УДК 004.891

к.т.н, доц. **Бойчук В.О.** (ХмНУ)
Герасимчук К.С. (ХмНУ)
к.т.н., с.н.с. **Дергільова О.В.** (НУОУ)

ВИКОРИСТАННЯ ЧАСОВОЇ ТЕМПОРАЛЬНОЇ ПАМ'ЯТІ В ІДЕНТИФІКАЦІЇ ШКІДЛИВИХ ВПЛИВІВ НА КОМП'ЮТЕРНІ СИСТЕМИ

У статті на основі огляду сучасних штучних нейронних мереж показані їх особливості і недоліки при використанні в ідентифікації шкідливих впливів на комп'ютерні системи. Розглянуті особливості ієрархічної часової пам'яті та проведений огляд принципів її функціонування. Запропоновано принципи використання ієрархічної часової пам'яті в ідентифікації шкідливих впливів на комп'ютерні системи.

Ключові слова: нейронні мережі, ієрархічна часова пам'ять, ланцюг Маркова.

Вступ. Сьогодні Інтернет являє собою практично величезний колективний розум, що складається з мільярдів компонентів. Це дата-центри, сервера, смартфони, планшети і ноутбуки, датчики і навігатори, і ще сотні найменувань пристроїв. Кабелі і безпровідні зв'язки обплутали планету щільним клубком. Безпілотні автомобілі, з'являються в масовому виробництві і будуть керуватись через мережу. Щодня до мережі Інтернет підключаються всі нові пристрої різного ступеня складності. Сотні тисяч сайтів пропонують інформацію про все на світі. Сьогодні є холодильники, годинники, автомобілі з виходом в Інтернет. У них є своя операційна система, якась оболонка ОС. А це означає, що теоретично вони можуть бути атаковані з Інтернету з нанесенням шкоди гаджету або пристрою. У мільйонів людей на планеті щодня заражаються комп'ютери. Крадуться паролі і зламуються електронні пошти. Блокуються комп'ютери з метою вимагання грошей. Розсилається спам. Крім корисних сайтів і програм в Інтернеті досить багато справжнісінької кіберзброї. Це коди, створені для шкідливого впливу на комп'ютери і інші пристрої. Також хакери цілими днями шукають діри і лазівки в наявних оболонках і пристроях, щоб використовувати їх у своїх цілях. Зрозуміло, що за даних обставин необхідні або відповідне програмне забезпечення, або більш складних випадках експерти, які змогли б виявляти шкідливі впливи на комп'ютерні системи. Використання висококваліфікованих експертів досить вартісне і тому пропонується замінити їх штучними нейронними мережами.

Аналіз останніх досліджень і публікацій. Нейронні мережі - це адаптивні системи для обробки та аналізу даних, які являють собою математичну структуру, яка імітує деякі аспекти роботи людського мозку і демонструють такі його можливості, як здатність до неформального навчання, здатність до узагальнення і кластеризації інформації.

Головною їх відмінністю від інших методів є те, що нейромережі не потребують заздалегідь відомої моделі, а будують її самі тільки на основі пропонованої інформації. Саме тому нейронні мережі увійшли в практику всюди, де потрібно вирішувати задачі прогнозування, класифікації, управління.. Для неформалізованих задач нейромережеві моделі можуть по ефективності значно перевершувати традиційні методи вирішення. Застосування нейронних мереж доцільно коли накопичені достатні обсяги даних про попередню поведінку системи і не існує традиційних методів або алгоритмів для вирішення проблеми, дані частково перекручені або не повні. Нейронні мережі найкращим чином проявляють себе там, де є велика кількість вхідних даних, між якими існують неявні взаємозв'язки і закономірності. Якщо між вхідними та вихідними даними існує зв'язок, то нейронна мережа здатна автоматично налаштуватися на неї із заданим ступенем точності.

Однак такі особливості штучних нейромереж накладають деякі обмеження на використання для ідентифікації і вироблення реакцій комп'ютерних систем на шкідливі впливи.

Наприклад, в роботі [1] зроблено у дечому негативний висновок про систему виявлення шкідливих впливів з мережі Інтернет, яка заснована виключно на нейронних мережах і яка має в практичному плані певні складнощі, що не виключає однак застосування нейронних

мереж (НМ) в автономних (офф-лайн) системах. Необхідність навчання, а також природа «чорного ящика» обумовлює обов'язкову наявність навчальної бази даних зловживань, а також потребує великих часових витрат і коригувань навчального процесу (вибору архітектури мережі, алгоритми навчання). Основні переваги нейромереж - це виявлення невідомих атак, функціонування в оточенні з великим значенням шумів, збереження працездатності при неповних або перекручених даних, прогнозування поведінки користувача і появи нових атак.

У роботі [2] проведене дослідження та імітаційне моделювання гомогенних НМ на експериментальних данних KDD Cup 99 в задачах виявлення і класифікації мережевих атак свідчить про задовільну ефективність нейромережевих технологій. Однак відмічається, що при використанні гетерогенних НМ поліноміального і діофантового типу, а також їх колективів результати розпізнавання мережевих атак можуть бути поліпшені.

В галузі ідентифікації вірусів також особливості НМ обумовлюють нечисленні реалізації антивірусних програм [3]. З використанням моделі штучного нейрона використовувався відкритий антивірус ClamAV. Даний антивірус має статус проекту з відкритим вихідним кодом, за ліцензією поширюється GPLv2. Проект почав функціонувати в 2002 році. Даний антивірус є фактично єдиним ефективним антивірусом з відкритим вихідним кодом, що становить конкуренцію комерційним антивірусів. Однак він не дозволяє лікувати файли - заражені файли або видаляються, або поміщаються в карантин. Використовується сигнатурний метод пошуку комп'ютерних вірусів. Для збільшення швидкодії антівіруса ClamAV в нього був доданий модуль швидкого детектування шкідливого коду в сканованих даних. Даний модуль являє собою програмну реалізацію кібернейрона, який має 2 входа по 24 біт кожен. Відповідно розмірність таблиці підстановки для кожного входа склала 16.777.216 по 8 комірок біт кожна. Всього під даний кібернейрон було відведено додатково 32 Мбайт оперативної пам'яті. Проблемою, що заважає повноцінній інтеграції кібернейрона в ClamAV, є проблема отримання якісних 6-й байтних сигнатур з стадартної бази сигнатур ClamAV. Для вирішення цієї проблеми потрібна повна колекція вірусів, що дозволить виділити сигнатури, які найбільш оптимально підходять для навчання кібернейрона.

Постановка задачі. Приступаючи до розробки і використання нейромережевої моделі, як правило, стикаються з проблемою вибору структури нейронної мережі. Створення найбільш ефективної нейронної мережі, розробка алгоритму її навчання вимагає розуміння різних видів архітектур нейронних мереж, включає в себе багато дослідницької та аналітичної роботи, і може зайняти досить багато часу.

Більшість застосовуваних нейронних мереж представляють мережі зворотного поширення - найбільш популярного сучасного алгоритму. Але при його використанні не існує гарантії, що нейронна мережа буде навчена за кінцевий час. Повторне навчання також може бути неефективним. Алгоритм зворотного поширення також може потрапити в так званий локальний мінімум помилки, і найкраще рішення не буде отримано [4].

Більшість нейронних мереж, не здатні масштабуватися до великого завдання. Кількість пам'яті і часу, необхідного для навчання, зростає експоненціально в міру зростання простору завдання, що робить непрактичним побудову великих систем.

При використанні традиційних моделей нейронних мереж не враховується часова складова вхідних данних, що не дає можливості динамічно оцінювати шкідливі впливи, які надходять на комп’ютерну систему..

Виклад основного матеріалу. Тому автори пропонують використовувати для реалізації нейромережевих моделей даних ієрархічну часову пам’ять [5], яка базується на архітектурах самонавчаючих і самоорганізованих штучних нейронних мереж Кохонена на основі радіально-симетричних (радіально-базисних) функцій. Ці мережі найбільш прості й ефективні для апроксимації даних.

В архітектурі ієрархічної часової пам'яті використовується складна структура нейронів і організація зв'язків між ними, які імітують елементи кори головного мозку людини.

Мережі ієрархічної часової пам'яті навчаються багаторазово на різних наборах вхідних даних, і принцип їх роботи заснований на запам'ятовуванні як множини вхідних векторів, так і їх послідовностей. На відміну від інших архітектур нейронних мереж ієрархічна часова пам'ять пов'язана з параметром часу.

Нейронна мережа ієрархічної часової пам'яті складається з вузлів, організованих в ієрархію. Вузол функціонуючої мережі являє собою один рівень і одну зі складових рівня ієрархії, коли таких вузлів на рівні декілька. При взаємодії між собою сусідніх рівнів ієрархії відбувається обмін сигналами (даними) між нижніми (дочірніми) і верхніми (батьківськими) рівнями. Вузли ієрархічної часової пам'яті являють собою шари зв'язаних між собою клітин, схожі на багатошарові перцептрони.

Для інтерпретації вхідних даних та прийняття відповідного рішення при оцінці шкідливих впливів найбільшу важливість має характер зміни статичних властивостей в часі. Щоб навчити нейронну мережу ієрархічної часової пам'яті, потрібно подати на її входи змінний в часі потік даних. Основне завдання алгоритмів навчання ієрархічної часової пам'яті - витяг часових послідовностей з потоку вхідних даних. Вона ускладнюється тим, що сама послідовність може починатися з довільного проміжного моменту часу і в будь-який момент обриватися. Крім того, можлива присутність шуму різного походження у вхідних даних. Довільний вузол нейронної мережі вивчає та узагальнює дані про об'єкт знаходженням вхідних векторів та їх пов'язаних послідовностей у вхідному потоці даних. Вузол працює на статистичних принципах, підбираючи часто повторювані комбінації вхідних бітів. Потім вузол визначає, яким чином вони утворюють послідовності в часі. Для розпізнавання досить складних вхідних даних може знадобитися кілька рівнів ієрархії вузлів. Мережі ієрархічної часової пам'яті навчаються протягом усього свого життєвого циклу, тому стадії розпізнавання і навчання функціонують синхронно. Якщо мережа вже вивчила базові статистичні структури з навколишнього її світу, основне навчання буде відбуватися тільки на верхніх рівнях ієрархії. При отриманні чергового вхідного набору мережу зіставляє його з вивченими раніше. Внаслідок впливу зовнішніх збурень різної природи вихідні дані, в загальному випадку, точно не повторюються. Архітектура передбачає можливість виявлення аналогії нового набору вхідних даних і одного з вже існуючих в пам’яті тільки по деякій його частині. Оскільки кожен вузол ієрархічної часової пам'яті зберігає не тільки вхідні образи, але і їх послідовності, вузол може сформувати прогноз щодо найбільш ймовірного наступного входу.

На вхід вузлів першого рівня подається надходить послідовність патернів, які змінюються у часі. Таким чином враховується часова складова сигналу. В першу чергу навчаються нижні рівні, а на основі їх даних навчаються наступні рівні. Вхідною інформацією для вузла, незалежно від рівня ієрархії, є бінарний вектор. Для вузлів першого рівня це вектор, який відображає деякі впливи на комп’ютерну систему. Кожен вузол містить набір груп. Задача вузла - вибрати групу, якій найбільше відповідає вхідній послідовності. Вибір групи відбувається в два етапи. На першому етапі порівнюється просторове розташування елементів у векторі (просторове об'єднання), в результаті чого вибирається найбільш підходящий просторовий центр. На другому етапі вибирається часова група, в якій об'єднані близькі за часом появи просторові центри (часове об'єднання). Просторове об'єднання необхідне для фільтрації та компресії вхідних даних і їх первинного узагальнення. На етапі навчання у вузлі з вхідних бінарних векторів формуються просторові центри. Щоб визначити, чи був даний центр вже збережений, розраховується евклідова відстань d_i між вхідним вектором та існуючими центрами. Якщо $d_i < \varepsilon$, де ε - задана похибка розпізнавання, то такий центр уже присутній у вузлі, інакше, додаємо в вузол новий центр. Навчання відбувається до тих пір, поки швидкість появи нових центрів не знизиться до деякого малого значення. Якщо вузол не є вузлом вхідного рівня, його просторові центри являють собою вектора з індексів часових груп попереднього рівня.

У процесі навчання мережі, крім запам'ятовування просторових центрів, відбувається їх об'єднання в часові групи. В одну групу потрапляють просторові центри, які часто приходять

на вхід вузла один за одним. Для цього складається матриця суміжності Т, що зберігає в себе кількість надходжень одного центру за іншим. По матриці Т будується ланцюг Маркова, де номера просторових центрів є вершинами, а частота їх взаємних переходів - вагою ребер. Після того, як навчальний сигнал закінчився, з вершин ланцюга Маркова формуються часові групи. В одну часову групу відбираються вершини, з'єднані ребрами з найбільшими вагами. Ключовим елементом у роботі мережі, який зв'язує етапи просторового часового об'єднання, є матриця P (C|G), рядки якої відповідають часовим групам, а стовпці - просторовим центрам. Якщо будь-який з центрів не міститься в певній часовій групі, то на перетині відповідного стовпця і рядка матриці P (C|G) буде міститись “0”, інакше цей елемент матриці містить відносну нормовану ймовірність, рівну відношенню частоти виникнення даного просторового центру у вхідному сигналі до частоти виникнення всіх просторових центрів даної часової групи. Навчання вузла верхнього рівня мережі може проводитися з учителем - елементом, який правильно розбиває просторові центри вузла за часовими групами на основі ярликів, присвоєних навчальним даним. У цьому випадку кожна часова група верхнього вузла однозначно відповідає певному класу об'єктів у вхідному сигналі.

Система з реалізованої в ній функцією реакції на шкідливі впливи повинна бути здатною навчатися шляхом знаходження характерних для шкідливих впливів патернів і їх послідовностей у вхідному потоці даних. Очевидно, що система не завжди здатна інтерпретувати дані, які надійшли, що не повинно заважати їй запам'ятовувати послідовності патернів в часі. Подібно біологічним системам, проектована система повинна бути здатною до безперервного навчання в ході реєстрації кожного патерна. Таким чином, пам'ять системи повинна зберігати в собі послідовності патернів. І шляхом їх зіставлення з поточними вхідними даними, система повинна формувати прогноз щодо імовірного наступного входу. Система повинна зберігати в собі переходи між розподіленими просторовими уявленнями вхідних даних, які являють собою сукупність взаємопов'язаних концептів (кожний з яких також може бути представлений просторово розподіленим патерном). У деяких випадках ці переходи можуть виглядати як лінійні послідовності, але в загальному випадку в один момент часу можливе передбачення багатьох ймовірних наступних варіантів. При цьому система повинна робити різні передбачення, грунтуючись на поточному контексті подій, який може сягати далеко в минуле. Основна частина системи повинна відводитися зберіганню переходів між просторовими патернами.

Ієрархічна темпоральна пам’ять може бути корисна для організації роботи з контекстами, для роботи в умовах шуму і пропусків, а також, можливо, для реалізації здатності системи до навчання і передбачення. Налаштувати подібну систему до етапу її безпосередньої експлуатації за призначенням досить складно, так як опис всіх зв’язків між численними нейронами практично не реалізовується. Ієрархічна темпоральна пам’ять не припускає самонавчання при відсутності вхідних даних від сенсорів, а дана здатність просто необхідна для інтелектуальних систем. Людина також здатна самостійно будувати нейронні зв'язки, але природно при цьому процесі вона оперує не нейронами і зв'язками, а уявними подіями, образами, процесами . Маніпуляції з уявними окремими подіями цілими процесами людина здійснює при ретроспективній і перспективній рефлексії.

Тому для передбачень необхідно надбудувати більш високий рівень в ієрархії пам’яті, що містить дані про події і їх послідовності, тобто система повинна бути в змозі будувати дерева можливих процесів, спираючись на попередній досвід і правила побудови процесів.

Після того, як побудується певний фрагмент спостережуваного процесу, система повинна вибрати на нього відповідну реакцію. Відповідна реакція може вибиратися як на основі попереднього досвіду, так і на основі аналізу можливих реакцій, опис яких побудовано в ході логічних виводів системи.

Вхідні патерни, повинні бути пов'язані з паттернами, які формують конкретні ефекторні реакції. Цей зв'язок необхідний для організації взаємодії між областю пам'яті, яка містить дані про спостережувані системою процеси, і областю пам'яті, що зберігає дані про те, які дії необхідно вчинити для досягнення системою бажаного майбутнього стану.

Сформована конфігурація даної взаємодії дозволить передбачити наступну за поточною подію і активувати відповідні патерни, що відповідають за управління ефекторами, діяльність яких спрямована на запобігання очікуваної небажаної події. Для того щоб виконання таких процедур стало можли-вим, пропонується спочатку будувати систему з внесеними як типовими патернами шкідливих впливів, з якими буде мати справу система в процесі свого функціонування, так і типовими реакціями на них. Далі коли надходить новий для системи патерн на основі рефлексії при використанні вищого рівня в ієрархії пам'яті, що містить про дані події і їх послідовності в більш загальному вигляді, система будує дерево реакцій. Після реалізації цього сценарію виконується підтвердження ефективності або неефективності сценарію.

Висновок. Отже, в результаті використання ієрархічної організації нейромереж істотно скорочується час навчання та необхідні обсяги пам'яті, оскільки вхідні вектора(патерни), узагальнюються та запам'ятовуються на кожному рівні ієрархії, використовуються багаторазово в комбінаціях на більш високих рівнях.

Також використання ієрархічної темпоральної пам'яті дозволяє враховувати часову складову вхідних даних, що важливо при динамічній зміні інформації, яка надходить в комп'ютерну систему.

Відповідно даний напрямок є перспективним і потребує розробки методів, алгоритмів, відповідних систем і прикладного програмного забезпечення.

ЛІТЕРАТУРА:

1. Исследование нейросетевого метода в обнаружении атак. / Електронний ресурс http://www.rusnauka.com/4_SND_2009/Tecnic/40373.doc.htm

2. Тимофеев А., Браницкий А. Исследование и моделирование нейросетевого метода обнаружения и классификации сетевых атак / International Journal "Information Technologies & Knowledge" Vol.6, Number 3, 2012.

3. Поликарпов С.В., Дергачёв В.С., Румянцев К.Е., Голубчиков Д.М. Новая модель искусственного нейрона: кибернейрон и области его применения / Електронний ресурс http://arxiv.org/ftp/arxiv/ papers/0907/0907.0229.pdf.

4. Anderson J. A. An Introduction to Neural Networks, Cambridge/ J. A. Anderson - MA: MIT Press, 1995. - 645 p.

5. Блейксли С. Об интеллекте/ С. Блейксли, Д. Хокинс – «Вильямс»; Москва-Санкт-Петербург-Киев, 2007. - 240 с.

REFERENCES:

1. Issledovanie nejrosetevogo metoda v obnaruzhenii atak. / Elektronnij resurs http://www.rusnauka.com/4_SND_2009/Tecnic/40373.doc.htm

2. Timofeev A., Branickij A. Issledovanie i modelirovanie nejrosetevogo metoda obnaruzhenija i klassifikacii setevyh atak / International Journal "Information Technologies & Knowledge" Vol.6, Number 3, 2012.

3. Polikarpov S.V., Dergachjov V.S., Rumjancev K.E., Golubchikov D.M. Novaja model' iskusstvennogo nejrona: kibernejron i oblasti ego primenenija / Elektronnij resurs http://arxiv.org/ftp/arxiv/ papers/0907/0907.0229.pdf.

4. Anderson J. A. An Introduction to Neural Networks, Cambridge/ J. A. Anderson - MA: MIT Press, 1995. - 645 p.

5. Blejksli C. Ob intellekte/ S. Blejksli, D. Hokins – «Vil'jams»; Moskva-Sankt-Peterburg-Kiev, 2007. - 240 s.

Рецензент: д.т.н., проф. Лєнков С.В., начальник науково-дослідного центру Військового інституту Київського національного університету імені Тараса Шевченка

к.т.н. Бойчук В.А., Герасимчук К.С., к.т.н., с.н.с. Дергилева О.В.

ИСПОЛЬЗОВАНИЕ ВРЕМЕННОЙ ТЕМПОРАЛЬНОЙ ПАМЯТИ В ИДЕНТИФИКАЦИИ ВРЕДНЫХ ВОЗДЕЙСТВИЙ НА КОМПЬЮТЕРНЫЕ СИСТЕМЫ

В статье на основе обзора современных искусственных нейронных сетей показаны их особенности и недостатки при использовании в идентификации вредных воздействий на компьютерные системы. Рассмотрены особенности иерархической временной памяти и проведен обзор принципов ее функционирования. Предложены принципы использования иерархической временной памяти в идентификации вредных воздействий на компьютерные системы.

Ключевые слова: нейронные сети, иерархическая темпоральная память, цепь Маркова

Ph.D. Boychuk V.A., Gerasymchuk K.S., Ph.D. Derhilova O.V.

USING A HIERARCHICAL TEMPORAL MEMORY IN THE ATTACKS DETECTION ON COMPUTER SYSTEMS

Using the modern artificial neural networks, their features and drawbacks were shows for the attacks detection on the computer's systems. The hierarchical temporal memory features were considered. The principles of the hierarchical temporal memory use in the attacks detection on the computer systems were proposed.

Keywords: neural networks, hierarchical temporal memory, Markov chain.