УДК 004.8

В.В. Шищук, аспір.
Європейський університет, м.Київ

ВИКОРИСТАННЯ ІНТЕЛЕКТУАЛЬНИХ ТЕХНОЛОГІЙ ПРИ ВИЯВЛЕННІ ВТОРГНЕНЬ

(Представлено д.т.н., проф. Грабаром І.Г.)

В статті описано принцип організації захисту інформаційних систем на основі нейромережевих технологій порівняно з використанням експертних систем, розкриваються переваги та недоліки даних підходів.

Постановка проблеми. В період всеохоплюючої комп'ютеризації та інформатизації всіх сфер людської діяльності немає необхідності в доказах щодо їх доцільності, але разом з усіма перевагами комп'ютеризовані об'єкти набули цілий ряд проблем, які пов'язані із захистом інформації. Якщо раніше даній проблемі надавалась незначна увага, то сьогодні це – чи не найперше питання, яке потрібно прийняти до уваги кожному керівнику підприємства при впровадженні чи розширенні власної інформаційної системи, оскільки в кожній частині світу знайдуться особи чи організації, які будуть мати специфічний інтерес до чужої інформації. Цей факт підтверджують статистичні дані досліджень (рис. 1) Internet Security Systems [3], крім того, відповідно до стратегічних звітів НАТО [4] існуючі системи виявлення вторгнень щоденно фіксують близько 500 спроб несанкціонованого автоматичного вторгнення, що складає, за думкою спеціалістів, 14–17 % від загальної кількості атак, які здійснюються. А за даними ФБР [2] в 2003 році 56 % опитаних компаній потерпали від атак (рис. 2). Отже проблема захисту є актуальною та постійно зростаючою.

На даний момент існує ряд робіт та цілий напрям в дослідженні економічної ефективності використання систем захисту інформації [8], [10]. При цьому потрібно мати на увазі, що за структурою існує багато варіантів побудови таких систем. Схеми виявлення вторгнень глобально можуть класифікуватися за двома категоріями: неправильне використання та виявлення аномалій. Неправильне використання належить до визначення відомих атак, які направлені на відомі вразливості системи. Аномалія означає незвичну діяльність взагалі, яка може вказувати на атаку. В даному випадку вважається, що атака відбувається, коли діяльність користувача (чи захисного засобу) відхиляється від поведінки, яка очікується.

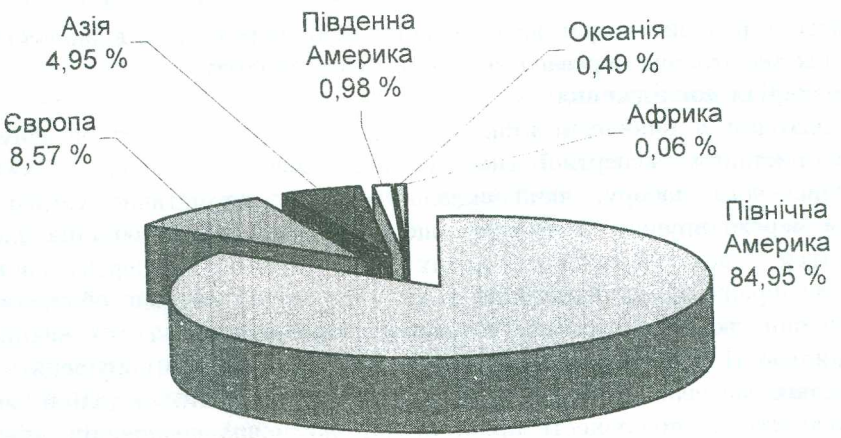

Рис. 1. Джерела проведених атак за IV квартал 2003 р.

До галузі практичного застосування першої схеми належать експертні системи, які діють на основі передбачених правил, відхилення від яких дозволяє ідентифікувати відомі атаки. Але такі системи виявляються безсилими проти нових видів атак, шаблони яких відсутні, а оскільки різновиди атак з'являються щоденно, надійність не є гарантованою. Щодо другої схеми виявлення вторгнень, то базою спостерігання за поведінкою виступають саме нейронні мережі, використання яких і є найбільш перспективним напрямом даної проблеми.

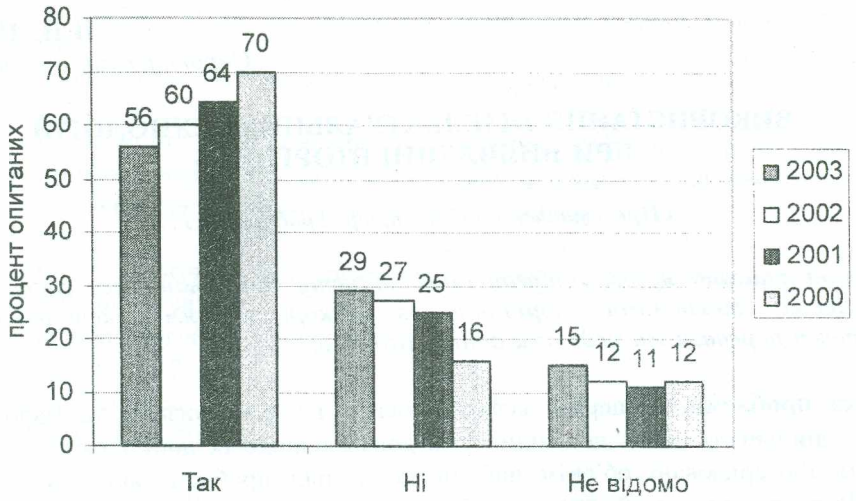

Рис. 2. Результати опитування щодо виявлення вторгнень в інформаційні системи

Аналіз останніх досліджень і публікацій виявляє пріоритетні напрями в організації систем захисту інформаційних ресурсів. Якщо раніше спеціалісти розглядали можливості захисту на системному чи мережевому рівні [5], [6], [7], то сьогодні перспективним напрямком виявляється залучення штучного інтелекту до процесу виявлення атак [4], [6]. Причому він виступає не лише в ролі обмеженої експертної системи, яка працює за шаблонами [4], [5], [6], але й системи розпізнання аномалій (в тому числі й раніше невідомих), наприклад на основі інваріантів подібності [4].

Невирішені раніше частини основної проблеми

Незважаючи на те, що застосування експертних систем та нейронних мереж в захисті інформаційних ресурсів розглядається вже досить давно, сьогодні з'являються нові ідеї та їх втілення в реальні системи захисту інформації. Одним з таких напрямів може бути використання нейромережі для визначення вторгнень або так званої аномальної поведінки користувачів на основі аналізу дій, здійснених кожним з них. Іншим – використання нейромережі як допоміжного засобу у вигляді мікроагентів до стандартних захисних засобів, таких як міжмережевий екран (firewall), при цьому визначається аномальна поведінка самого засобу.

Метою статті є розкриття суті використання нейромережі для визначення вторгнень та аномалій, а також висвітлення переваг і недоліків такого підходу.

Основний матеріал дослідження

Сучасним підходом у виявленні атак, який реалізований в багатьох існуючих системах захисту, є використання експертної системи, яка проводить аналіз на основі правил з попередньо визначеного набору, який складається або автоматично самою системою або адміністратором мережі вручну. Саме тому, що інформація, яка необхідна для ідентифікації атаки, зберігається у великій кількості даних аудиту, робить експертну системою набагато ефективнішою за працю людини-адміністратора. Експертні системи об'єднують величезний досвід, накопичений людиною, в комп'ютерному втіленні, який потім використовують для ідентифікації діяльності, що відповідає визначеним характеристикам порушень.

При безперечних перевагах експертні системи показали істотні недоліки, які полягають в недостатній гнучкості та повільності пристосувань до нових різновидів атак. Якщо атака ідентифікується системою як вторгнення, то незначні варіації в послідовності дій останньої може призвести до ідентифікації такої дії як коректної. Крім того, такі системи не вміють визначати атаки, які розподілені в часі, тобто здійснюються протягом тривалого періоду, або які розподілені в просторі, тобто здійснюються декількома виконавцями, що працюють узгоджено. Від подібних істотних недоліків звільнені інші технології, які грунтуються на нейронних мережах [1].

Інтелектуальні нейронні мережі (Artificial Neural Networks – ANN) складаються з простих одиниць (нейронів), які працюють паралельно і які є абстракцією біологічних нейронів. Як і в

природі, функція мережі визначається зв'язками між нейронами. Виділяють три основних елементи моделі нейрона: набір ваг синапсів, інтеграція та функція активації. На рис. 3 показана схема нейрона.

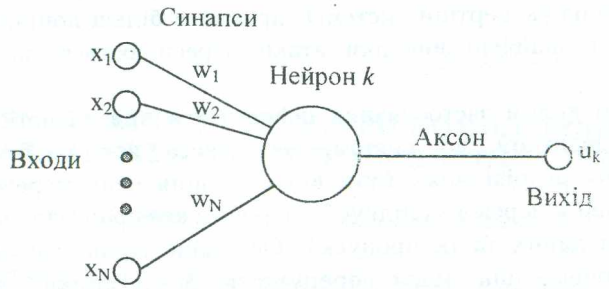

Рис. 3. Схема нейрона

Математична модель нейрона k описується наступними рівняннями:

$$u_k = \sum_{i=1}^{N} w_{ki} x_i + b_k \,, \tag{1}$$

$$y_k = \varphi(u_k) \tag{2}$$

де x_i – вихід i-го нейрону, w_{ki} – вага від i-го до k-го нейрону, b_k - систематична помилка (відхилення) k-го нейрону, u_k – збудження нейрону k, $\varphi()$ – функція активації та y_k – вихід k-го нейрону (значення аксона).

Існує декілька типів функцій активації, які використовуються в ANN, але найчастіше використовується так званий сігмоїд, який має вигляд:

$$\varphi(u) = \frac{1}{1 + e^{-\alpha u}} \tag{3}$$

Сигмоїдна функція генерує безперервні вихідні значення між 0 та 1, оскільки на чистому виході нейрона значення змінюється від від'ємної до додатної нескінченності. Вона визначена як строго зростаюча функція, гладка та має асимптотичні властивості. Сигмоїдна функція є диференційованою на всій осі абсцис і має дуже просту похідну (4), що є важливою особливістю нейромережевої теорії.

$$\varphi'(u) = \alpha\varphi(u)(1 - \varphi(u)) \,. \tag{4}$$

При зменшенні параметра α сигмоїд стає більш пологим, вироджуючись в горизонтальну лінію на рівні 0,5 при $\alpha = 0$. При збільшенні α сигмоід все більше наближається до функції одиничного скачка.

Набір нейронів складає нейромережу. Причому нейромережі розрізняються своєю архітектурою: структурою зв'язків між нейронами, кількістю шарів, функцією активації нейронів, алгоритмом навчання [9]. З цієї точки зору серед відомих ANN можна виділити: статичні, динамічні мережі, fuzzy-структури, одно- та багатошарові мережі. Відмінності обчислювальних процесів у мережах частково обумовлені способом взаємозв'язку нейронів: мережі прямого розповсюдження, з оберненими зв`язками, з боковими оберненими зв'язками, гібридні мережі.

Суть роботи нейромережі полягає в тому, що вона проводить аналіз інформації і дозволяє оцінити, чи відповідають дані характеристикам, які вона навчена розпізнавати. При цьому достовірність прийнятих рішень повністю залежить від ступеню навченості. Спочатку нейромережу навчають правильній ідентифікації на попередньо підібраних прикладах. Її реакція вивчається і система налагоджується таким чином, щоб досягти бажаних результатів. Крім того, нейромережа продовжує навчатися і під час її експлуатації, оскільки вона весь час аналізує дані, які надходять.

На відміну від експертних систем, нейромережі гнучкі, оскільки вони аналізують будь-які дані – неповні, спотворені, причому робити це потрібно в нелінійному режимі й від багатьох джерел, що робить їх більш надійним при проведенні скоординованої атаки з різних місць. Але при цьому істотним недоліком нейромережі є необхідність її навчання, для якого потрібна велика кількість тестових прикладів, причому наявність атаки під час навчання може бути сприйнята як коректна подія.

Взагалі існує два підходи використання нейромереж в системах ідентифікації атак – разом з експертною системою (існуючою або видозміненою) або як окремої системи. Перший спосіб дає більший захист, оскільки реалізується два рівні захисту (фільтрується трафік та пересилаються „підозрілі" події на аналіз експертній системі), другий – більш доцільний зі сторони швидкості (трафік аналізується, і знайдені випадки атаки пересилаються на систему реагування або адміністратору).

Але це не є повним колом застосування нейромереж при захисті інформаційних ресурсів. Вони можуть бути додатком до систем мережевого або системного рівнів. Найбільш перспективним в даному розрізі може бути використання нейромережі разом з міжмережевим екраном. При цьому нейромережа „слідкує" за роботою екрану та навчається ідентифікувати його події (блокування даних та їх пропуск). Оскільки екран має свої недоліки, пов'язані з функціональною стороною, він може пропускати деякі атаки, які будуть сприйматися нейромережею як відступ від правил і, відповідно, буде генерувати необхідну дію (повідомлення, пересилання на систему реагування і т.ін.).

Висновки та перспективи подальших розвідок

Інтелектуальність машин в наш час стає реальністю, а не далекою фантастикою, і використання штучного інтелекту надає людині багато переваг, передусім в питаннях захисту інформаційних ресурсів. Нейромережі стали об'єктом дослідження як перспективний напрямок в ідентифікації зловживань завдяки своїй гнучкості та універсальності, і незважаючи на недоліки, такі як „чорний ящик" та необхідність навчання, вони стають невід'ємним елементом в нових системах захисту. Крім того, вихідні дані нейромереж виражаються в формі ймовірності, що являє собою можливість здійснювати прогнозування майбутніх зловживань.

ЛІТЕРАТУРА:

1. Artificial Neural Networks: Concepts and Theory, IEEE Computer Society Press, 1992.
2. CSI/FBI 2003 Computer Crime and Security Survey // Computer Security Institute. – 2004.
3. Internet Risk Impact Summary: Internet Security Systems, 2003.
4. *Беляев А., Петренко С.* Системы обнаружения аномалий: новые идеи в защите информации // Экспресс электроника. – № 2. – 2004.
5. *Лукацкий А.В.* Обнаружение атак. – СПб.: БХВ-Петербург, 2001. – 624 с.
6. *Лукацкий А.В., Цаплев Ю.Ю.* Обнаружение атак: сетевой или системный уровень? // СЕТИ. – № 10. – 2002.
7. *Медведовский И.Д., Семьянов П.В., Леонов Д.Г.* Атака на Internet. – М.: ДМК, 1999.
8. *Петренко С., Симонов С., Кислов Р.* Информационная безопасность: экономические аспекты // Jet Info Online. – № 10. – 2003.
9. *Терехов В.А., Ефимов Д.В., Тюкин И.Ю.* Нейросетевые технологии управления: Учеб. пособие для вузов. – М.: Высш. шк., 2002. – 183 с.
10. *Шищук В.В.* Використання формальних моделей при аналізі ефективності систем захисту інформації // Інформаційні технології в економіці, менеджменті і бізнесі: Проблеми науки, практики і освіти: Матеріали VII Міжнародної наук.-практ. конф. – К.: Європейський університет, 2004.

ШИЩУК Вадим Володимирович – аспірант кафедри математики та інформаційних технологій відокремленого підрозділу Європейського університету в м. Житомирі.

Наукові інтереси:

- програмування;
- захист інформації.

Тел.: (0412) 418-719.

E-mail: sh_vadim@yahoo.com

Подано 22.09.2004