У випадку з наведеною вище системою на вхід мережі будуть подані певні параметри хатньої тварини, її морфологічні промірки, вік, стать, порода. Згідно з сукупності цих параметрів мережа визначатиме, до якого з класів відносити стан тварини, тобто оцінюватиме її стан здоров'я.

Таким чином, використання нейронної мережі Хопфілда дає змогу поліпшити та автоматизувати процес розпізнавання образів. Алгоритм мережі Хопфілда має ряд переваг над іншими мережами, зокрема простота та циклічний принцип функціонування, а також жорсткі порогові функції нейронів. Виходячи з цього, мережа Хопфілда добре підійде для використання у системі розпізнавання образів з метою оцінювання стану хатніх тварин.

Список літератури

1. Мережі Хопфілда та Хеммінга [Електронний ресурс]
http://apsheronsk.bozo.ru/Neural/Lec6.htm
2. Нейронна мережа Хопфілда [Електронний ресурс]
https://ru.wikipedia.org/wiki/Нейронная_сеть_Хопфилда
3. Лепський О.Е., Броневич О.Г. Математичні методи розпізнавання образів: Курс лекцій. – Таганрог: Вид-во ТТИ ЮФУ, 2009. – 155 с.

УДК 004.32:004.056.55(043.2)

Рогожук Н.В., студент 3 курсу спеціальності «Комп'ютерні науки»
Січко Т.В., к.т.н., доцент, доцент кафедри інформаційних технологій

ПЕРЕДАЧА ДАНИХ НЕБЕЗПЕЧНИМ КАНАЛОМ ЗВ'ЯЗКУ, З ВИКОРИСТАННЯМ ШИФРУВАННЯ ВІДКРИТИМ КЛЮЧЕМ

Донецький національний університет імені Василя Стуса, м. Вінниця

У часи глобалізації Інтернету, завдяки якому ми обмінюємось повідомленнями, фотографіями, здійснюємо банківські платежі, керуємо багатомільйонними компаніями та зберігаємо приватні дані, потрібно бути впевненим про безпеку даних. Саме для цього використовують шифрування.

Шифрування - це спосіб перетворення даних, з форми доступної для читання людиною, у форму, яку людина прочитати неспроможна. За рахунок цього дані залишаються конфіденційними і недоступними. В свою чергу з операцією шифрування обов'язково повинна існувати операція дешифрування - отримання початкового виду. Шифрування дозволяє бути впевненим, в тому, що все, що передає та отримує користувач, проаналізовано зловмисниками [1].

В свою чергу розповсюдженим та одним з найбезпечніших способів побудувати безпечний канал передачі інформації між двома користувачами, або між сервером та користувачем є шифрування з відкритим ключем.

Проблема з ключами була вирішена тільки в 1975 році, коли Уітфілд Діффі (Bailey Whitfield 'Whit' Diffie) і Мартін Хеллман (Martin E. Hellman) запропонували концепцію шифрування з парою ключів: відкритим (публічним - public key), який зашифровує дані, і відповідним йому закритим (приватним - private key), який їх дешифрує.

Ця асиметрична система шифрування отримала назву криптографії з відкритим ключем.

Основна властивість шифрування з відкритим ключем - це створення приватного ключа на обох сторонах, та на основі нього створення публічного ключа. Під час ініціалізації з'єднання, клієнти, або клієнт та сервер обмінюються публічним ключем, перехоплення якого зловмиснику не дає абсолютно нічого. Далі під час відправлення даних клієнтом A до клієнта B дані шифруються публічним ключем, який був отриманий від клієнта B і розшифровуються, відповідно, приватним ключем клієнта B. Отже дані шифруються публічним ключем, а дешифруються приватним. Отже ці ключі завжди працюють в парі. Приватний ключ не може існувати без публічного, так само публічний, не працює без приватного. Властивість цих ключів забезпечує асиметричне шифрування. Ідея у тому що, для нього використовуються односторонні функції. Тобто, нехай маємо $f(x) = y$. Отримати y, знаючи x просто. Але знаючи y, отримати x за розумний час неможливо [2].

Шифрування з відкритим ключем використовується майже всюди, де є необхідність у побудові закритого каналу зв'язку. Цей метод використовується при підключенні до Wi-Fi, при відправці повідомлень в месенджерах, в усіх сайтах, адреса яких починається з https://. Зараз великими компаніями, такими як Google, активно розповсюджуються політика, основною ціллю якої є повна відмова та заборона сайтів без підтримки протоколу https https. Також на основі асиметричної криптографії побудований алгоритм блокчейна, на якому, в свою чергу побудовані всі криптовалюти, включаючи Bitcoin.

Переваги шифрування з відкритим ключем:

- безпека;
- відносна легкість побудови на основі будь якого каналу передачі інформації
- популярність;
- постійне вдосконалення.

Недоліки шифрування з відкритим ключем – більше навантаження на пристрої, в порівнянні з використанням незахищеного каналу.

Можна стверджувати, що на сьогоднішній день, відмовитись від шифрування, зокрема шифрування відкритим ключем просто недопустимо. Всі хочуть почувати себе у безпеці, і бути впевненим, що особиста інформація не зможе потрапити у руки злодіїв. Зараз всі користувачі розуміють, що якщо сайт працює з https, значить він надійний, і можна безпечно на нього зайти, не хвилюючись, що зловмисники можуть перехватити інформацію. У найближчій перспективі всі сайти будуть зобов'язані перейти на протокол з використанням

шифрування відкритим ключем. І можна бути впевненим, що наше перебування у інтернет буде максимально безпечним.

Список літератури

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: Триумф, 2002. 816 с.

2. Public Key Cryptography – A Comprehensive Guide. Medium: веб-сайт. URL: https://medium.com/blockwhat/public-key-cryptography-a-comprehensive-guide-1e8489e08104

3. Криптография с открытым ключом (Асимметричная криптография). Youtube: веб-сайт. URL: https://www.youtube.com/watch?v=d-qzWp5WUWI