Гречук Д.В. студентка гр. 125-20-3
Науковий керівник: Олішевський І.Г., асистент кафедри БІТ
(*Національний технічний університет "Дніпровська політехніка", м. Дніпро, Україна*)

МАШИННЕ НАВЧАННЯ – ЗАСТОСУВАННЯ ТА БЕЗПЕКА

Сьогодні комп'ютери пишуть картини, алгоритми складають вірші і класифікують фотографії, роботи самостійно пересуваються в довкіллі, а деякі з них навіть самі вміють приймати різні рішення. Усе це можливо завдяки машинному навчанню. Цю область називають найбільш перспективною і складною областю штучного інтелекту (ШІ). Єдиного визначення для machine learning (машинного навчання) поки немає. Але більшість дослідників формулюють його приблизно так: машинне навчання - це наука про те, як змусити штучний інтелект вчитися і діяти як людина, а також зробити так, щоб він сам постійно покращував своє навчання і здібності на основі наданих нами даних про реальний світ.

Існує декілька видів машинного навчання, які ієрархічно зображені на Рис. 1. Розглянемо їх детальніше.

Класичне

Класичне навчання буває з учителем і без нього. Якщо машина тренується вирішувати завдання з учителем, вона отримує розмічені дані. Таким чином, комп'ютеру вдається швидше видавати результати.

Якщо алгоритми тренуються без учителя, їм доводиться самостійно аналізувати інформацію і шукати закономірності. Такий підхід займає більше часу, проте розробникам не треба готувати базу даних заздалегідь.

З підкріпленням

Навчання з підкріпленням використовується, щоб роботи навчилися виживати в різних середовищах і адаптуватися до умов. Такий метод також застосовують для навчання персонажів в іграх і безпілотних автомобілів. Їм необхідно узагальнити ситуацію і отримати з неї вигоду.

Ансамблі

Якщо розробники використовують метод ансамблів, вони збирають разом декілька машин з різними методами навчання. Далі машини вчаться виправляти помилки один одного.

Глибоке

Глибоке навчання використовується для нейромереж. З його допомогою нейронні мережі виконують завдання комп'ютерного зору, розпізнавання мови і машинного перекладу.

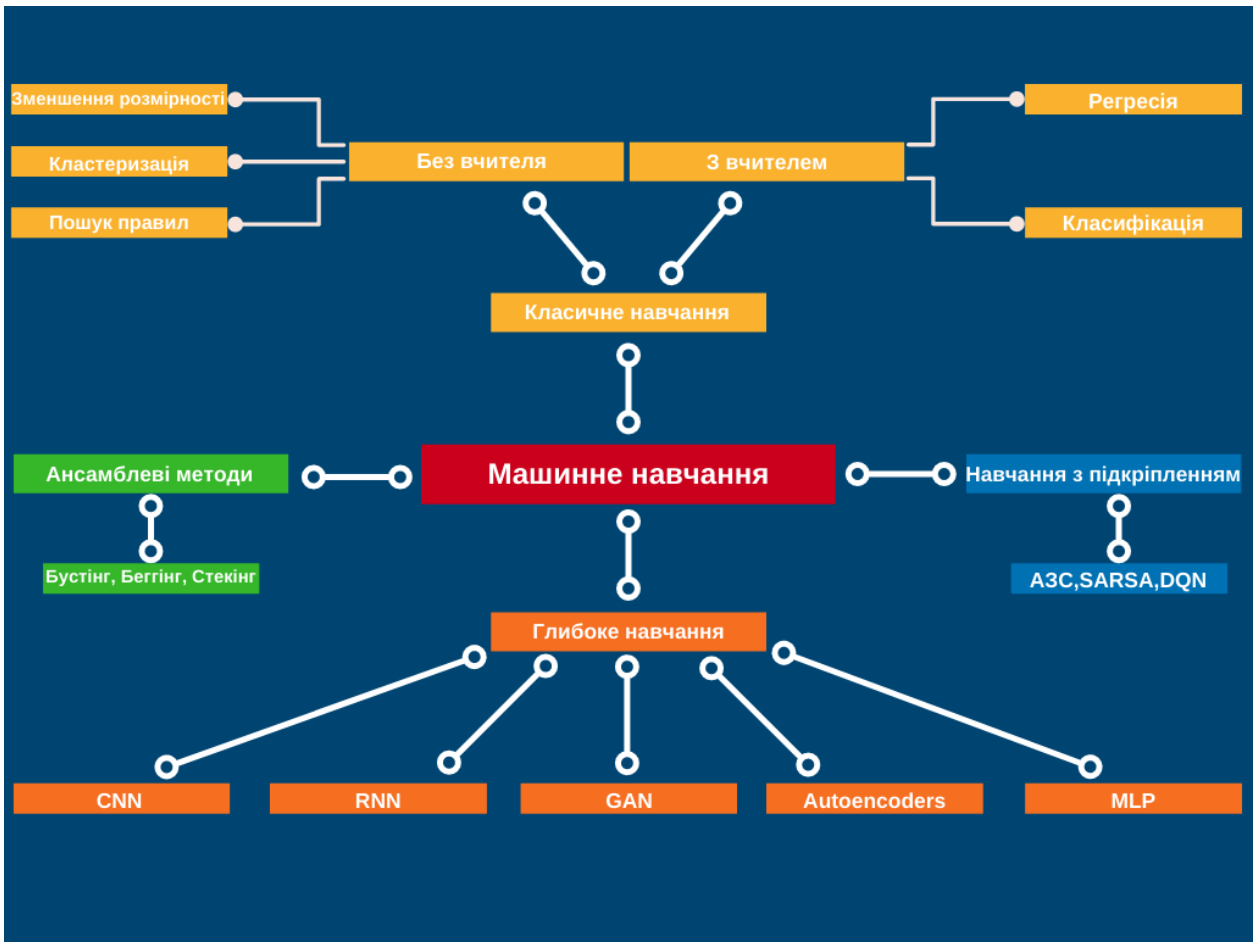

Рис. 1. – Види машинного навчання

Сьогодні існує безліч застосувань машинного навчання.

Головні напрямки застосування технології:

- розпізнавання мовлення у віртуальних асистентах;
- розпізнавання рукописних букв;
- визначення мов;
- рекомендації на сайтах;
- пошук документів;
- визначення підозрілих транзакцій;
- прогнозування вартості валют;
- аналіз попиту;
- навчання розумної техніки і т.д.

Один з найвідоміших прикладів у сфері бізнесу - американська торгова мережа Target, яка використовує машинне навчання, щоб передбачати поведінку покупців. На основі даних про покупки алгоритми визначають зміни в житті, інтересах і потребах клієнтів, щоб пропонувати їм рекламу актуальних для них товарів.

Окрім іншого, машинне навчання широко використовується в комп'ютерній безпеці. Де різні методи давно застосовуються в захисті даних від витоків і вірусних атак, оскільки, традиційні методи захисту даних вже не можуть впоратися з цими завданнями повною мірою.

Поєднання різних методів машинного навчання підвищує ефективність розпізнавання шкідливого ПЗ і попередження атак. Таким чином реалізується поведінкова аналітика, наприклад, коли логується, а потім аналізується послідовність подій в період виконання процесу. Класифікувавши подію, ML- модель зводить його до набору бінарних векторів і навчає глибоку нейронну мережу відрізняти небезпечну активність від логів легітимних подій.Ще один корисний варіант використання(use case) машинного навчання в кібербезпеці - це автоматичний моніторинг поведінки комплексних Big Data систем і корпоративної IT-інфраструктури. Наприклад, в різних банках фахівцям з експлуатації банківських сервісів Machine Learning допомагає своєчасно визначити аномальну активність окремих компонентів або користувачів.

Машинне навчання не майбутнє, а реалії сьогоднішнього дня. Завдяки розвитку технологій машинного навчання програміст не повинен вручну прописувати усі можливі проблеми і їх рішення, тепер це робить програма: в неї закладають певний алгоритм, по якому вона самостійно знаходить рішення і будує прогнози. Проте якщо хтось упевнений в користі, у тих виникають неабиякі побоювання. Адже якщо машини здатні так швидко навчатися і в рази ефективніше вирішувати практично усі завдання, то який ринок праці нас чекає в майбутньому? Машини вже зараз автоматизують багато процесів і відбирають робочі місця у адміністраторів, аналітиків, оптимізаторів. Можна припустити, що машини продовжать перевершувати нас в рішенні складних і часто повторюваних завдань, тоді як люди можуть зайнятися рішенням нових, цікавіших ситуацій. Такі людські якості, як емоційна стійкість, креативність, інтуїція цінуватимуться ще більше.Наше завдання в поточних реаліях - розуміти сучасний світ і швидко адаптуватися. При цьому інвестувати не лише в технології, але і у свою власну освіту: набувати нового бачення світу, при цьому посилювати і розвивати навички, які недоступні машинам.

Перелік посилань

1. «Безопасность машинного обучения: эффективные методы защиты или новые угрозы?», Positive Technologies, 2018
2. «Машинное обучение наступает: новые реалии жизни, новые возможности в маркетинге», Анастасия Скороходова
3. «Что такое машинное обучение и как оно работает», Ася Зуйкова, 2021