ISSN 2411-3816 (Print)
СУЧАСНА СПЕЦІАЛЬНА ТЕХНІКА
MODERN SPECIAL TECHNICS
DOI (Issue): https: //doi.org/10.36486/mst2411–3816.2020.2(61)
Issue 2(61) 2020

УДК 621.397.42

Буран Вікторія Володимирівна,
здобувач, старший науковий співробітник
ДНДІ МВС України, м. Київ, Україна,
ORCID ID 0000-0001-6647-1399

ШТУЧНИЙ ІНТЕЛЕКТ У ВІДЕОСПОСТЕРЕЖЕННІ

У статті розглянуто основні дослідження в галузі штучного інтелекту як науки, що займається створенням автоматизованих інтелектуальних систем, які застосовуються в відеоспостереженні. Досліджено технологічні аспекти створення систем штучного інтелекту. У статті розкрито сутність та уявлення про штучний інтелект, який постійно змінюється, трансформуються бачення шляхів його розвитку, підходи до вивчення та функціонування загалом. Визначено найбільш перспективні напрями в пізнанні штучного інтелекту.

Ключові слова: *штучний інтелект, відеоспостереження, машинне навчання, нейронні мережі, експертні системи, технологія Deep Learning.*

В статье рассмотрены основные исследования в области искусственного интеллекта как науки, занимается созданием автоматизированных интеллектуальных систем, применяемых в видеонаблюдении. Исследованы технологические аспекты создания систем искусственного интеллекта. В статье раскрыты сущность и представление об искусственном интеллекте, который постоянно меняется, трансформируются видение путей его развития, подходы к изучению и функционированию в целом. Определены наиболее перспективные направления в познании искусственного интеллекта.

Ключевые слова: *искусственный интеллект, видеонаблюдение, машинное обучение, нейронные сети, экспертные системы, технология Deep Learning.*

Машинне навчання й штучний інтелект останнім часом потрапили в центр уваги наукового співтовариства. Протягом десятиліть для обробки цих даних використовувалися тільки класичні алгоритми, однак ситуація змінилася з розвитком мініатюрної продуктивної обчислювальної техніки.

Штучний інтелект (ШІ) дозволяє автоматизувати повторювані процеси навчання й пошуку за рахунок використання даних. Однак ШІ відрізняється від роботизації, у основу якої покладено застосування апаратних засобів. Мета ШІ – не автоматизація ручної праці, а надійне й безперервне виконання численних великомасштабних комп'ютеризованих завдань. Така автоматизація вимагає участі людини у первинному налаштуванні системи й правильної постановки питань.

ШІ робить наявні продукти інтелектуальними. Як правило, технологія ШІ не реалізується як окремий додаток. Функціонал ШІ інтегрується в наявні продукти, дозволяючи вдосконалити їх так само, як технологія Siri була додана у пристрої Apple нового покоління. Автоматизація, платформи для спілкування, боти й

"розумні" комп'ютери в поєднанні з великими обсягами даних можуть поліпшити різні технології, які використовуються у будинках і в офісах: від систем аналізу даних про безпеку до інструментів інвестиційного аналізу.

ШІ адаптується завдяки алгоритмам прогресивного навчання, щоб подальше програмування здійснювалося на основі даних. ШІ виявляє в даних структури й закономірності, які дозволяють алгоритму засвоїти певну навичку: алгоритм стає класифікатором або предикатором. Таким чином, за тим самим принципом, за яким алгоритм засвоює гру в шахи, він може навчитися пропонувати відповідні продукти онлайн. При цьому моделі адаптуються в ході надходження нових даних. Зворотне поширення – це метод, що забезпечує корегування моделі за допомогою навчання на базі нових даних, якщо первинна відповідь виявляється невірною.

ШІ здійснює більш глибокий аналіз великих обсягів даних за допомогою нейромережі з безліччю прихованих рівнів. Кілька років тому створення системи виявлення шахрайства з п'ятьма прихованими рівнями було практично неможливим. Чимало змінилося зі швидким зростанням обчислювальних потужностей і появою "великих даних". Для моделей глибокого навчання необхідна величезна кількість даних, тому що саме на їхній основі вони й навчаються. Тому чим більше даних, тим точніші моделі.

Глибинні нейромережі дозволяють ШІ досягти безпрецедентного рівня точності. Наприклад, робота з Alexa, пошуковою системою Google Search і сервісом Google Photos здійснюється на основі глибокого навчання, і чим частіше ми використовуємо ці інструменти, тим ефективнішими вони стають. У галузі охорони здоров'я діагностика ракових пухлин на знімках МРТ за допомогою технологій ШІ (глибоке навчання, класифікація зображень, розпізнавання об'єктів) за точністю не поступається висновкам висококваліфікованих рентгенологів.

ШІ дозволяє видобути максимальну користь із даних. З появою алгоритмів, що самонавчаються, самі дані стають об'єктом інтелектуальної власності. Дані містять у собі потрібні відповіді – потрібно лише знайти їх за допомогою технологій ШІ. Оскільки нині дані відіграють набагато важливішу роль, чим коли-небудь раніше, вони можуть забезпечити конкурентну перевагу. За використання однакових технологій у конкурентному середовищі виграє той, у кого найбільш точні дані.

Deep Learning (з англ. "глибоке навчання") – це напрям, пов'язаний зі штучним інтелектом (ШІ) і машинним навчанням, у якому використовуються принципи побудови людського мозку (рис. 1). Після глибинного навчання штучні нейронні зв'язки формуються подібно до людських. Термін з'явився близько 40 років тому, але до кінця 2012 р. для реалізації передової технології не вистачало технологічних потужностей. Першим зі світових ЗМІ про Deep Learning опублікував матеріал "The New York Times". Приводом стало дослідження Алекса Крижевського, Джеффа Хінтона й Іллі Сатскевера з університету Торонто. Вони здійснили аналіз результатів розпізнавання картинок, де з великим відривом нейромережа, написана за допомогою глибокого навчання, випередила інші способи.

Ендрю Янг, один з головних фахівців із глибокого навчання, називає технологію "новою електрикою". Він вважає, що творці стартапів, які оминають розвиток прогресу, незабаром зрозуміють, що програли в гонці конкурентів.

Рис. 1

Першим кроком до розуміння того, як працює Deep Learning, є усвідомлення відмінностей між пов'язаними з ним термінами

ШІ – це здатність машини або програми знаходити рішення за допомогою обчислень. Машинне навчання припускає побудову алгоритмів, які самостійно навчаються, тобто без закодованих правил. Глибоке навчання імітує людське мислення.

Технологія Deep Learning відкриває можливості для створення нового класу програм – вирішальні когнітивні завдання. Це може значно підвищити якість життя людини. Основним же завданням глибокого навчання є часткова або повна автоматизація вирішення складних завдань у різних областях діяльності.

Сфера застосувань технології постійно розширюється: це технічна й медична діагностика, виявлення спама й шахрайства, біржовий технічний аналіз, категоризація документів, фінансовий нагляд і кредитний скоринг.

Технологія використовується у ході роботи зі штучними нейромережами, які мають кілька шарів. Більшість проєктів з Deep learning реалізовані у вигляді розпізнавання фото або аудіо, діагностики захворювань. Глибоке навчання вже застосовується в "Гугл" для перекладу тексту із зображення.

Ще один проєкт – система DeepFace, що вміє розпізнавати обличчя з точністю до 97 % – приблизно такий самий результат показує людина.

У 2016 р. з'явилася WaveNet від Google. Ця система може імітувати людську мову. Для того, щоб реалізувати програму, компанія завантажила в систему записані голосові запити користувачів із проєкту ОК Google. Після засвоєння цих даних нейромережа змогла самостійно скласти пропозицію із правильними акцентами, наголосами й без нелогічних зупинок.

Глибоке навчання не тільки сегментує зображення й відео, але й виділяє контури.

Технологія використовується у автотранспортних засобах без водія, які зчитують інформацію з дорожніх знаків, розмітку й визначають наявність перешкод на дорозі. Також Deep Learning використовують для визначення діабетичної ретинопатії в пацієнтів за фотографією очей.

Контрольоване навчання використовує маркіровані набори даних, які складаються із вхідних даних й очікуваних результатів. Коли ви навчаєте штучний інтелект за допомогою контрольованого навчання, ви подаєте на вхід дані й вказуєте, яким повинен бути результат. Якщо результат, що видав ШІ відрізняється від очікуваного, то ШІ повинен виправити свої обчислення. Процес повторюється багаторазово над масивом даних доти, поки ШІ припускається помилок. Прикладом контрольованого навчання може слугувати ШІ, що передбачає погоду. Він навчається передбачати погоду, використовуючи історичні дані. Вхідними даними є тиск, вологість і швидкість вітру, а, як наслідок, ми повинні отримати температуру. Неконтрольоване навчання – це завдання, яке полягає в навчанні ШІ з використанням неструктурованих даних. Коли ви тренуєте штучний інтелект за допомогою неконтрольованого навчання, то дозволяєте ШІ здійснити логічну класифікацію даних. Приклад штучного інтелекту, що використовує неконтрольоване машинне навчання – робот, який передбачає поводження клієнтів інтернет-магазина. Він навчається, не використовуючи заздалегідь відомі вхідні й вихідні дані. Замість цього він повинен самостійно класифікувати вхідні дані. Алгоритм повинен визначити й повідомити вам, який тип користувачів віддає перевагу певним продуктам.

Отже, Deep Learning – це один із підходів до машинного навчання. Він дозволяє передбачати результати за заданими вхідними даними. Для тренування ШІ можна використати обидва описаних вище варіанти: контрольоване й неконтрольоване навчання. Ми будемо розбиратися з тим, як працює Deep Learning на наочному прикладі: припустимо, нам потрібно розробити сервіс передбачення цін на авіаперельоти. Навчати наш алгоритм ми будемо контрольованим методом. Ми хочемо, щоб наш сервіс за передбаченням цін на авіапереліт прораховував ціну за наступними вхідними даними (зворотний переліт ми не враховуємо для простоти подачі матеріалу):

– аеропорт відправлення;
– аеропорт прибуття;
– планована дата вильоту;
– авіакомпанія.

Як і в випадку біологічних живих істот, у нашого провісника в “голові” є нейрони. На малюнку 2 вони представлені у вигляді кіл. Нейрони з’єднані між собою.

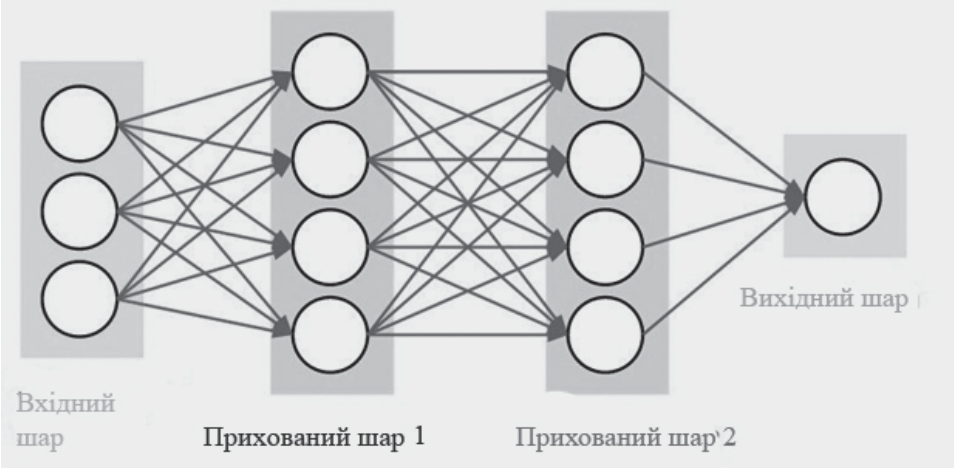

Рис. 2

На зображенні (рис. 2) нейрони об'єднані в три групи шарів:
– вхідний шар (input layer);
– прихований шар 1 (hidden layer 1) і прихований шар 2 (hidden layer 2);
– вихідний шар (output layer).

На вхідний шар заходять якісь дані. У цьому випадку маємо чотири нейрони на вхідному шарі: аеропорт відправлення, аеропорт прибуття, дата вильоту, авіакомпанія (рис. 3). Вхідний шар передає дані на перший прихований шар. Приховані шари виконують математичні обчислення, оперуючи отриманими вхідними даними. Одним з основних питань при побудові нейромереж є вибір кількості прихованих шарів і кількості нейронів у кожному шарі.

Слово Deep (глибокий) у словосполученні Deep Learning саме й вказує на наявність більш ніж одного прихованого шару.

Вихідний шар повертає нам результуючу інформацію. У нашому випадку – очікувану ціну перельоту.

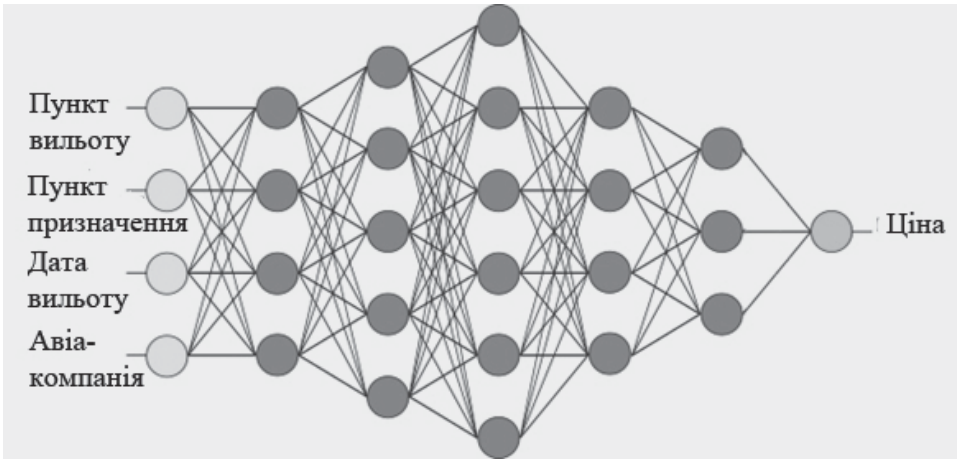

Рис. 3

Найцікавіше ми поки пропустили: як саме відбувається обчислення очікуваної ціни? Отут і починається особливість Deep Learning. Кожному з'єднанню між нейронами привласнюється певна вага (коефіцієнт). Ця вага визначає важливість вхідного значення (рис. 4). Початкові ваги встановлюються випадковим чином. Коли передбачаєш вартість авіаперельоту, дата відправлення впливає на ціну найбільше. Тому з'єднання нейрона "дата відправлення" мають більшу вагу.

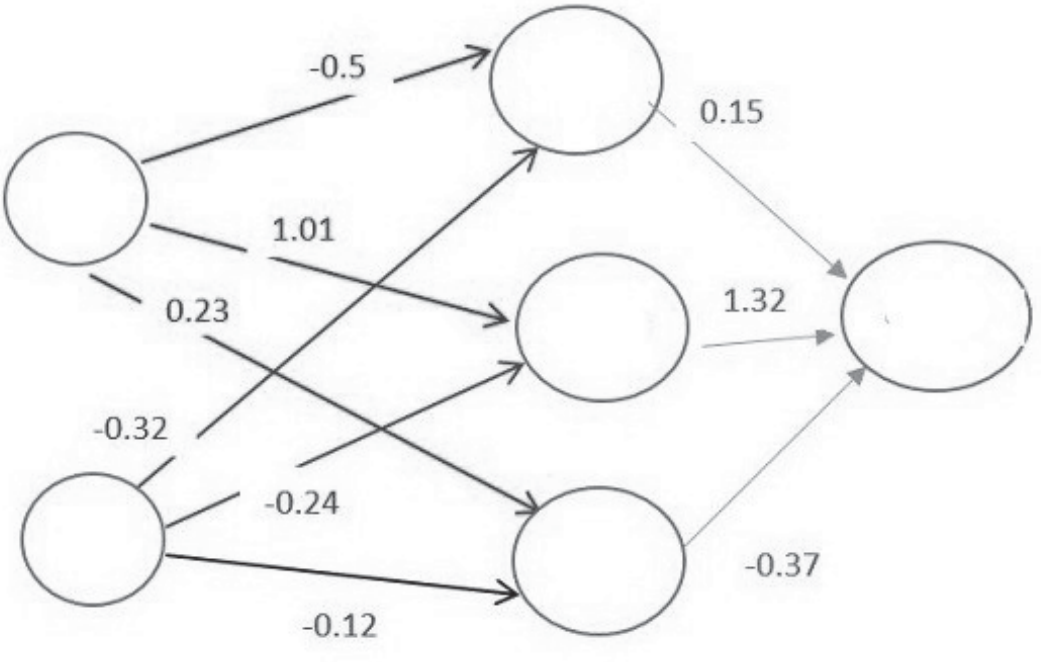

Рис. 4

До кожного нейрона прив'язана функція активації. Що являє собою ця функція, без математичних знань зрозуміти важкувато. Тому давайте підемо на деяке спрощення: зміст функції активації в тому, щоб "стандартизувати" вихідні дані від нейрона. Після того, як набір даних пройшов через всі шари нейромережі, вона повертає результат через вихідний шар.

Навчання нейромережі – найбільш складна частина Deep Learning тому, що потрібний великий обсяг даних та великі обчислювальні потужності. Для нашого проєкту нам необхідно знайти історичні дані вартості авіаквитків. Причому для всіляких комбінацій аеропортів вильоту й призначення, дат відправлення й різних авіаліній. Нам потрібен дуже великий обсяг даних із цінами на квитки. Ми повинні подавати на входи нашої нейромережі вхідні дані з нашого набору й перевіряти, чи збігаються вони з тими результатами, які в нас уже є. Якщо одержувані штучним інтелектом результати відрізняються від очікуваних, це означає, що він ще недостатньо натренувався. Після того, як ми пропустили через нейромережу весь обсяг даних, можемо побудувати функцію, яка вкаже, наскільки результати ШІ відрізняються від фактично наявних результатів у нашому наборі даних. Така функція називається функцією вартості (рис. 5). У ідеальному випадку, до якого ми прагнемо, значення функції вартості

дорівнюють нулю. Це означає, що результати вартості, підібрані нейромережею, не відрізняються від реальної вартості квитків у нашому наборі даних.

Як ми можемо зменшити значення функції вартості?

Ми змінюємо ваги з'єднань між нейронами. Це можна зробити випадковим чином, однак такий підхід неефективний. Натомість ми будемо використовувати метод, що називається "градієнтний спуск".

Градієнтний спуск – це метод, який дозволяє нам знайти мінімум функції.

У нашому випадку ми шукаємо мінімум функції вартості.

Цей алгоритм працює шляхом поступового збільшення ваг після кожної нової ітерації обробки нашого масиву даних. Обчислюючи похідну (або градієнт) функції вартості для певних наборів ваг, ми можемо побачити, за яким напрямом перебуває мінімум.

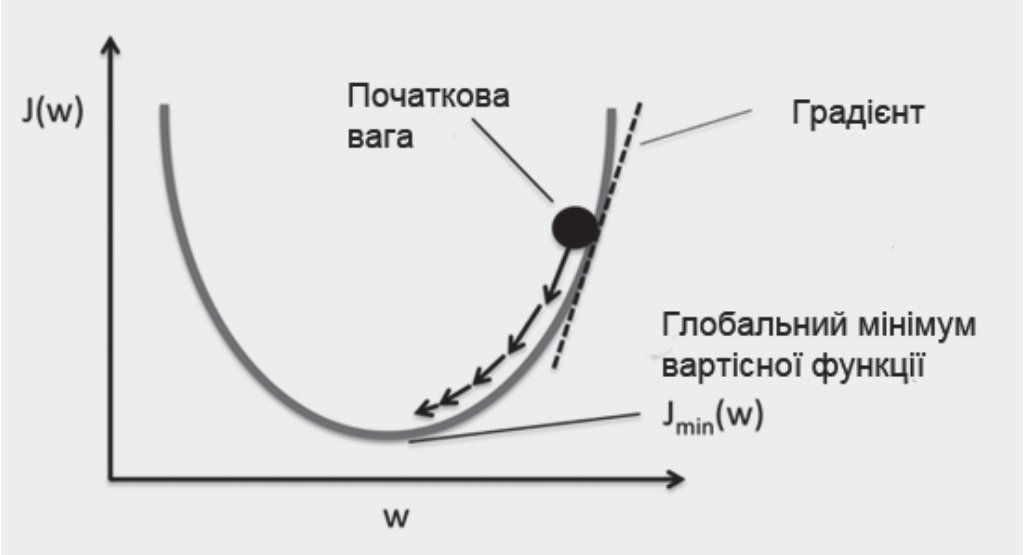

Рис. 5

На картинці Initial weight – споконвічна вага, Global cost minimum – глобальний мінімум вартісної функції. Для мінімізації функції вартості ми повинні провести обчислення над нашим масивом даних багато разів. От чому вам потрібно багато обчислювальних потужностей. Відновлення ваги за допомогою методу градієнтного спуска відбувається автоматично. От вона – особливість Deep Learning! Після того, як ми "навчили" наш І сервіс "пророкуванню" цін на авіаперельоти, ми можемо сміливо використовувати його для пророкування цін у реальності.

Штучний інтелект навчить камери "думати"

Технології штучного інтелекту (AI) перетворюють звичайну камеру відеоспостереження на розумний пристрій, здатний навчатися й надавати корисні дані в реальному часі.

Сучасні IP-камери пропонують користувачам більше, ніж безпека. Завдяки застосуванню технологій глибинного навчання й штучного інтелекту, з використанням належним чином розмічених даних, камери можна "навчити" надавати

корисну інформацію. Кібербезпека стала ще одним із пріоритетів в індустрії відеоспостереження. Після того як в 2016 році масовані DDoS-атаки призвели до великих технічних збоїв у всьому світі, уряди багатьох країн почали приділяти програмам розвитку кібербезпеки особливу увагу.

Натепер робиться акцент не тільки на використанні розумних технологій, а й на забезпеченні безпеки користувачів, які завдають користь суспільству, підвищують якість і зручність життя.

Нині робиться акцент не лише на використанні розумних технологій як таких, а саме на забезпеченні максимальної користі від їх застосування задля безпеки пересічних мешканців. Колись більшість установлених відеокамер використовувалися виняткова для запису величезних обсягів даних, однак у більшості відеоархіви не становили жодного практичного інтересу. Знайти конкретну подію у відеоархіві було вкрай складно: для оброблення гігантських обсягів відеоінформації були потрібні високопродуктивні комп'ютери. Тепер відеокамери можуть навчатися на розмічених даних, а також на нових даних, що підвищує точність відеоаналізу й дозволяє виявляти саме ті події, які цікавлять користувача.

Рис. 6

Кордони використання систем відеоспостереження для вирішення завдань безпеки зламала концепція Інтернет речей. Попит на мобільні додатки, підключені будинки, автомобілі й пристрої на основі безлюдних технологій, такі як безпілотні літальні апарати й роботи, також стимулює розвиток традиційних систем й устаткування безпеки. Особливу важливість здобувають нестандартні підходи до рішення завдань споживачів у різних галузях і створення цінності за рамками охорони й безпеки. Одне із застосувань штучного інтелекту у відеоспостереженні полягає в тому, щоб камера "думала" відповідно до поставленого завдання або оточення. Ідеться про те, щоб пристосувати до середовища або умов експлуатації не тільки апаратну частину, але й алгоритм дій камери.

Безумовно, усі компоненти системи відеоспостереження повинні бути надійно захищені, і не тільки фізично. Важливо захистити IP-компоненти, а також дані, що будуть створюватися системами відеоспостереження. Штучний інтелект розширює можливості відеоспостереження, але розвиток технологій AI перебуває

на ранньому етапі, що ще не дозволяє однозначно прогнозувати ефект від їхнього широкого застосування. Охоронні відеокамери є об'єктом кібератак, оскільки постійно підключені до мережі, а системи відеоспостереження традиційно розвивалися без огляду на кіберзагрози, що робить навіть сучасні камери вразливими. Проте на сьогодні превалює винятково позитивний потенціал штучного інтелекту.

Штучний інтелект дозволяє відеокамерам спостереження й іншому устаткуванню, що використовується в сучасних системах безпеки, виявляти загрози в режимі реального часу.

Система відеоспостереження зі штучним інтелектом може складатися із сотень або навіть тисяч відеокамер спостереження, дані яких обробляються автоматично. Нові технології дозволяють співробітникам служб безпеки негайно реагувати на загрози, захищаючи людей й активи. Щоб більше організацій могли скористатися даними перевагами, сучасні компанії впроваджують у свої рішення для відеоспостереження передові технології штучного інтелекту. Це означає, що відеокамери спостереження нового покоління тепер можуть самостійно "дізнаватися" про можливі загрози, розпізнавати у своєму полі зору людей, а також транспортні засоби й навіть підозрілу поведінку. Рішення для відеоспостереження, оснащені штучним інтелектом, автоматично сповіщають користувача про те, що відбувається. Система відеоспостереження негайно повідомить, що в зоні з обмеженим доступом з'явилася людина, або що автомобіль із номерами, які занесені в чорний список, в'їхав на територію вашої компанії. Завдяки оповіщенням, співробітники служби безпеки можуть швидко реагувати на загрози й захищати людей і майно більш ефективно.

У системах відеоспостереження зі штучним інтелектом використовуються алгоритми, які ґрунтуються на глибокому навчанні. До технологій зі штучним інтелектом відносять:

– розпізнавання осіб – дозволяє поліції знаходити підозрюваних, а комерційним організаціям – ідентифікувати VIP-клієнтів;

– ідентифікація автомобілів – може застосовуватися для ідентифікації транспортних засобів з метою забезпечення контролю доступу на охоронюваній території;

– охорона периметра – допомагає виявляти загрози, відрізняючи людей й автомобілі від інших об'єктів з мінімумом фіктивних тривог;

– бізнес-аналітика – технології підрахунку людей, виявлення черг і створення теплових карт із метою підвищення ефективності роботи організацій.

У Києві в рамках проєкту "Безпечне місто" (Kyiv Smart Safe City) проводиться тестування модуля розпізнавання осіб. Унікальний модуль дозволяє шукати правопорушників не тільки завдяки спеціалізованим камерам розпізнавання особи. Модуль фіксує зображення з будь-якої камери, установленої в рамках мережі, і порівнює їх із базою правопорушників, створеною правоохоронними органами. Якщо система виявляє подібність, оператор відразу одержує тривожний сигнал. Таким чином, система прискорює розшук злочинців і правопорушників. Зараз камери розташовані в місцях великого скупчення людей: у дошкільних навчальних закладах, школах, метрополітені, вокзалах, лікарнях і т. д.

До складу нового аналітичного модуля розпізнавання осіб входять аналітична система й база даних, що складається зі списку розшукуваних людей. Система має

два режими роботи: онлайн й оффлайн. У режимі онлайн модуль, одержавши зображення особи, порівнює його з наявними зображеннями в базі пошуку. У випадку виявлення подібності з даними бази оператор одержує сигнал тривоги. Оффлайн-режим дозволяє шукати людей у базі за фотографією особи. При пошуці в системі можна настроїти параметри, наприклад: "людина в шапці", "людина в окулярах", "темні кольори волосся", навіть вік або стать. Модуль розпізнавання – апаратно-програмний. Він є частиною інтегрованого комплексу, центра обробки даних (ЦОД), що перебуває в Києві. Апаратна й програмна частини модуля розроблені підрозділами компанії Hikvision. Розробники аналітичного модуля орієнтувалися саме на інтелектуальну систему розпізнавання осіб "Sky Net", що сьогодні використовується в 16 найбільших містах Китаю.

Як відзначив директор Департаменту інформаційно-комунікаційних технологій Юрій Назаров, одночасно система може обробляти 450 потоків, 1100 осіб у секунду.

Унікальність аналітичного модуля полягає в тому, що він здатний аналізувати потоки з різних типів камер, а не тільки з тих, які оснащені функціями розпізнавання осіб. Торік розпочато установку камер у київському метрополітені. Усього буде встановлено 198 камер на входах-виходах 52 станцій метро. Модуль розроблений з метою полегшення роботи співробітників правоохоронних органів і швидкого пошуку зловмисників.

Зараз у київському метрополітені завершується установка 198 камер відеоспостереження. Вони будуть розміщатися безпосередньо на входах і виходах вестибюлів метро. Усі камери мають функцію розпізнавання особи. Вони підключені до Єдиного центра обробки даних (ЦОД), що дозволяє спостерігати за ситуацією в онлайн-режимі. Дані з камер передаються на сервер, де зберігаються протягом 30 днів.

Сьогодні системою відеоспостереження користуються вповноважені співробітники СБУ, Національної поліції, Національної гвардії, прокуратури, МВС, Керування державної охорони, НАБУ. Крім того, підключені й муніципальні служби: районні адміністрації, структурні підрозділи КГГА, Державна служба України з надзвичайних ситуацій, "Киевавтодор" і Центр організації дорожнього руху.

Крім оповіщення про виникнення певних подій, рішення, засновані на глибокому навчанні, дозволяють виявляти на відео дані, що піддаються кількісному вимірюванню і з яких можна отримати корисну інформацію. Завдяки можливостям глибокого навчання і штучного інтелекту, передова відеоаналітика може знаходити, розпізнавати, класифікувати і індексувати об'єкти. Це забезпечує ефективність пошуку потрібної інформації в матеріалах, які створюють IP-відеокамери спостереження. Оператори систем відеоспостереження тепер можуть переглянути все відео за лічені хвилини і швидко ідентифікувати людей та об'єкти, які їх цікавлять.

Майбутнє, безумовно, за технологіями й автоматизацією. Так, у штучного інтелекту є величезний потенціал прискорити процес обробки даних, розвантажити роботу, зробити її ефективною. Однак дуже важливим при використанні ШІ є дотримання фундаментальних принципів, таких як верховенство права, недискримінація, неупередженість, справедливість, безпека та ін.

Для світового співтовариства питання впровадження штучного інтелекту наразі залишається дискусійним і супроводжується різними підходами.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Мусиенко Д.И.* Искусственный интеллект в видеонаблюдении. Бизнес и безопасность. 2020. № 1. С. 67–75.

2. Столичне комунальне підприємство "Інформатика" проводить тестування нового аналітичного модуля відеоспостереження у рамках проекту "Безпечне місто" (Kyiv Smart Safe City). URL: https://www.ukrinform.ua/rubric-kyiv/2641100-kyiv-smart-city-u-stolici-testuut-kameri-so-identifikuut-pravoporusnikiv.html (дата звернення: 09.06.2020).

3. Що таке MACHINE LEARNING та як це працює? URL: https://www.everest.ua/wp-content/upload s/2019/07/Everest-AI-Review-10.pdf (дата звернення: 09.06.2020).

REFERENCES

1. *Musiyenko, D.I.* (2020) Iskusstvennyy intellekt v videonablyudenii. "Artificial Intelligence in Video Surveillance". Business and Security 1, 67–75 [in Russian].

2.Stolychne komunalne pidpryyemstvo "Informatyka" provodyt testuvannya novoho analitychnoho modulya videosposterezhennya u ramkakh proektu "Bezpechne misto" (Kyiv Smart Safe City). "The Capital's Communal Enterprise Informatika is Testing a New Analytical Module of Video Surveillance within the Framework of the Kyiv Safe City Project". URL: https://www.ukrinform.ua/rubric-kyiv/2641100-kyiv-smart-city-u-stolici-testuut-kameri-so-identifikuut-pravoporusnikiv.html (Date of Application: 09.06.2020) [in Ukrainian].

3. Shcho take MACHINE LEARNING ta yak tse pratsyuye? What is MACHINE LEARNING and how does it work? URL: https://www.everest.ua/wp-content/upload s / 2019/07 / Everest-AI-Review-10.pdf (Date of Application: 09.06.2020) [in Ukrainian].

UDC 621.397.42

Buran Victoriia,
applicant, senior researcher of the State
Research Institute MIA Ukraine, Kyiv, Ukraine,
ORCID ID 0000-0001-6647-1399

ARTIFICIAL INTELLIGENCE IN VIDEO SURVEILLANCE

Research article considers modern research in the field of artificial intelligence as a science that deals with the creation of automated intelligent systems used in video surveillance. The technological aspects of the creation of artificial intelligence systems are studied, different approaches to their design are revealed. Paper reveals the essence and idea of artificial intelligence, which is constantly changing, transforms the vision of ways of its development, approaches to the study and functioning in general. The most promising areas in the knowledge of artificial intelligence are neural networks, evolutionary computing, expert systems. Neural networks are able to solve such applied problems as: financial forecasting, control over the activities of networks, data encryption, system diagnostics. The development of intelligent expert systems and neural networks are only the first steps towards creating a strong artificial intelligence. Within this, the requirements for modern video surveillance systems are changing.

The author gives an example of using the analytical module of video surveillance within the project "Safe City" (Kyiv Smart Safe City) in the capital, which allows you to search for offenders not only through specialized face recognition cameras. The module captures images from any camera installed in the network and compares it with the information database of offenders created by law enforcement agencies. If the system detects any similarity, the operator immediately receives an alarm. In addition, the offline mode allows you to search for people in the database by face photography. Cameras capture a person's face, this data remains in the archive. With the help of a photo of the intruder obtained from the cameras, the system analyzes the database and finds the right person. Thus, the innovation system accelerates the search for criminals and offenders.

In the conclusions, the author concludes that currently for the world scientific community the issue of introduction of artificial intelligence remains debatable and is accompanied by different approaches.

Keywords: artificial intelligence, video surveillance, machine learning, neural networks.

Отримано 12.05.2020