5. За матеріалами сайту http://www.winsecurity.ru/articles/.
6. За матеріалами сайту http://wiki.kspu.kr.ua.
7. Ken Dunham, Jim Melnick. Malicious Bots: An Inside Look into the Cyber-Criminal Underground of the Internet, 2008. – 168 p.
8. За матеріалами сайту http://infoch.info.
9. За матеріалами сайту http://www.winsecurity.ru/articles/.
10. За матеріалами сайту http://www.cisco.com.
11. Галушкін А.І. Нейронні мережі. Основи теорії. М.: Телеком, 2010. – 496 с.

Надійшла: 02.08.2012 р.

Рецензент: д.т.н., професор Юдін О.К.

УДК 004.056.5(045)

Пархоменко І.І., Пасько О.З.

ШТУЧНІ БІОЛОГІЧНІ СИСТЕМИ ЗАХИСТУ КОМП'ЮТЕРНИХ МЕРЕЖ

Ця стаття присвячена аналізу особливостей побудови штучних біологічних мереж як способу захисту комп'ютерних систем від зовнішніх атак. Прототипами цих штучних систем є захисні механізми живих істот: імунітет та нейрони.

Ключові слова: штучні нейронні мережі, штучні імунні мережі, нейромережний імунний детектор, багатошаровий персептрон, рециркуляційна нейронна мережа.

Постановка проблеми. В ході інтенсивного розвитку інформаційної сфери та ускладнення методів здійснення атак на її об'єкти, гостро постає проблема побудови надійної системи захисту. Дослідження, які проводяться в даній області, напрямлені на побудову досить специфічних мереж, прототипами яких є системи, що захищають живі організми від зовнішнього вторгнення або, якщо воно вже відбулось, спрямовані на ліквідування його наслідків. Такими системами, зокрема, являються нейронні та імунні механізми.

У даній роботі буде розглянуто:

1.Особливості функціонування штучних нейронних мереж;

2.Особливості функціонування штучних імунних мереж;

3.Можливість синтезу імунної та нейронної мережі для створення елементів (детекторів) єдиної захисної системи;

4.Особливості побудови та функціонування нейромережних імунних детекторів.

Аналіз останніх досліджень та публікацій. Проблема створення та функціонування нейронних та імунних мереж розглянута в публікаціях Галушкіна А.І. «Нейронні мережі. Основи теорії», Головко В.А. та Безобразова С.В «Штучні імунні системи для захисту інформації: виявлення і класифікація комп'ютерних вірусів», а також «Нейронні мережі: навчання, організація, застосування».

Постановка завдання. Розглянемо особливості створення та функціональні можливості штучної біологічної мережі, яка є синтезом як нейронної, так й імунної системи.

Основна частина. Спершу ознайомимось із самим поняттям штучних нейронних та імунних систем.

Штучна нейронна мережа [1, ст.93]. Штучні нейронні мережі (ШНМ) будуються по аналогії з відповідною системою живого організму. Проте перш ніж почати своє функціонування нейронні мережі спершу повинні навчатись протягом деякого періоду з метою формування вхідного вектору даних, за допомогою якого в майбутньому система буде вирішувати являється поведінка нормальною чи ні. Після навчання нейронна мережа запускається в режимі розпізнавання. Якщо у вхідному потоці не вдається розпізнати нормальну поведінку - фіксується факт атаки. Класичні нейронні мережі мають високу обчислювальну складність навчання, що ускладнює їх застосування на великих потоках даних.

Штучна імунна мережа [2]. Так як і нейронні мережі, імунні є механізмом класифікації та будуються у відповідності з імунною системою живого організму. Основна їх перевага полягає у можливості вироблення «антитіл» до невідомих атак.

Для побудови ефективної системи захисту використовують особливості обох мереж. Зокрема, на основі їх синтезу побудований нейромережний імунний детектор, що входить до складу штучної біологічної системи для виявлення вторгнень, а також алгоритми його навчання та функціонування.

Уявімо нейромережний імунний детектор (НІД) [3] у вигляді чорного ящика, який має *n*-входів на які подається підмножина елементів X_i та два виходи, де утворюється вихідна підмножина Z_i (рис. 1).

Вихідні значення детектора формуються після подачі всіх образів на нього у відповідності з наступним виразом:

$$Z_1 = \begin{cases} 1, \text{якщо чистий файл} \\ 0, \text{інакше} \end{cases}, \tag{1}$$

$$Z_2 = \begin{cases} 1, \text{ якщо вірус} \\ 0, \text{інакше} \end{cases}. \tag{2}$$

Рис.1. Нейромережний імунний детектор

Навчальна вибірка формується з чистих файлів (клас чистих програм) та шкідливих програм (клас шкідливих програм). Бажано також мати представників усіх типів шкідливих програм - вірусів, троянських програм, макровірусів і т.д.. При навчанні нейронної мережі потрібно вказати, де дані з чистих файлів, а де - із шкідливих програм.

Зокрема, нехай T - безліч чистих файлів, а F - безліч шкідливих файлів. З них випадковим чином формується безліч вхідних образів для навчання *i*-го детектора.

$$Xi = \begin{matrix} X_i^1 \\ \dots \\ X_i^L \end{matrix} = \begin{matrix} X_{i1}^1 & \dots & X_{in}^1 \\ \dots & \dots & \dots \\ X_{i1}^L & \dots & X_{in}^L \end{matrix}, \tag{3}$$

де L - розмірність навчальної вибірки. Відповідно, безліч еталонних образів виглядають наступним чином:

$$Li = \begin{matrix} l_i^1 \\ \dots \\ l_i^L \end{matrix} = \begin{matrix} l_{i1}^1 & l_{i2}^1 \\ \dots & \dots \\ l_{i1}^L & l_{i2}^L \end{matrix}. \tag{4}$$

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

$$l_{i1}^k = \begin{cases} 1, \text{якщо } X_i^k \in T \\ 0, \text{інакше} \end{cases}$$

$$l_{i2}^k = \begin{cases} 1, \text{якщо } X_i^k \in F \\ 0, \text{інакше} \end{cases}. \tag{5}$$

Навчання кожного детектора здійснюється з метою мінімізації сумарної квадратичної помилки детектора.

Сумарна квадратична помилка і-го детектора визначається таким чином:

$$E_i = \frac{1}{2}\sum_{k=1}^{L}\sum_{j=1}^{2}(Z_{ij}^k - l_{ij}^k)^2, \tag{6}$$

де Z_{ijk} - значення *j*-го виходу *i*-го детектора при подачі на вхід його *k*-го образу.

Загальний алгоритм функціонування нейромережної імунної системи можна представити у вигляді такої послідовності:

1. Генерація початкової популяції імунних детекторів, кожен з яких представляє собою штучну нейронну мережу із випадковими синаптичними зв'язками:

$$D = \{D_i, i = \overline{1, r}\}, \quad (7)$$

де D_i - і-й нейромережний імунний детектор, r- загальна кількість детекторів.

2. Навчання сформованих імунних нейромережних детекторів. Навчальна вибірка формується випадковим чином із сукупності чистих файлів (як правило, це різноманітні системні утиліти), та із сукупності шкідливих програм, або їх сигнатур.

3. Відбір нейромережних імунних детекторів на тестовій вибірці. На даному кроці знищуються ті детектори, які виявились нездатними до навчання, і детектори, в роботі яких спостерігаються різні недоліки (наприклад, помилкові спрацьовування). Для цього кожен з них перевіряється на тестовій вибірці. В результаті для кожного детектора визначається значення квадратичної помилки E_i. Селекція детектора проводиться таким чином:

$$D_i = \begin{cases} 0, \text{якщо } E_i \neq 0 \\ D_i, \text{інакше} \end{cases}, \quad (8)$$

де 0 означає операцію знищення детектора.

4. Кожен детектор наділяється часом життя і випадковим чином вибирає файл для сканування із сукупності файлів, які він не перевіряв.

5. Сканування кожним детектором вибраного файлу, в результаті якого визначаються вихідні значення детекторів Z_{i1}, Z_{i2}, i = 1, ..., r.

6. Якщо i-й детектор не виявив вірус в сканованому файлі, тобто Z_{i1} = 1 і Z_{i2} = 0, то він вибирає наступний файл для сканування. Якщо час життя i-го детектора закінчилося, то він знищується і замість нього генерується новий.

7. Якщо i-й детектор виявив вірус в сканованому файлі, тобто Z_{i1}=0 і Z_{i2}=1, то подається сигнал про виявлення шкідливого файлу і здійснюють операції клонування та мутації відповідного детектора. В результаті створюється сукупність детекторів, настроєних на виявлену шкідливу програму:

$$D_i = (D_{i1}, D_{i2}, \dots D_{in}). \quad (9)$$

8. Відбір клонованих детекторів, які є найбільш пристосованими до виявлення шкідливої програми. Якщо E_{ij}<E_i, то детектор пройшов відбір. Тут E_{ij} - сумарна квадратична помилка j-го клона i-го детектора, яка обчислюється на шкідливий файл.

9. Детектори-клони здійснюють сканування файлового простору комп'ютерної системи до тих пір, поки не відбудеться знищення всіх проявів шкідливої програми.

10. Формування детекторів імунної пам'яті. На цьому кроці визначаються НІД [3, ст.12], що показали найкращі результати при виявленні присутнього в комп'ютерній системі вірусу. Детектори імунної пам'яті знаходяться в системі достатньо тривалий час та забезпечують захист від повторного зараження.

Особливістю запропонованого алгоритму є те, що кожен нейромережний імунний детектор є повністю самостійним об'єктом. Він випадковим чином вибирає файл зі списку для його перевірки. Після перевірки одного файлу детектор переходить до наступного випадково обраного файлу.

У процесі циркуляції НІД відбувається їх безперервна еволюція шляхом знищення старих і формування нових детекторів. Після генерації нових детекторів відбувається процес їх навчання, складність якого пропорційна розмірності навчаючої вибірки. При цьому для збільшення швидкодії нейромережної штучної імунної системи необхідно вибрати такий клас нейронної мережі, який характеризується мінімальним розміром навчальної вибірки.

Функціональні особливості штучних нейронних мереж. Штучні нейронні мережі в загальному випадку являють собою організовану певним чином сукупність вузлів (нейронів) і зв'язків між ними [4, ст.15].

Робота з нейронною мережею передбачає наявність наступних етапів:

1. Збір і підготовка вихідних даних;

2. Побудова і навчання мережі;

3. Тестування мережі та аналіз результатів.

На першому етапі здійснюється захоплення трафіку мережі. Збір необхідних даних виконує спеціальне програмне забезпечення (як правило це сніфер).

Результати першого етапу не можуть бути відразу використані класифікатором, оскільки вони представлені в "сирому" вигляді і потребують попередньої обробки.

Тому другий етап пов'язаний з обчисленням параметрів, що характеризують активність мережі і представлених в тій формі, в якій їх зможе прийняти класифікатор [5, ст.22]. Третій етап полягає у виявленні і розпізнаванні атак та їх подальшої класифікації. З цією метою застосовуються різні нейронні мережі.

Розглянемо різні архітектурні рішення для побудови систем детектування та розпізнавання атак. Зокрема для цих цілей використовують багатошаровий персептрон (MLP), навчання якого проводиться згідно правилу зворотного поширення помилки (рис.2).

Для формування вхідного вектору даних можна використати рециркуляційну нейронну мережу (RNN) (рис.3). Вона представляється багатошаровим персептроном [6], який здійснює лінійне або нелінійне стиснення вхідних даних. Як видно, мережа складається з трьох шарів. Прихований шар здійснює стиснення вхідного вектору (рис. 3).

Зупинимось на декількох алгоритмах навчання RNN. Перший алгоритм - це лінійне правило навчання, другий - зворотного поширення помилки для нелінійної рециркуляційної нейронної мережі.

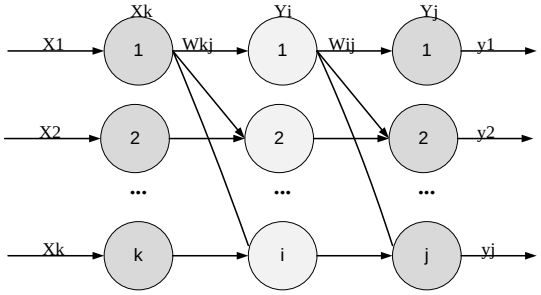

Рис.2. Архітектура MLP

Комбінуючи RNN і MLP нейронні мережі, можна отримати різні архітектури систем виявлення атак (рис.4).

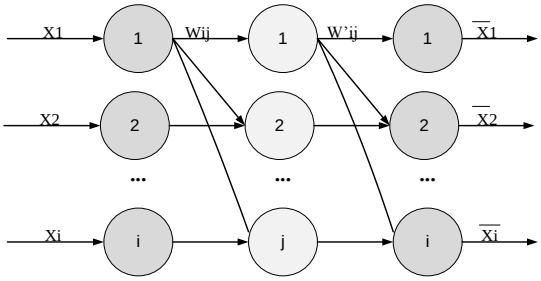

Рис.3. Архітектура RNN

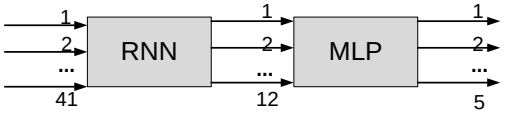

Рис.4. Перший варіант IDS

На рис. 4 приведена система виявлення атак, яка складається з рециркуляційної нейронної мережі та багатошарового персептрона, які з'єднані послідовно.

Завданням RNN є стиснення вхідного 41-розмірного вектора в 12-розмірний вихідний вектор. Багатошаровий персептрон здійснює обробку стислого простору вхідних образів (головних компонент) з метою розпізнавання класу атаки.

На рис. 5. приведена друга схема системи виявлення атак.

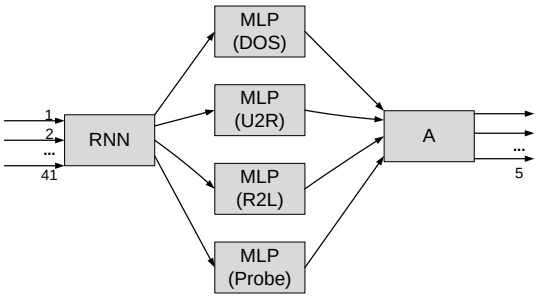

Рис.5. Другий варіант IDS

Ця схема характеризується тим, що головні компоненти з виходів RNN одночасно надходять на чотири окремих багатошарових персептрони, кожен з яких відповідає певному класу атаки (DoS, U2R, R2L, Probe) [6].

Атаки діляться на чотири основні класи: DoS, U2R, R2L і Probe:

1. Атака DoS - відмова в обслуговуванні, характеризується генерацією великого обсягу трафіку, що призводить до перевантаження та блокування сервера.

2. Атака U2R передбачає отримання зареєстрованим користувачем привілеїв локального адміністратора.

3. Атака R2L характеризується отриманням доступу незареєстрованого користувача до комп'ютера з боку віддаленої машини.

4. Атака Probe полягає в скануванні портів з метою отримання конфіденційної інформації.

З виходів MLP дані надходять на арбітр, який і приймає остаточне рішення про стан системи. У якості арбітра може використовуватися як лінійний так і багатошаровий персептрон. Така схема може здійснювати ієрархічну класифікацію атак. У цьому випадку арбітр визначає один з п’яти класів атак, а відповідний багатошаровий персептрон - її тип. Наступний варіант структури IDS (рис. 6) базується на застосуванні модулярної нейронної мережі. Під модулярністю розуміється розбиття складної обчислювальної задачі на безліч невеликих і простих частин, які вирішуються окремими модулями системи (експертами). Далі результати всіх експертів інтегруються в загальне рішення, яке має пріоритет над рішенням кожного окремого експерта.

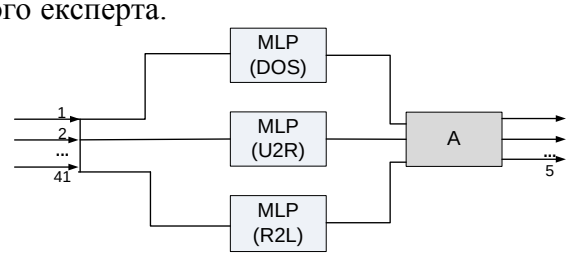

Рис.6. Третій варіант IDS

Висновки. У даній статті були розглянуті механізми функціонування штучних нейронних та імунних мереж, а також можливість їх синтезу для створення нейромережних імунних детекторів єдиної захисної системи. Особливості їх побудови полягають в тому, що вони можуть не тільки користуватись вже набутою пам’яттю для проведення роботи по виявленню аномалій та вторгнень в систему, а й проводити власну еволюцію на протязі всього життєвого циклу. Під час виявлення шкідливого коду НІД не тільки проводить його знищення, а й «запам’ятовує» характерні особливості для формування власної сигнатурної бази. Крім того він запускає процес клонування з метою генерації собі подібних елементів, оскільки даний механізм надає можливість збільшити кількість детекторів, які виявились найбільш ефективними. З іншого боку всі нейромережні імунні детектори, що не пройшли перевірку на ефективність (не виявили жодного шкідливого коду) після закінчення свого життєвого циклу самознищуються. Подібний механізм дозволяє залишити найкращі елементи, що в майбутньому скоротить час реагування на виявлення та нейтралізацію

інфікування. Враховуючи все вище сказане можна сказати, що використання штучних нейромережних імунних детекторів призводить до вироблення системою власного імунітету, це щось на кшталт поведінки лейкоцита у живому організмі.

ЛІТЕРАТУРА

1. Галушкін А.І. Нейронні мережі. Основи теорії. М.: Телеком, 2010. – 496 с.
2. За матеріалами сайту: http://inf-bez.ru.
3. Головко В.А. Нейронні мережі: навчання, організація, застосування //Нейрокомп'ютери та їх застосування: навч. посібник. М., 2001. - 256 с.
4. Хайкін С. Нейронні мережі: повний курс. М.: Вільямс, 2006. - 1104с .
5. Безобразов С.В., Головко В.А. Штучні імунні системи для захисту інформації: виявлення і класифікація комп'ютерних вірусів //Нейроінформатика - 2008: матеріали IX всерос. наук.-техн. конф., М., МІФІ, 2008. - С. 23-27.
6. За матеріалами сайту: http://bstu.by.

Надійшла: 18.07.2012 р.

Рецензент: д.т.н., професор Юдін О.К.

УДК 621.395 **Толюпа С.В.**

МЕТОД БАГАТОКРИТЕРІАЛЬНОГО АНАЛІЗУ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ ТА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІНФОКОМУНІКАЦІЙНИХ СИСТЕМ

У даній статті запропонований імовірнісний метод багатокритеріального аналізу ефективності функціонування та забезпечення інформаційної безпеки інфокомунікаційних систем, який дозволяє на основі результатів аналізу проводити оптимізацію рішень на етапах планування й оперативного управління зв’язком у системі із урахуванням всіх видів випадкових впливів на неї.

Ключові слова: мережа, ефективність, безпека, показник якості, захист інформації.

Проблема багатьох інфокомунікаційних систем (ІКС) зв’язку зводиться до того, що кількість параметрів, необхідних для опису поводження системи (розмірність системи), виявляється дуже великою і прийняти правильне рішення в таких мережах досить складно, враховуючи, що інформація про стан мережі може бути досить суперечливою. Збільшення розмірності сучасної технології представляється об’єктивною тенденцією, яку можна спостерігати в історичному зрізі протягом усього розвитку цифрових ІКС.

Поява концепції інфокомунікаційних мереж нового покоління (*NGN* та *FN* – мереж майбутнього) дозволить операторам значно розширити горизонти своєї діяльності, спектр послуг. Проте шлях переходу до мереж, на базі яких можливе надання мультисервісних послуг, складний і тернистий. Тому ставиться питання, чи не простіше продовжувати експлуатувати існуючі мережі, поки є попит на перелік послуг, що вже склався і піклуватися про їх якість.

Безумовно в стрімкому розвитку мереж нового покоління можна назвати і “болючі точки” експлуатації інфокомунікаційних мереж нового покоління з погляду оператора**.** Ключові моменти в експлуатації мережі – її надійність і досконаліть системи управління. До “болючих точок” експлуатації мереж нового покоління можна віднести не стільки проблеми з технологіями, які застосовуються, скільки завдання забезпечення стійкої роботи мережевого устаткування, стиковка протоколів, інтерфейсів різних постачальників та забезпечення інформаційної безпеки.

Гарантування безпеки інформації в мережах нового покоління взагалі та їх системах управління є складним комплексним завданням. У міжнародних стандартах проблеми захисту інформації вирішуються одночасно зі стратегічними та конкретними питаннями розвитку архітектури мережі.