Рівень безпеки захисту для кожного класу забезпечується експертною оцінкою та моніторингом стану безпеки КС від атак НСД за певними методиками [6, 7].

Висновок

Викладені рекомендації можуть бути корисними для формування політики безпеки КС - найбільш суттєвої і ще мало визначеної складової при створенні, експлуатації та забезпеченні безпеки інформації в захищених КС.

Список літератури

1. *В.В.Шорошев, Близнюк І.Л.* Огляд способів вчинення комп'ютерних злочинів. Бизнес и безопасность № 2, 2004. С.44-50.

2. *НД ТЗІ 1.4-004-99.* Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. ДСТСЗІ СБУ, 1999.

3. *НД ТЗІ 2.5-008-2002.* Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2. ДСТСЗІ СБУ, 2002.

4. *НД ТЗІ 2.5-010-2003.* Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу. ДСТСЗІ СБУ, 2003.

5. *А.Ю. Ільніцький, В.В.Шорошев, І.Л.Близнюк.* Монографія "Базова модель експертної системи оцінки безпеки інформації в комп'ютерних система органів внутрішніх справ України" (шифр "Торсіон-1 ").

- К.: Видавництво НАВСУ, 2003р. - 316с.

6. *Зегжда Д.П., Ивашко А.М.* Основи безопасности информационних систем. - М: Горячая линия - Телеком, 2000. - 452 с. 15.

7. *НД ТЗІ 1.4-004-99.* Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. ДСТСЗІ СБУ, 1999

Надійшла 12.11.2007р.

УДК 681.3.06 **Терейковський І.А.**

ПЕРСПЕКТИВИ ПРАКТИЧНОГО ВИКОРИСТАННЯ НЕЙРОННИХ МЕРЕЖ В ЗАДАЧАХ ЗАХИСТУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Використання нейронних мереж (НМ) в галузі комп'ютерного забезпечення технічних та економічних систем триває вже декілька десятиліть. Розроблені належні теоретичні та практичні рекомендації в яких наведена досить чітка методика визначення відповідності архітектури мережі з характером прикладної задачі. На цьому фоні за останні декілька років помітно зріс інтерес до застосування НМ при вирішенні задач захисту програмного забезпечення інформації. Відомі дослідження в яких показано методику вирішення окремих задач за допомогою НМ. Разом з тим, коло практичних задач захисту інформації (ЗЗІ) розв'язувати які доцільно за допомогою НМ окреслено не достатньо чітко. Крім того, відсутня загальна методика визначення відповідності архітектури та характеру застосування НМ до прикладної ЗЗІ. По цим причинам метою даної статі є – визначення кола практичних задач захисту програмного забезпечення які доцільно вирішувати за допомогою НМ та формування рекомендацій що до застосування конкретного типу мережі.

Передумови застосування штучних нейронних мереж

Під терміном штучні НМ розуміють мережу елементів (штучних нейронів), пов'язаних між собою синаптичними зв'язками [1, 2]. Нейрони та зв'язки між ними

утворюють структуру НМ. З точки зору методики реалізації обчислювальних процесів НМ моделюють функціонування біологічних процесів, які відбуваються в людському мозку. Однак в порівнянні з людським мозком сучасні НМ представляють собою значно спрощену абстракцію. Робота НМ полягає в перетворенні вхідної інформації у певну сукупність вихідних сигналів. Перетворення відбувається за рахунок зміни внутрішнього стану НМ. При цьому НМ, як правило, оперують цифровими величинами. Зв'язки, по яких інформація передається в напрямку вхід – вихід, називаються прямими. Зв'язки, по яких інформація передається в напрямку вихід – вхід, називаються зворотніми. Мережі, в яких існують тільки прямі зв'язки, називаються мережами з прямим розповсюдженням сигналу. Мережі з зворотніми зв'язками називаються рекурентними. Досить часто в структурі НМ виділяють групу нейронів з однаковими зв'язками – нейронний шар. Загальновідомим прикладом НМ, яка складається із декількох шарів нейронів, є багатошаровий перспетрон (БШП). Шаблон, що визначає наявність зв'язків між окремими нейронами, називається топологією мережі [1,2]. Розрізняють повнозв'язну та не повнозв'язну топологію НМ. Нейрони, з яких складається НМ, представляють собою прості процесори, обчислювальні параметри яких обмежуються деякими правилами комбінування вхідних сигналів и правилом активації, яке дозволяє визначити вихідний сигнал по сукупності вхідних. Вихідний сигнал нейрону може передаватись іншим нейронам мережі по синаптичним (зваженим) зв'язкам, кожному із яких відповідає ваговий коефіцієнт, що також називається вагою зв'язку. Вхідні зв'язки нейронів отримали назву дендритів, а вихідний зв'язок – аксону. Нейрони, призначені для безпосереднього прийому інформації із зовнішнього середовища, називаються вхідними. Нейрони, що віддають інформацію безпосередньо у зовнішнє середовище, називаються вихідними. Інші нейрони називаються проміжними або схованими. Вони утворюють один або декілька схованих шарів нейронів (СШН). Комбінування вхідних сигналів (зв'язків) нейрону полягає в розрахунку суми їх зважених значень та деякої константи, яка дістала назву зсуву. Сумарний вхідний сигнал нейрону (*NET*) розраховується так:

$$NET = \sum_{i=1}^{K} x_i w_i , \qquad (1)$$

де K – кількість вхідних зв'язків, x_i – величина і-го зв'язку, w_i – вага і-го зв'язку.

В загальному випадку вхідні сигнали, зсув та вагові коефіцієнти можуть приймати будь-які значення із діапазону дійсних чисел, а на практиці їх величини визначається специфікою конкретної задачі. Зв'язки, яким призначені від'ємні вагові коефіцієнти називаються гальмуючими, а зв'язки з додатніми коефіцієнтами – збуджуючими. Блок активації нейрону призначений для розрахунку вихідного сигналу нейрону. Як правило, для цього сумарний вхідний сигнал підлягає нелінійному перетворенню:

$$OUT = F(NET - \theta), \qquad (2)$$

де θ – гранична величина або зсув, F –функція активації.

Досить часто зсув інтерпретують як зв'язок з ваговим коефіцієнтом, що дорівнює w_0. В цьому випадку вирази (1, 2) можна записати так:

$$NET = \sum_{i=0}^{K} x_i w_i , \qquad (3)$$

$$OUT = F(NET) \qquad (4)$$

де θ – порогове значення (зсув), а – коефіцієнт крутизни, σ – радіус функції Гауса.

Відзначимо, що механізм обробки інформації в формальній моделі нейрону (1-4) багато в чому відрізняється від свого біологічного прототипу. Основні відмінності полягають в наступному:

- Не існує механізму визначення затримки реалізації вихідного сигналу.
- Відсутня модуляція рівня вхідного сигналу щільністю нервових імпульсів.

– В більшості НМ не використовується ефект синхронізації функціонування нейронів.
– Відсутній сторонній механізм типу гормональної регуляції активностей нейронів, що регулює функціонування НМ в цілому.
– Не використовується механізм динамічної настройки активаційного порогу та вагових коефіцієнтів в процесі функціонування НМ.
– Використовується тільки збуджуючі та гальмуючі зв'язки між нейронами.

За рахунок вказаних відмінностей використання НМ для моделювання динамічних систем потребує додаткових елементів, які не входять до складу мережі. Також слід розраховувати, що пластичність НМ та її адаптація до зміни зовнішніх умов значно поступаються біологічним аналогам.

Більшість моделей НМ потребують навчання, в процесі якого визначаються такі внутрішні параметри мережі, при яких вона найкраще вирішує поставлену задачу. Найчастіше навчання НМ полягає в розрахунку вагових коефіцієнтів синаптичних зв'язків між нейронами, а структура НМ (кількість нейронів та наявність зв'язків між нейронами) визначається перед навчанням. В процесі навчання мережі пред'являються навчальні приклади, кожному з яких відповідає власний вектор ознак. При цьому вагові коефіцієнти змінюються так, щоб НМ найкраще відповідала цим прикладам. Зміна коефіцієнтів реалізується відповідно наперед заданому алгоритму навчання. В деяких алгоритмах, наприклад, "нейронний газ" крім модифікації коефіцієнтів передбачено зміну кількості нейронів в мережі. Розрізняють два основних типи навчання НМ – безпосередньої обробки навчальних даних та ітераційний [1, 2]. В першому випадку вагові коефіцієнти визначаються шляхом безпосередньої одноразової обробки параметрів навчальних прикладів. Другий випадок характеризується багатократним пред'явленням НМ навчальних прикладів. Вагові коефіцієнти уточнюються під час показу кожного прикладу доти, доки мережа не буде виконувати свої функції з заданою якістю. Ітераційне навчання що базується на прикладах, до складу яких входять тільки вхідні дані НМ, називається навчанням "без вчителя". Якщо ж в прикладах крім вхідних є очікувані вихідні дані, то таке навчання називається навчанням "з вчителем". Крім того, існують менш відомі проміжні методики навчання, наприклад – "з підкріпленням". При апріорно заданих показниках якості, основною характеристикою методики навчання є термін її проведення, який напряму *залежить від кількості ітерацій. На сьогодні найбільш потужними* є НМ, які навчаються по методиці навчання "з вчителем". Відзначимо, що можливість використання тієї чи іншої методики навчання залежить від наявності навчальних даних, топології НМ, правил комбінування вхідних сигналів нейрону та виду функції активації. Наприклад, НМ з нейронами в яких використовується порогова функція активації не можливо навчати за допомогою методу "зворотнього розповсюдження помилок", який є найбільш відомим серед методів навчання "з вчителем". Після навчання НМ може розпізнавати невідомі вхідні дані, або нести якесь інше змістовне навантаження. Інформація про отриманий під час навчання досвід зберігається у вигляді вагових коефіцієнтів зв'язків.

Основними конструктивними параметрами НМ є кількість вхідних, схованих і вихідних нейронів, структура зв'язків (топологія мережі), правила розповсюдження сигналів в мережі, правила комбінування сигналів, що входять в нейрон, правила обчислення вихідного сигналу нейрона та правила навчання, що коректують зв'язки в мережі. Ці параметри використовують в якості критеріїв класифікації НМ. Наприклад, по критерію структури зв'язків, розрізняють одно- та багатошарові НМ. Крім того, застосовуються цілий ряд додаткових критеріїв класифікації НМ. Наприклад, серед багатошарових НМ виділяють монотонні мережі. Сукупність вказаних параметрів визначають архітектуру мережі. Відомий ряд архітектур, що вже стали класичними – мережа пошуку максимума, вхідна та вихідна зірка, одношаровий перспетрон, БШП, мережа з радіальною базисною функцією (РБФ), мережі Хопфілда, Хеммінга, Коско, Маккаллока-Питтса, Кохонена, Гросберга, ймовірністні мережі та мережа АРТ. Крім того, розроблена значна кількість специфічних

архітектур – рекурсивна автоасоціативна пам'ять, модульні НМ, когнітрон, неокогнітрон, мережі, що використовують апарат нечіткої логіки, СНМ, різні типи рекурентних мереж та багато інших. При цьому для кожного класу прикладних задач використовується своя архітектура НМ.

З точки зору теорії технічного контролю, найбільш важливою характеристикою НМ, яка взагалі визначає можливість її практичного використання, є помилка контролю мережі. Під цим терміном будемо розуміти помилку при класифікації мережею вхідного образу (вектору), як одного із еталонних образів. В теорії НМ аналогом помилки контролю є помилка узагальнення мережі. Зазначимо, що властивість узагальнення характеризує можливості НМ проводити правильну класифікацію вхідних образів, що не були представлені в навчальних даних. Розрахунковий вираз помилки узагальнення складається із двох частин – помилки опису моделі та помилки апроксимації навчальних даних. Таким чином, помилка узагальнення характеризує не тільки помилку розпізнавання невідомих образів, але й помилку НМ на навчальних даних.

При визначеній моделі НМ помилка апроксимації в першу чергу залежить від методу та алгоритму навчання мережі. В випадку використання ітераційних алгоритмів навчання помилка апроксимації також залежить від максимально допустимої кількості ітерацій. Для сучасних НМ можливо досягнути достатньо низьких величин помилки апроксимації. Наприклад, максимальна відмінність між модельними та вхідними даними при апроксимації нелінійних функцій за допомогою БШП становить близько 1%. Зазначимо, що в багатьох випадках зменшення помилки апроксимації пропорційне збільшенню потужності НМ. Тобто для досягнення необхідної помилки апроксимації рекомендується збільшити кількість нейронів, шарів нейронів та кількість синаптичних зв'язків. Помилка опису моделі характеризує адекватність побудованої НМ тим процесам, що лежать в основі формування вхідних образів. Величина помилки опису залежить від формальної моделі нейрону, топології НМ, потужності НМ, адекватності навчальної інформації. Наведемо загальноприйняті шляхи зменшення помилки опису моделі:

– Використання тієї архітектури НМ, яка найбільш повно відповідає специфіці прикладної задачі. На сьогодні вибір архітектури відбувається емпірично та значною мірою залежить від традиційної сфери її застосування та наявного програмно-апаратного забезпечення. Найчастіше використовують НМ з однією із класичних архітектур. Інколи розробляють НМ з оригінальною архітектурою, що включає формальну модель нейрону, яка відрізняється від загальновідомої моделі (1.1-1.4).

– Використання із декількох можливих НМ з заданою топологією найменш потужної. При цьому мінімально допустима потужність мережі визначається максимально допустимою помилкою апроксимації навчальних даних. Водночас помилку апроксимації можливо розрахувати тільки при навчанні вже побудованої НМ. Тому досить часто визначення достатньої потужності НМ реалізується експериментально.

– Невідомі вхідні образи не повинні значно відрізнятись від навчальних даних. Наприклад, при апроксимації функції виду $y = f(x)$ інтервал навчальних даних $X_н = [a, b]$ повинен перекривати інтервал невідомих даних $X_р = [c, d]$. Однак в загальному випадку чіткого алгоритму визначення відповідності навчальних та невідомих вхідних даних на сьогодні не існує.

– Основний закон, який повинен моделюватись мережею повинен добре прослідковуватись в навчальних даних, а не затінюватись в них несуттєвими закономірностями. Для цього навчальні дані перед використанням в НМ проходять попередню обробку. Під цією обробкою розуміється нормалізація даних, їх фільтрація та перекодування.

– Вважається, що в багатьох практичних сферах НМ дозволяють досягти помилки узагальнення 10% при одночасній помилці апроксимації ≈0-2%. При цьому однією із

основних передумов використання НМ є складність формалізації задачі, що призводить до неефективності застосування класичних математичних методів для її вирішення.

В теоретичних роботах, присвячених НМ, наголошується, що використовувати їх доцільне в задачах: класифікації та кластеризації образів, апроксимації функцій, визначення прогнозованих величин деякого процесу, оптимізації складної функції, управління з еталонною моделлю, створення інформаційно-обчислювальних систем з пам'яттю, що адресується за змістом (асоціативної пам'яті)..

Перелік традиційних передумов та сфер застосування НМ підтверджують доцільність їх використання для розв'язання задач контролю параметрів безпеки комп'ютерних систем (КС) та управління засобами захисту інформації (ЗЗІ). По-перше, контроль параметрів безпеки є важкоформалізуємою задачею по причині суб'єктивних процесів, що є основою зміни цих параметрів. По друге, розпізнавання небезпечного стану контрольованих параметрів КС та оптимізація управління параметрами захисту відносяться до тих задач, де НМ вже довели свою ефективність. Водночас слід врахувати обмеження на використання НМ. В першу чергу це стосується тих задач захисту інформації (ЗІ), для розв'язання яких існує формалізований математичний апарат. Крім того, деякі фахівці застерігають, що НМ багато в чому є аналогом статистичних методів аналізу інформації і, як наслідок, схильні помилятись при застосуванні зловмисником нестандартних прийомів. Однак в багатьох випадках появі нестандартних прийомів можливо запобігти як при постановці задачі, так і за допомогою стандартних ЗЗІ. Також в роботах [1,2] зазначається, що представлення НМ у вигляді простого статистичного фільтру є дещо поверхневим. Разом з тим в новітніх типах НМ додатково реалізована аналогія з засобами класичного штучного інтелекту, наприклад, з семантичними мережами. Тому слід сподіватись, що сучасні типи НМ дозволять правдиво діагностувати ситуації, які не були представлені в початкових статистичних даних. Окреслюючи сферу застосування НМ слід врахувати, що можливості мережі значною мірою залежать від її архітектури. При цьому розвиток сучасних НМ йде шляхом пристосуванні базових архітектур для вирішення практичних задач. Разом з тим ряд класичних архітектур вже втратили свої передові позиції і використовуються тільки в якості допоміжних. Тому слід зосередити увагу на адаптації НМ з найбільш перспективною базовою архітектурою до проблем моніторингу параметрів захисту КС та управління ЗЗІ. Базуючись на висновках [1, 2, 3] та аналізі вказаної проблеми, для розгляду виберемо БШП, РБФ, НМ адаптивної резонансної теорії (АРТ), мережі Хеммінга, Хопфілда, Коско та Кохонена. Відзначимо, що вибрані мережі погано пристосовані для аналізу тексту, який є важливою складовою при розпізнаванні спаму. Тому, крім класичних архітектур, доцільно розглянути синаптичну нейронну мережу (СНМ), яка є однією із найбільш досконалих мереж в галузі обробки текстової інформації [4]. Відзначимо, що внаслідок заданого обсягу публікації остаються без уваги деякі інші, можливо і перспективні, але не достатньо апробовані та теоретично вивчені архітектури.

Задачі захисту інформації які доцільно вирішувати за допомогою НМ

Можна сформулювати висновок, що основними напрямками застосування НМ в галузі комп'ютерного забезпечення технічних та економічних систем є розпізнавання образів, визначення оптимальних управляючих рішень та створення асоціативної пам'яті. До першого напрямку віднесемо задачі класифікації образів, кластеризації образів та апроксимації функцій. Зазначимо, що до групи задач апроксимації функції слід віднести розрахунок параметрів процесів, що відбуваються в технічних системах. Адже по своїй суті оцінка регресивних або прогнозованих значень параметрів деякого процесу є апроксимацією функції, що описує цей процес. До другого напрямку віднесемо власне задачі оптимального управління та задачі управління з еталонною моделлю. До третього напрямку входять задачі створення інформаційно-обчислювальних систем з пам'яттю, що адресується за змістом. Зрозуміло, що використання НМ для вирішення конкретної задачі галузі захисту ПЗ КС повинно починатись із визначення до якого із вказаних напрямків відноситься задача.

Відповідно [3, 4] на практиці найбільш актуальними та важливими задачами захисту є створення СВВ (систем визначення вразливостей), СВА (систем визначення атак), антивірусів, антикейлогерів, систем протидії спаму та фішінгу, систем управління функціональними параметрами та параметрами безпеки, систем резервування та відновлення даних. Типовий алгоритм функціонування СВВ, СВА, антивірусів, антикейлогерів, систем протидії спаму та фішінгу такий:

– Проводиться початкова настройка параметрів системи захисту. Як правило в початкових настройках відображається режим контролю, підконтрольні параметри та деякі параметри захисних заходів. Наприклад в антивірусних системах може настроюватись період контролю об'єктів файлової системи, режим функціонування постійного захисту, номенклатура заходів проти заражених файлів (блокування, лікування та знищення).

– З визначеною періодичністю реєструються певні параметри КС. Наприклад, в СВВ реєструються відкриті порти операційної системи, імена користувачів, версія операційної системи, права користувачів та ін. В СВА можуть реєструватись параметри мережених запитів, обсяг мережевого трафіку, кількість мережевих запитів за певний проміжок часу. В антивірусах та антикейлогерах можуть реєструватись фрагменти програмного коду, що відповідають сигнатурам вірусів та/або програмні події які супроводжують функціонування вірусу (звернення до системного реєстру, звернення до поштової програми) або кейлогеру (перехват натиску клавіш, запис змісту екрану). В антиспамових системах реєструються адреси відправника електронної пошти та окремі слова електронного листа.

– Проводиться первинна обробка зареєстрованих параметрів. Наприклад, в СВА підраховується частота мережевих запитів за одиницю часу. В антиспамових системах підраховується частота зустрічі кожного із зареєстрованих слів. При необхідності первинна обробка проводиться до реєстрації або паралельно з нею. Наприклад в антивірусах та антикейлогерах програмний код при необхідності дешифрується.

– На основі зареєстрованих даних за допомогою спеціального алгоритму приймається рішення про безпеку КС. Наприклад, в СВВ це рішення про потенційні вразливості, в СВА це рішення про наявність атаки.

– Адміністратор системи інформується про виявлену загрозу або потенційну вразливість.

– Спрацьовує захисний модуль системи. При цьому, спочатку приймається рішення про захисний захід, а потім цей захід реалізується. В простих випадках рішення про захисний захід приймається на основі тільки початкових настройок системи, а в складних випадках – за допомогою набору спеціальних правил. Наприклад, заражений вірусом файл необхідно спробувати вилікувати. Якщо ж спроба лікування не вдалась, то файл необхідно знищити. В антиспамових системах електронний лист класифікований як спам може бути знищений або тільки помічений як нецільовий. Водночас адреса відправника цього листа може бути помічена як підозріла або повністю заблокована.

– Якщо в розглянутій системі модуль реакції на загрозу відсутній, то висновок про небезпеку може бути переданий іншій системі, що управляє параметрами захисту. Наприклад, в СВА рішення про наявність атаки може бути передане системі захисту від мереженої атаки.

Як свідчить практичний досвід та висновки [3, 4] основні труднощі при розробці вказаних систем полягають у розробці ефективного контуру розпізнавання. При цьому, з точки зору теорії НМ задачі, що вирішується за допомогою даного блоку відносяться до найбільш дослідженого напрямку розпізнавання образів. На наш погляд це вказує на беззаперечні перспективи використання НМ для розпізнавання вірусів, кейлогерів, спаму, мережевих атак на КС та вразливостей КС.

Другий та третій напрямок застосування НМ (визначення оптимальних управляючих рішень та створення систем з асоціативною пам'яттю) менш досліджені. Крім зазначених задач визначення захисних заходів в СВВ, СВА, антивірусах, антикейлогерах, системах

протидії спаму та фішінгу до другого напрямку можна віднести задачі визначення функціональних параметрів та параметрів політики безпеки конкретної КС. Наприклад, за допомогою НМ можливо визначити розподіл навантаження декількох комп'ютерів–серверів, необхідність та тривалість блокування ресурсу, захищеного паролем, або необхідність та тривалість блокування доступу до ресурсу з певної IP-адреси. Відзначимо, що до параметрів політики безпеки слід включити параметри режиму контролю КС за допомогою конкретної системи захисту. Наприклад, на практиці доцільно визначити оптимальний період контролю антивірусом або/та антикейлогером конкретної локальної мережі. Третій напрямок застосування НМ може знайти своє відтворення в системах резервного збереження даних та відновлення пошкодженої інформації. Однак, на сьогодні недостатня теоретична база перешкоджає практичному використанню НМ для вирішення задач другого та третього напрямків. Відомі лише окремі спроби вирішення оптимізаційних задач за допомогою мереж Хопфілда та Кохонена. Крім того, відповідно висновків [1, 2], створення ефективних КС з асоціативною пам'яттю багато в чому є проблемою розробки оригінального, а значить і достатньо дорогого апаратного забезпечення. В підсумку, характер застосування НМ при вирішенні деяких актуальних задач захисту ПЗ можна оцінити за допомогою табл. 1.

Таблиця 1

Оцінка перспектив використання НМ в розповсюджених системах захисту

Назва системи захисту	Мета застосування НМ	Функціональний блок	Вид задачі
1	2	3	4
Антивірус	Розпізнавання вірусів	Розпізнавання атак (загроз)	Розпізнавання образів
Антикейлогер	Розпізнавання кейлогерів		
СВА	Розпізнавання мережевих та локальних атак		
Антиспамова система	Класифікація електронних листів		
СВВ	Розпізнавання неправильних настройок та параметрів	Розпізнавання вразливостей	
Антивірус	Визначення параметрів протидії розпізнаним вірусам	Прийняття рішення про захисні заходи	Визначення оптимальних управляючих рішень
Антикейлогер	Визначення параметрів протидії розпізнаним кейлогерам		
СВВ	Визначення величини корекції параметрів		
СВА (в комплексі з системою протидії)	Визначення параметрів протидії атаці		
Антиспамова система	Визначення параметрів протидії спаму та підозрілим листам		
Система захисту від НСД	Визначення прав користувачів, визначення параметрів протидії спробі НСД		
Система балансування навантаження серверів	Визначення серверу, який буде виконувати черговий запит		

1	2	3	4
Система резервування даних	Підвищення живучості даних	Зберігання даних	Система з асоціативної пам'яттю

Визначення доцільності застосування конкретного типу нейронної мережі

Аналіз сучасного стану нейромережевих технологій дозволяє сформулювати висновок про те, що доцільність застосування конкретного типу НМ слід визначати на основі співставлення характеристик мережі з умовами прикладної задачі. До вказаних характеристик НМ відносяться:

1. Параметри навчальних даних.
2. Загальні обмеження процесу навчання НМ
3. Вимоги до обчислювальних потужностей НМ.
4. Вимоги до вихідної інформації НМ.
5. Обмеження технічної реалізації НМ.
6. Сфера застосування.

Розглянемо вказані характеристики в ракурсі захисту ПЗ КС.

1. До основних параметрів навчальних даних відносяться:

– Кількість параметрів, що характеризують навчальний приклад.
– Вид параметрів, дискретний (символьний) чи безперервний (числовий).
– Загальна кількість навчальних прикладів.
– Наявність помилок (шуму) в навчальних прикладах.
– Наявність кореляції навчальних прикладів.
– Можливість та необхідність попередньої обробки вхідних даних з метою їх нормалізації та видалення шуму.
– Можливість відображення в навчальній виборці всіх аспектів процесу, що моделюється. Наприклад, чи можливо відобразити в навчальній виборці сигнатури всіх вірусів, або сигнатури мережевих атак певного типу.
– Пропорційність навчальних прикладів, що відповідають різним аспектам процесу, що моделюється. Наприклад скільки навчальних прикладів відповідають мереженій атаці типу А, а скільки прикладів – атаці типу В.

2. Загальні обмеження процесу навчання обумовлюються:

– Максимальним терміном навчання.
– Необхідністю представлення в навчальних даних очікуваного вихідного сигналу НМ. Таким чином визначається можливий тип навчання – з вчителем або без вчителя.
– Можливістю автоматизації процесу навчання, яка визначається кількістю та важливістю емпіричних параметрів. Вказана можливість багато в чому визначає умови застосування НМ. Мережі в яких процес навчання не автоматизовано можуть використовуватись тільки в лабораторних умовах.
– Можливістю донавчання в процесі експлуатації.
– Вимогами до якості навчання, яке звичайно оцінюють по величині максимальної та середньої помилки розпізнавання навчальних та тестових даних. При цьому тестові дані повинні не значно відрізнятись від навчальних.
– Можливістю навчання НМ в лабораторних умовах. Наприклад, в лабораторних умовах потенційно можливо навчити НМ розпізнавати мережеві атаки певного типу. В той же час неможливо навчити НМ класифікувати електронні листи відповідно інтересам конкретного користувача. Доцільність навчання в лабораторних умовах пояснюється потребами оптимального механізму створення та оновлення бази знань НМ.

3. На практиці вимоги до обчислювальних потужностей визначаються максимальною кількістю прикладів (обсяг пам'яті), яку може запам'ятати мережа для досягнення необхідної достовірності прийняття рішення. В свою чергу достовірність прийняття

рішення характеризується допустимими величинами максимальної та середньої помилки мережі на реальних даних які в загальному випадку можуть виходити за межі множини навчальних даних. Відповідно виникає задача екстраполяції результатів навчання НМ за межі навчальних прикладів. Відзначимо, що обчислювальна потужність мережі залежить від її типу та алгоритму навчання. Ще однією вимогою може бути незмінність виходу мережі для різних прикладів з однаковими параметрами.

4. Вимоги до вихідної інформації НМ вказують на те в якому вигляді має бути представлена ця інформація. Наприклад, при розпізнавані вірусів може виникнути необхідність не тільки визначення ситуації "вірус А присутній", але й розрахунку ймовірності цієї ситуації. Стосовно класифікації електронних листів вихідною інформацією НМ може бути відображення листів на площину, яке дозволить провести остаточну класифікацію користувачеві. Ще однією вимогою може бути необхідність визначення вербальних залежностей між вхідною та вихідною інформацією.

5. Обмеження технічної реалізації НМ стосуються:

– Швидкості прийняття рішення.

– Обсягу та складності програмної реалізації. Для зменшення обсягу можливо розділити програмний код для навчання мережі від коду, що відповідає за її функціонування.

– Інтеграції в існуючі ЗЗІ.

6. Сфера застосування визначає засоби захисту інформації в яких буде використовуватись НМ. На сьогодні достатньо дослідженим є використання НМ для розпізнавання образів та при проведенні оптимізаційних розрахунків. Відзначимо, що системи розпізнавання образів принципово відрізняються від систем аналізу тексту тим, що в них кількість вихідних та кількість комбінацій вхідних параметрів принципово обмежена. В системах аналізу тексту ця кількість принципово необмежена. Відповідно в системах виявлення атак та виявлення вразливостей слід використовувати НМ призначені для розпізнавання образів. В системах захисту від спаму можливо використати НМ призначені для аналізу тексту. В системах керування параметрами засобів захисту слід застосувати НМ призначені для проведення оптимізаційних розрахунків. В перспективі доцільно застосувати НМ з метою реалізації паралельних розрахунків в комп'ютерних системах, що дозволить значно підвищити їх стійкість від багатьох типів атак з метою відмови в обслуговуванні. Крім того, сфера застосування визначається пристосованістю мережі до автономного функціонування. Для цього в архітектурі НМ повинно бути передбачено можливість повної автоматизації процесу донавчання на експлуатації.

Якісні оцінки відповідності основних характеристик НМ умовам задач захисту програмного забезпечення для перспективних типів мереж наведені в табл. 2. В табл. 2 відсутні характеристики, які хоча і застосовуються при побудові мережі, але не впливають на вибір типу НМ. Оцінки відповідності виставлені в числовому вигляді по трьохбальній системі (-1 – мінімальна, 0 – середня, 1 – максимальна). Величини оцінок розраховані в результаті порівняльного аналізу розглянутих типів НМ, проведеного в [1, 2, 5]. Відсутність оцінки означає, що для її визначення потрібні додаткові дослідження.

Слід відзначити, що в задачах які зводяться до розпізнавання образів при відсутності обмежень на використання методу навчання "з вчителем", термін навчання, донавчання, автономність функціонування, представлення результатів розпізнавання, обсяг програмної реалізації, кількість та якість навчальних даних найбільш ефективним є використання БШП. Його ефективність пояснюється найбільшою обчислювальною потужністю, можливістю автоматизації процесу навчання та вербалізації отриманих результатів. Інші типи НМ доцільно застосувати для оперативного попереднього аналізу або в специфічних випадках, що характеризуються певними обмеженнями.

Таблиця 2

Якісні оцінки відповідності НМ умовам задач захисту

Умова	БШП	РБФ	Кохонена	АРТ	СНМ	PNN/ GRNN	Асоціа-тивні
1	2	3	4	5	6	7	8
Навчальні дані							
Допустимість шуму	1	0	1	-1	1	0	-1
Допустимість кореляції	1	1	1	1	1	1	-1
Необхідність відображення всіх аспектів процесу	-1	1	1	-1	-1	1	0
Необхідність пропорційного представлення прикладів	1	-1	-1	-1	-1	-1	0
Загальні обмеження процесу навчання							
Короткий термін навчання (малий обсяг навчальних ітерацій)	-1	0	1	1	0	1	1
Необхідність представлення в навчальних прикладах очікуваного виходу	1	1	-1	-1	-1	1	1
Автоматизація процесу навчання	1	-1	0	1	1	1	0
Можливість донавчання	0	1	1	1	1	1	0
Якість навчання	1	0	0	1	1	1	1
Обчислювальні потужності							
Обсяг пам'яті	1	-1	-1	-1		-1	0
Екстраполяції результатів навчання	1	-1	-1	-1		-1	1
Незмінність результатів	1	1	0	1	1	1	0
Вихідна інформація							
Можливість інтерпретація виходу у вигляді ймовірності	0	0	-1	-1	-1	1	0
Можливість інтерпретації виходу у графічному вигляді	-1	-1	1	-1	-1	-1	-1
Можливість вербалізації	1	0	-1	-1	-1	0	-1
Обмеження технічної реалізації НМ							
Швидкості прийняття рішення	1	1	1	1	0	1	-1
Обсяг програмної реалізації	-1	1	-1	0	-1	-1	0
Сфера застосування							
Системи розпізнавання образів	1	1	1	1	0	1	1
Системи аналізу тексту	-1	-1	1	0	1	0	-1
Системи управління	-1	-1	1	-1	-1	-1	1
Пристосованість до автономного функціонування	-1	-1	-1	1	1	-1	-1

Висновки

НМ слід використовувати тільки для вирішення тих задач захисту програмного забезпечення які відносяться до класу розпізнавання образів, оптимального управління та систем асоціативної пам'яті.

З точки зору теорії НМ практичний ефект можна очікувати при їх застосуванні в контурі розпізнавання атак (загроз) антивірусів, СВА, антиспамових систем, антикейлогерів та в контурі розпізнавання вразливостей СВВ.

Визначити принципову доцільність застосування одного або декількох типів НМ можливо на основі рекомендацій, наведених в табл. 2. Остаточне рішення про використання конкретного типу НМ повинно бути прийнято після проведення порівняльних експериментів.

Список літератури

1. *Ежов А.А., Шумский С.А.* Нейрокомпьютинг и его применения в экономике и бизнесе. – М.: МИФИ, 1998. – 224 с.

2. *Каллан Р.* Основные концепции нейронных сетей. – М.: Вильямс, 2003. – 288 с.

3. *Шуклін Д. Є.* Моделі семантичних нейронних мереж та їх застосування в системах штучного інтелекту: 05.13.23.. // Дис. …канд. техн. наук. – Харків, 2003. – 196 с.

4. *Терейковский И.А.* Использование искусственных нейронных сетей в задачах распознавания атак на компьютерные системы. // Захист інформації, 2006, №3. – С.57-65 .

5. *Хорошко В.А., Чекатов А.А.* Методы и средства защиты информации. – К.: Изд. Юниор, 2003. – 504 с.

6. *Лукацкий А.В.* Обнаружение атак .– СПб.: БХВ–Петербург, 2003.–624 с.

Надійшла 15.11.2007р.

УДК 004.056.5:519.17

Кобозева А.А., Хорошко В.А.

ИСПОЛЬЗОВАНИЕ ТЕОРИИ ГРАФОВ ДЛЯ АНАЛИЗА СТРУКТУРЫ ТЕРРОРИСТИЧЕСКИХ СЕТЕЙ

Постановка проблемы в общем виде, анализ последних достижений и публикаций

Для возможности использования математических методов и средств вычислительной техники для обработки и анализа информации о произвольном объекте, в первую очередь, необходимо представление данных об объекте на языке математических формул и выражений, т.е. создание его математической модели. В последнее время чрезвычайно активизировалась работа по использованию достижений современной математической науки в области борьбы с различными криминальными организациями, террористическими группами (далее – противником). Активно ведутся поиски эффективных методов моделирования деятельности криминальных групп [1-5], а также формализации анализа структуры этих организаций и результатов применения тех или иных контртеррористических действий при помощи средств вычислительной математики. Однако ни одна, из построенных в [1-5] моделей не является удовлетворительной по тем или иным причинам для решения наиболее традиционных задач, связанных с контртеррористической деятельностью.

В [6] была предложена графовая модель противника со строго обоснованным учетом иерархии группы при помощи использования взвешенного неориентированного графа, что никогда не делалось ранее. Предлагаемая математическая модель успешно использовалась для решения задачи о разрушении моделируемой группировки противника, а также численной оценки ущерба, наносимого противнику посредством контртеррористических действий. Данная графовая модель чрезвычайно перспективна [6]