УДК 004.056(075)
Матвейчук О.В.[1], Воскобойник В.О.[2]
[1] студ. гр. РТ-819м НУ «Запорізька політехніка»
[2] проф. НУ «Запорізька політехніка»

ВИКОРИСТАННЯ МЕТОДІВ ШТУЧНИХ НЕЙРОННИХ МЕРЕЖ ДЛЯ ЗАХИСТУ КОМП'ЮТЕРІВ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

Метою даної роботи є аналіз методів захисту інформації від несанкціонованого доступу. Як правило, використовуються такі методи як ідентифікація, автентифікація, управління доступом і технічні засоби. Біометрична автентифікація заснована на унікальності певних антропометричних характеристик людини. В області інформаційних технологій поняття біометрія застосовується в значенні технології ідентифікації особистості. Біометричний захист більш ефективний ніж такі методи, як використання смарт-карт, паролів, PIN-кодів. Найчастіше використовуються: параметри голосу, візерунок райдужної оболонки ока і карта сітківки ока, форма долоні, відбитки пальців, форма і спосіб особистого підпису та риси обличчя.

Для вирішення задач біометричної автентифікації використовуються штучні нейронні мережі (ШНМ). Це паралельно розподілена система обробки інформації, утворена тісно зв’язаними простими обчислювальними вузлами (однотипними або різними), що має властивість накопичувати експериментальні знання, узагальнювати їх і робити доступними для користувача у формі, зручній для інтерпретації й прийняття рішень.

Розпізнавання образів (зображень, текстів, звуку, мови тощо) є тією галуззю, де найбільш яскраво виявляються переваги ШНМ. Найбільш придатною для розпізнавання зображень і їх класифікації є архітектура згорткових нейронних мереж (ЗНМ). Вона обробляє дані не цілком, а фрагментами, але при цьому дані не дробляться на частини, а здійснюється послідовний прогін. Потім дані передаються далі по верствам. З її допомогою

можливо розпаралелювання обчислень, і, як наслідок, використання графічних процесорів. Однак ця архітектура потребує налаштування великої кількості варійованих параметрів, таких як кількість шарів, кількість ядер в кожному шарі, функції активації кожного нейрона і багато інших.

Для рішення задачі верифікації буде використовуватися ЗНМ, а саме попередньо навчена нейронна мережа ResNet. Для навчання ЗНМ використовується алгоритм зворотного поширення помилки з обмеженням на ваги. Від мережі відрізаються шари, що відповідають за класифікацію, і залишаються тільки згорткові шари, які витягують ключові ознаки з зображення. Результат роботи - набір чисел, який називається дескриптором. Дескриптор – ідентифікатор особливої точки (вектор), який робить її унікальною щодо інших особливих точок. Такі дескриптори будуть знайдені з фотографій, одна з яких попередньо завантажена в програму, а інша завантажується з web-камери.

Мережа навчена спеціальним чином так, щоб дескриптори фотографій однієї людини перебували поруч один з одним, а різних людей - далеко один від одного. Щоб оцінити близькість дескрипторів в dlib використовується Евклідова відстань. Якщо значення Евклідової відстані між дескрипторами менше 0.6, то вважається, що на фотографіях одна й та сама людина. Попередньо навчений метод виявлення орієнтирів особи в бібліотеці dlib використовується для оцінки місця розташування 68 (x, y) - координат, які співставляються з лицьовими структурами.

Якщо витягувати дескриптор з фотографії повернутого обличчя, не знаходячи ключових точок, він може сильно відрізнятися від дескриптора фотографії особи в фас. Щоб вирішити цю проблему, dlib використовує афінне перетворення фотографії з використанням ключових точок. Проводиться перенесення ключових точок в таку позицію, як нібито людина дивиться прямо в камеру. Дескриптори витягуються тільки після афінного перетворення зображення.

Розроблене ПЗ може застосовуватися в різних сферах діяльності, задачах забезпечення безпеки інформаційної діяльності з використанням методів автентифікації та верифікації. Дане ПЗ може застосовуватися в банківській сфері для автентифікації співробітника або клієнта. Для співробітника, - це може використовуватись для доступу в систему на робочому комп'ютері, а для клієнта - верифікації, наприклад, при пред'явленні паспорта (що буде завантаженою фотографією) і фотографією з web-камери для, наприклад, доступу до своїх даних або для обліку клієнтів співробітниками банку. Також ця програма може бути застосована на пропускних контролях підприємства разом із використанням пропуску або

замість нього. Попередньо в базу даних будуть внесені фотографії кожного із співробітників, і ШНМ визначатиме, співробітник чи це і який саме, дозволяючи або забороняючи певний тип доступу або доступ взагалі. Також на підприємствах за допомогою даного ПЗ може проводитися автентифікація при доступі до робочого комп'ютера, що також підвищить безпеку підприємства.