загроз, все одно потрібно турбуватися про 20%, що залишилися. Інші 20% загроз, швидше за все, включають складні загрози, які можуть завдати значної шкоди [4]. Більшість традиційних систем захисту призначені для виявлення та блокування загроз на етапі їх спроби втручання в систему об'єкта інформаційної діяльності, отже, якщо загроза все ж проникне, то зможе безперешкодно існувати в скомпрометованій системі. Активним виявленням загроз займаються так звані "мисливці" - досвідчені фахівці з кібербезпеки, що діють за певним алгоритмом, в залежності від вихідних даних, отриманих розвідкою загроз. Розвідка даних - це знання, створені з фактичних даних (механізми, послідовності подій, контекст).

ІТ-індустрія відчуває значне піднесення галузі кібербезпеки завдяки сприятливим умовам та інвестиціям бізнесу й державних організацій. Концепція активного виявлення загроз є зручною та дуже гнучкою, цілком можливо, що ще багато компаній почне адаптувати власні продукти кіберзахисту під неї.

Список літератури

1. Вдосконалення кіберзахисту інформаційних систем за рахунок адаптивних технологій розпізнавання кібератак: https://jrnl.nau.edu.ua/index.php/ZI/article/view/10588

2. Застосування штучного інтелекту у сфері кіберзахисту: http://ir.stu.cn.ua/bitstream/handle/

3. Інтелектуальна система кіберзахисту: http://elartu.tntu.edu.ua/bitstream/

4. Threat-hunting: https://www.ibm.com/topics/threat-hunting

УДК 004.94+004.8

Мисько Б.В. та Первачук Р.Ю.
спеціальності 122 «Комп'ютерні науки»
Ніколюк П.К., професор
кафедри інформаційних технологій

БАЗОВЕ ВИКОРИСТАННЯ МОДЕЛЕЙ МАШИННОГО НАВЧАННЯ ДЛЯ АНАЛІЗУ ЗВУКУ

Донецький національний університет імені Василя Стуса, м. Вінниця

У сучасному світі відбулося багато інноваційних досягнень, які сильно вплинули на життя людей. Одним із найбільш актуальних відкриттів був «Штучний інтелект».

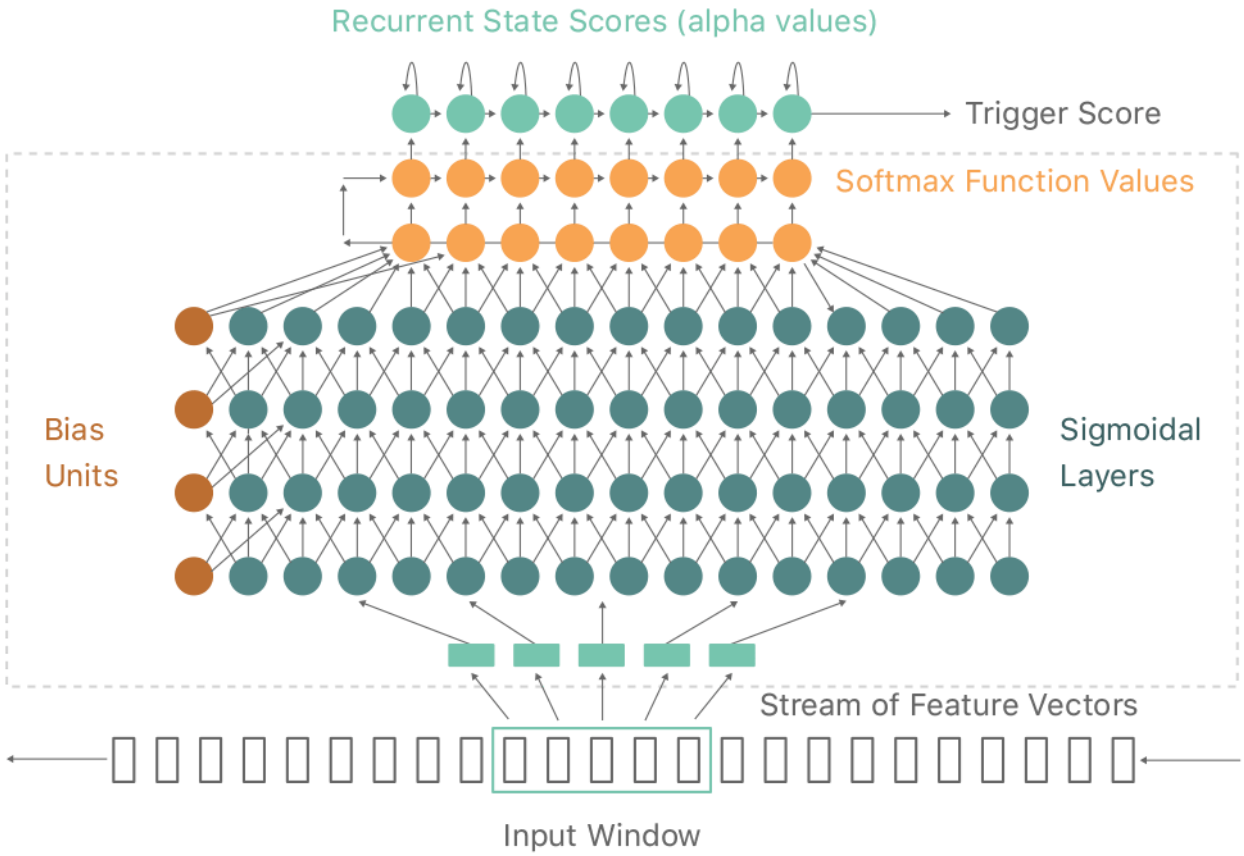
Штучний інтелект (ШІ) – це набір алгоритмів, за допомогою яких, машина обробляє і використовує інформацію. Наприклад, вдосконалює знання та вміння, вчиться ухвалювати правильні рішення, тобто імітує людину.
Поняття штучного інтелекту пов'язане з такими термінами, як:

- Нейромережа – це обчислювальна система, яка здатна до самонавчання. Вона вдосконалюється шляхом аналізу прикладів і поступово покращується.
- Машинне навчання – блок методів в області штучного інтелекту, за допомогою яких, машини вчаться виконувати певні задачі на власному досвіді, а не просто діють згідно з інструкціями. Тобто, машина обробляє величезні масиви даних, і шукає в них закономірності.
- Опрацювання природної мови – це напрям штучного інтелекту, який вчиться синтезувати та імітувати людське спілкування, а саме аналізує текстові, аудіо- та відеодані.
- Глибинне навчання – це набір методів, за допомогою яких використовуються багатошарові штучні нейронні мережі, щоб забезпечити максимальну точність виконання завдань. За допомогою нейромереж тренують машину сприймати великі обсяги необроблених даних (текст, аудіо, відео тощо)[1].

На сьогоднішній день штучний інтелект присутній майже повсюди. Наприклад, коли ми використовуємо камеру в смартфоні, коли оплачуємо товари, робимо пошук інформації в інтернеті, прослуховуємо музику за допомогою різних стрімінгових сервісів (штучний інтелект аналізує наші вподобання і рекомендує найбільш цікаві для нас треки) і т.д.

Проте не варто забувати про голосовий пошук (голосових асистентів), що є однією із найсучасніших технологій з підтримкою штучного інтелекту, які допомагають нам у виконанні певних задач. Найпопулярнішими з них є: Siri, Google Assistant, Alexa та Cortana. Наразі голосові асистенти оснащені програмами обробки і розпізнавання людського голосу, що робить їх інструментами ШІ. А також, через свою розповсюдженість голосовий пошук доступний на 3,9 мільярдах пристроїв, що закріплює його популярність серед інших штучних інтелектів[2].

Розглянемо як саме працюють голосові асистенти на прикладі «Siri» від компанії Apple. Передусім, варто зазначити, що Siri може працювати без натискання додаткових кнопок/функцій, а лише за допомогою контролю голосом. Так, мікрофон в пристрої трансформує отриманий звук на потік фонем – миттєвих зразків звукового сигналу. На етапі спектрального аналізу вони перетворюються на послідовність фреймів (кадрів), кожне з яких відображає приблизно 0,01 с звукового спектру. Приблизно 20 таких фонем за раз надходять до моделі – DNN (Deep Neural Network – глибокої нейронної мережі), яка перетворює кожен із цих звукових патернів на набір імовірностей комбінацій фонем(з якої імовірністю після «с» буде «і», з якою – «р» і т.д.) Це допомагає визначити можливі слова/фрази, що були сказані, навіть коли не всі звуки були сприйняті добре. Щоб виявити ключову фразу «Гей, Сірі» DNN складається здебільшого з матричних множень і логістичних нелінійностей. Кожен «прихований» шар є проміжним представленням, виявленим DNN під час навчання для перетворення вхідних даних банку фільтрів у звукові класи[4].



Зображення 1. Глибанна нейрона мережа(DNN)

Ми хочемо виявити «Гей, Сірі», якщо вихідні сигнали акустичної моделі високі в правильній послідовності для цільової фрази. Щоб створити єдину оцінку для кожного кадру, ми накопичуємо ці локальні значення в дійсній послідовності з часом. У данній формулі, усередині кожного блоку є максимальна операція та доповнення:

$$F_{i,t} = max\{s_i + F_{i,t-1}, m_{i-1} + F_{i-1,t-1}\} + q_{i,t} \quad (1)$$

$F_{i.t}$ – накопичений бал для моделі в позиції «i»;

$q_{i,t}$ — результат акустичної моделі — логарифмічний показник для фонетичного класу, пов'язаного з i-м станом, з огляду на акустичну картину навколо часу t;

s_i — це вартість, пов'язана із перебуванням у позиції i;

m_i — вартість переходу з позиції i;

I s_i, і m_i базуються на аналізі тривалості сегментів із відповідними мітками в навчальних даних. (Ця процедура є застосуванням динамічного програмування та може бути отримана на основі ідей про приховані марковські моделі — HMM.)

Кожна накопичена оцінка $F_{i.t}$ пов'язана з маркуванням попередніх кадрів станами, як задано послідовністю рішень максимальною операцією. Остаточна оцінка для кожного кадру є $F_{i.t}$, де останнім станом фрази є стан I, а в послідовності кадрів, що ведуть до цієї оцінки, є N кадрів. Майже всі обчислення в детекторі "Гей, Сірі" виконуються в акустичній моделі.

Обчислення часової інтеграції є відносно дешевим, тому ми не враховуємо його, оцінюючи розмір або обчислювальні ресурси[3].

Список літературних джерел

1. *«Від Ш до І: що таке штучний інтелект та як він трансформує світ» URL: https://cutt.ly/cM5T7Ej (дата звернення: 01.11.2022)*
2. *«Всі говорять про штучний інтелект. Простими словами пояснимо, що це» URL: https://espreso.tv/article/2017/11/04/shtuchnyy_intelekt (дата звернення: 01.11.2022)*
3. *«Hey Siri: An On-device DNN-powered Voice Trigger for Apple's Personal Assistant» URL: https://machinelearning.apple.com/research/hey-siri (дата звернення: 01.11.2022)*
4. *«Голосовий асистент: як працює робот у смартфоні» URL: https://cutt.ly/iM5YcJr (дата звернення: 01.11.2022)*

УДК 004.056.53:(004.75:002.1-021.51)

Мосєвніна А.С., здобувач вищої освіти
Зелінська О.В., доцент,
доцент кафедри інформаційних технологій,

КАНАЛИ НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО ІНФОРМАЦІЇ

Донецький національний університет імені Василя Стуса, м. Вінниця

Найпоширенішим та найрізноманітнішим способом впливу на інформаційну систему є несанкціонований доступ. Цей спосіб надає можливість завдати шкоди будь-якій із складових інформаційної безпеки.

Несанкціонований доступ – незаконне спеціальне оволодіння конфіденційною інформацією людиною, яка не має права доступу до цієї інформації [1].

Канали несанкціонованого доступу упорядковують за компонентами автоматизованих інформаційних систем:

1) через людину:
• розкрадання носіїв інформації;
• отримання інформації з екрана чи клавіатури;
• отримання інформації з друку;
2) через програму:
• перехват паролів;
• розшифрування зашифрованої інформації;
• відтворення інформації з носія;
3) через апаратуру:
• підключення спеціальних розроблених апаратних засобів, які постачають доступ до інформації;