SCI-CONF.COM.UA

INNOVATIVE DEVELOPMENT OF SCIENCE AND EDUCATION

ABSTRACTS OF I INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE MARCH 29-31, 2020

ATHENS 2020

РОЗРОБКА ВДОСКОНАЛЕНОГО АЛГОРИТМУ ЗАХИСТУ ЗОВНІШНІХ НОСІЇВ ІНФОРМАЦІЇ

Сачанюк-Кавецька Наталія Василівна
к.т.н., доцент
Вінницький національний технічний університет
м. Вінниця, Україна

Використання інформаційних комп'ютерних систем для вирішення управлінських та підприємницьких завдань, реалізації в мережевому режимі різноманітних зв'язків підприємств з їх партнерами, клієнтами, владними структурами призвело до зростання інформаційних потреб і зумовило зростання інвестицій у комп'ютерні технології. Інформація та інформаційні системи, мережі, в яких вона функціонує, є важливими ресурсами організації. Їх доступність, цілісність та конфіденційність можуть мати особливе значення для забезпечення конкурентоспроможності організації, руху коштів, рентабельності, відповідності правовим нормам та іміджу організації. Поширення інформаційних та комунікаційних систем надає все нові можливості для несанкціонованого доступу до інформаційних ресурсів, а тенденція до переходу на розподілені обчислювальні системи зменшує можливості спеціалістів централізовано контролювати інформаційні системи та мережі. Тому актуальним є питання захисту інформації від несанкціонованих управлінських дій і доступу сторонніх осіб або програм до комп'ютерних даних [1]. Захист інформації являє собою комплекс заходів, спрямованих на запобігання несанкціонованому витоку, модифікації і видаленню інформації, здійснюваних із застосуванням технічних, в тому числі програмних, засобів.

Основною задачею забезпечення безпеки інформаційних комп'ютерних систем є обмеження кола осіб, що мають доступ до критичної інформації. Задачею систем ідентифікації є визначення і верифікація набору повноважень суб'єкта при доступі до інформаційних систем. Ідентифікація – це пред'явлення користувачем якогось унікального, властивого тільки йому ідентифікатора

(ознаки) [2]. Існує три найпоширеніші види ідентифікації: парольна, апаратна та біометрична. При парольній ідентифікації кожен зареєстрований користувач будь-якої системи одержує набір персональних реквізитів, які він повторює при кожній спробі входу в систему. Перевага такого підходу – простота реалізації та використання, мінімізація витрат. Головним недоліком даного виду ідентифікації є величезна залежність надійності від користувачів. При апаратній ідентифікації визначення особистості користувача ґрунтується на якомусь «ключі», що перебуває в його ексклюзивному користуванні. Головною перевагою застосування апаратної ідентифікації є досить висока надійність. Слід відмітити, що найбільш серйозною небезпекою такої ідентифікації є можливість крадіжки зловмисниками токенів або карт у зареєстрованих користувачів, плюс їх висока ціна. Останнім часом досягнуто успіхів у розробці біометричних методів, що базуються на ідентифікації людини за унікальними, властивими тільки їй біологічними ознаками. Сьогодні експлуатується вже більше десятка різних біометричних ознак, однією з яких є клавіатурний почерк Головною перевагою біометричних технологій є найвища надійність та відносно низька вартість реалізації. Слід відмітити, що для використання власного підпису або клавіатурного почерку, як способу ідентифікації суб'єкта, достатньо мати лише Web-середовище в якому для відтворення підпису достатньо мати лише комп'ютерну мишку або стилус на портативних пристроях, а для перевірки клавіатурного почерку клавіатуру.

Останні кілька років ми спостерігаємо вибух інтересу до нейронних мереж, які практично використовують у всіх галузях, де потрібно розв'язувати завдання прогнозування, класифікації або прийняття рішень. Таким чином, актуальним є вдосконалення алгоритмів захисту зовнішніх носіїв інформації шляхом поєднання біометричних технологій ідентифікації та нейронних мереж [3].

Для реалізації методу ідентифікації користувача за клавіатурним почерком необхідно врахувати його основні параметри: час утримання натиснутої клавіші, час відпускання і інтервали часу між натисканнями [4, 5]. Однак на сьогоднішній день виділені і інші параметри клавіатурного почерку:

загальний час набору парольної фрази, частота виникнення помилок при наборі тексту, факт використання додаткових клавіш (використання числової клавіатури), особливості введення великих та малих літер (використання клавіші «Shift» або «CapsLock»). Окрему увагу необхідно приділити таким характеристикам:

швидкість spm - кількість набраних символів в хвилину;

швидкість нетто - чиста швидкість набору тексту, вважається для всіх невидалених символів тексту;

швидкість wpm - кількість символів в хвилину; в англомовних країнах швидкість вважається саме в цих одиницях, причому довжина «Слова» завжди дорівнює 5 символам, інакше кажучи, це швидкість нетто, поділена на 5;

швидкість брутто - швидкість набору з урахуванням віддалених символів, дозволяє оцінити втрати швидкості в зв'язку з неправильним введенням;

швидкість брутто + - швидкість набору з урахуванням віддалених символів і натискань «BackSpace», дозволяє оцінити втрати швидкості, пов'язані з неправильним введенням і його виправленням;

швидкість брутто * - при розрахунку цієї швидкості не враховують натискання помилково введених символів, клавіші «BackSpace», а також час, витрачений на ці натискання; дозволяє оцінити швидкість при наборі даного тексту, у разі коли помилок не було зовсім.

Для проходження реєстрації та навчання системи користувач вводить ключову фразу 2 рази, ключові фрази змінюються. Під час вводу ключових фраз функції синхронізації аналізують текст, який вводить користувач. Отримані дані додаються до векторних функцій, а потім одразу зберігаються у вигляді шаблонів до бази даних, для того щоб порівнювати їх під час входу в систему. Після того, як зареєстрований користувач захоче отримати доступ до системи, йому необхідно буде ввести 2 рази ключовий запропонований текст. Під час вводу тексту, функції синхронізації будуть перевіряти правильність вводу та порівнювати їх з шаблонами зареєстрованих користувачів на етапі навчання нейронної мережі. Після цього доступ користувачу дозволяється або

забороняється. Після того як користувач створений він повинен провести навчання нейронної мережі, яка також зберігається в базі даних. Спроектована модель системи, включаючи навчену нейронну мережу, шаблони текстових наборів та функцій тепер готові для використання ідентифікації користувача.

Спроектована блок-схема роботи засобу ідентифікації користувача системи безпеки за клавіатурним почерком на основі нейромереж зображена на рисунку 1.

Основні головні етапи розробленого методу:

1) збір всіх необхідних даних;

робота модуля асинхронної взаємодії;

основний аналіз модулів мережі;

підбір параметрів навчання;

навчання мережі;

перевірка коректності роботи мережі.

Запропонований підхід до розпізнавання користувачів по клавіатурному почерку є надійним та немає недоліків класичних статистичних методів і здатний забезпечити високі показники розпізнавання та максимальну точність мітки. Нейронна мережа є інструментом узагальнення. Причиною вибору нейромережевого підходу серед числа інших методів класифікації є те, що нейронна мережа проста у використанні і може легко вирішувати складні проблеми. Виділені особливості клавіатурного почерку виступають в якості вхідного шаблону для нейронної мережі, які навчаються відповідно до цілі, де ваги оновлюються для отримання мінімальної помилки.

Для того щоб дізнатися кількість необхідних нейронів в прихованому шарі, скористаємось формулою:

$$N = \frac{N^W}{N_x + N_y} \qquad (1)$$

де N_y - розмірність вихідного сигналу;

N_w - необхідне число синапатичних зв'язків;

N_x - розмірність вхідного сигналу;

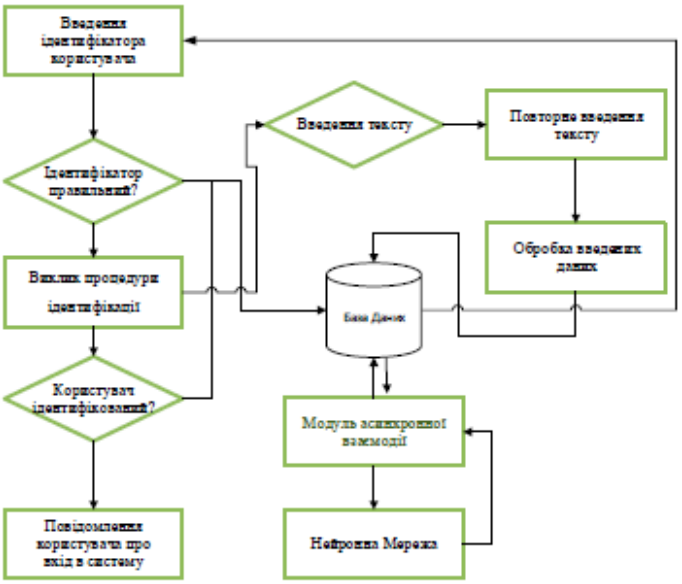

Рис. 1. Спроектований метод роботи системи

Таким чином, число нейронів в прихованому шарі буде в діапазоні $1 < N < 70$. Досліджуємо весь діапазон і виберемо ту кількість нейронів на прихованому шарі, при якому помилка навчання буде менше – 70 нейронів. Основне розрахункове навантаження лягає на нейрони прихованого шару, тому його активаційну функцію слід зробити сигмоїдною. У нейронних мережах прямого поширення синапатичні зв'язки організовані таким чином, що кожний нейрон даного рівня ієрархії сприймає інформацію тільки від деякої непустої множини нейронів, які розташовані на більш низькому рівні. Назва мереж вказує на те, що у них існує виділений напрям поширення сигналів, які рухаються, починаючи з входу, через один або декілька прихованих шарів до вихідного шару. Легко помітити, що багатошарова нейронна мережа може бути одержана шляхом каскадного об'єднання одношарових мереж з матрицями вагових коефіцієнтів $W^1, W^2, \ldots, W^p$, де p — кількість шарів нейронної мережі.

Запропонована нейронна мережа являє собою двошарову систему прямого доступу до мережі з 70 сигмовидних прихованих нейронів та 10 сигмовидних вихідних нейронів як показано на рисунку 2.

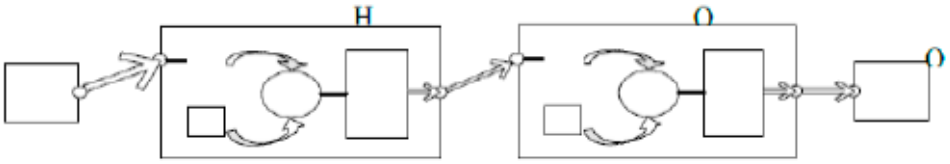

Рис. 2. Розроблена архітектура нейромережі

Вхідними даними для мережі буде час утримання клавіш та тимчасові інтервали між натисканням клавіш.

Навчання, враховуючи всі переваги та недоліки, здійснюється так:

Рандомізуємо всі ваги мережі в малі величини.

На вхід мережі подається вхідний навчальний вектор X і обчислюється сигнал NET від кожного нейрона, використовуючи стандартний вираз

$$NETW_j = \sum_i xw \tag{2}$$

Обчислюється значення порогової функції активації для сигналу NET від кожного нейрона.

Обчислюється помилка для кожного нейрона за допомогою віднімання отриманого виходу з необхідного виходу:

$$error_j = target_j - OUT_j \tag{3}$$

Кожна вага модифікується в такий спосіб:

$$W_{ij}(t+1) = w_{ij}(t) + a_x error_j \tag{4}$$

Повторюються кроки з другого по п'ятий доти, поки помилка не стане досить малою.

Існує розроблений засіб ідентифікації користувача за клавіатурним почерком на базі нейромережі, зі зручним користувацьким інтерфейсом, який забезпечує високий рівень захищеності. Даний програмний продукт розповсюджуватиметься по типу Trial – умовно-безкоштовне програмне забезпечення з повним функціоналом, але з часом використання 30 днів. Подальше використання без придбання ліцензійного ключа буде неможливим. Програму можна буде завантажити з Інтернету, купуватиметься лише електронний ключ, який є унікальним для кожної ліцензійної копії.

Список літератури

1. DigitalPersona Fingerprint Identity Solutions for Identity Protection, Security and Compliance [Електронний ресурс]. – Режим доступу: http://www.digitalpersona.com.

2. Identix – Protecting and Securing Personal Identities and Assets [Електронний ресурс]. – Режим доступу: http://www.11id.com/pages/17.

3. Данилюк І. І., Карпінець В. В., Приймак А. В., Яремчук Ю. Є., Костюченко О. І. Метод ідентифікації користувача за клавіатурним почерком на основі нейромереж. *Реєстрація зберігання і оброблення даних*. 2018. Том 20, №2. С. 68-77.

4. Галатенко В. А. под ред. академика РАН В. Б. Бетелина Основы информационной безопасности: учебное пособие, 4-е изд. Москва: Интернет-Университет Информационных технологий; Бином. Лаборатория знаний, 2008. 205 с.

5. Ахрамович В. М. Ідентифікація й аутентифікація, керування доступом // *Сучас. захист інформації*. 2016. №4. С. 47-51.