Міністерство освіти і науки, молоді та спорту України
Вінницький національний технічний університет
Інститут менеджменту
Кафедра менеджменту і безпеки інформаційних систем

Науково-дослідна робота на тему:
«Прогнозування мережевого трафіку в системах безпеки з використанням нейронних мереж»

Виконав: ст.гр. УБ-11 Франчук А.Ю.
Керівник: Куземко С.М.
Перевірив: Карпінець В.В.

Вінниця 2013

ЗМІСТ

ВСТУП

В сучасних умовах з розвитком комп'ютерних мереж та інтеграцією цих новітніх систем у повсякденне життя постає потреба контролю, аналізу та прогнозування мережевого трафіку.

Статистичні методи є порівняно ефективними, якщо відомі точні характеристики атаки. Однак мережеві атаки постійно змінюються, оскільки зловмисники використовують індивідуальні підходи, а також у зв'язку з регулярними змінами в ПЗ і апаратних засобах систем. Це вимагає гнучкої захисної системи, яка здатна аналізувати велику кількість мережевого трафіку способом, який є менш структурованим, ніж системи на основі правил.

Нейромережа може бути навчена розпізнавати відомі підозрілі події з високим ступенем точності. Мережа також має здатність використовувати ці знання для ідентифікації атак, які неточно відповідають характеристикам попередніх вторгнень, оскільки хакери часто модифікують відомі сценарії атак.

Важливою особливістю є те, що прогноз грунтується не тільки на попередніх значеннях прогнозованої величини, але також враховує вплив різних додаткових факторів, представлених часовими рядами . Таким чином, в даному випадку прогнозування здійснюється на основі спільної обробки декількох часових рядів.

Також необхідно враховувати, що при побудові моделі прогнозу істотний інтерес представляє не стільки сама прогнозована величина, скільки передбачення змін в її поведінці. Традиційні методи статистичного прогнозування не дозволяють повною мірою враховувати фактори , що впливають на зміну прогнозованої величини в часі. Для вирішення завдання прогнозування можна використовувати штучні нейронні мережі, що надає можливість прогнозувати мережевий трафік за певними критеріями, які власне визначаються самою нейромережею.

1 ЗАГАЛЬНІ ВІДОМОСТІ ПРО НЕЙРОННІ МЕРЕЖІ

1.1 Означення нейронної мережі

Штучні нейронні мережі (ШНМ) – математичні моделі, а також їх програмні або апаратні реалізації, побудовані за принципом організації й функціонування біологічних нейронних мереж – мереж нервових кліток живого організму. Це поняття виникло при вивченні процесів, що протікають у мозку, і при спробі змоделювати ці процеси. Першою такою спробою були нейронні мережі Маккалока й Піттса. Згодом, після розробки алгоритмів навчання, одержувані моделі стали використовувати в практичних цілях: у завданнях прогнозування, для розпізнавання образів, у завданнях керування й ін. [1]

ШНМ являють собою систему з'єднаних і взаємодіючих між собою простих процесорів (штучних нейронів). Такі процесори звичайно досить прості, особливо в порівнянні із процесорами, використовуваними в персональних комп'ютерах. Кожний процесор подібної мережі має справу тільки із сигналами, які він періодично одержує, і сигналами, які він періодично посилає іншим процесорам. Проте, з'єднавши їх в досить велику мережу з керованою взаємодією, такі локально прості процесори разом здатні виконувати досить складні завдання. З погляду машинного навчання, нейронна мережа являє собою окремий випадок методів розпізнавання образів, методів кластеризації й т.п. З математичної точки зору, навчання нейронних мереж – це багатопараметричне завдання нелінійної оптимізації. З погляду кібернетики, нейронна мережа використовується в завданнях адаптивного керування і як алгоритми для робототехніки. З погляду розвитку обчислювальної техніки й програмування, нейронна мережа – спосіб розв'язку проблеми ефективного паралелізму. А з погляду штучного інтелекту, ИНС є основним напрямком у структурному підході по вивченню можливості побудови (моделювання) природнього інтелекту за допомогою комп'ютерних алгоритмів.

Нейронні мережі не програмуються у звичному змісті цього слова, вони навчаються. Можливість навчання – одне з головних переваг нейронних мереж перед традиційними алгоритмами. Технічно навчання полягає в знаходженні коефіцієнтів зв'язків між нейронами. У процесі навчання нейронна мережа здатна виявляти складні залежності між вхідними даними й вихідними, а також виконувати узагальнення. Це значить, що, у випадку успішного навчання, мережа зможе повернути вірний результат на підставі даних, які були відсутні в навчальній вибірці, а також неповних і/або «зашумлених», частково перекручених даних.

1.2 Структура штучного нейрона

Нейрон є складовою частиною нейронної мережі. На рисунку 1.1 представлена його структура. Він складається з елементів трьох типів: помножувачів (синапсів), суматора і нелінійного перетворювача. Синапси здійснюють зв’язок між нейронами, множать вхідний сигнал на число, що характеризує силу зв’язку, (вагу синапса). Суматор виконує додавання сигналів, що надходять по синаптичним зв’язках від інших нейронів і зовнішніх вхідних сигналів. Нелінійний перетворювач реалізує нелінійну функцію одного аргументу – виходу суматора. Ця функція називається функцією активації чи передатною функцією нейрона.

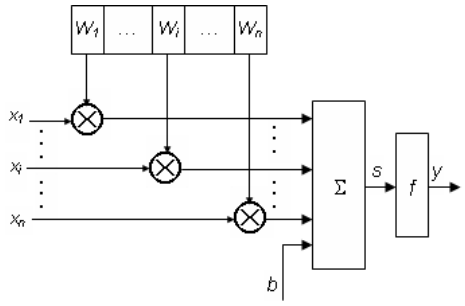

Рисунок 1.1. – Структура штучного нейрона

1.3 Архітектура нейронної мережі

Існуючі на даний час, нейромережі є групуванням штучних нейронів. Це групування обумовлено створенням з'єднанних між собою прошарків. На рис. 1.2 показана типова структура штучних нейромереж. Хоча існують мережі, які містять лише один прошарок, або навіть один елемент, більшість застосувань вимагають мережі, які містять як мінімум три нормальних типи прошарків – вхідний, прихований та вихідний. Прошарок вхідних нейронів отримує дані або з вхідних файлів, або безпосередньо з електронних давачів. Вихідний прошарок пересилає інформацію безпосередньо до зовнішнього середовища, до вторинного комп'ютерного процесу, або до інших пристроїв. Між цими двома прошарками може бути багато прихованих прошарків, які містять багато нейронів у різноманітних зв'язаних структурах. Входи та виходи кожного з прихованих нейронів просто йдуть до інших нейронів.

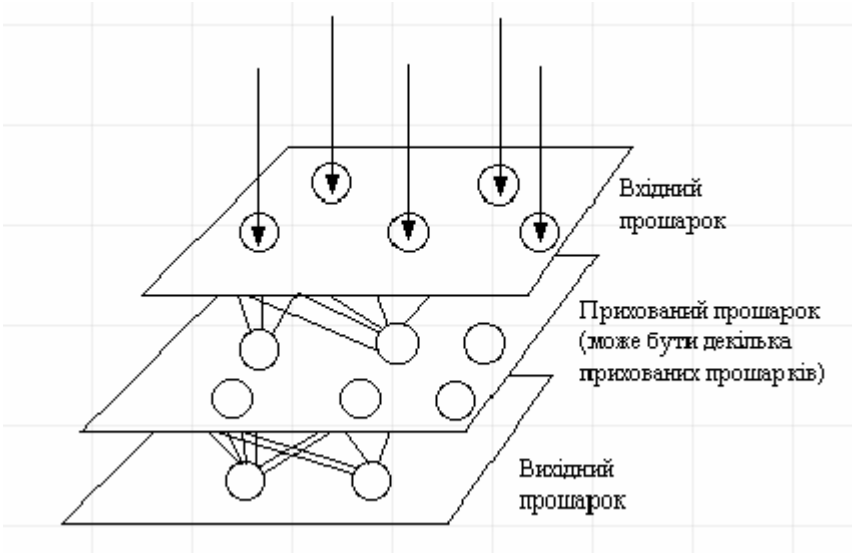

Рисунок 1.2 – Діаграма простої нейронної мережі

Напрямок зв'язку від одного нейрону до іншого є важливим аспектом нейромереж. У більшості мереж кожен нейрон прихованого прошарку отримує сигнали від всіх нейронів попереднього прошарку та звичайно від нейронів вхідного прошарку. Після виконання операцій над сигналами, нейрон передає свій вихід до всіх нейронів наступних прошарків, забезпечуючи шлях передачі вперед (feedforward) на вихід. Багатошарові нейронні мережі можна поділити на: - мережі прямого розповсюдження ; - мережі зі зворотними зв’язками. У мережах прямого розповсюдження нейрони вхідного шару отримають вхідні

сигнали, перетворюють і передають їх нейронам першого шару, останні – нейронам другого, потім третього і так дальше аж до вихідного шару, який видає їх користувачу. У мережах зі зворотними зв’язками інформація з подальших шарів передається на попередні. [2]

1.4 Навчання штучної нейронної мережі

Здатність до навчання є фундаментальною властивістю мозку. Процес навчання може розглядатися як визначення архітектури мережі і налаштування ваг зв'язків для ефективного виконання спеціальної задачі. Нейромережа налаштовує ваги зв'язків по наявній навчальній множині. Властивість мережі навчатися на прикладах робить їх більш привабливими в порівнянні із системами, які функціонують згідно визначеній системі правил, сформульованої експертами.

Для процесу навчання необхідно мати модель зовнішнього середовища, у якій функціонує нейронна мережа – потрібну для вирішення задачі інформацію. По-друге, необхідно визначити, як модифікувати вагові параметри мережі. Алгоритм навчання означає процедуру, в якій використовуються правила навчання для налаштування ваг.

Існують три загальні парадигми навчання: "з вчителем", "без вчителя" (самонавчання) і змішана. [5]

У першому випадку нейромережа має у своєму розпорядженні правильні відповіді (виходи мережі) на кожен вхідний приклад. Ваги налаштовуються так, щоб мережа виробляла відповіді як можна більш близькі до відомих правильних відповідей.

Навчання "без вчителя" не вимагає знання правильних відповідей на кожен приклад навчальної вибірки. У цьому випадку розкривається внутрішня структура даних та кореляція між зразками в навчальній множині, що дозволяє розподілити зразки по категоріях.

При змішаному навчанні частина ваг визначається за допомогою навчання зі вчителем, у той час як інша визначається за допомогою самонавчання.

У загальному використанні є багато правил навчання, але більшість з цих правил є деякою зміною відомого та найстаршого правила навчання, правила Хеба. Дослідження різних правил навчання триває, і нові ідеї регулярно публікуються в наукових та комерційних виданнях. Представимо декілька основних правил навчання.

Правило Хеба. Опис правила з'явився у його книзі "Організація поведінки" у 1949 р. "Якщо нейрон отримує вхідний сигнал від іншого нейрону і обидва є високо активними (математично мають такий самий знак), вага між нейронами повинна бути підсилена". При збудженні одночасно двох нейронів з виходами (xj, yi) на t-тому кроці навчання вага синаптичного з'єднання між ними зростає, в інакшому випадку – зменшується.

Може застосовуватись при навчанні "з вчителем" і "без вчителя".

Правило Хопфілда. Є подібним до правила Хеба за винятком того, що воно визначає величину підсилення або послаблення. "Якщо одночасно вихідний та вхідний сигнал нейрона є активними або неактивними, збільшуємо вагу з'єднання оцінкою навчання, інакше зменшуємо вагу оцінкою навчання".

Правило "дельта". Це правило є подальшою зміною правила Хеба і є одним із найбільш загально використовуваних. Це правило базується на простій ідеї неперервної зміни синаптичних ваг для зменшення різниці ("дельта") між значенням бажаного та біжучого вихідного сигналу нейрона.

За цим правилом мінімізується середньоквадратична похибка мережі. Це правило також згадується як правило навчання Відрова-Хофа та правило навчання найменших середніх квадратів.

У правилі "дельта" похибка отримана у вихідному прошарку перетворюється похідною передатної функції і послідовно пошарово поширюється назад на попередні прошарки для корекції синаптичних ваг.

Процес зворотного поширення похибок мережі триває до досягнення першого прошарку.

При використанні правила "дельта" важливим є невпорядкованість множини вхідних даних. При добре впорядкованому або структурованому представленні навчальної множини результат мережі може не збігтися до бажаної точності і мережа буде вважатись нездатною до навчання.

Правило градієнтного спуску. Це правило подібне до правила "дельта" використанням похідної від передатної функції для змінювання похибки "дельта" перед тим, як застосувати її до ваг з'єднань. До кінцевого коефіцієнта зміни, що діє на вагу, додається пропорційна константа, яка пов'язана з оцінкою навчання. І хоча процес навчання збігається до точки стабільності дуже повільно, це правило поширене і є загально використовуване.

Доведено, що різні оцінки навчання для різних прошарків мережі допомагає процесу навчання збігатись швидше. Оцінки навчання для прошарків, близьких до виходу, встановлюються меншими, ніж для рівнів, ближчих до входу.

Навчання методом змагання. На відміну від навчання Хеба, у якому множина вихідних нейронів може збуджуватись одночасно, при навчанні методом змагання вихідні нейрони змагаються між собою за активізацію. Це явище, відоме як правило "переможець отримує все". Подібне навчання має місце в біологічних нейронних мережах. Навчання за допомогою змагання дозволяє кластеризувати вхідні дані: подібні приклади групуються мережею відповідно до кореляцій і представляються одним елементом.

При навчанні модифікуються синаптичні ваги нейрона-переможця. Ефект цього правила досягається за рахунок такої зміни збереженого в мережі зразка (вектора синаптичних ваг нейрона-переможця), при якому він стає подібним до вхідного приклада. Нейрон з найбільшим вихідним сигналом оголошується переможцем і має можливість гальмувати своїх конкурентів і збуджувати сусідів. Використовується вихідний сигнал нейрона-переможця і тільки йому та його сусідам дозволяється коректувати свої ваги з'єднань. [5]

Розмір області сусідства може змінюватись під час періоду навчання. Звичайна парадигма повинна починатись з великої області визначення сусідства і зменшуватись під час процесу навчання. Оскільки елемент-переможець визначається по найвищій відповідності до вхідного зразку, мережі Кохонена моделюють розподіл входів. Це правило використовується в самоорганізованих картах.

2 МЕТОДИ ПРОГНОЗУВАННЯ ЧИСЛОВИХ ПОСЛІДОВНОСТЕЙ

2.1 Задачі прогнозування

Особливе значення мають задачі передбачення та прогнозування часових рядів, серед яких виділяються завдання з набором певних специфічних ознак, тому варто провести їх класифікацію. Задачі дослідження явищ, розвиток яких пов'язаний із часом, можна поділити на декілька класів:

За характером основних ознак об'єкту:

- прогнозування явищ, реалізації яких представлені у вигляді детермінованих часових рядів. Такі задачі, зокрема, можна вирішити шляхом застосування методів математичного аналізу;

- прогнозування явищ, реалізації яких представлені у вигляді індетермінованих часових рядів. Вирішення цих задач традиційно здійснюється шляхом застосування методів теорії ймовірностей та математичної статистики.

Зокрема, реалізації таких явищ, можуть мати вигляд:

а) стаціонарного часового ряду, який характеризується однорідністю в часі, без суттєвих змін характеру коливань та їх середньої амплітуди;

б) нестаціонарного часового ряду, який характеризується певною тенденцією розвитку в часі; при дослідженні нестаціонарних процесів можна виділити ділянки, на яких процес можна вважати стаціонарним; вибір проміжку для формування навчальної множини в такому випадку обирається згідно задачі прогнозування;

За числом ознак об'єкту досліджень:

- одновимірна задача; явище представлене лише однією ознакою, зміни якої відбуваються в часі;

- багатовимірна задача; об'єкт або явище представлені кількома ознаками; задача прогнозування може бути розширена завдяки представленню даних в просторі.

За часом випередження розрізняють види прогнозів:

- згладжування, R= 0;
- короткотерміновий прогноз, R= 1… 2;
- середньотерміновий прогноз, R= 3 … 7;
- довготерміновий прогноз, R= 10 … 15.

Очевидно, що вид прогнозу суттєво впливає на вибір засобів і методику його реалізації.

Дані про поведінку об'єкта, ознаки якого пов'язані з часом, представлені як результати спостережень в рівномірні відліки часу. Для моментів часу t=1, 2, ..., n дані спостережень набувають вигляду часового ряду x(t1), x(t2), ..., x(tn). Інформація про значення часового ряду до моменту n дозволяє давати оцінки параметрів x(tn+1), x(n+2), ..., x(n+m). Для здійснення прогнозування елементів часових рядів широко використовують так званий метод "часових вікон". [4]

В залежності від кількості ознак, що представляють значення рядів при формуванні множин даних, виділимо задачі двох типів.

2.2 Однопараметрична задача прогнозування

Нехай часовий ряд x(t) задано відліками процесу x(t1), x(t2),..., x(ti) в дискретні моменти часу t. Задамо ширину (кількість дискретних відліків) вхідного часового вікна m, ширину вихідного вікна p. Вхідне та вихідне вікна накладаються на дані ряду, починаючи з першого елемента (рис. 2.1).

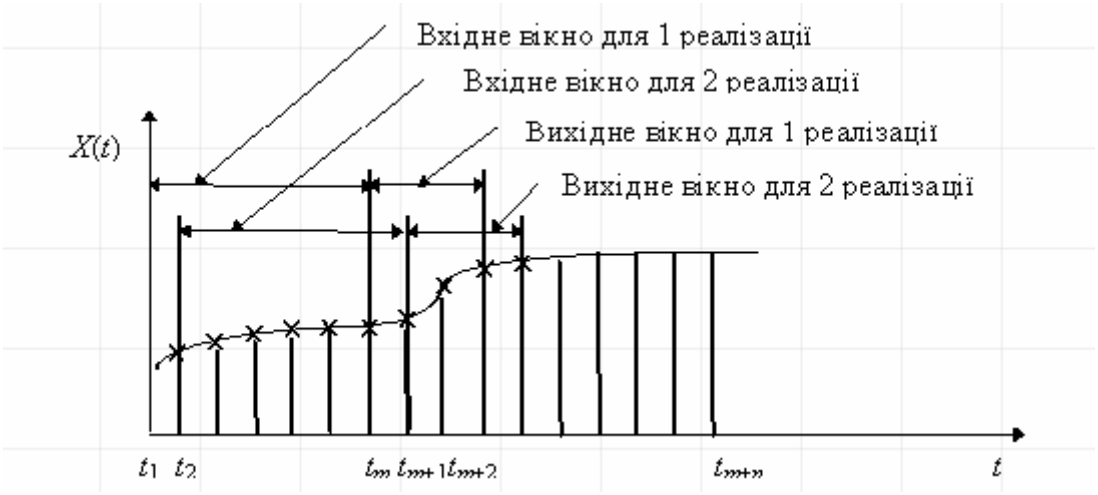

Рисунок 2.1 – Формування множин даних для однопараметричної задачі за методом "часових вікон"

Вхідне вікно формує дані для входів нейронної мережі, а вихідне, відповідно, для виходів. Подібна пара вхідного та вихідного векторів приймається за одну реалізацію часового ряду. При зсуві часових вікон за часовим рядом з кроком s, отримуємо другу і наступні реалізації. [3]

Значення ширини вікон та кроку зміщення повинні узгоджуватись з особливостями часового ряду, що забезпечується шляхом проведення експериментів.

2.3 Багатопараметрична задача прогнозування

В багатопараметричних задачах прогнозування підходи до розв'язання проблеми залишаються подібними (рис.2.2).

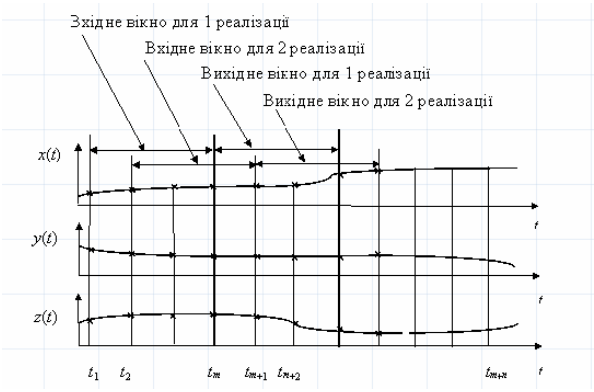

Рисунок 2.2 – Формування множин даних для багатопараметричної задачі

Функціонування нейромережі здійснюється у відповідності з показаним методом часових вікон, зберігаючи значення ширини вікон та кроку зсуву. Конкретизація підходів до реалізації прогнозування в значній мірі залежить також від особливостей явища, що досліджується.

2.4 Однокрокове та багатокрокове прогнозування

Задача однокрокового прогнозування зводиться до задачі відображення, коли один вхідний вектор відображається у вихідний (рис. 2.3).

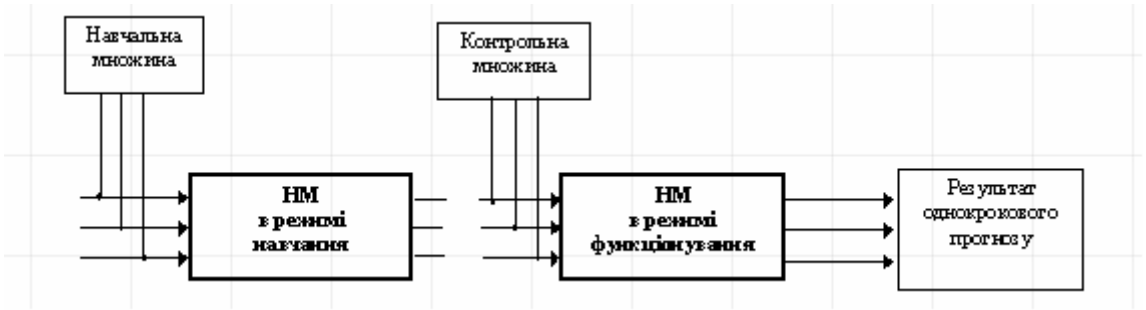

Рисунок 2.3 – Послідовність використання нейромереж для задач передбачення

Показаний режим є однокроковим, який працює в режимі відображення (реальний вхід - прогнозований вихід). Передбачення застосовують також для моделювання дискретних послідовностей, що не пов'язані з часом. Враховуючи специфіку часових рядів, такий тип прогнозу не завжди є доцільним, але для певних випадків короткотермінових прогнозів ним можливо скористатись.

Багатокрокове прогнозування застосовують лише для явищ, ознаки яких представлені у вигляді часових рядів.

Багатокрокове прогнозування дозволяє робити коротко- та середньотермінові прогнози, оскільки суттєвий вплив на точність має накопичення похибки на кожному кроці прогнозування. При застосуванні довготермінового багатокрокового прогнозування спостерігається характерне для багатьох прогнозуючих систем поступове затухання процесу, фазові зсуви і інші спотворення картини прогнозу. Такий тип прогнозування підходить для часових рядів, які підпадають під означення стаціонарного процесу з невеликою випадковою складовою.

2.5 Нейромережеві моделі прогнозування

На даний час найперспективнішим методом прогнозування є використання нейронних мереж. Можна назвати багато переваг нейронних мереж над іншими алгоритмами, нижче наведено два основні.

При використанні нейронних мереж легко досліджувати залежність прогнозованої величини від незалежних змінних.

Потрібно побудувати систему, яка б усе це природнім чином враховувала і будувала б короткострокові прогнози. У такій постановці завдання застосування більшої частини класичних методів прогнозування буде просто неможливим.

Використовуючи ж навіть найпростішу нейромережеву архітектуру (перцептрон з одним схованим шаром) і базу даних легко одержати працюючу систему прогнозування. Причому враховувати, чи не враховувати зовнішні параметри системою буде визначатися включенням, або виключенням відповідного входу в нейронну мережу.

Експерт може скористатися яким-небудь алгоритмом визначення важливості і відразу визначити значимість вхідних змінних, щоб потім виключити з розгляду параметри, що мають незначний вплив.

Ще одна серйозна перевага нейронних мереж полягає в тому, що експерт не є заручником вибору математичної моделі поведінки часового ряду. Побудова нейромережевої моделі відбувається адаптивно під час навчання, без участі експерта. При цьому нейронній мережі пред'являються приклади з бази даних і вона сама підлаштовується під ці дані.

Недоліком нейронних мереж є їхня недетермінованість. Мається на увазі те, що після навчання є "чорний ящик", який якимось чином працює, але логіка прийняття розв'язків нейромережею зовсім схована від експерта. У принципі, існують алгоритми "витягу знань із нейронної мережі", які формалізують навчену нейронну мережу до списку логічних правил, тим самим створюючи на основі мережі експертну систему. На жаль, ці алгоритми не вбудовуються в нейромережеві пакети, до того ж набори правил, які генеруються такими алгоритмами досить об'ємні.

Проте, для людей, що вміють працювати з нейронними мережами й знаючими нюанси налаштування, навчання й застосування, у практичних завданнях непрозорість нейронних мереж не є настільки серйозним недоліком.

3 ПІДХОДИ ДО РЕАЛІЗАЦІЇ БЛОКУ ПРОГНОЗУВАННЯ МЕРЕЖЕВОГО ТРАФІКУ

Оперативне прогнозування навантаження мереж відноситься до класу задач, де залежність вихідних характеристик від вхідних змінних досить багатогранна і складна. Знаходження закономірностей, які у великому обсязі даних, вимагає нестандартних алгоритмів.

3.1 Методика побудови нейромережевої моделі прогнозування

Виділяють чотири етапи створення формалізованої методики побудови моделі прогнозування на основі нейронних мереж (рисунок 3.1). [3]

На першому етапі, на основі експертної оцінки, визначається надлишковий набір факторів V, що впливають на об'єкт прогнозу.

На другому етапі проводиться визначення параметрів моделі: знаходження параметрів ретроспективної вибірки (тобто, число попередніх значень по кожному фактору, на підставі яких будується прогноз), визначення складу вхідних факторів (з визначеного на першому етапі надлишкового набору) і структури мережі (число шарів і нейронів), завдання параметрів навчання.

На третьому етапі відбувається формування навчальних прикладів, навчання мережі та оцінка якості моделі. У процесі формування навчальних прикладів вихідний масив даних представляється у вигляді, в якому дані можуть бути оброблені нейронною мережею. Кожен навчальний приклад містить історію значень за факторами, що значно впливають на значення прогнозованої величини та історію значень самої прогнозованої величини, а також необхідний вихід нейронної мережі.

Четвертий етап являє собою отримання реального прогнозу на даних, раніше невідомих мережі, а також проведення процедур, зворотних процедурам перепідготовки даних етапу 1 для знаходження істинного (ненормованого) значення прогнозованої величини. На четвертому етапі також проводиться

оцінка необхідності перенавчання мережі , яке необхідно або при незадовільній точності прогнозу, або при зміні зовнішніх даних.

Рисунок 3.1 – Етапи створення формалізованої методики прогнозування

Результатом аналізу можливості прогнозування трафіку корпоративних обчислювальних мереж є висновок про теоретичну можливість такого прогнозу, який обгрунтовується наявністю довготривалої пам'яті, персистентності мережевого трафіку і нескінченно протяжним інтервалом

кореляції . Застосування нейромережевих технологій для прогнозування мережевого трафіку теоретично може виявити статистичні залежності між накопиченими значеннями інтенсивності споживання трафіку, що дасть можливість побудувати адекватну модель короткострокового прогнозування із заданою точністю прогнозу, яка буде залежати від ступеня самоподібності трафіку. [2]

3.2 Обгрунтування вибору методу прогнозування

Для реалізації блоку прогнозування в алгоритмі перерозподілу смуги пропускання необхідно враховувати специфіку прогнозування споживання трафіку.

Виходячи зі специфіки завдання, вибір методу прогнозування вступників пакетів мережевого трафіку грунтувався на наступних вимогах: [1]

1) метод прогнозу повинен показувати позитивні результати як у випадку великих, так і малих обсягів даних по трафіку для вирішення проблем відсутність статистики по споживанню мережевого трафіку;

2) швидкість побудови прогностичної моделі повинна бути мінімальною;

3) розробка моделі прогнозування повинна здійснюватися без участі експерта з математичних методів аналізу;

4) метод прогнозування повинен працювати коректно і з сильно зашумленими даними.

У нейромережевих технологіях завдання прогнозування формалізується за допомогою розпізнавання образів. При прогнозуванні трафіку мереж образ становлять дані статистики про інтенсивність за деякий проміжок часу. Завдання розпізнавання образів вирішується методом вікон. Даний метод передбачає використання двох вікон з фіксованими розмірами, що переміщаються по часовій послідовності статистичних даних. Перше вікно, отримавши дані про обсяг інтенсивності спожитого трафіку, передає їх на вхід нейронної мережі, друге вікно – на вихід. Сукупність отриманих даних обох

вікон є елементом навчаючої нейромережу вибірки, тобто розпізнаваним образом.

При цьому передбачається наявність прихованих залежностей прогнозованої інтенсивності обсягу споживаного трафіку користувачів мережі. Нейронна мережа навчається на накопиченій статистиці споживання трафіку і налаштовує свої коефіцієнти для формування прогнозу.

Для короткострокового прогнозування використовуються тільки реальні дані і здійснюється прогноз тільки на один крок вперед. Для здійснення довгострокового прогнозування використовується багатокрокова стратегія, при якій вже спрогнозовані нейромережею значення використовуються в якості вхідних даних для побудови подальшого прогнозу інтенсивності трафіку.

Для побудови короткострокової моделі прогнозування за допомогою нейромережевих технологій необхідно вибрати конфігурацію штучної нейронної мережі, сформувати навчальну вибірку даних, навчити і протестувати нейронну мережу.

3.3 Нейромережева модель короткочасного прогнозування

З метою підвищення точності прогнозу розроблена нейромережева модель короткочасного прогнозування, що складається з трьох штучних нейронних мереж (алгоритм побудови моделі показаний на рисунку 3.2). Перші дві нейронні мережі використовують для навчання метод вікон різних розмірів.

Для формування навчальної вибірки використовується інформація з накопиченої статистики за обсягом споживання трафіку. Статистика збирається з портів комутаторів і маршрутизаторів корпоративної обчислювальної мережі. Перед процедурою прогнозування накопичена статистика по трафіку аналізується на предмет самоподібності (обчислюється значення параметра Херста). [3]

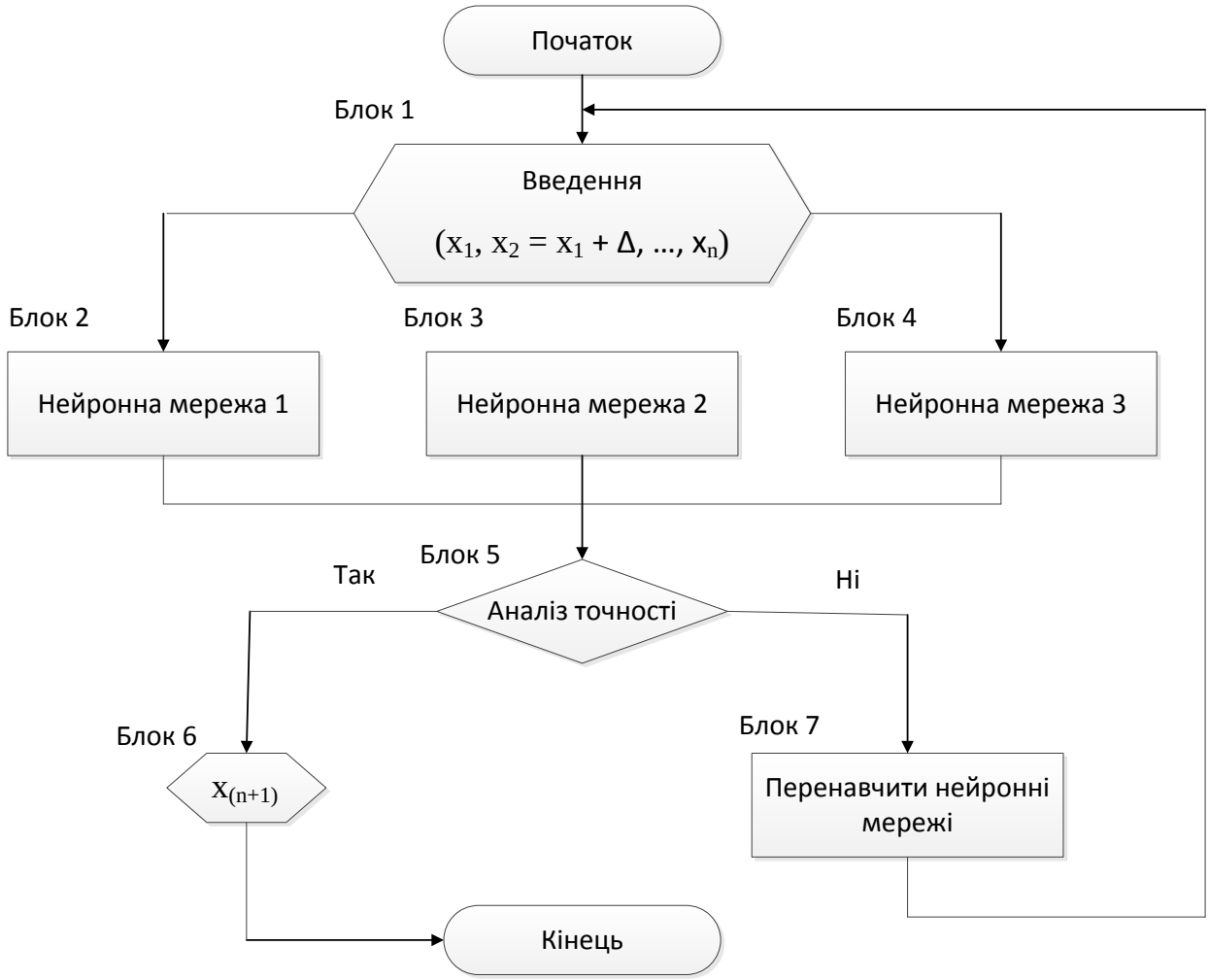

Рисунок 3.2 – Алгоритм побудови моделі короткочасного прогнозу споживання трафіку

Нейронна мережа 1 прогнозує значення обсягу споживаного трафіку на хвилину вперед. Для навчання використовується метод вікон, що припускає використання двох вікон фіксованого розміру. Вікна переміщаються по всіх елементах часового ряду з самого початку. Кожен наступний вектор утворюється в результаті зсуву вікон па один елемент часового ряду вперед. Отримана на кожному кроці пара використовується як елемент навчальної вибірки для нейромережі. Дані першого вікна передаються на входи, другого – на виходи нейронної мережі. Розмір першого вікна – 10, другого – 1. До кожного з прихованих вузлів нейронної мережі та вихідного вузла для різних за значущістю з'єднань застосовувалася функція сигмоїди (1/(1+exp(-x))). Навчання проводилося в режимі оффлайн (Resilent Propagation), тобто корекція ваг проводиться після пред'явлення всіх прикладів навчальної множини,

враховується тільки знак градієнта за кожною вагою. Число прихованих шарів – 3 (9, 10, 8).

Нейронна мережа 2 прогнозує значення обсягу споживаного трафіку на найближчі п'ять хвилин. Для навчання використовується метод вікон. Розмір першого вікна – 12, другого – 1. Число прихованих шарів – 3 (12, 9, 11). В іншому – аналогічно нейронній мережі 1.

Нейронна мережа 3 прогнозує обсяг споживаного трафіку на основі оптимальної екстраполяції функції споживання мережевого трафіку.

Результати прогнозів трьох нейронних мереж аналізуються в спеціальному модулі для забезпечення найкращої точності прогнозу.

У разі великої помилки прогнозування запускається процедура перенавчання відповідної нейромережі. Вихідне значення прогнозованого споживання трафіку формується на виході як зважене середнє. Число кількості накопичених секундних значень статистики по трафіку – 604800.

Нейромережева модель дозволяє зменшити помилку прогнозу, в середньому, на 4 %. [5]

Для оцінки точності прогнозу необхідно визначити (у відсотках) середню абсолютну помилку (Mean Absolute Percentage Error, MAPE), яка обчислюється шляхом ділення абсолютної помилки в кожній момент часу на її реальне значення статистики, що спостерігається по інтенсивності споживання трафіку в той момент.

Структура інтелектуальної системи управління трафіком на базі нейронних мереж, складається з таких підсистем: збору трафіку, прогнозування, аналізу та управління.

У підсистему збору трафіку, що виконує функції статистики та захоплення мережевого трафіку, можуть входити наступні модулі: модуль програми статистики і модуль захоплення мережевого трафіку (сніффер), що гнучко налаштовується для використання відповідних функцій комутаторів Cisco Catalyst. Такою функцією, наприклад, є дзеркалювання портів: весь трафік , що передається по одному порту, автоматично дзеркально передається

на інший, до якого підключена персональна ЕОМ із запущеною програмою захоплення всього трафіку.

Підсистема прогнозування трафіку повинна включати в себе модуль побудови нейронних мереж, з можливістю їх гнучкого налаштування і управління параметрами.

Підсистема аналізу трафіку повинна виконувати функції статистичного аналізу, передобробки даних (пониження розмірності , видалення непотрібних параметрів та їх подання в потрібному вигляді). Крім цього, дана підсистема виконує розрахунок показника Херста за необхідний інтервал часу.

Підсистема управління смугою пропускання реалізує динамічне виділення відповідної смуги на комутаторі/маршрутизаторі для потрібного трафіку (виділення відбувається за рахунок передачі відповідних команд комутатора по протоколах SSH, SNMP).

ВИСНОВКИ

В науково-дослідній роботі було проведено огляд і аналіз нейронних мереж та методів прогнозування числових послідовностей. Аналіз показав, що для виявлення атак застосовують системи захисту інформації, в якості інтелектуального інструменту в яких, як правило, використовуються нейронні мережі, системи нечіткої логіки і засновані на правилах експертні системи; що необхідно вирішувати не окремі завдання захисту інформації, а розробляти єдиний підхід застосування інтелектуальних засобів для створення комплексної адаптивної системи захисту ІТ.

Також було досліджено вплив алгоритму навчання нейронної мережі на точність прогнозування мережевого трафіку, запропоновано методику прогнозування зміни мережевого трафіку та схему управління мережевим трафіком.

Отримані результати дозволяють динамічно відслідковувати зміну величини трафіку в мережі та оперативно реагувати на наближення порогу перевантаження. Комбінована нейронна мережа дозволяє визначити структурний склад навчальної вибірки для виключення помилкового навчання нейронної мережі на некоректних даних.

Побудована модель короткочасного прогнозування мережевого трафіку на базі нейронних мереж, що складається з трьох незалежних нейронних мереж, які дозволяють покращити точність прогнозу інтенсивності споживаного трафіку, в середньому, на 4 % і може бути врахована при плануванні системи безпеки.

ПЕРЕЛІК ПОСИЛАНЬ

1. Круглов В. В., Борисов В. В. Искусственные нейронные сети. Теория и практика. – М.: Горячая линия - Телеком, 2001. – 382 с.

2. Анил К. Джейн, Жианчанг Мао, Моиуддин К.М. Введение в искуственные нейронные сети.

3. Крисилов В.А., Чумичкин К.В., Кондратюк А.В. Представление исходных данный в задачах нейросетевого прогнозирования. – Одесса: ОНПУ, 2002-2003.

4. Тарасенко Р.А., Крисилов В.А. Предварительная оценка качества обучающей выборки для нейронных сетей в задачах прогнозирования временных рядов. // Труды Одесского политехнического университета, Вып.1 (13). 2001, с. 90

5. Олешко Д.Н., Крисилов В.А.Повышение качества и скорости обучения нейронный сетей в задаче прогнозирования поведения временных рядов. – Одесса: ОНПУ, 2002.