УДК 004.056.53; 004.89

М.П. КОМАР

Тернопільський національний економічний університет, Україна

ІНТЕЛЕКТУАЛЬНА ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ВИЯВЛЕННЯ МЕРЕЖЕВИХ АТАК У СИСТЕМІ РЕАЛЬНОГО ЧАСУ

Розроблена структура та алгоритми функціонування нейромережевої імунної системи виявлення мережевих атак, що складається з підсистем попередньої обробки трафіку, створення, навчання і відбору детекторів, аналізу трафіку і виявлення мережевих атак, адаптації. Запропонований спосіб адаптації розробленої системи до зміни тенденцій організації мережевих атак, що дозволяє виявляти нові, раніше невідомі атаки, аналізувати їх і адаптуватися під нові реалії з метою підвищення якості виявлення. Запропонована реалізація основних блоків нейромережевої імунної системи виявлення мережевих атак, яка базується на модульному принципі. Проведені експерименти по тестуванню запропонованої системи, які показують здатність нейромережевих імунних детекторів ефективно виявляти різнотипні мережеві атаки.

Ключові слова: *інтелектуальна інформаційна технологія, мережева атака, нейронна мережа, імунна система, мережевий трафік, нейромережевий імунний детектор.*

Вступ

На сьогоднішній день кіберзлочинці продовжують удосконалювати і розвивати методи і засоби організації мережевих вторгнень, тому комп'ютерні системи безперервно піддаються різного роду атакам і користувач не може бути впевнений у захищеності важливої інформації. Традиційні методи виявлення мережевих атак нездатні забезпечити надійний захист комп'ютерних систем. Ситуація, що склалася стимулює пошук і розробку нових методів і рішень, спрямованих на підвищення рівня захищеності комп'ютерних систем від шкідливих впливів.

Методи штучного інтелекту дозволяють створювати принципово нові засоби виявлення мережевих атак на комп'ютерні системи, засновані на застосуванні нейронних мереж [1, 2] та штучних імунних систем [3], а також будувати на їх основі інтелектуальні інформаційні технології виявлення мережевих вторгнень, що дозволить підвищити рівень захищеності комп'ютерних систем від несанкціонованого впливу.

В попередніх роботах [4 – 6] розроблена і представлена система аналізу мережевого трафіку, що базується на нейромережевих методах виявлення мережевих атак. Для збільшення швидкодії в таких системах, а також для підвищення якості виявлення мережевих атак запропоновано метод головних компонент [7, 8]. В роботі [9] представлена інтеграція методів штучних імунних систем та нейронних мереж для виявлення мережевих атак, що дозволяє збільшити надійність виявлення атак, а також робить систему захисту більш гнучкою і здатною до навчання, що дозволяє їй адаптуватися до виявлення нових, раніше не відомих типів атак.

Метою дослідження є розробка структури та алгоритмів функціонування нейро-імунної системи виявлення мережевих атак, що включає підсистему попередньої обробки трафіку, підсистему створення, навчання і відбору детекторів, підсистему аналізу трафіку і виявлення мережевих атак, підсистему адаптації та реалізація основних блоків запропонованої системи на базі модульного принципу.

Структура та алгоритми функціонування нейромережевої імунної системи виявлення мережевих атак

Нейромережева імунна система виявлення мережевих атак складається з наступних основних підсистем:

1. Підсистема попередньої обробки мережевого трафіку.
2. Підсистема створення, навчання і відбору імунних нейромережевих детекторів.
3. Підсистема аналізу мережевого трафіку і виявлення мережевих атак.
4. Підсистема адаптації.

Розглянемо більш детально кожну з описаних підсистем.

Підсистема попередньої обробки трафіку призначена для представлення параметрів трафіку в зручному для аналізу вигляді. Вона складається з двох модулів – модуля захоплення мережевого трафіку в комп'ютерній мережі і модуля обчислення

головних компонент з параметрів захопленого трафіку.

Для захоплення мережевого трафіку використовується спеціалізоване програмне забезпечення, так званий сніфер (sniffer) [10]. Сніфер (аналізатор трафіку) – це програмний мережевий аналізатор трафіку, призначений для перехоплення і подальшого аналізу мережевого трафіку.

Захоплений сніфером мережевий трафік аналізується – з нього виділяється 41 параметр мережевого з'єднання, які і характеризують дане з'єднання і включають час роботи з'єднання, тип протоколу, тип служби, кількість переданих байт і т.д.

Оскільки, різні параметри мережевого з'єднання мають різний тип інформації (наприклад, параметр «час роботи з'єднання» задається в секундах, «тип протоколу» - в символьному вигляді, а «кількість байт від джерела до приймача» задається в байтах), то для того, щоб аналізувати такі різнорідні дані, їх треба привести до загального вигляду. Перш ніж поступити на вхід модуля обчислення головних компонент параметри мережевого з'єднання піддаються процедурі перетворення (символьні значення перетворюються в цілочисельні).

Як було показано в [7, 8], 41 параметр мережевого трафіку є зайвими, і для успішного аналізу трафіку з метою виявлення мережевих атак необхідно скоротити кількість аналізованих параметрів. Для зменшення розмірності аналізованих даних використовується модуль, що виконує виділення головних компонент. Модуль PCA є програмною реалізацією математичного методу обчислення головних компонент і призначений для скорочення розміру аналізованих даних, що приводить до підвищення якості виявлення мережевих атак і швидкості аналізу мережевих пакетів. На вхід модуля поступають дані з сніфера – 41 параметр мережевого з'єднання. На виході модуля PCA, після виконання всіх перетворень і обчислень, отримуємо дані, які є 12 головними компонентами. Як було показано в [7, 8], в 12 головних компонентах параметрів мережевого трафіку міститься 99,9% інформації.

В результаті, на вхід підсистеми попередньої обробки мережевого трафіку подається мережеве з'єднання в такому вигляді як воно є, а на виході з підсистеми отримуємо дані, які знаходяться в зручній для аналізу формі. Далі вони передаються в підсистему аналізу трафіку і виявлення мережевих атак.

Підсистема створення, навчання і відбору детекторів призначена для створення нейромережевих імунних детекторів, які є основними елементами виявлення мережевих атак. Кожен окремий імунний детектор є штучною нейронною мережею [4, 5]. Опишемо функціонування даної підсистеми, починаючи із створення нейромережевого імунного детектора і закінчуючи впровадженням коректного детектора в підсистему аналізу мережевого трафіку.

Модуль створення детекторів призначений для генерації нейронних мереж, які і складають основу детекторів. На вхід даного модуля подаються такі дані як: кількість нейронів в першому шарі і кількість нейронів в прихованому шарі. Далі модуль генерує нейронну мережу із заданими параметрами і ініціалізує вагові коефіцієнти між нейронними елементами згідно випадковому розподілу.

Нейронна мережа, що згенерована і проініціалізована, подається на вхід модуля навчання детекторів, завданням якого є навчити детектор коректно класифікувати образи нормальних мережевих з'єднань і мережевих атак. Для цього на вхід модуля навчання також подаються дані з навчальної вибірки, які і складають навчальну вибірку для навченого детектора. Слід зазначити, що дані з навчальної вибірки для навчання кожної нейронної мережі вибираються випадковим чином і, отже, є унікальними для кожної окремої нейронної мережі, що забезпечує велику структурну різноманітність нейромережевих імунних детекторів.

Для навчання однієї нейронної мережі використовується дані, що складаються з 64 з'єднань з одного з чотирьох класів комп'ютерних атак (що складає 80 відсотків зі всіх навчальних даних для нейронної мережі) і 16 з'єднань, що відносяться до класу легітимних мережевих з'єднань (що складає 20 відсотків навчальної вибірки). Дане співвідношення класів в навчальній вибірці було отримане експериментальним шляхом і показало якнайкращі результати.

В результаті, кожна нейронна мережа навчається на параметрах 80 мережевих з'єднань. При навчанні нейронної мережі використовується контрольоване конкурентне навчання [1, 2] відповідно до правила «переможець бере все». Тобто дані з навчальної вибірки, сформованої спеціально для даної нейронної мережі, послідовно подаються на її вхід і залежно від узгодженості поданих даних і даних на виході нейронної мережі коректуються вагові коефіцієнти відповідно до формул (3) і (4) представлених в [9].

Процес навчання нейронної мережі проводиться до бажаного ступеня узгодження між вхідними і ваговими векторами. Якщо в процесі навчання не відбувається досягнення бажаного значення середньоквадратичної помилки відповідно до формули (5) представленої в [9], то вважається, що нейронна мережа не здатна навчитися, і вона знищується. На рис. 1 відображені графіки зміни середньоквадратичної помилки в процесі навчання нейронної мережі.

Час навчання однієї нейронної мережі складає в середньому 1–3 секунди.

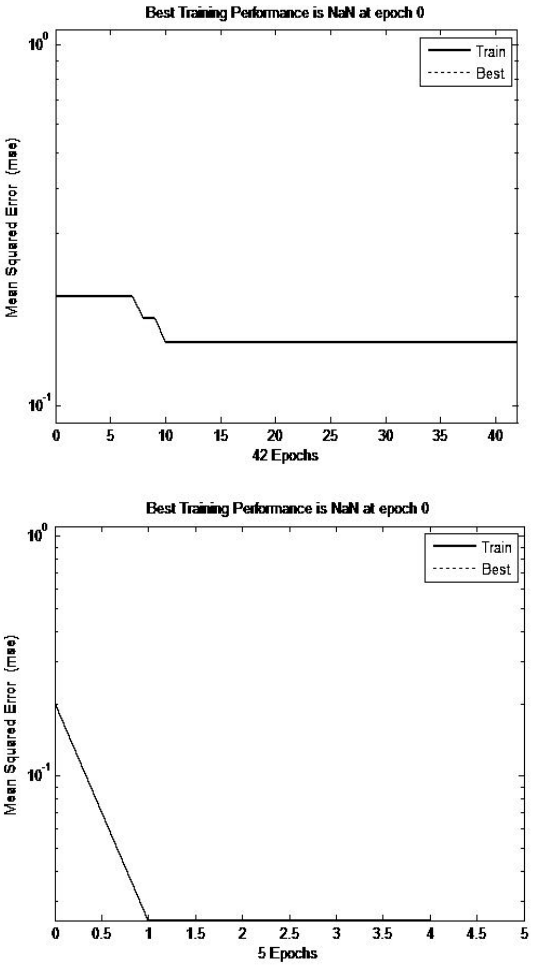

Рис. 1. Графіки зміни середньоквадратичної помилки в процесі навчання нейронної мережі

Навчені нейронні мережі повинні пройти процес верифікації з метою підтвердження їх коректності при класифікації різних образів мережевого трафіку. Функцію перевірки коректності функціонування навчених нейронних мереж виконує модуль відбору детекторів.

Навчена нейронна мережа перевіряється на спеціально підготовленій тестовій вибірці, що складається з параметрів легітимних мережевих з'єднань. Нейронна мережа аналізує і класифікує дані з тестової вибірки і, якщо вона виявляє в ній мережеву атаку, то вважається некоректною (оскільки тестова вибірка містить тільки легітимний трафік) і знищується. Якщо нейронна мережа не виявляє в тестовій вибірці мережевих атак, то вона «проходить» стадію відбору, стає нейромережевим імунним детектором і впроваджується в підсистему аналізу мережевого трафіку і виявлення мережевих атак.

Схему алгоритму функціонування підсистеми створення, навчання і відбору нейромережевих імунних детекторів представлено в наступному вигляді на рис. 2.

Рис. 2. Схема алгоритму функціонування підсистеми створення, навчання і відбору детекторів

Механізм верифікації функціонування нейронних мереж, що пройшли стадію навчання, дозволяє позбавитися від виникнення помилок першого роду, тобто тих помилок, коли легітимне з'єднання класифікується як мережева атака.

Нейромережеві імунні детектори, які успішно пройшли стадії навчання і відбору складають основу підсистеми аналізу мережевого трафіку і виявлення мережевих атак. Сукупність нейромережевих імунних детекторів, яка аналізує мережевий трафік, представлена на рис. 3.

Як було відмічено, при навчанні нейромережевого імунного детектора використовуються навчальна вибірка, що складається з параметрів окремого класу мережевих атак (наприклад, DoS-атак*)* і легітимного з'єднання.

Таким чином, окремий детектор настроєний виявляти комп'ютерні атаки певного класу. Сукупність нейромережевих імунних детекторів забезпечує виявлення мережевих атак, що належать до будь-якого з класів.

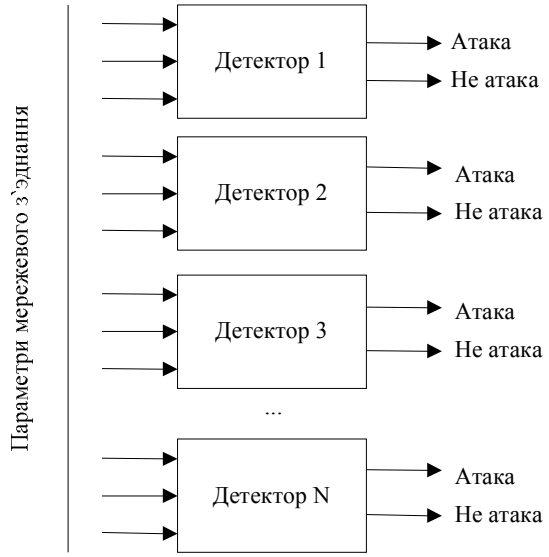

Рис. 3. Сукупність нейромережевих імунних детекторів для аналізу мережевого трафіку

Для аналізу мережевого трафіку паралельно на вхід кожного з функціонуючих нейромережевих імунних детекторів з підсистеми попередньої обробки мережевого трафіку подаються дванадцять параметрів мережевого з'єднання. Детектори аналізують ці параметри і ухвалюють рішення. Якщо всі детектори визначили аналізоване з'єднання як легітимне (не атака), то воно допускається до обробки і виконання. Якщо ж хоч би один з детекторів класифікував поточне з'єднання як мережеву атаку, то воно блокується і видається повідомлення про те, що на комп'ютерну систему проводиться атака, і що небезпечне мережеве з'єднання буде завершено. Таким чином, функціонування підсистеми аналізу мережевого трафіку і виявлення мережевих атак можна представити у вигляді алгоритму (рис. 4).

Як показано в [9], кожен нейромережевий імунний детектор має так званий «час життя», впродовж якого він може аналізувати мережевий трафік. Такий обмежений проміжок існування детекторів необхідний для того, щоб позбавлятися від «слабких» детекторів. Справа у тому, що після навчання і відбору нейромережевих детекторів немає гарантії в тому, що детектор здатний виявляти мережеві атаки. Точніше сказати, може виникнути така ситуація, коли детектор класифікуватиме невідомий образ як атаку тільки у тому випадку, коли цей образ точно співпадатиме з навчальною вибіркою.

Така ситуація може виникнути через те, що навчальна вибірка для кожного детектора формується випадковим чином, і, можлива така ситуація, коли нейронна мережа, що лежить в основі детектора на навчальних даних не зможе виявити закономірності в параметрах з'єднань, що відносяться до різних класів.

Механізм обмеження часу функціонування, коли детектор знищується, якщо він не виявив протягом заданого часу атаку, дозволяє позбавитися від «слабких» детекторів. При знищенні детектора, на його місце приходить новий нейромережевий імунний детектор, тільки що навчений і такий, що пройшов стадію відбору.

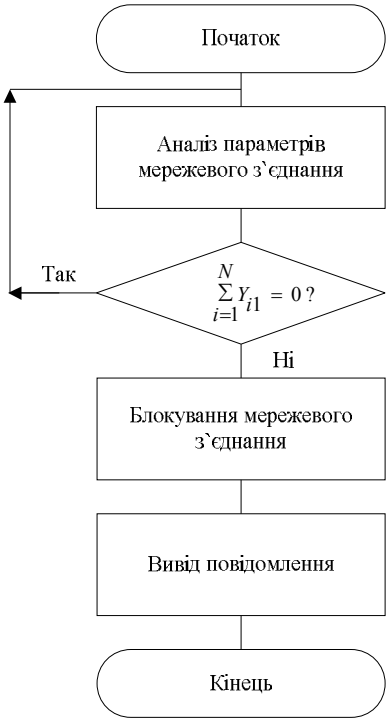

Рис. 4. Схема алгоритму функціонування підсистеми аналізу мережевого трафіку і виявлення мережевих атак

Сучасна система захисту комп'ютерів від мережевих атак повинна не тільки надійно захищати від вже відомих мережевих атак, але і також від невідомих, таких, що раніше не зустрічалися. Тобто система повинна мати властивість до самоадаптації – до зміни «сигнатур» мережевих атак і методів їх організацій і здійснення. За самоадаптацію в розробленій і пропонованій системі виявлення атак відповідає підсистема адаптації.

Підсистема адаптації заснована на дослідженні характеристик виявленої мережевої атаки і здатності нейромережевих імунних детекторів до донавчання. При виявленні атаки одним з детекторів, відбувається блокування даного мережевого з'єднання і генерується повідомлення користувачу. Проте, окрім перерахованих дій, система запам'ятовує характеристики мережевого з'єднання, яке класифіковане як атака імунним детектором.

Далі, параметри даної атаки порівнюються з параметрами атак, що знаходяться в базі даних для навчання детекторів. Якщо атака з такими або достатньо близькими характеристиками вже існує, то

нічого не відбувається. Проте, якщо атаки з такими характеристиками в базі не існує, або характеристика виявленої атаки досить сильно відрізняються від вже відомих, то проводяться наступні операції:

1. На основі нейромережевого детектора, який виявив мережеву атаку, створюється новий детектор, так званий детектор імунної пам'яті. На першому етапі це просте дублювання детектора.

2. Проводиться донавчання нового детектора на параметрах нової виявленої атаки.

3. Новий детектор, що донавчається, впроваджується в підсистему аналізу мережевого трафіку і виявлення мережевих атак.

4. Параметри нової мережевої атаки заносяться в базу, що зберігає дані для навчання нейромережевих імунних детекторів.

Описаний алгоритм дозволяє всій системі виявлення мережевих вторгнень аналізувати виявлену мережеву атаку і, якщо виявляється її унікальність, тобто атака є новою, раніше невідомою, то адаптуватися до неї шляхом створення детекторів імунної пам'яті і внесенням характеристик (сигнатури) нової мережевої атаки до навчальної вибірки для подальших нових детекторів. У загальному вигляді схема алгоритму функціонування підсистеми адаптації представлена на рис. 5.

Рис. 5. Схема алгоритму функціонування підсистеми адаптації

Експериментальні дослідженні інтелектуальної інформаційної технології виявлення мережевих атак

З метою усунення недоліків відомих рішень, підвищення достовірності та ефективності виявлення мережевих атак розроблено інтелектуальну інформаційну технологію (рис. 6) на основі методів нейронних мереж та імунних систем.

Для розрахунку достовірності виявлення мережевих атак на основі інтелектуальної інформаційної технології був проведений наступний експеримент.

Опишемо умови експериментів, що проводилися і порядок проходження операцій:

1. Створення нейронної мережі заданої структури, тобто кількість вхідних нейронів дорівнює 12, кількість нейронів шару Кохонена – 10 і кількість вихідних нейронів – 2.

2. Проводиться ініціалізація вагових коефіцієнтів.

3. Навчання нейронної мережі.

4. Якщо значення сумарної середньоквадратичної помилки дорівнює нулю, то перехід до пункту 5. Інакше знищення нейронної мережі і перехід до пункту 1.

5. Перевірка коректності функціонування навченої нейронної мережі на тестовій вибірці. Якщо нейронна мережа виявляє в тестовій вибірці мережеву атаку, то вона знищується і здійснюється перехід до кроку 1. Інакше перехід до пункту 6.

6. Аналіз параметрів мережевих з'єднань на основі бази KDD 99 [11], над якими проведена попередня обробка по описаній раніше методиці.

7. Виведення результатів.

У табл. 1 представлені результати виявлення мережевих атак на основі 10 нейромережевих імунних детекторів. У таблиці вказані класи атак і відсоток їх виявлення детекторами.

Висновки

Аналізуючи результати проведених експериментів, можна зробити висновок, що запропонована інтелектуальна інформаційна технологія виявлення мережевих атак здатна ефективно виявляти різноманітні мережеві вторгнення. Також слід зазначити здатність одного детектора виявляти не тільки тип атак, на яких проводилося його навчання, але також і інші атаки з абсолютно різних класів. Це відбувається завдяки властивості нейронної мережі до узагальнення, яка покладена в основу детектора. При навчанні нейронна мережа знаходить приховані взаємозв'язки в даних і в майбутньому при аналізі невідомого образу коректно його класифікує.

Необхідно звернути увагу, що представлені результати аналізу мережевого трафіку тільки десятьма

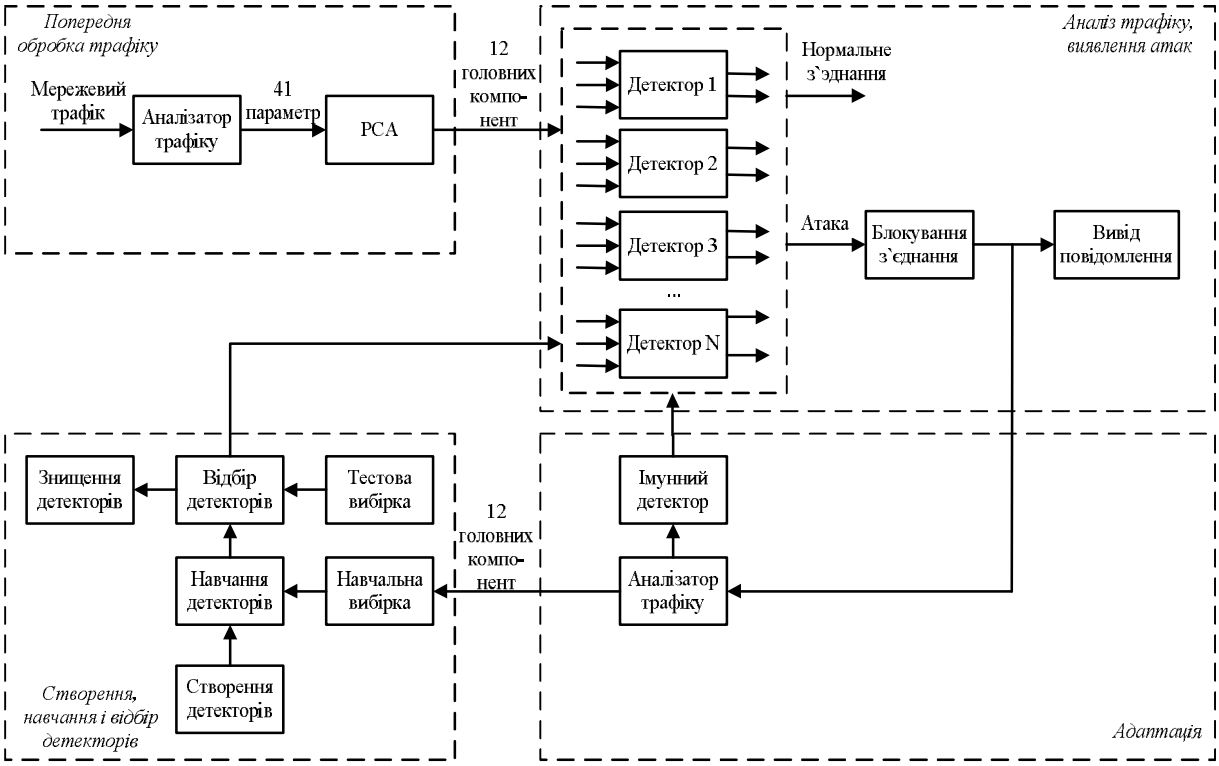

Рис. 6. Схема інтелектуальної інформаційної технології виявлення мережевих атак

Таблиця 1

Результати виявлення мережевих атак

Тип атаки	D1	D2	D3	D4	D5	D6	D7	D8	D9	D10
d_back	**99,05**	0,00	0,00	0,00	0,00	0,00	**99,05**	0,00	0,00	0,27
d_land	0,00	**100**	**100**	61,91	4,76	80,95	9,52	100	4,76	23,81
d_neptune	**99,07**	80,91	**100**	0,00	0,00	**99,99**	**99,85**	**100**	**99,95**	0,00
d_pod	0,00	2,27	0,00	0,34	0,00	31,06	12,88	0,00	0,00	**99,89**
d_smurf	0,00	0,00	0,00	**99,92**	**100**	0,14	0,03	0,00	0,00	0,00
d_teardrop	0,00	0,00	2,66	0,00	32,99	**100**	10,93	8,79	7,66	0,00
p_ipsweep	**99,08**	7,22	6,58	65,20	45,07	6,98	5,69	6,98	6,74	0,96
p_nmap	80,52	0,00	0,00	0,00	0,00	**96,10**	**100**	0,00	0,00	0,00
p_portsweep	2,02	15,88	**98,85**	0,48	1,44	**97,79**	30,80	**99,90**	**98,56**	0,10
p_satan	13,28	11,01	88,80	0,00	13,59	**93,90**	**96,04**	**92,20**	**94,59**	2,08
r_ftpwrite	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	**100**
r_gpasswd	0,00	3,77	**94,34**	0,00	0,00	0,00	0,00	1,89	0,00	5,66
r_imap	0,00	83,33	83,33	0,00	**99,10**	16,67	0,00	75,00	0,00	0,00
r_multihop	0,00	0,00	0,00	**97,60**	0,00	0,00	0,00	0,00	0,00	57,14
r_phf	0,00	**98,70**	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
r_spy	**100**	0,00	0,00	0,00	0,00	50,00	**100**	0,00	0,00	0,00
r_wclient	1,08	0,20	0,20	**90,00**	0,00	0,00	0,59	0,20	0,00	65,00
r_wmaster	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	**90,00**
u_overflow	0,00	0,00	0,00	0,00	**99,00**	0,00	0,00	3,33	0,00	83,33
u_loadmodule	88,89	0,00	0,00	0,00	0,00	11,11	**100**	0,00	0,00	0,00
u_perl	33,33	0,00	0,00	0,00	0,00	**97,00**	0,00	0,00	0,00	0,00
u_rootkit	0,00	0,00	0,00	0,00	0,00	30,00	0,00	**98,00**	0,00	20,00

детекторами. Збільшення їх кількості приведе до підвищення відсотка виявлення різноманітних атак.

Запропонований спосіб адаптації розробленої системи до зміни тенденцій організації мережевих атак. Система здатна виявляти нові, раніше невідомі атаки, аналізувати їх і адаптуватися під нові реалії з метою підвищення достовірності виявлення.

Запропонована реалізація основних блоків нейромережевої імунної системи виявлення мережевих атак, яка базується на модульному принципі.

Література

1. Головко, В.А. Нейронные сети : обучение, организация и применение [Текст]: учеб. пособие / В. А. Головко. – М.: Радиотехника, 2001. – 256 с.

2. Хайкин, С. Нейронные сети: полный курс [Текст]: пер. с англ. / С. Хайкин. – М.: Вильямс, 2006. – 1104 с.

3. Дасгупта, Д. Искусственные иммунные системы и их применение [Текст]: пер. с англ. / Д. Дасгупта. – М.: Физматлит, 2006. – 344 с.

4. Комар, М.П. Система анализа сетевого трафика для обнаружения компьютерных атак [Текст] / М.П. Комар // Вестн. Брестского гос. техн. ун-та. Сер. Физика, математика и информатика. – 2010. – №5. – С. 14 – 16.

5. Комар, М.П. Нейромережевий метод ідентифікації комп'ютерних атак [Текст] / М.П. Комар // Оптико-електронні інформаційно-енергетичні технології. – 2010. – № 2. – С. 105 – 109.

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

7. Комар, М.П. Використання методу головних компонент для вирішення задачі виявлення комп'ютерних атак [Текст] / М.П. Комар // Методи та засоби кодування, захисту й ущільнення інформації: мат. 3-ої Міжн. НПК, Вінниця, 20-22 квіт. 2011 р. – Вінниця, 2011. – С. 131 – 132.

8. Komar, M. Intelligent system for detection of networking intrusion [Text]./ M. Komar, V. Golovko, A. Sachenko, S. Bezobrazov // Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications: Proc. of the 6th IEEE International Conference, Prague (Czech Republic), September 15-17, 2011. – Prague, 2011. – Vol. 1. – P. 374 – 377.

9. Комар, М.П. Методы искусственных иммунных систем и нейронных сетей для обнаружения компьютерных атак [Текст] / М.П. Комар // Інформаційна безпека. – 2011. – №1(5). – С. 154 – 160.

10. Sniffer Pro network optimization and troubleshooting handbook [Text] / R.J. Shimonski, W. Eaton, U. Khan, Y. Gordienko // Syngress. – 2002. – 560 p.

11. KDD Cup 1999 Data [Електронний ресурс]. – Режим доступу: http://kdd.ics.uci.edu/databases /kddcup99/kddcup99.html. – 28.03.2011 р.

Поступила в редакцію 05.12.2011

Рецензент: д-р техн. наук, проф., проф. каф. комп'ютерних наук М.П. Карпінський, Тернопільський національний технічний університет, Тернопіль.

ИНТЕЛЛЕКТУАЛЬНАЯ ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ ОБНАРУЖЕНИЯ СЕТЕВЫХ АТАК В СИСТЕМЕ РЕАЛЬНОГО ВРЕМЕНИ

М.П. Комар

Разработана структура и алгоритмы функционирования нейросетевой иммунной системы обнаружения сетевых атак, которая состоит из подсистем предварительной обработки трафика, создания, обучения и отбора детекторов, анализа трафика и обнаружения сетевых атак, адаптации. Предложенный способ адаптации разработанной системы к изменению тенденций организации сетевых атак, что позволяет обнаруживать новые, ранее неизвестные атаки, анализировать их и адаптироваться под новые реалии в целях повышения качества обнаружения. Предложена реализация основных блоков нейросетевой иммунной системы обнаружения сетевых атак, основанная на модульном принципе. Проведенные эксперименты по тестированию предложенной системы, которые показывают способность нейросетевых иммунных детекторов эффективно выявлять разнотипные сетевые атаки.

Ключевые слова: интеллектуальная информационная технология, сетевая атака, нейронная сеть, иммунная система, сетевой трафик, нейросетевой иммунный детектор.

INTELLIGENT INFORMATION TECHNOLOGY OF DETECTION NETWORK ATTACKS IN REAL TIME SYSTEM

M.P. Komar

The structure and algorithms of neural network immune system of the detection computer attacks are developed, that consists of such subsystem as: traffic pretreatment, training and selection of detectors, traffic analysis and detection of computer attacks, adaptation. The adaptation method of developed system to the trends of computer attacks that can detect new, previously unknown cyber attacks, analyze them and adapt to new realities in order to improve the quality of detection. The implementation of the basic blocks of the neural network immune system of the detection computer attacks is proposed that is based on the modular principle. The experiments on testing the proposed system are made, which show the ability of neural network immune detectors effectively detect polytypic cyber attacks.

Key words: intelligent information technology, network attacks, neural network, immune systems, network traffic, immune neural network detector.

Комар Мирослав Петрович – аспірант кафедри інформаційно-обчислювальних систем та управління, Тернопільський національний економічний університет, Тернопіль, Україна, e-mail: mko@tneu.edu.ua.