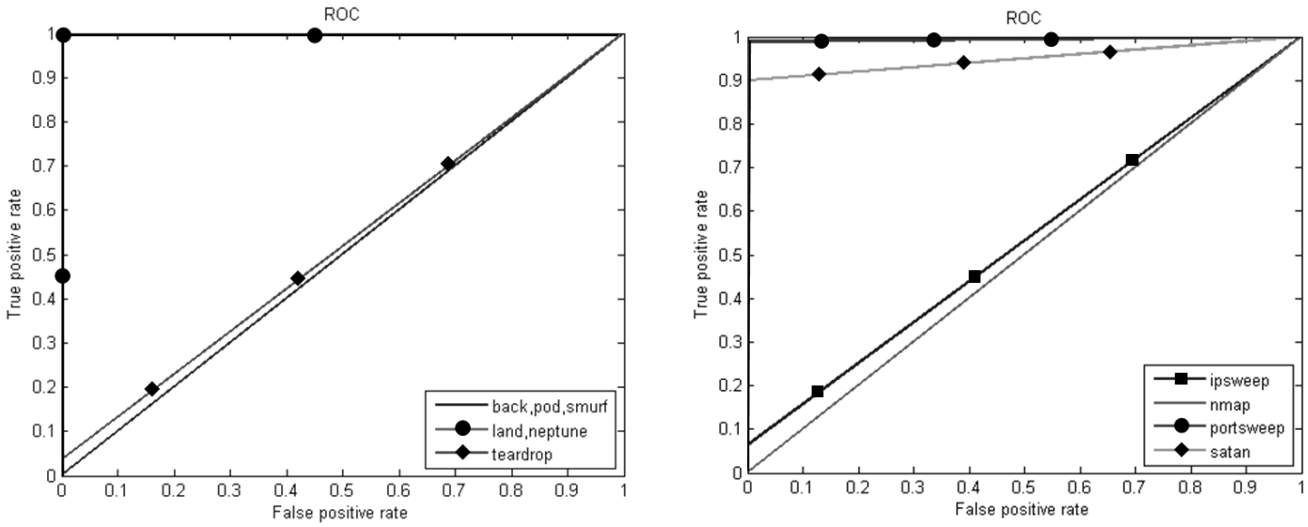


Рисунок 5 – ROC-криві виявлення і класифікації атак нейромережевим імунним детектором 1

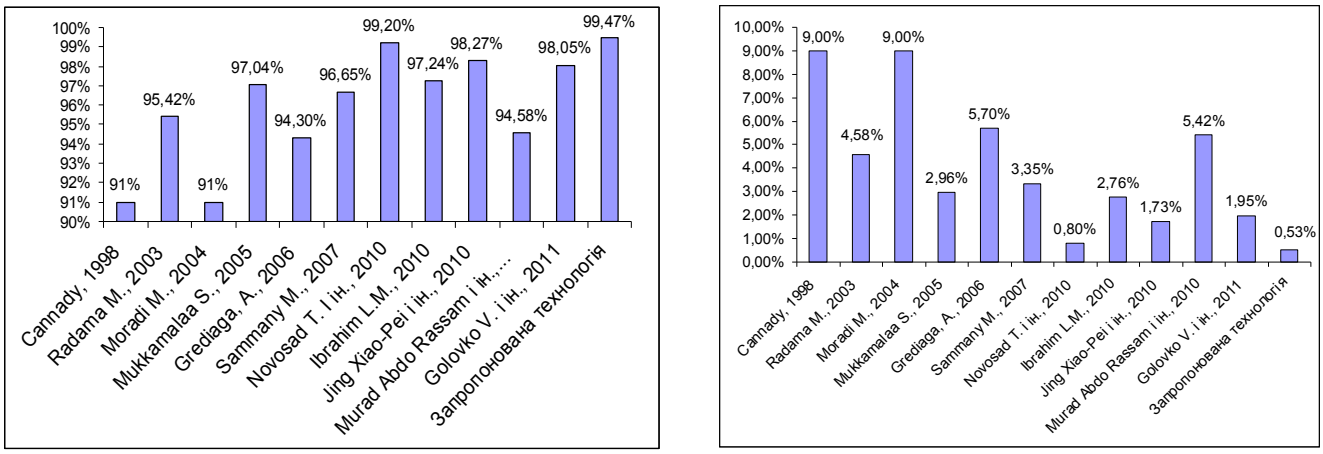
Як видно з таблиці 3 і рисунку 5, достовірність виявлення і класифікації атак типу *DoS_neptune* детектором 1 склала 100% при рівні помилок другого роду (FPR) – 0,1%. Окрім цього, достовірність виявлення і класифікації атак *DoS_land* склала 100%, *Probe_portsweep* – 98,9%, *Probe_satan* – 90,0% і *Probe_ipsweep* – 6,5%.

Достовірність виявлення і класифікації мережевих атак сукупністю нейромережевих імунних детекторів в розрізі типів представлено в таблиці 4.

Таблиця 4 – Достовірність виявлення і класифікації мережевих атак

d_back	d_land	d_neptune	d_pod	d_smurf	d_teardrop	p_ipsweep	p_nmap
100	100	100	100	100	100	99,90	100
p_prtsweep	p_satan	r_ftpwrite	r_gpasswd	r_imap	r_multihop	r_phf	r_spy
99,99	99,99	100	99,85	99,89	99,30	100	100
r_wclient	r_wmaster	u_overflw	u_ldmodul	u_perl	u_rootkit		
99,50	99,60	99,20	100	100	98,60		

Проведено порівняльний аналіз інтелектуальної інформаційної технології виявлення і класифікації атак на ІТМ з існуючими технологіями (рисунок 6).



а *б*

Рисунок 6 – Результати порівняльного аналізу інтелектуальної технології виявлення і класифікації атак на ІТМ з відомими технологіями: *а* – достовірність виявлення і класифікації атак, *б* – помилка першого роду (ймовірність пропуску атак)

Результати експериментальних досліджень підтверджують вірність наукових положень запропонованої інформаційної технології, оскільки її впровадження дало можливість підвищити достовірність виявлення і класифікації атак на ІТМ на 0,27-8,5% у порівнянні з відомими рішеннями. При цьому рівень помилок першого роду (ймовірність пропуску атаки) склав 0,53%, тобто рівень даних помилок знижено не менше як в 1,5 рази, а рівень помилок другого роду (ймовірність помилкових спрацювань) склав 0,6%. Що торкається достовірності виявлення і класифікації невідомих атак, то вона, в окремих випадках, може досягати 100%.

ВИСНОВКИ

У дисертаційній роботі вирішено актуальну задачу розробки і дослідження інтелектуальної інформаційної технології на базі теорії штучних нейронних мереж і штучних імунних систем з метою підвищення достовірності виявлення і класифікації атак на ІТМ.

При цьому отримані наступні основні результати:

1. На основі огляду відомих підходів і порівняльного аналізу існуючих інформаційних технологій виявлення і класифікації атак на ІТМ обгрунтовано доцільність створення нової інформаційної технології на базі штучних нейронних мереж і штучних імунних систем з використанням, в якості тестових наборів, часто вживаної бази даних KDD. Показано, що одним з основних критеріїв оцінки ефективності інформаційної технології виявлення і класифікації мережевих атак є достовірність результатів її функціонування, тому в якості засобу оцінки достовірності результатів запропоновано вибрати ROC-аналіз. На цій основі обґрунтовано шляхи вдосконалення методів виявлення і класифікації атак на ІТМ та сформульовано задачі дослідження.

2. Запропоновано узагальнену функціональну модель прийняття рішень при виявленні і класифікації атак на ІТМ у розрізі наступних етапів: отримання параметрів мережевих з’єднань, обробка інформації, формування рішення нейромережевим аналізатором, що дозволило підвищити достовірність виявлення і класифікації мережевих атак.

3. На базі результатів теоретичних та експериментальних досліджень можливих нейронних мереж для виявлення і класифікації атак на ІТМ, в якості основи нейромережевого детектора, вибрано нейронну мережу векторного квантування LVQ з нейронними елементами Кохонена в прихованому шарі, що дозволило суттєво зменшити розмірність навчальної вибірки (в кращому випадку до 20 векторів) і, відповідно, час навчання.

4. Розроблено та досліджено метод побудови нейромережевих детекторів атак, який базується на нейронній мережі векторного квантування LVQ, де 80% нейронних елементів Кохонена в прихованому шарі відповідають типу атаки, а решта – нормальному з’єднанню. Запропонований метод характеризується малим об’ємом навчальної вибірки і структурою нейронної мережі, в якій співвідношення атак і нормальних з’єднань дорівнює 4:1, що дозволило окремо здійснити кластеризацію атак і нормальних з'єднань в прихованому шарі в порівнянні з іншими підходами, а в результаті підвищити достовірність виявлення і класифікації атак на ІТМ. В рамках цього методу розроблено алгоритм навчання нейромережевого детектора, який вра-

ховує особливості його структури.

5. Розроблено та досліджено метод побудови сукупного класифікатора для ієрархічної класифікації атак на ІТМ на основі багатоканальних нейромережевих детекторів, що дало можливість зменшити розмірність аналізованої інформації в 3,4 рази при втраті відносної інформативності 0,8% за рахунок стиснення вхідної інформації (для отримання найбільш інформативних ознак), а також класифікувати мережеві атаки за рахунок об'єднання навчених на певний тип атаки нейромережевих детекторів. Запропонований метод дозволив усунути конфлікти в роботі нейромережевих детекторів.

6. Розроблено та досліджено комбінований метод, який базується на інтеграції нейромережевих детекторів в штучну імунну систему, що дозволило нейромережевим імунним детекторам адаптуватися до невідомих атак на ІТМ за рахунок здійснення операцій клонування і мутації, а також підвищило достовірність виявлення і класифікації невідомих атак в 2-3 рази.

7. На основі запропонованих методів розроблено інтелектуальну інформаційну технологію, яка практично реалізована в рамках нейромережевої імунної системи виявлення і класифікації як відомих, так і невідомих атак на ІТМ, характеризується генеруванням множини нейромережевих детекторів для кожного типу мережевої атаки. Розроблені алгоритми функціонування системи.

8. Результати експериментальних досліджень підтверджують вірність наукових положень дисертаційної роботи, а впровадження запропонованої інформаційної технології дало можливість підвищити достовірність виявлення і класифікації атак на ІТМ на 0,27-8,5% у порівнянні з відомими рішеннями. При цьому рівень помилок першого роду (ймовірність пропуску атаки) склав 0,53%, тобто рівень даних помилок знижено не менше як в 1,5 рази, а рівень помилок другого роду (ймовірність помилкових спрацювань) – 0,6%. Що торкається достовірності виявлення і класифікації невідомих атак, то вона, в окремих випадках, може досягати 100%.

9. Теоретичні та практичні результати, отримані в дисертаційній роботі, використані приватним підприємством «МагнетікВан» (м. Тернопіль), товариством з обмеженою відповідальністю «СофтІнвест» (м. Брест, Республіка Білорусь), Науково-дослідним інститутом інтелектуальних комп’ютерних систем в рамках науково-дослідної роботи, а також в рамках двостороннього договору про партнерство, співпрацю і науковий обмін між Тернопільським національним економічним університетом і Брестським державним технічним університетом і в навчальному процесі Тернопільського національного економічного університету.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Комар М.П. Інтелектуалізована інформаційна технологія виявлення комп’ютерних атак / М.П. Комар, Д.І. Боднар, А.О. Саченко // Вимірювальна та обчислювальна техніка в технологічних процесах. – 2010. – №2. – С. 133–137.

2. Комар М.П. Нейромережевий метод ідентифікації комп’ютерних атак / М.П. Комар // Оптико-електронні інформаційно-енергетичні технології. – 2010. – №2. – С. 105–109.

3. Комар М.П. Методы искусственных иммунных систем и нейронных сетей

для обнаружения компьютерных атак / М.П. Комар // Інформаційна безпека. – 2011. – №1(5). – С. 154–160.

4. Комар М.П. Інтелектуальна система виявлення мережевих атак на інформаційні ресурси на основі методу головних компонент / М.П. Комар // Системи обробки інформації. – 2011. – №8(98). – С. 203–207.

5. Комар М.П. Інтелектуальна інформаційна технологія виявлення мережевих атак у системі реального часу / М.П. Комар // Радіоелектронні і комп'ютерні системи. – 2011. – № 4(52). – С. 92–98.

6. Комар М.П. Метод построения совокупного классификатора трафика информационно-телекоммуникационных сетей для иерархической классификации компьютерных атак / М.П. Комар // Системи обробки інформації. – 2012. – №3(101). – С. 134–138.

7. Пат. №74822 Україна, МПК(2012) H04W 12/08, G06F 21/00, G06F 12/14. Спосіб виявлення комп'ютерних атак нейромережевою штучною імунною системою / Комар М. П., Саченко А. О., Головко В. А., Безобразов С. В.; заявник і патентовласник Тернопільський національний економічний університет. – № u201205349 ; заявл. 28.04.12 ; опубл. 12.11.12, Бюл. № 21.

8. Комар М.П. Нейросетевой подход к обнаружению компьютерных атак на информационные ресурсы / М.П. Комар, И.О. Палий, Р.П. Шевчук, Т.Б. Федысив // Інформатика та математичні методи в моделюванні. – 2011. – Т. 1, №2. – С. 156–163.

9. Комар М.П. Система анализа сетевого трафика для обнаружения компьютерных атак / М.П. Комар // Вестник Брестского государственного технического университета: Физика, математика и информатика. – 2010. – №5. – С. 14–16.

10. Komar M. Intelligent System for Detection of Networking Intrusion / M. Komar, V. Golovko, A. Sachenko, S. Bezobrazov // Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS-2011): IEEE international conference, 15–17 September 2011. – Prague, Czech Republic, 2011. – V1. – P. 374–377.

11. Комар М.П. Інтеграція нейромереж та штучних імунних систем для виявлення комп'ютерних атак / М.П. Комар, А.О. Саченко, В.А. Головко, Т.Г. Фортуна // Захист інформації і безпека інформаційних систем: міжнар. наук.-техн. конф., 31 травня – 01 червня 2012 р.: тези доп. – Львів, 2012. – С. 108–109.

12. Komar M. Method of Aggregate Classifier Construction for Hierarchical Classification of Computer Attacks / V. Golovko, O. Lyashenko, A. Sachenko // CAD in Machinery Design. Implementation and Educational Issues (CADMD 2012): international conference, 11-13 October 2012: proceedings. – Lviv, Ukraine, 2012. – P. 80–82.

13. Golovko V. Principles of Neural Network Artificial Immune System Design to Detect Attacks on Computers / V. Golovko, M. Komar, A. Sachenko // Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET'2010): international conference, 23-27 February, 2010: proceedings. – Lviv-Slavsko, Ukraine, 2010. – P. 237.

14. Комар М.П. Методы искусственных нейронных сетей для обнаружения сетевых вторжений / М.П. Комар // Internet–Education–Science (IES-2010): international conference, September 28 – October 3, 2010: proceedings. – Vinnytsia, Ukraine, 2010. – V1. – P. 410–413.

15. Комар М.П. Алгоритми штучних нейронних мереж для виявлення мережевих вторгнень / М.П. Комар // Актуальні задачі сучасних технологій: міжнар. наук.-техн. конф., 21-22 грудня 2010 р.: тези доп. – Тернопіль, 2010. – С. 89.

16. Комар М.П. Використання методу головних компонент для вирішення задачі виявлення комп'ютерних атак / М.П. Комар // Методи та засоби кодування, захисту й ущільнення інформації: міжнар. наук.-практ. конф., 20-22 квітня 2011 р.: тези доп. – Вінниця, 2011. – С. 131–132.

17. Комар М.П. Інформаційна модель процесу виявлення комп'ютерних атак на основі нейромережевих класифікаторів / М.П. Комар // Обчислювальний інтелект (результати, проблеми, перспективи) (ОІ-2011): міжнар. наук.-техн. конф., 10-13 травня 2011 р.: тези доп. – Черкаси, 2011. – С. 179–180.

18. Golovko V. Evolution of Immune Detectors in Intelligent Security System for Malware Detection / V. Golovko, S. Bezobrazov, V. Melianchuk, M. Komar // Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS-2011): IEEE international conference, 15–17 September 2011. – Prague, Czech Republic, 2011. – V2. – P. 722–726.

19. Комар М.П. Підхід до ідентифікації комп'ютерних атак засобами інтелектуальних інформаційних технологій / М.П. Комар // Комп'ютерні системи та мережеві технології (CSNT-2009): міжнар. наук.-техн. конф., 10-12 червня 2009 р.: тези доп. – К.: «НАУ-друк», 2009. – С.53.

20. Комар М.П. Использование искусственных иммунных систем и нейронных сетей для обнаружения компьютерных атак / М.П. Комар // Современные проблемы математики и вычислительной техники: республ. научн. конф. молодых ученых и студентов, 26-28 ноября 2009 г.: тезисы докл. – Брест, Республика Беларусь, 2009. – Т.1. – С. 16–18.

АНОТАЦІЯ

Комар М.П. Інтелектуальна інформаційна технологія виявлення і класифікації атак на інформаційні телекомунікаційні мережі. – На правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.06 – інформаційні технології. – Тернопільський національний економічний університет, Тернопіль, 2012.

Дисертація присвячена актуальним питанням розробки нових методів виявлення і класифікації атак на інформаційні телекомунікаційні мережі (ІТМ) шляхом використання штучних нейронних мереж і штучних імунних систем і практичної реалізації розробленої на їх основі інтелектуальної інформаційної технології, а також оцінці її достовірності.

Вдосконалено метод побудови нейромережевого детектора атак на ІТМ на основі нейромережі векторного квантування, який використовує 80% нейронних елементів в прихованому шарі, які відповідають типу атаки, а останні – нормальному з'єднанню, яка характеризується малим об'ємом навчальної вибірки.

Для ієрархічної класифікації мережевих атак вдосконалено метод побудови сукупного класифікатора на основі багатоканальних нейромережевих детекторів, який поєднує використання методу головних компонент, об'єднання і усунення

конфліктів між навченими на певний тип атак нейромережевими детекторами, що дозволило зменшити розмірність аналізованої інформації та класифікувати мережеві атаки.

Розроблено комбінований метод на основі інтеграції нейромережевих детекторів в штучну імунну систему, що дозволило НІД адаптуватися до невідомих атак на ІТМ за рахунок здійснення операцій клонування і мутації.

На основі запропонованих методів отримала подальший розвиток інтелектуальна інформаційна технологія виявлення і класифікації атак на ІТМ шляхом використання базових принципів функціонування імунної системи з метою формування найкращої популяції детекторів, яка характеризується генеруванням множини детекторів для кожного типу мережевої атаки.

Ключові слова: інформаційна телекомунікаційна мережа, нейронна мережа, штучна імунна система, нейромережевий імунний детектор, інтелектуальна інформаційна технологія, нейромережева імунна система.

АННОТАЦИЯ

Комар М.П. Интеллектуальная информационная технология обнаружения и классификации атак на информационные телекоммуникационные сети. – На правах рукописи.

Диссертация на соискание ученой степени кандидата технических наук по специальности 05.13.06 – информационные технологии. – Тернопольский национальный экономический университет, Тернополь, 2012.

Диссертация посвящена актуальным вопросам разработки новых методов обнаружения и классификации атак на информационные телекоммуникационные сети (ИТС) путем использования искусственных нейронных сетей и искусственных иммунных систем и практической реализации разработанной на их основе интеллектуальной информационной технологии, а также оценке ее достоверности.

Усовершенствован метод построения нейросетевого детектора атак на ИТС на основе нейросети векторного квантования, который использует 80% нейронных элементов в скрытом слое, которые отвечают типу атаки, а последние – нормальному соединению, которая характеризуется малым объемом обучающей выборки, что позволило отдельно осуществить кластеризацию атак и нормальных соединений в скрытом слое и повысить достоверность обнаружения атак при малом объеме обучающей выборки.

Для иерархической классификации сетевых атак усовершенствован метод построения совокупного классификатора на основе многоканальных нейросетевых детекторов, который совместно использует метод главных компонент, объединение и устранение конфликтов между нейросетевыми детекторами, каждый из которых обучен на определенный тип атаки, что позволило уменьшить размерность анализируемой информации и классифицировать сетевые атаки.

Разработан комбинированный метод на основе интеграции нейросетевых детекторов в искусственную иммунную систему, что позволило им адаптироваться к неизвестным атакам за счет осуществления операций клонирования и мутации с целью повышения достоверности их обнаружения и классификации.

В диссертации на основе предложенных методов получила дальнейшие развитие интеллектуальная информационная технология обнаружения и классификации атак на ИТС путем использования базовых принципов функционирования иммунной системы с целью формирования наилучшей популяции детекторов, которая характеризуется генерированием множественного числа детекторов для каждого типа сетевой атаки, что позволило повысить достоверность обнаружения и классификации как известных, так и неизвестных сетевых атак.

Ключевые слова: информационная телекоммуникационная сеть, нейронная сеть, искусственная иммунная система, нейросетевой иммунный детектор, интеллектуальная информационная технология, нейросетевая иммунная система.

ANNOTATION

Myroslav P. Komar. Intelligent Information Technology for Attacks Detection and Classification in Information Telecommunication Networks. – Manuscript.

Thesis for the Ph.D (candidate of technical sciences) degree in speciality 05.13.06 - Information Technology. – Ternopil National Economic University, Ternopil, 2012.

The thesis is devoted to topical issues of the development of new methods for the detection and classification of attacks on information telecommunication networks (ITN) by using artificial neural networks and artificial immune systems, and implementation of intelligent information technology that is based on mentioned above, and the assessment of its reliability.

The method designing the neural network detector attacks on ITN is improved, and it's based on neural network of vector quantization which uses 80% of the neural elements in the hidden layer that meet the type of attack, and the last – to the normal connection which is characterized by a small number of the training set.

The method designing a comprehensive classifier is improved for the hierarchical classification of network attacks. This method is based on multi-channel neural network detectors, which is uniting the principal component analysis, consolidation and elimination of conflicts between the neural network detectors, each of which is trained for a certain type of attack, which allowed reducing the dimension of the analyzed information and classifying the network attacks.

There is developed a combined method that is based on the integration of neural network detectors in an artificial immune system, this allowing them to adapt to unknown attacks with the help of cloning and mutation operations.

On the basis of proposed methods was developed further intelligent information technology for detecting and classifying attacks on ITN by using the basic principles of the immune system in order to create the best population of detectors. Developed technology is characterized by the generating the detectors set per each type of network attack.

Keywords: information telecommunication networks, neural network, artificial immune systems, neural network immune detector, intelligent information technology, neural network immune system.