СЕКЦІЯ 4. ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА ТЕЛЕКОМУНІКАЦІЇ

УДК 004.4

Д.П. Федоренко, магістрант, гр. ІПЗм-21-2
Т.А. Вакалюк, доктор педагогічних наук, професор,
проф. каф. інженерії програмного забезпечення
О.Г. Чижмотря, старший викладач кафедри
інженерії програмного забезпечення
Державний університет «Житомирська політехніка»

ОГЛЯД МОВ ПРОГРАМУВАННЯ ДЛЯ СТВОРЕННЯ СЕРВЕРНОЇ ЧАСТИНИ ВЕБСАЙТУ

На сьогоднішній день все більше і більше користувачів використовують світову павутину під назвою Інтернет та не мають уявлення яким чином працюють ресурси які вони відвідують. Щорічно з'являються нові технології розробки вебсайтів, та методі і алгоритми програмування які тісно пов'язані з ними.

Backend – це все, що пов'язано з роботою на сервері. Реалізувати цю частину сервісу можна за допомогою безлічі мов. На сьогоднішній день основну нішу для серверної частини кожного вебсайт займають такі мови програмування як PHP, Javascript, Java та .NET(фреймворк на мові C#). Кожна з них має свої переваги і недоліки.

За допомогою PHP працює близько 78.2 % всіх вебсайтів. Мова вперше була представлена в 1995 році, коли для створення динамічних сайтів існувало не так багато можливостей. Оскільки це динамічно типізована мова, для однієї проблеми можна знайти відразу декілька рішень. Правда, це одночасно означає і те, що одна і та ж ділянка коду може вести себе по-різному в залежності від конкретної ситуації, що робить програми на PHP складно масштабованими і в деяких випадках повільними. Мова програмування PHP підходить як для новачків так і для користувачів які мають вже досвід у сфері програмування. Вона легка в освоєнні, що дозволяє вдосконалювати свої навички розробника, та створювати більш складні алгоритми для досягнення своїх цілей при розробці серверної частини будь-якого сайту.

.NET – це відповідь компанії Microsoft на мову Java. .NET являє собою фреймворк, який використовується для створення сайтів на таких мовах, як Visual Basic (VB), C#, F# та інші. В основі мови лежить – архітектурний шаблон MVC (Model-View-Controller). У цій схемі контролер приймає запити користувача і взаємодіє з моделлю для обробки даних. Потім результат вже передається в уявлення, відображаючись у вигляді інтерфейсу вебсторінки. .NET був викладений у відкритий доступ в 2016 році, і вже може інтегруватися з мобільною операційною системою iOS та Android через технологію .NET Core. Код дуже стабільний і надійний, що робить мову популярним корпоративним рішенням. Крім того, оскільки .NET – продукт компанії Microsoft, а це означає, що у нього хороша підтримка та велика база користувачів і документації які допоможуть у разі виникнення будь-яких проблем.

Java – строго типізована об'єктно-орієнтована мова програмування випущена в 1995 році. Вона не втрачає величезної популярності вже третій десяток років і залишається одним з найбільш вимогливих і універсальних інструментів для розробки будь-якого виду програмного забезпечення (від мобільних ігор до серверної частини для сайту).

Мова значно запозичила синтаксис із C і C++. Зокрема, взято за основу об'єктну модель C++, проте її модифіковано. Усунуто можливість появи деяких конфліктних ситуацій, що могли виникнути через помилки програміста та полегшено сам процес розробки об'єктно-орієнтованих програм. Ряд дій, які в C/C++ повинні здійснювати програмісти, доручено віртуальній машині. Передусім Java розроблялась як платформо-незалежна мова, тому вона має менше низькорівневих можливостей для роботи з апаратним забезпеченням, що в порівнянні, наприклад, з C++ зменшує швидкість роботи програм. За необхідності таких дій Java дозволяє викликати підпрограми, написані іншими мовами програмування.

Головна причина універсальності Java криється в віртуальній машині JVM. У більшості інших мов після компіляції отриманий код може проявляти себе по-різному на всіх платформах і типах пристроїв. Але в Java такої проблеми немає. Після обробки в JVM програма буде однаково коректно виконуватися на будь-якому пристрої, незалежно, де була здійснена компіляція коду. Мова програмування не підходить лише для новачків, але так як із-за свого довготривалого існування в сфері IT технологій має велику користувацьку базу та купу документації, що допоможуть у вирішенні будь-яких проблем з якими буде зустрічатися розробник при розробці свого програмного коду.

Javascript – це універсальна мова, яку застосовують і в фронтенді, і в бекенді. Її теж можна рекомендувати початківцям, тому що в ній лише декілька налаштувані і працювати можна безпосередньо в браузері. Можливості JavaScript сильно залежать від оточення, в якому він працює. Однак гнучкість коду іноді дорого обходиться цій мові, тому що вона виливається в такі наслідки, як: повільна робота скриптів, складна підтримка і масштабування (як, втім, у багатьох мовах з динамічною типізацією).

Отже, було проведено огляд деяких мов програмування, виявлено їх переваги та недоліки для використання їх у серверній розробці програмного забезпечення.

УДК 004

М.С. Колощук, студентка групи КБм-21-1
А.А. Єфіменко, к.т.н., доц., завідувач кафедри комп'ютерної інженерії та кібербезпеки
Т.А. Вакалюк, д.пед.н., проф., професор кафедри інженерії програмного забезпечення
Державний університет «Житомирська політехніка»

ВИДИ ІНСТРУМЕНТІВ ТА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ВИКОРИСТАННЯ СИСТЕМИ SIEM

Вибір відповідного інструменту SIEM залежить від низки факторів, включаючи бюджет та рівень безпеки. Проте слід шукати інструменти SIEM, які пропонують такі можливості [2]:

- звітність про відповідність;
- реагування на інциденти та експертиза;
- моніторинг доступу до бази даних і серверів;
- виявлення внутрішніх і зовнішніх загроз;
- моніторинг загроз у реальному часі, кореляція та аналіз у різних програмах і системах;
- система виявлення вторгнень (IDS), IPS, брандмауер, журнал подій додатків та інші програми та системні інтеграції;
- розвідка загроз;
- моніторинг активності користувачів (UAM).

На ринку є ряд програмного забезпечення щодо безпеки інформації та керування подіями. Одними з найпопулярніших є Arcsight ESM, IBM QRadar і Splunk. Нижче перерахуємо всі види програмного забезпечення, які використовують систему захисту SIEM.

ArcSight – збирає та аналізує дані журналів із корпоративних технологій безпеки, операційних систем і програм. Після виявлення зловмисної загрози система повідомляє про це співробітників служби безпеки. ArcSight також може запустити автоматичну реакцію, щоб зупинити шкідливу дію. Ще однією особливістю є можливість інтегрувати сторонні канали розвідки загроз для більш точного виявлення загроз [1].

IBM QRadar – збирає дані журналів із джерел в інформаційній системі підприємства, включаючи мережеві пристрої, операційні системи, програми та діяльність користувачів.

QRadar SIEM аналізує дані журналу в режимі реального часу, дозволяючи користувачам швидко ідентифікувати та зупинити атаки. QRadar також може збирати події журналу та дані мережевого потоку з хмарних програм. Цей SIEM також підтримує канали розвідки загроз. [1]

Splunk Enterprise Security забезпечує моніторинг загроз у режимі реального часу, швидкі розслідування з використанням візуальних кореляцій та слідчий аналіз для відстеження динамічних дій, пов'язаних із розширеними загрозами безпеки.

Splunk SIEM доступний як локально встановлене програмне забезпечення або як хмарна служба. Він підтримує інтеграцію каналів розвідки загроз із сторонніх програм [1].

Azure Sentinel – це система SIEM (Security Information and Event Management) та Security Orchestration and Automated Respons (SOAR) на загальнодоступній хмарній платформі Microsoft. Може забезпечити єдине рішення для виявлення попереджень, видимості загроз, активного пошуку та реагування на загрози. Збирає дані з різних джерел даних, виконує кореляцію даних і візуалізацію оброблених даних на одній інформаційній панелі. Azure Sentinel допомагає збирати, виявляти, досліджувати та реагувати на загрози та інциденти безпеці [1].

LogRhythm – хороша система SIEM для невеликих організацій, об'єднує SIEM, керування журналами, моніторинг мережі та кінцевих точок, криміналістичну експертизу та аналітику безпеки [3].

Exabeam пропонує кілька можливостей, включаючи UEBA, озеро даних, розширену аналітику та пошук загроз [3].

RSA NetWitness – це інструмент виявлення загроз та реагування, який включає збір, пересилання, зберігання та аналіз даних. RSA також пропонує SOAR [3].

Список використаної літератури:

1. What Is SIEM? Security Information And Event Management (SIEM). URL: https://networkwarehouse.co.uk/blogs/news/what-is-siem-security-information-and-event-management-siem.
2. Security information and event management (SIEM) URL: https://www.imperva.com/learn/application-security/siem/.
3. Security information and event management (SIEM) URL: https://www.techtarget.com/searchsecurity/definition/security-information-and-event-management-SIEM.

УДК 004

Д.С. Охріменко, магістрант 1 курсу спец. «Інформаційні системи та технології»
А.А. Ефіменко, к.т.н, доц., завідувач кафедри комп'ютерної інженерії та кібербезпеки
Т.А. Вакалюк, д.пед.н., проф., професор кафедри інженерії програмного забезпечення
Державний університет «Житомирська політехніка»

SIEM-СИСТЕМА QRADAR ДЛЯ ПРОВЕДЕННЯ АУДИТУ ПОДІЙ КІБЕРБЕЗПЕКИ НА ПІДПРИЄМСТВІ

На сьогоднішній день все більше компаній стикається з необхідністю обробки журналів подій, які реєструються в інформаційних системах, з метою виявлення можливих атак, тому інформаційна безпека – один з напрямків, що найбільш швидко розвиваються. Це пов'язано з кількістю загроз, кібератак та інших негативних факторів, що впливають на інфраструктуру підприємства. Оскільки інформація є одним з найголовніших активів підприємства, вона потребує побудови комплексної ефективної системи захисту мережі. Аудит інформаційної безпеки – головний інструмент для контролю рівня захисту інформаційних активів.

Створення комплексної системи захисту інформації (КСЗІ) на основі результатів аудиту інформаційної безпеки дозволяє мати постійний контроль над системою, відстежувати всі події, модифікації даних та вчасно реагувати на них. Щоб протидіяти кіберзлочинцям, фахівці інформаційної безпеки змушені аналізувати та інтерпретувати величезну кількість подій на день. На підприємствах перед фахівцями з кібербезпеки постає складне завдання – оптимізувати процес аналізу журналів та записів подій. Для цього існує велика кількість різноманітних SIEM-рішень від великої кількості розробників, що відрізняються функціоналом.

Компанія IBM для захисту від загроз мережевої безпеки пропонує рішення IBM QRadar Security Intelligence Platform, яке надає єдину архітектуру для інтегрування інформації про безпеку та управління подіями (SIEM) та журналами, визначення аномальних ситуацій, аналізу інцидентів, реагування на них, управління налаштуваннями та усунення вразливостей.

Єдина архітектура QRadar Security Intelligence Platform дозволяє аналізувати журнали, мережеві потоки, пакети, уразливості, а також дані про користувачів та ресурси. Використання Sense Analytics дає змогу проводити аналіз кореляції для виявлення найбільш серйозних загроз, атак та вразливостей у реальному часі. В результаті дане рішення дає можливість швидко реагувати на інциденти та мінімізувати їх наслідки.

Забезпечення прозорості в реальному часі дозволяє виявити неправильне використання додатків, внутрішнє шахрайство і невеликі загрози, які можна було б випустити з уваги серед мільйонів подій, що відбуваються щодня. Рішення дозволяє забезпечити збір журналів та подій з різних джерел, включаючи пристрої безпеки, операційні системи, програми, бази даних та системи керування доступом та ідентифікацією. Дані мережевих потоків надходять від комутаторів та маршрутизаторів, включаючи дані рівня 7 (рівень додатків).

Функціонал QRadar SIEM також забезпечує збір інформації про несанкціоновані дії користувачів (наприклад, доступ до недозволених ресурсів, розсилка спаму, перехід по фішингових посилань) і активності мережі на рівні додатків. Після встановлення операційної системи Qradar Community Edition, за допомогою інтерфейсу веб-браузера переходимо до Dashboard-панелі IBM QRadar SIEM де можна вивести всі необхідні звіти та графіки.

Компанія IBM включила в платформу QRadar кілька модулів: QRadar SIEM, Log Manager (управління журналами), Risk Manager (управління ризиками), Vulnerability Manager (управління вразливостями), колектори QFlow і VFlow і Incident Forensics. Основний модуль IBM QRadar – QRadar SIEM. Даний модуль представляє саму систему, яка збирає, аналізує та управляє подіями та потоками мереж із пристроїв, кінцевих токів, серверів, антивірусів, брандмауерів та різних системних запобігань проникненню. Основний елемент IBM QRadar SIEM – база даних, яка зберігає інформацію про події і потоках в мережі. Система оснащена технологією DPI (deep packet inspection), яка збирає події з брандмауерів і інших мережевих ресурсів і виконує глибокий аналіз мережевих пакетів. QRadar збирає та корелює події безпеки, що отримуються від різних зовнішніх пристроїв. IBM QRadar SIEM є однією з найефективніших аналітичних систем безпеки.

Отже, IBM QRadar допомагає організаціям покращити свою безпеку та захистити себе від потенційних загроз. IBM QRadar SIEM є однією з найефективніших аналітичних систем безпеки.

УДК 004.4

Д.П. Федоренко, магістрант, гр. ІПЗм-21-2
Т.А. Вакалюк, д.пед.н., проф., професор кафедри інженерії програмного забезпечення
О.В. Чижмотря, старший викладач кафедри інженерії програмного забезпечення
Державний університет «Житомирська політехніка»

ПІДХІД ДО УПРАВЛІННЯ ТРАНСПОРТНИМИ ПОТОКАМИ

На сьогоднішній день у багатьох країнах світу, зокрема в Україні, зростає попит на вирішення глобальних проблем, пов’язаних з транспортними комплексами. Це, насамперед, пов'язане з вимогами підвищення безпеки та ефективності перевезень. Збільшення потоку пасажирів і вантажів є передумовою підвищення завантаженості транспортних шляхів та скупчення транспорту зниження швидкості перевезень, виникнення "заторів" тощо. Все це зрештою негативно позначається на економічній та екологічній ситуаціях.

Можливо виділити декілька шляхів вирішення цих проблем. Наприклад, підвищення капітальних вкладень у будівництво інфраструктури: трас, магістралей, тунелів, портів, мостів та ін. Однак це потребує чималих фінансових витрат. Але можна підійти до вирішення «транспортних» питань з іншого боку. Це оптимізація та керування транспортними потоками завдяки застосуванню нових технологій, технологій інтелектуальної транспортної системи.

Інтелектуальні транспортні системи (ІТС) – це великий комплекс сервісних послуг, що надаються користувачам для зручності користування та досягнення максимальної пропускної спроможності дорожньої мережі [1]. Набір цих послуг може формуватися і розширюватися залежно від поставлених цілей. Величезні масштаби транспортної системи України і безліч ІТС-технологій призводять до того, що процес їх реалізації не може охопити всі підсистеми та елементи одночасно. Звідси випливають принципи поетапного розвитку та модульності створення ІТС.

У світовій практиці ІТС визнано як загальнотранспортну ідеологію у всі види транспортної діяльності для вирішення проблем економічного та соціального характеру – скорочення аварійності, підвищення ефективності громадського транспорту та вантажоперевезень. Розробка та розгортання ІТС – являє собою ефективний конкурентоспроможний та інноваційний стимул розвитку нового високотехнологічного сектору промисловості. Методи реалізації відрізняються у різних країнах, проте ключові компоненти однакові. Впровадження ІТС носить стратегічний характер, визначає загалом конкурентоспроможність кожної країни на світовому ринку та у зв'язку зі значною капіталомісткістю не реалізується без безпосередньої участі держави.

З точки зору технічних систем, в наш час помітно збільшилось обладнання із використанням GPS. Враховуючи велике поширення GPS на автотранспортних засобах, на комп'ютерній техніці та мобільному зв'язку, потрібно оцінювати можливості використання цієї технології для отримання детальної інформації щодо пасажирських перевезень і перевезень вантажів.

Ці тенденції набувають небувалого розвитку в транспортній логістиці. GPS відкрило для нас нову еру у використанні ІТС: з'явилася можливість отримувати інформацію про місцезнаходження стаціонарних та мобільних об'єктів у будь-якому місці та у будь-який час [2]. Найпростіше використання програмного забезпечення для відстеження транспортних засобів (GPS) – це запис розташування конкретрного автомобіля на карті. Це дозволяє бачити, який автомобіль рухається та в якому напрямку.

За допомогою технології GPS-стеження можливим є відстежувати швидкість автомобіля, маршрути, запуск та вимикання двигуна, переглядати маршрути тощо. Також можливим є перегляд руху автомобіля до пункту призначення, чи раніше пройдені маршрути та коли автомобіль стоїть на місці. Він також стане в нагоді при пошуку викраденого автомобіля. Такий контроль автопарку – ключовий елемент успіху у транспортно-логістичному бізнесі. Системи стеження за автомобілем зазвичай складаються з двох частин: GPS-трекера, який встановлюється в автомобілі або вантажівці, та програмного забезпечення для моніторингу. Доступ до сучасного програмного забезпечення GPS-відстеження транспортних засобів також можна отримати з планшетів та смартфонів, вони використовуються багатьма транспортними та логістичними компаніями для управління автопарком та забезпечення безпеки.

Таким чином ІТС дозволяє зменшити матеріальні витрати, ресурси, формування звітної документації та автоматизувати процеси, що допоможе оптимізувати прийом та відправку автомобіля в рейс.

Список використаної літератури:

1. Intelligent Transport Systems (ITS): an area to be strengthened in the Transport sector [Електронний ресурс]. – Режим доступу до ресурсу: http://www.unece.org/trans/theme_its.html.
2. Інновації – спутникові та геоінформаційні технології [Електронний ресурс]. – Режим доступу: https://www.vniias.ru/2011-10-04-11-18-31.
3. Системи GPS стеження для контролю та моніторингу транспорту [Електронний ресурс]. – Режим доступу: https://intelli.com.ua/ua/statti/systemy-gps-stezhennia-dlia-kontroliu-i-monitorynhu-transportu.html.

УДК 004

Б.Ю. Олексюк, студент групи КБм-21-1
А.А. Єфіменко, кандидат технічних наук, доцент,
завідувач кафедри комп'ютерної інженерії та кібербезпеки
Т.А. Вакалюк, доктор педагогічних наук, професор,
професор кафедри інженерії програмного забезпечення
Державний університет «Житомирська політехніка»

ВИДИ МЕТОДІВ МАШИННОГО НАВЧАННЯ

Алгоритми машинного навчання в основному поділяються на чотири категорії: навчання з наглядом, навчання без нагляду, напівнавчання та навчання з підкріпленням [1].

З наглядом: навчання під керівництвом зазвичай є завданням машинного навчання для вивчення функції, яка відображає вхідні дані на вихідні на основі зразків пар вхід-вихід. Він використовує позначені навчальні дані та набір навчальних прикладів, щоб зробити висновок про функцію.

Кероване навчання здійснюється, коли визначені певні цілі, які мають бути досягнуті з певного набору вхідних даних тобто підхід, орієнтований на завдання.

Найпоширенішими контрольованими завданнями є «класифікація», яка розділяє дані, і «регресія», яка відповідає даним. Наприклад, прогнозування мітки класу або настрою фрагмента тексту, як-от твіт або огляд продукту, тобто класифікація тексту, є прикладом навчання з наглядом [3].

Без нагляду: навчання без нагляду аналізує немарковані набори даних без необхідності втручання людини, тобто процес, керований даними. Це широко використовується для виділення генеративних ознак, визначення значущих тенденцій і структур, групування в результатах і дослідницьких цілей.

Найпоширенішими завданнями навчання без нагляду є кластеризація, оцінка щільності, вивчення ознак, зменшення розмірності, пошук правил асоціації, виявлення аномалій тощо.[4]

Напівконтрольоване навчання: Напівконтрольоване навчання можна визначити як гібридизацію вищезгаданих методів із наглядом і без нагляду, оскільки воно працює як з міченими, так і з немічеными даними. Таким чином, він знаходиться між навчанням «без нагляду» і навчанням «з наглядом». У реальному світі мічені дані можуть бути рідкісними в кількох контекстах, а немарковані дані є численними, де навчання з напівнаглядом корисно [4].

Кінцевою метою моделі навчання з напівнаглядом є забезпечення кращого результату для передбачення, ніж результат, отриманий з використанням лише мічених даних з моделі. Деякі області застосування, де використовується напівконтрольоване навчання, включають машинний переклад, виявлення шахрайства, маркування даних і класифікацію тексту.

Підкріплення: навчання з підкріпленням – це тип алгоритму машинного навчання, який дозволяє програмним агентам і машинам автоматично оцінювати оптимальну поведінку в певному контексті або середовищі, щоб підвищити її ефективність [5], тобто підхід, керований середовищем. Цей тип навчання заснований на винагороді або покаранні, і його кінцева мета полягає в тому, щоб використати знання, отримані від екологічних активістів, щоб вжити заходів для збільшення винагороди або мінімізації ризику [6].

Це потужний інструмент для навчання моделей штучного інтелекту, який може допомогти підвищити автоматизацію або оптимізувати операційну ефективність складних систем, таких як робототехніка, завдання автономного водіння, виробництво та логістика ланцюга поставок, однак не бажано використовувати його для вирішення основних або простих проблем.

Список використаної літератури:

1. Essien A, Petrounias I, Sampaio P, Sampaio S. Improving urban traffic speed prediction using data source fusion and deep learning. In: 2019 IEEE International Conference on Big Data and Smart Computing (BigComp). IEEE. 2019: 1–8.
2. Anzai Y. Pattern recognition and machine learning. Elsevier; 2012.
3. Han J, Pei J, Kamber M. Data mining: concepts and techniques. Amsterdam: Elsevier; 2011.
4. Khadse V, Mahalle PN, Biraris SV. An empirical comparison of supervised machine learning algorithms for internet of things data. In: 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), IEEE. 2018; 1–6.
5. Mahdavinejad MS, Rezvan M, Barekatain M, Adibi P, Barnaghi P, Sheth AP. Machine learning for internet of things data analysis: a survey. Digit Commun Netw. 2018; 4 (3):161–75.
6. Mohammed M, Khan MB, Bashier Mohammed BE. Machine learning: algorithms and applications. CRC Press; 2016.

УДК 004

V.Yu. Petrenko, Master of the 1 year study in "Software Engineering"
T.A. Vakaliuk, doctor ped. sciences, Prof.,
Professor of the Department of Software Engineering,
O.H. Chyzhmotria, Senior Lecturer of the
Department of Software Engineering
Zhytomyr Polytechnic State University

OVERVIEW OF IMAGE ANTI-ALIASING METHODS

Image anti-aliasing is relevant with the advent of the first monitors. Anti-aliasing is a technology to eliminate the "jagged" effect that occurs at the edges of simultaneously displayed sets of individual flat or three-dimensional images from each other. From a mathematical point of view, distortion occurs when converting a continuous "signal" into a discrete set of values. Rasterization of straight or curved lines causes spatial distortion – these geometric shapes actually consist of an infinite number of points between two points in space, and its reflection with a fixed number of pixels always approximates this line regardless of the number of pixels used. Because the pixelated version of a line is no longer a true line, moving or placing it next to other shapes creates many visual artifacts. This problem is especially relevant in VR technologies, where the resolution is lower than in modern monitors.

Super Sample Anti-Aliasing is the most widely used technology. In the process of rasterization, the image is increased by 2^N times, followed by sampling and mixing the result into fewer pixels [1]. For example, on a monitor with a resolution of 1920 x 1080 and anti-aliasing SSAA 4x, the video card must render images at a resolution of 3840x2160.

The obvious problem with SSAA is that anti-aliasing is performed for the entire image, while the artifacts are mostly on the edge of the primitives. To solve this problem, an algorithm was created – Multi Sample Anti-Aliasing. The algorithm is similar to SSAA, with the difference that it is performed only for the edges of the object [2].

Another popular anti-aliasing algorithm is fast approximate anti-aliasing (FXAA). The algorithm is performed at the post-processing stage. For the operation of the algorithm, data on the brightness of each pixel is transmitted. Then the contrast between adjacent pixels is calculated. If the difference between the contrast of the pixels is large, it means that this place is the edge of the primitive. Using the contrast difference is the direction of this edge. Once all the edges are fully defined, all pixel points along these edges rise: up or down in the case of a horizontal edge, or sideways for a vertical one. They increase by a negligible amount, so small that the new position is within the area of the original pixel. After such a slight smear, the pixels that define the edge will be changed, reducing the effect of distortion. [3] The main advantage is low computational complexity. Also, the algorithm smoothes all edges, not just the perimeters of shapes, so unlike SSAA and MSAA smoothes transparent textures.

With the development of artificial intelligence technologies and processors, Nvidia has developed an anti-aliasing algorithm based on artificial intelligence – DLSS (Deep learning super sampling). Nvidia has developed a neural network that receives low-resolution images at the input and higher-resolution images at the output [4]. First, rasterization of the low-resolution frame with SSAA smoothing is performed, after which the neural network returns the frame in high-resolution [4]. This technology is revolutionary because the image quality is almost the same as when using the SSAA algorithm, but requires much less computational effort. A significant disadvantage is that for this algorithm to work, the video card must have tensor cores - AI accelerators.

Given all the above, we can conclude that the non-universality of image smoothing methods. Each of these types has its own characteristics, advantages and disadvantages, the possibility and impossibility of using different data sets. It is necessary to analyze the target platform on which the smoothing will be performed, and the effort to implement the algorithm.

References:

1. 3dfx. 2021. Super-sampling Anti-Aliasing Analyzed [online] Available at: http://www.x86-secret.com/articles/divers/v5-6000/datasheets/FSAA.pdf
2. Habr. 2021. Как работает рендеринг 3D-игр: сглаживание с помощью SSAA, MSAA, FXAA, TAA и других методик. [online] Available at: https://habr.com/ru/post/558552/
3. Nvidia. 2021. App Note Template - FXAA_WhitePaper. [online] Available at: https://developer.download.nvidia.com/assets/gamedev/files/sdk/11/FXAA_WhitePaper.pdf
4. Nvidia. 2021. NVIDIA-Turing-Architecture-Whitepaper. [online] Available at: https://images.nvidia.com/aem-dam/en-zz/Solutions/design-visualization/technologies/turing-architecture/NVIDIA-Turing-Architecture-Whitepaper.pdf

УДК 004

I.O. Smutnykh, Master of 1 year study in "Software Engineering"
T.A. Vakaliuk, Dr. Ped. Sciences, Prof.,
Professor of the Department of Software Engineering,
O.V. Chyzhmotria, Senior Lecturer of the
Department of Software Engineering
Zhytomyr Polytechnic State University

OVERVIEW OF APPLIED MACHINE LEARNING METHODS

Nowadays, machine learning is probably the most relevant topic not only in the field of information technology, but also in sociology, marketing, medicine and business in general. No wonder machine learning is the most common form of artificial intelligence.

Machine learning, in contrast to traditional methods of data analysis, has one important feature. It is based on the hypothesis that all subsets of homogeneous data show the same relationships between attributes and the distribution of values of these attributes remains unchanged throughout the set of input data. This means that machine learning algorithms work effectively with both existing and new data.

In the most general case, there are two types of machine learning. This is deductive learning and precedent learning, or inductive learning. Deductive learning belongs to the field of expert systems. In turn, when we talk about machine learning, we primarily mean learning by precedent. But this training is divided into 3 different and independent types: controlled training, uncontrolled training and reinforced training [2].

Controlled learning, or learning with a teacher, is used when working with large data sets [2]. It's like learning about the world by babies. The input data already contain the correct answers, so the purpose of such training is not to give an answer, but to identify patterns and "understand" why this answer is correct. This is implemented as follows.

Consider an example of an algorithm that must determine from a photograph what is shown in a photograph: a cat or a dog. To do this, the system is first "taught" by providing input in the form of photos of cats and dogs with labels that answer the question: is it a cat or a dog. The machine independently determines the set of attributes by which it distinguishes cats from dogs. Because of the ability to independently define a set of attributes, the algorithm can be quickly changed to recognize tigers and lions.

Uncontrolled learning, or learning without a teacher, is much more complex. Its advantage is that the algorithm works with a data set that does not have shortcuts with the correct answer. The system itself reveals patterns, structure and classification [1]. Such algorithms are used in the media space: creating recommendations for the client based on his preferences for certain products or services.

Learning with reinforcement is something like controlled learning. The difference is that the correct answers are obtained by the system not together with the input data, but by experiment. That is, having received the input data, the machine interacts with the working environment and gets a certain result.

An example of the use of such algorithms is the training of navigation systems. Such systems, having received input data, interact in some way with the work environment and receive from it the result on the basis of which they "learn". However, there is still controversy about the effectiveness of such algorithms. Basically, they come down to the fact that modern algorithms with reinforced learning require almost as much time to solve the problem as the usual random search [3].

Given all the above, we can conclude that machine learning methods are non- universal. Each of these types has its own characteristics, advantages and disadvantages, the possibility and impossibility of using different data sets. Therefore, the choice of machine learning method must be approached extremely responsibly, having previously determined which criteria for its use are the most important in a particular case.

References:

1. Frontiers. 2021. Machine Learning and Artificial Intelligence: Two Fellow Travelers on the Quest for Intelligent Behavior in Machines [online] Available at: https://www.frontiersin.org/articles/10.3389/fdata.2018.00006/full
2. SberCloud. 2021. Машинное обучение: просто о сложном. [online] Available at: https://sbercloud.ru/ru/warp/machine-learning-about
3. Sorta Insightful. 2021. Deep Reinforcement Learning Doesn't Work Yet. [online] Available at: https://www.alexirpan.com/2018/02/14/rl-hard.html

УДК 004

V.Yu. Petrenko, Master of 1 year study in "Software Engineering",
T.A. Vakaliuk, Dr. Ped. Sciences, Prof., Professor of the Department of Software Engineering,
O.V. Chyzhmotria, Senior Lecturer of the Department of Software Engineering
Zhytomyr Polytechnic State University

ADVANTAGES OF MESSAGE-BASED MIDDLEWARE

In modern cloud architecture, programs are divided into small independent elements that are easier to design, deploy, and maintain. This raises the question of how best to organize the interaction of these independent modules.

Message-oriented middleware are solving this problem. It is a software or hardware infrastructure that supports sending and receiving messages between distributed systems. MOM allows you to distribute application modules on heterogeneous platforms and reduces the complexity of developing applications that cover multiple operating systems and network protocols. Middleware software creates a distributed communication layer that isolates the program developer from the details of different operating systems and network interfaces using the message queue [1]. This allows software components that have been developed independently and run on different platforms to interact with each other. Programs distributed on different nodes of the network use the program interface for communication. In addition, the administrative interface makes this new virtual system of interconnected applications reliable and secure [2].

Analogs of message-oriented middleware are remote procedure call (RPC) based middleware and object request broker (ORB) based middleware. Messages are stored in the queue until they are processed and deleted. Message queues can be used to separate complex processing, buffering, or organize batch processing, as well as to smooth peak loads. Message queues can greatly simplify program code with disconnected components, as well as increase their performance, reliability, and scalability.

Another advantage of messaging between clients is that by adding an administrative interface, you can control and tweak performance. In this way, client programs effectively get rid of all problems, except the problem of sending, receiving and processing messages. Solving issues such as compatibility, reliability, security, scalability, and performance depends on the code that implements the MOM system and the administrator. Many implementations of message-oriented middleware depend on the message queuing system. Some implementations allow you to provide routing logic at the very level of messaging, while others depend on client programs that provide routing information or combine both paradigms. Some implementations use broadcast or multicast paradigms.

In the middleware system, the message received at the destination does not have to be identical to the message sent first. The system can transform the message and route according to the requirements of the sender or recipient [3]. Combined with routing and broadcast / multicast capabilities, one program may send a message in its own native format, and two or more other programs may receive a copy of the message in its own format. Many modern MOM systems provide sophisticated message conversion (or display) tools that allow programmers to specify conversion rules.

The main disadvantage of many message-oriented middleware systems is that they require an additional component in the architecture, the messaging agent (message broker). As with any system, adding another component can reduce performance and reliability, and can make the system as a whole more complex and expensive to maintain. In addition, most communications between programs are synchronous, and the sender specifically wants to wait for a response to the message before continuing. Because message-based communication is inherently asynchronous, it may not be appropriate in such situations. However, most MOM systems have the means to group request and response as a single pseudo-synchronous transaction.

Historically, message queues have used their own closed protocols, limiting the ability of different operating systems or programming languages to interact in a heterogeneous set of environments. Over time, three standards have emerged that are used in open source message queue implementations: Advanced Message Queuing Protocol (AMQP), Text Messaging Protocol (STOMP), and MQTT (formerly MQ Telemetry Transport). The most widespread protocol is AMQP, which was standardized by ISO [4].

Taking into account all the above advantages and disadvantages, it can be argued that the software based on messages is much better than other analogues, but increases the complexity of the system. The functionality of this software depends on the message queue used and the message broker.

References:

1. Curry, Edward. (2005). Message-Oriented Middleware. URL: http://www.edwardcurry.org/publications/curry_MfC_MOM_04.pdf
2. Oracle. 2021. Message-Oriented Middleware (MOM). URL: https://docs.oracle.com/cd/E19340-01/820-6424/aeraq/index.html
3. Edward Curry. 2011. Extending Message-Oriented Middleware using Interception. URL: https://web.archive.org/web/20110726015301/http://www.edwardcurry.org/web_publications/curry_DEBS_04.pdf
4. ISO. 2021. ISO/IEC 19464:2014 Information technology – Advanced Message Queuing Protocol (AMQP) v1.0 specification. URL: https://www.iso.org/standard/64955.html

УДК 004.85

I.A. Zabrodskyi, Master of 1 year study in "Software Engineering"
O.V. Korotun, Candidate of Pedagogical Sciences,
associate professor of Computer Science
T.A. Vakaliuk, Doctor of Pedagogical Sciences, professor,
professor of the Department of Software Engineering
Zhytomyr Polytechnic State University

DEVELOPMENT OF SERVICE OF AUTOMATION OF TRANSPORT LOGISTICS BASED ON THE ANT COLONY OPTIMIZATION (ACO) ALGORITHM

The Logistics services in Ukraine are developing rapidly every year, and the COVID-19 pandemic and quarantine restrictions have only accelerated this process. In particular, food delivery is now booming, as demand and, consequently, supply has increased significantly. Couriers often have to travel to many places in different parts of the city during the working day, delivering goods to customers, and as the number of delivery points increases, the choice of the best route becomes less and less obvious. Congestion is also a significant problem in transfer logistics, which should be avoided if possible. The development of a suboptimal route will inevitably lead to an increase in delivery time and increase the cost of the service.

To save the resources of the logistics company, you can develop a special service to automate these processes. This program will include, in addition to the main thing - the development of optimal routes, as well as information about each order, tools for dispatchers, monitoring of movements and delivery according to plan, collecting statistics for analysis and decision making, and more. The following factors are taken into account when calculating delivery routes: – dimensions, load capacity, type of car; – the type of ordered goods, their weight, overall dimensions; – temporary restrictions on delivery of goods; – category of roads, the direction of traffic, marking, speed limit.

The criterion for the efficiency of the transportation process is the maximum load of transport units and the minimum length of routes.

The search for the optimal route can be done using the method of branches and boundaries, genetic and ant colony optimization (ACO) algorithms, or artificial neural networks – all of them belong to the highly efficient optimization methods. However, in this work, the ACO algorithm will be used because it adapts well to changes, which is extremely important in the field of transport logistics [1]. The algorithm is based on the behavior of an ant colony – marking successful roads with a large amount of pheromone. In a series of experiments on a colony of ants, which had the option of choosing between two routes of different lengths leading to a food source, biologists observed that ants tend to use the shortest route [2]. This behavior is explained as follows: the first ant moves mostly by accident, but finding a source of food, it returns to the nest, leaving a pheromone trail. These pheromones are tempting, the next ants will be more inclined to follow this route and, returning to the colony, will further strengthen it. Thus, if there are two routes to the same food source, more ants will travel a shorter route than a longer one. The short route will become more and more attractive and thus more attractive, and the long one will disappear over time as the pheromones evaporate. If evaporation did not occur at all, the routes chosen by the first ant could naturally become extremely attractive for the next ones. The ACO algorithm is a meta-algorithm, ie one that determines the general principles of operation of specific algorithms, such as Ant-Q, Ant Colony System, Max-min Ant System. Regardless of the modifications, any ACO algorithm consists of the following repetitive steps: - create ants; - we deny the probability of transition from one vertex to another; - update the pheromone.

In addition to the classical search for optimal routes, the ACO algorithm is used to develop graphics, Bayesian networks, solve problems of protein coagulation, and even in systems of automatic control of the ship's course [2]. The best-known companies using this algorithm are Eurobios and AntOptima, and they were among the first to use it commercially to develop numerous software products.

In the end, I would like to note that the development of this service is quite time-consuming, but at the same time interesting from a technical point of view and, most importantly, is in great demand in the market today.

References:

1. T. Stützle, M. López-Ibáñez, P. Pellegrini, M. Maur, M. de Oca, M. Birattari, Michael Maur, M. Dorigo, “Parameter Adaptation in Ant Colony Optimization” [online] Available at: https://www.researchgate.net/publication/228577382_Parameter_Adaptation_in_Ant_Colony_Optimization
2. Goss, S.; Aron, S.; Deneubourg, J.L.; Pasteels, J. M. (1989). Self-organized shortcuts in the Argentine ant. [online] Available at: https://www.researchgate.net/publication/215444190_Self-organized_shortcuts_in_the_Argentine_Ant_Naturwissenschaften_76_579-581
3. Ant Colony Optimization Algorithm Applied to Ship Steering Control. [online] Available at: https://www.sciencedirect.com/science/article/pii/S1877050914010527

УДК 004.85

I.A. Zabrodskyi, Master of 1 year study in "Software Engineering"
O.V. Korotun, Candidate of Pedagogical Sciences,
associate professor of Computer Science
T.A. Vakaliuk, Doctor of Pedagogical Sciences, professor,
professor of the Department of Software Engineering
Zhytomyr Polytechnic State University

DEVELOPMENT OF ALGORITHM OF OPTIMIZATION OF TRANSPORT LOGISTICS

The main tasks in the optimization of transport logistics are laying the optimal route, the so-called salesman's task, and the optimal loading of vehicles. The classic task of a salesman is to find a route with a minimum length that passes through these cities at least once. However, in practice, it is necessary to clarify this task. In real conditions, we face several restrictions imposed on the road graph: speed limits, congestion, restrictions on the size and weight of the vehicle. In addition, the company has more than one car and may have more than one warehouse, so there will be several starting points for sets of cars. It may also be necessary to visit the point accurately at a certain time, in addition, points may have priority. Thus, at the input of the algorithm, we have a road graph with irregular weight of ribs and restrictions on the weight and dimensions of vehicles, a fleet of cars with their characteristics, and a list of applications for the delivery of goods.

To find the optimal route, we use the ant algorithm, as it can be used for both static and dynamic optimization problems. The essence of the approach is to analyze and use the model of the behavior of ants looking for a way from the colony to food. Each ant has the following properties:

- *memory* - each vertex of the graph can be passed only once, so the ants have a list of passed vertices.
- *vision* - inversely proportional to the length of the rib, determines the "greed" of the ant's choice, the closer the top of the graph, the stronger the ant wants to get to it.
- *sense of smell* - the ability to feel the traces of the pheromone, which increases the desire to walk on the appropriate rib.

Modeling the behavior of ants is associated with the distribution of the pheromone on the edge of the graph in the task of the salesman. The probability of including a rib in the route of an individual ant is proportional to the amount of pheromone on this rib, and the amount of deposited pheromone is proportional to the length of the route. The shorter the route, the more pheromone will be deposited on its edges, so more ants will include them in the synthesis of their routes. Modeling such an approach, which uses only positive feedback, leads to premature convergence - most ants move along a locally optimal route. This can be avoided by simulating negative feedback in the form of pheromone evaporation. Moreover, if the pheromone evaporates quickly, it leads to memory loss of the colony and forgetting good solutions, on the other hand, increasing the evaporation time can lead to a stable local optimal solution.

To solve this problem you should use the following algorithm:

1. Set the initial pheromone level. The initial level of the pheromone is initialized with a small positive number so that at the initial stage the probabilities of transition to the next peak are not zero. The initial level of the pheromone is selected experimentally.

2. Choice of vehicle. The choice of vehicle is made at random from the relevant list.

3. Passing the route.

The starting point where the vehicle is placed in the warehouse or fleet. Next, the selected car passes the route by local rules of conduct when choosing a route.

4. Next, the next vehicle is selected until all delivery requests have been fulfilled or all vehicles have been used during the working day. Thus, flight routes and loading schemes are formed, estimated by the total length, flight time, vehicle load factor, and, most importantly, fuel consumption.

5. Remember the formed routes with the corresponding loading schemes and estimations. Then we repeat the process again and thus form a population of solutions.

6. After forming a population of solutions, we choose the best and carry out the procedure to update the pheromone.

In the future, it is planned to obtain experimental results of the specified algorithm on real data.

УДК 004.85

І.А. Забродський, магістр 1 курс, спец. «Інженерія програмного забезпечення»
О.В. Коротун, к.пед.н., доцент кафедри комп'ютерних наук
Т.А. Вакалюк, д.пед.н., проф., професор кафедри інженерії програмного забезпечення
Державний університет «Житомирська політехніка»

РОЗРОБКА СЕРВІСУ АВТОМАТИЗАЦІЇ ТРАНСПОРТНОЇ ЛОГІСТИКИ НА ОСНОВІ МУРАШИНОГО АЛГОРИТМУ

Сфера логістичних послуг в Україні з кожним роком стрімко розвивається, а пандемія COVID-19 та карантинні обмеження лише пришвидшили цей процес. Зокрема, сфера доставки продовольчих товарів зараз переживає розквіт, бо значно зріс попит і, відповідно, пропозиція. Нерідко кур'єру за робочий день потрібно проїхати безліч місць в різних частинах міста, доставляючи товари замовникам, і, зі зростанням кількості пунктів доставки, вибір найкращого маршруту стає все менш очевидним. Також суттєвою проблемою трансферної логістики є затори, котрі, за можливості, варто оминути. Розробка ж неоптимального маршруту неодмінно призведе до збільшення терміну доставки і зросту собівартості послуги.

Щоб зберегти ресурси логістичної компанії можна розробити спеціальний сервіс для автоматизації зазначених процесів. Дана програма вміщуватиме в себе, крім головного – розробки оптимальних маршрутів, також інформацію про кожне замовлення, інструментарій для роботи диспетчерів, моніторинг пересувань та ходу доставки згідно з планом, збір статистики для аналізу і прийняття рішень та інше.

Під час розрахунку маршрутів доставки враховуються наступні фактори: габарити, вантажопідйомність, тип автомобіля; тип замовлених товарів, їхня вага, габаритні розміри; тимчасові обмеження по доставці товару; категорія доріг, напрямок руху, розмітка, обмеження швидкості. Критерієм ефективності перевізного процесу є максимальне завантаження транспортних одиниць та мінімальна довжина маршрутів.

В даній роботі опишемо мурашиний алгоритм, оскільки він добре адаптується до змін, що є вкрай важливим в сфері транспортної логістики [1]. В основі алгоритму лежить поведінка мурашиної колонії – маркування вдалих доріг великою кількістю феромону.

У серії дослідів над колонією мурах, котрі мали можливість вибору між двома маршрутами різної довжини, які ведуть до джерела їжі, біологи спостерігали, що мурахи тяжіють до використання найкоротшого маршруту [2].

Мурашиний алгоритм є мета-алгоритмом, що визначає загальні принципи роботи конкретних алгоритмів, таких як Ant-Q, Ant Colony System, Max-min Ant System. Незалежно від модифікацій, будь-який мурашиний алгоритм складається з наступних повторюваних кроків: створюємо мурах, обраховуємо ймовірність переходу з однієї вершини в іншу, оновлюємо феромон.

Крім класичного пошуку оптимальних маршрутів, мурашиний алгоритм використовується в розробці графіки, байєсівських мереж, при вирішення проблем згортання білків і навіть в системах автоматичного керування курсом судна [2]. Найвідомішими компаніями, що використовують цей алгоритм, є Eurobios та AntOptima і саме ці компанії були одними з перших, хто почав його використовувати в комерційних цілях, розробивши численні програмні продукти.

У кінцевому підсумку хотілось би зазначити, що розробка даного сервісу є достатньо трудомісткою справою, але водночас й цікавою з технічної точки зору і, головне, має великий попит на ринку в умовах сьогодення.

Список використаної літератури:

1. T. Stützle, M. López-Ibáñez, P. Pellegrini, M. Maur, M. de Oca, M. Birattari, Michael Maur, M. Dorigo, "Parameter Adaptation in Ant Colony Optimization". [online] Available at: https://www.researchgate.net/publication/228577382_Parameter_Adaptation_in_Ant_ColonyOptimization
2. Goss, S.; Aron, S.; Deneubourg, J. L.; Pasteels, J. M. (1989). Self-organized shortcuts in the Argentine ant. [online] Available at: https://www.researchgate.net/publication/215444190_Self-organized_shortcuts in_the_Argentine Ant Naturwissenschaften_76_579-581
3. Ant Colony Optimization Algorithm Applied to Ship Steering Control. [online] Available at: https://www.sciencedirect.com/science/article/pii/S1877050914010527

УДК 004.85

І.Ю. Ліневич, магістрант 1 року навчання
спеціальності «Інженерія програмного забезпечення»
О.В. Коротун, к.пед.н., доцент кафедри комп'ютерних наук
Т.А. Вакалюк, д.пед.н., проф., професор кафедри інженерії програмного забезпечення
Державний університет «Житомирська політехніка»

ВИКОРИСТАННЯ ОБРОБКИ ПРИРОДНЬОЇ МОВИ ДЛЯ АНАЛІЗУ BIG DATA

Великі дані (Big Data) – це дані, які постійно збираються з різних інформаційних каналів, наприклад, інтернет покупки клієнтів, активність користувачів в соціальних мережах тощо. Ці дані постійно надходять у реальному часі, зберігаються в хмарних сховищах і їх обсяг на великих підприємствах може займати понад петабайт. Big Data буває декількох видів: структурована, неструктурована та слабоструктурована. Структуровані дані означають, що вони зберігаються та використовуються в певному форматі. В той час як неструктуровані дані тяжко категоризувати чи структурувати. Слабоструктуровані дані включають в себе два вищезазначених типи, які не можна категоризувати, але які мають певні властивості [1]. Оскільки дані беруться з джерел в оригінальному стані, без змін, то вони в основному є неструктурованими. Формат цих даних переважно представляє з себе текст, яким поширюються в соціальних мережах чи у відгуках клієнтів про продукти. Big Data отримується у вигляді природньої мови, набір слів, який звичайна людина використовує в розмовах у реальному житті. Для аналізу вмісту такого роду даних потрібно застосувати обробку природньої мови (Natural language processing, NLP). NLP – це галузь штучного інтелекту, яка займається взаємодією між комп'ютерами та людьми за допомогою природної мови. Кінцева мета NLP полягає в тому, щоб читати, розшифровувати, розуміти й визначати сенс людської мови в цінний спосіб [2]. NLP використовує ряд методологій для розшифровки неоднозначностей в мові, включаючи автоматичне підсумовування, тегування частин мови, виділення сутностей та вилучення зв'язків [3]. Щоб ідеально використовувати NLP для аналізу Big Data потрібно розуміти, які саме кроки виконуються в цьому процесі і як саме відбувається перехід від вхідних даних до кінцевого результату. Перш за все вхідними даними для обробки природної мови є простий потік символів Unicode, тож потрібна базова обробка для перетворення цього потоку у слова, фрази та синтаксичні маркери, які потім можна буде використовувати для кращого розуміння вмісту. Далі потрібно визначитися з ціллю аналізу. Дивлячись на великий блоку тексту, навіть людині може бути складно визначити, про що саме йде мова. Це те, що називається макро розумінням і мікро розумінням. NLP обмежена факторами обрахунків та часу, а певні рівні обробки просто недоступні через ці обмеження. Тож коли ви отримаємо уявлення про те, до якого масштабу ви прагнемо, ви можемо вирахувати потенційні затрати та перейти до вилучення інформації.

Макро розуміння допомагає визначити основу суть документа, який оброблюється. Ви можете використовувати це для класифікації, вилучення тем, підбиття підсумків, семантичного пошуку, виявлення дублікатів і вилучення ключових слів або фраз. Якщо ж говорити про мікро розуміння, можна використовувати обробку для більш глибокого розуміння тексту, вилучення імен людей, дат, акронімів та власних назв тощо. У мікро розуміння порядок слів надзвичайно важливий, тож він має бути збережений бід час обробки.

Після вилучення даних з конкретного документу, ви напевно захочете впевнитись, звідки саме йдуть ці дані. Наявність посилання на вихідний документ може заощадити багато часу у довгостроковій перспективі. Це може допомогти відстежити можливі помилки в тексті, і якщо один з вихідних документів буде оновлено до новішої версії, майбутні зміни можуть бути відображені в отриманій інформації з мінімумом затрат на повторну обробку, що заощадить час та обчислювальну потужність.

Наостанок, щоб покращити аналіз Big Data, потрібно приймати до уваги відгуки користувачів про те, як працює система NLP, щоб адаптувати її роботу до бажаних результатів.

У підсумку, самі по собі великі дані є складними і повторюваними, тому в них може бути заховано багато інформації. Тож розробляючи модель NLP для аналізу Big Data, ви водночас отримуєте шукані дані і в той же час навчаєте комп'ютер мислити як людина, що однозначно покращує його майбутні результати.

Список використаної літератури:

1. Все, что нужно знать о разных типах данных (2021), Devrepublik, [Online], Available at: https://www.devrepublik.com/ru/all-you-need-to-know-about-different-types-of-data/#structured.
2. Medium (2021), A Simple Introduction to Natural Language Processing, [Online], Available at: https://becominghuman.ai/a-simple-introduction-to-natural-language-processing-ea66a1747b32.
3. Expert.ai (20210, NLP for Big Data: What everyone should know?, [Online], Available at: https://www.expert.ai/blog/nlp-big-data-everyone-know/.

УДК 004.422

О.В. Ванільчук, магістр
Д.К. Марчук, асистент кафедри КН
Державний університет «Житомирська політехніка»

ВИКОРИСТАННЯ СТРУКТУРИ ДАНИХ ДЕРЕВО

Дерево – це структура даних, яка доволі часто використовується під час створення програмного забезпечення. Дерева мають широке застосування: у трансляторах, при роботі з арифметичними висловлюваннями, під час створення та ведення таблиць символів, у багатьох пошукових програмах, у багатьох мовних бібліотеках, дерево кодування Хаффмана використовується в алгоритмах стиснення, у криптографічних додатках. Дерева найкраще пристосовані для вирішення завдань штучного інтелекту та синтаксичного аналізу.

Дерево може описувати сценарії виконання у системі (рис.1). Щоб програмне забезпечення чітко розуміло що можна виконати, варто зберігати поточний стан задля розуміння наступних дозволених дій.

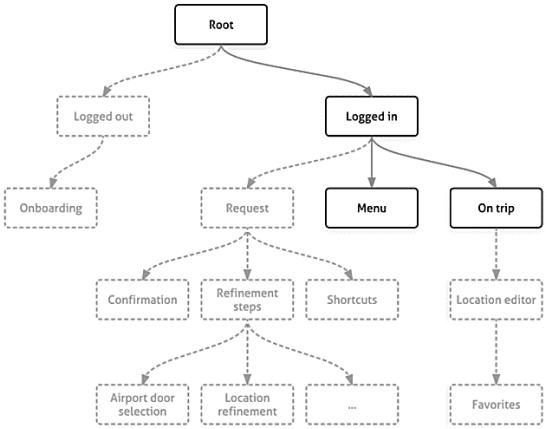

Рис. 1. Дерево сценаріїв

Дерева поведінки використовуються студіями, що розробляють ігрове програмне забезпечення для створення реалістичного ігрового інтелекту. Behavior Tree (BT) – це деревоподібна структура, що складається з вузлів поведінки. Вузол у дереві поведінки буде викликатись у певному кадрі, після чого має бути негайно отримано один із наступних результатів: успіх, збій, виконання. Потім відбувається перехід до наступного кроку відповідно до значення, що повертається.

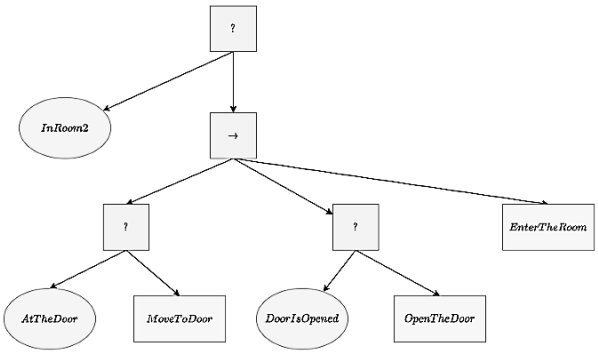

Рис. 2. Behavior Tree

BT буде йти зверху вниз, шукати в дереві відповідно до правил вузол поведінки, який необхідно виконати. Вузлу не потрібно підтримувати перетворення у інші вузли, тому він має кращу інкапсуляцію та модульність, що робить логіку гри більш інтуїтивно зрозумілою.

Дерева поведінки використовуються у комп'ютерних іграх як потужний інструмент моделювання поведінки неігрових персонажів (як приклад роботи BT можно розглядати ігри Halo, Bioshock). Unity має безліч плагінів для побудови дерев поведінки, таких як Rain AI, Behavior Designer, Bolt тощо.

Список використаної літератури:

1. Zhu Xianwen. Behavior tree design of intelligent behavior of non-player character (NPC) based on Unity3D. Journal of Intelligent & Fuzzy Systems, vol. 37, no. 5, pp. 6071-6079, 2019/ DOI: 10.3233/JIFS-179190

УДК 621.317

В.В. Чухов, к.т.н., доц.
І.Є. Ожегов, студент гр. ТР-14
Державний університет «Житомирська політехніка»

РОЗРОБКА ПЛАТИ КЕРУВАННЯ ФРЕЗЕРУВАЛЬНОГО ВЕРСТАТА НА БАЗІ КОНТРОЛЕРА ESP32

Розвиток мікроелектроніки все більше викликає потребу у аматорів виготовляти власні друковані плати, корпуси для електронних приладі та унікальні деталі. Вирішити ці проблеми допоможе фрезерувальний верстат з числовим програмним керуванням (ЧПК). Верстат може проводити фрезерування площин і пазів, свердління, зенкерування, розгортання та попереднє розточування отворів.

Обробка з ЧПК дозволяє використовувати комп'ютеризовані засоби керування для видалення шарів матеріалу з заготовки, та виготовляти деталі. Цей процес підходить для широкого спектру матеріалів, включаючи метали, пластмаси, дерево, скло, пінопласт і композити.

У межах данної роботи буде розроблено плату керування фрезерувального верстата з ЧПК на базі контролера ESP32. Розглянуто конструктивні особливості друкованих плат, основні способи виготовлення друкованих плат. Правила розміщення поверхневого монтажу електронних компонентів на друкованих платах. Огляд та порівняння характеристик різних драйверів крокових двигунів. Дослідження програмного забезпечення EasyEDA. Створення принципової схеми та проектування друковоної плати в EasyEDA.

EasyEDA дозволяє створювати та редагувати принципові схеми, SPICE моделювання змішаних аналогових і цифрових схем, а також створення та редагування макетів друкованих плат і, за бажанням, виготовлення друкованих плат.

ESP32 – це недорогий мікроконтролер з низьким рівнем споживання енергії з інтегрованим Wi-Fi і Bluetooth. Це наступник ESP8266, який також є недорогим мікрочіпом Wi-Fi, хоча і з обмеженою функціональністю.

Існує багато типів модулів ESP32. Плата, яку буде розроблено у даній роботі, призначена для роботи з модулем від розробника LuaNode32 побудований на мікромодулі ESP-WROOM-32, який виконаний на базі популярного двоядерного чіпсету ESP32. Використовуватися буде мікропрограмне забезпечення з відкритим кодом FluidNC.

FluidNC – це мікропрограмне забезпечення ЧПК, оптимізоване для використання з потужним і гнучким контролером ESP32. Це наступне покоління прошивки від творців Grbl_ESP32. Вона має багато покращень у порівняні з Grbl_ESP32.

FluidNC підтримує декілька шпинделей на одній машині. Шпинделями можна керувати за допомогою різних апаратних інтерфейсів, таких як реле, ШІМ, ЦАП. Також є можливість використовувати лазер як шпиндель. Змінювати різні шпинделі командою G-Code «M6 Tn», де n- номер інструмента. Це дозволяє перемикати на одному верстаті шпиндель і лазер між собою. Містить вбудований веб-інтерфейс на основі браузера (Esp32 WebUI), щоб керувати верстатом з комп'ютера, телефону або планшета в одній мережі Wi-Fi (рис. 1).

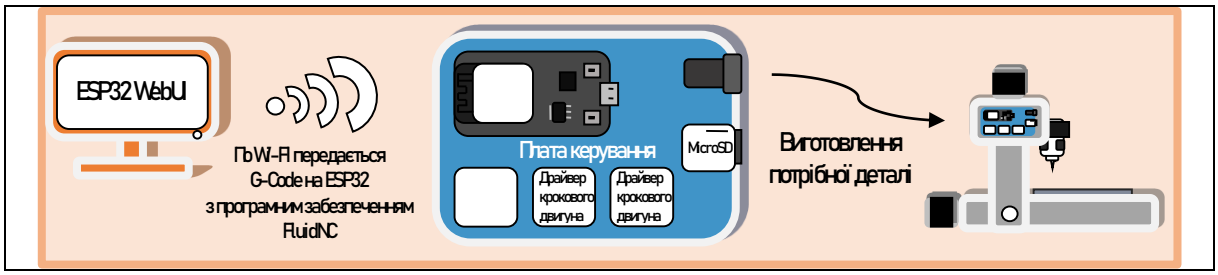

Рис.1. Алгоритм роботи фрезерувального верстата на базі контролера ESP32

Функції та характеристики плати керування:

- Напруга живлення: 12 - 24 В;
- Контролер: ESP32;
- Можливість під'єднати до трьох драйверів крокового двигуна та перемикати мікрокрок;
- Керування трьома осями, кожна вісь може мати по одному кроковому двигуну;
- Підтримка MicroSD;
- Керування верстатом з комп'ютера, телефону або планшета в одній мережі Wi-Fi;
- Кількість входів для кінцевих вимикачів: 6; Можливість змінювати швидкість обертання шпинделя.

УДК 004.4

О.В. Ванільчук, магістр
Г.В. Марчук, ст. викладач
Державний університет «Житомирська політехніка»

ПОРІВНЯННЯ ІНСТРУМЕНТІВ КОНТЕЙНЕРІЗАЦІЇ: DOCKER SWARM ТА KUBERNETES

Протягом багатьох років розробники публікують свої додатки в хмарні середовища. Ще деякий час тому фахівці з хмарних рішень страждали з розгортання додатків на серверах через складність конфігурувань та нюансів машин на яких розгортаються розроблені додатки. Велика кількість розробників почали проектувати платформу для контейнеризації, як для загального так і для безкоштовного користування. Бачення щодо певного механізму контейнеризації було різне, тому були сформовані спільноти розробників, які дійшли згоди, головної ідеї та принципів розробки програмного забезпечення для певного механізму контейнеризації.

Головною ідеєю контейнерів було розробити платформу для запуску додатків в ізоморфному середовищі задля гарантування запуску на будь-якій іншій машині. Програмне забезпечення для запуску додатків у контейнерах зробила великий крок у розгортанні проектів, тому наступним кроком розвитку було вирішено розробити інструмент для кластеризації контейнерів. Найпопулярнішою open-source платформою для контейнеризації на даний час є Docker. Kubernates [1] та Docker Swarm [2] є двома рішеннями для розгортання та розробки проєктів у контейнерах. В основі Kubernates лежать наступні сутності:

- Nodes;
- Pods;
- Replication controllers;
- Services;
- Volumes;
- Labels;
- Kubectl Command Line Interface.

Запущений кластер Kubernetes включає агента, що працює на вузлах (kubelet) і головних компонентах (API, scheduler тощо) поверх рішення розподіленого зберігання.

В основі Docker Swarm лежать наступні сутності:

- Node;
- Service;
- Manager;
- Task.

Після ініціалізації Swarm на ньому можна запустити будь-яку кількість служб. Стан такого кластера буде суперечливим (узгоджений стан досягається, коли кількість менеджерів не менше 3). І, звісно, ні про яке масштабування та відмовостійкість у цьому випадку не може бути й мови. Для цього до кластера потрібно підключити ще як мінімум два вузли керування.

Порівнюючи два програмних забезпечення, можна зрозуміти що вони мають спільні концепції, але різні у використанні. Docker Swarm являється легким застосунком для кластеризації, має мінімальний, але зручний для використання функціонал.

Kubernetes є більш складною технологією, але має широкий спектр наданих можливостей. Функції які надає Kubernetes одразу після інсталяції – self-healing та auto-scaling. Self-healing – це можливість відслідковувати стан роботи контейнера та перезапускати його у разі виникнення помилки або іншої причини зупинення додатку. Auto-scaling – автоматичний запуск додатку у разі великого навантаження на вже запущені контейнери.

Отже, можна зрозуміти, що кожна технологія має свої переваги та недоліки. Для маленьких проектів буде достатньо Docker Swarm, а для великих та сильно-навантажених проектів необхідно використовувати Kubernates.

Список використаної літератури:

1. Офіційна документація Kubernetes [Електронний ресурс]. – Режим доступу : https://kubernetes.io/uk/docs/home/.
2. Офіційна документація Docker Swarm [Електронний ресурс]. – Режим доступу : https://docs.docker.com/engine/swarm/.

УДК 61:621+004.78.056

О.Р. Борисевич, студент гр. БІ-21, IV курс
Р.О. Коломієць, к.т.н., доц. каф. БІтаТ
Державний університет «Житомирська політехніка»

ПРИСТРІЙ КОНТРОЛЮ ТА ПЕРЕДАЧІ ТЕЛЕМЕДИЧНИХ ДАНИХ

Розвиток телемедицини в Україні дозволить суттєво покращити якість медичного обслуговування. Буде вирішено проблему підвищення кваліфікації медперсоналу та надання медичної допомоги мешканцям віддалених районів.

Серед первинних завдань телемедичних технологій у вітчизняній охороні здоров'я можна виділити три базові: підвищення рівня медичного обслуговування за рахунок залучення ширшого кола лікарів до обговорюваної проблеми, у тому числі фахівців великих медичних центрів, унікальних фахівців; забезпечення якісною медичною допомогою мешканців віддалених регіонів; підвищення кваліфікації та навчання медичного персоналу.

Важливість телемедицини полягає насамперед у можливості використання технологій для регулярного одноразового обміну актуальною інформацією в системі. Саме тому створення пристрою контролю та передачі телемедичних даних і становить зараз одне з найбільш пріоритетних завдань у рамках реформи охорони здоров'я.

Розроблений пристрій призначений для передачі різноманітних медичних даних, які представляються у форматі DICOM. Цей стандарт регламентує уніфіковану модель представлення даних пацієнта, медичного обладнання, на якому проводилися дослідження, а також самі результати медичних досліджень. По отриманим даним кваліфікований лікар ставить діагноз.

Пристрій складається з модуля електроживлення, основного модуля, сенсорного дисплея для відображення отриманих даних, а також GSM-модуля SIM800C для передачі інформації бездротовим способом через інтернет-мережу.

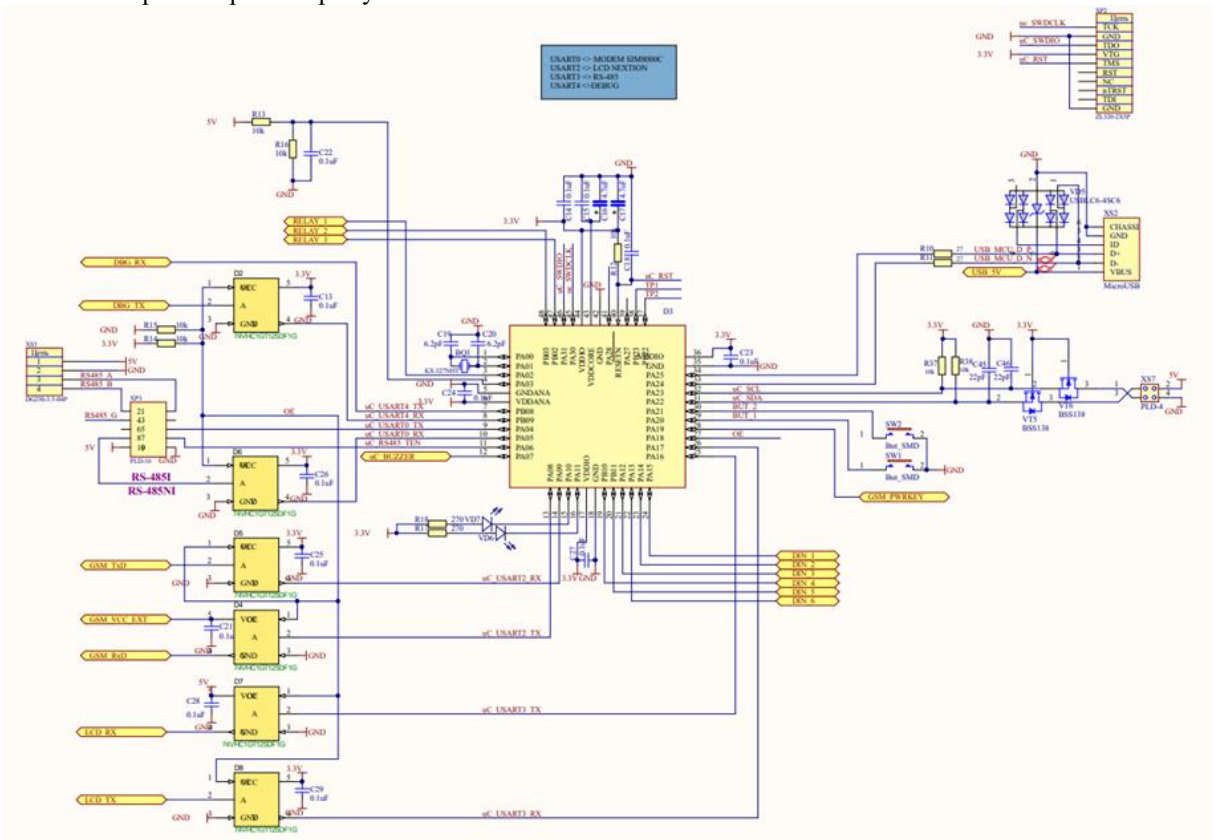

Рис. 1. Електрична принципова схема основної частини пристрою для контролю та передачі телемедичних даних.

В ході розгляду різних патентних рішень було обрано за ядро основної частини високопродуктивний флеш-мікроконтролер ARM® Cortex®-M0+ від Microchip з низьким енергоспоживанням, ATSAMD21G18

який ідеально підходить для широкого спектру автоматизації, споживчих, вимірювальних і промислових застосувань. Схема основної частини представлена на рис. 1.

В зв'язку з потребою моніторингу телемедичної інформації було обрано сенсорний дисплей який би одночасно виконував функцію контролю. Було обрано панель Nextion Discovery Series NX4832T035 – через відносну дешевизну і легкість конфігурації та написання програми. Обмін даними з панеллю ведеться всього по двом лініям UART. Саме налаштування та прошивка панелі ведеться через програму виробника Nextion editor.

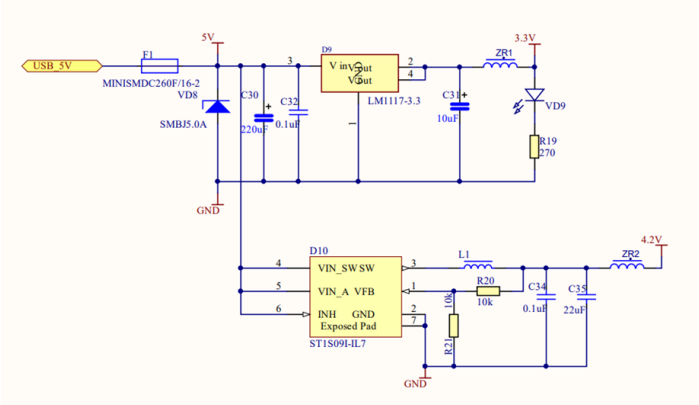

Рис. 2. Стабілізатор електроживлення для пристрою контролю та передачі телемедичних даних

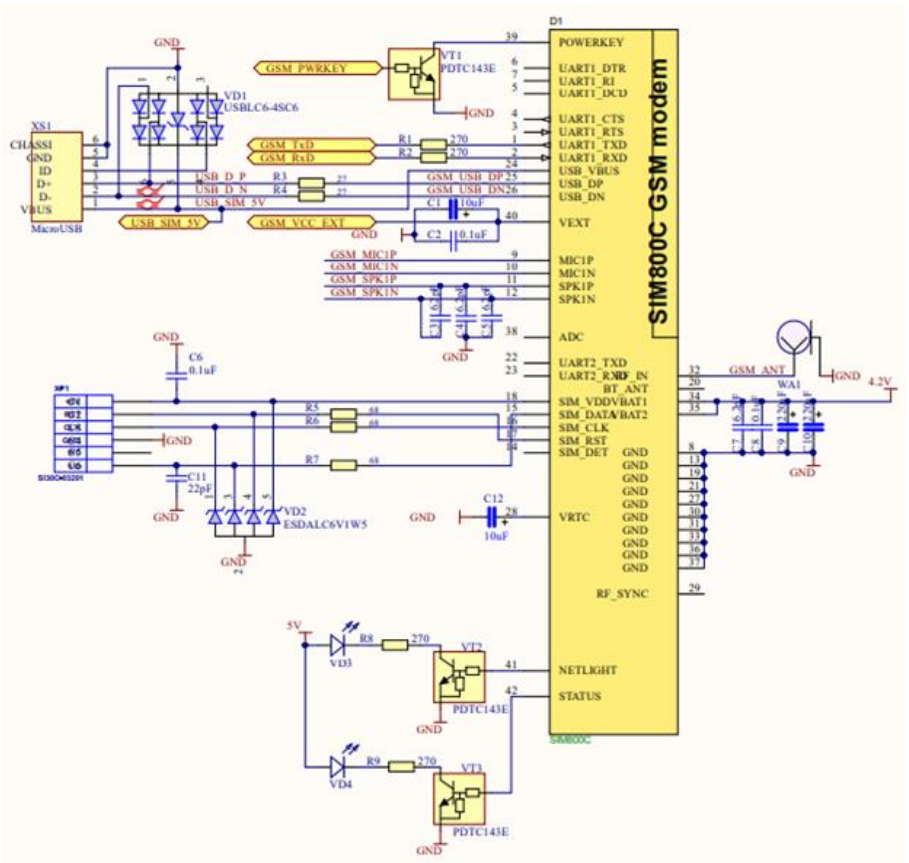

Рис. 3. Схема підключення модуля SIM800C

Для полегшення написання початкових драйверів було обрано середовище конфігурування ATMELSTART. Це новий, інтуїтивно зрозумілий графічний інтерфейс для розробки та конфігурації додатків, що вбудовуються, що дозволяє розробникам створювати унікальні програмні рішення. Побудована на основі новітньої версії Microsoft Visual Studio Shell, середовище Atmel Studio 7 та ATMELSTART значно скорочує загальний час проектування, дозволяючи істотно збільшити ефективність розробки та налагодження, за рахунок простого у використанні інтерфейсу користувача, і більш оперативно реагувати на сучасні вимоги ринку споживчої та промислової електроніки.

УДК 621.317

В.В. Чухов, к.т.н., доц.
О.Ю. Павицький, студент гр. ТР-14
Державний університет «Житомирська політехніка»

РОЗРОБКА ОПТИКО-ЕЛЕКТРОННОГО ПЕРЕТВОРЮВАЧА ЧАСТОТИ ОБЕРТАННЯ ВАЛУ

У сучасному світі безліч речей щоденного вжитку виробляються на підприємствах у промислових масштабах. В свою чергу на будь-якому виробництві дуже важливо контролювати кожен етап виготовлення того чи іншого продукту. Навіть контроль кількості обертів двигуна за одиницю часу відіграє дуже важливу роль. Саме для визначення швидкості обертання двигуна використовують вимірювач частоти обертання, тахометр.

Тахометр може швидко і точно виміряти, наприклад, витрати сировини, час напрацювання обладнання, час обкатки механізмів чи випробування машин. Датчик може вимірювати і рахувати імпульси не тільки у прямому, а й у зворотному напрямку. Можна попередньо запрограмувати, аби інформація про кількість обертів виводилась в реальних одиницях вимірювання. Тахометр відразу рахуватиме в метрах і сантиметрах, хвилинах і годинах, пакетах і коробках (якщо це необхідно).

Існує декілька основних типів тахометрів: механічні, аналогові та цифрові.

Механічні тахометри – складаються з тросика, який під'єднано до валу, що безпосередньо обертається, та перехідних частин, по типу шестерень. Такими тахометрами вимірюють кутову та лінійну швидкості. Їхньою перевагою є висока точність вимірювань, можливість вимірювання як кутової, так і лінійної швидкостей, а основним недоліком – необхідність безпосереднього контакту датчика тахометра з елементом, що обертається.

Аналогові тахометри – пристрій зазвичай складається з магнітної котушки, датчика та шкали зі стрілкою. Є, по суті, безконтактними вимірювачами частоти обертання.

Цифрові тахометри – складаються з оптичного перетворювача, АЦП, мікроконтролера, допоміжних каскадів. В основу їхньої роботи покладено принцип підрахунку кількості імпульсів від мітки, що обертається, за одиницю часу, тобто вимірювання частоти. Таким чином, маємо безконтактне вимірювання частоти обертання. До переваг безконтактних тахометрів потрібно віднести: власне безконтактне вимірювання (наприклад, мінімізація впливу вібрацій на сам тахометр), великий діапазон вимірюваних значень частоти обертання (до 100 тисяч оберт./хв., що недосяжно для контактних тахометрів), доволі велика відстань до мітки, якщо для зчитування імпульсів з неї використовувати лазерний промінь (типове мінімальне значення цієї відстані 50 мм, а її максимальне значення – до 500...800 мм). Проте вони мають дещо меншу точність порівняно з контактним способом.

В якості оптичного перетворювача тахометрів також можна використовувати оптопару.

У пропоновані розробці в якості первинного перетворювача і планується використати оптопару. У свою чергу оптопари мають доволі широку класифікацію. Якщо взяти до уваги класифікацію за типом, то оптопари бувають відбивні та щілинні. Планується використання відбивної оптопари, що дозволить спростити вузол-формувач мітки – циліндр з двоколірними мітками, а не шестерня.

Пристрій працюватиме таким чином: інфрчервоний сенсор (оптопара) посилає генерує випромінювання на обертовий механізм (вал, ротор двигуна), на якому повинна бути невелика наклейка з відбивним покриттям (для прикладу з фольги). Завдяки цій наклейці, кожен оберт валу викликає появу відбитого імпульсу ІЧ випромінювання.

Таким чином, використовуючи оптопару, можна вирахувати час повного оберту валу, а далі, знаючи час (по Т у секундах), можна обчислити кількість обертів на хвилину, використовуючи простий вираз 60/Т.

Для зниження вартості пристрою та складності виготовлення, а також для підвищення гнучкості системи, найефективніше буде підключати ІЧ сенсор до мікроконтролера ESP-32, та реалізовувати всю обробку одержуваного сигналу програмно. Відразу варто помітити, що це не так просто, так як сигнал, що отримується з ІЧ фотодіода містить шуми, а зовнішнє освітлення постійно впливає на нього.

Також, на базі пристрою буде реалізовано IoT (Internet of Things) систему. Дані з ІЧ сенсору будуть передаватися на ESP-32, який в свою чергу буде передавати дані до системи Blynk. Призначення та мета створення пристрою: прилад призначений для вимірювання частоти обертання різних типів двигунів, з використанням системи «призма – відбивна оптопара». Планований діапазон вимірюваних частот – від нуля до 4000 об/хв.

З додаткових сервісних функцій приладу – віддалене отримання вимірювальних даних і керування ним за допомогою хмарного сервісу.

УДК 621.3:004.891

О.Ф. Дубина, к.т.н., доц. кафедри БІ та Т,
Д.О. Тальченко, студент гр. КБ-2,
Державний університет «Житомирська політехніка»

ПРОЄКТ ІНТЕГРОВАНОЇ СИСТЕМИ ОХОРОНИ НА БАЗІ ОБЛАДНАННЯ CISCO

Різноманітність технічних засобів охорони на сучасному ринку та різноманіття рішень щодо їх застосування підштовхує сучасність до уніфікації. Вимоги до рівнів забезпечення безпеки та способів їхньої реалізації звичайно є різними.

Проблема фізичного захисту об'єктів, як не дивно, справді посідає чільне місце у нашому житті. Реалізація фізичної захисту дозволить уникнути різноманітних несанкціонованих проникнень на контрольований об'єкт, крадіжок важливих матеріалів та взагалі дозволить забезпечити надійний захист такого об'єкта.

Розв'язання цього завдання можливе лише за умови професійного оснащення об'єкта охорони сучасними високонадійними технічними засобами охоронної сигналізації. Звичайно, недостатньо знати, що техніка та система в цілому буде працювати задовільно. Необхідна ще й впевненість у тому, що її нелегко буде вивести з ладу.

Крім того, варто враховувати залежність надійності системи безпеки від її вартості. Виробники зазначають, що технічні засоби безпеки мають використовуватися спільно, оскільки саме такий підхід дає максимальний ефект. Виходячи з цього, доцільним рішенням при побудові комплексної системи безпеки є створення інтегрованої охоронної системи.

У сучасному світі захист людини, майна, інформації займає одне з перших місць серед потреб людини і суспільства в цілому. Поява та створення нових загроз, розвиток вже існуючих, змушують людей впроваджувати та розробляти нові охоронні системи.

Різні технічні засоби охорони дають можливість забезпечити цілісність, доступність та конфіденційність інформації, послабити чи усунути вплив загроз на людину та її майно у будь-яких сферах життєдіяльності.

Нині заснування будь-якої організаційної фірми не обходиться без заходів спрямованих на впровадження, розвиток та підтримання систем безпеки у своїх організаціях. Інтегрована охоронна система є комплексною багатофункціональною системою безпеки, що поєднує у собі функції всіх традиційних автономних систем. Система передбачає об'єднання на базі сучасних інформаційних технологій та програмно-апаратної інтеграції декількох підсистем, функціонально та інформаційно пов'язаних один з одним, а також їх роботу по єдиному алгоритму.

Можливі два шляхи вирішення проблеми інтеграції компонентів охоронної системи: апаратний та програмний. Апаратна інтеграція часто утруднена у зв'язку з використанням виробниками різноманітних інтерфейсів та стандартів, що обмежує гнучкість систем з апаратною інтеграцією. Програмний метод інтеграції позбавлений цієї особливості. Інтеграція на рівні драйверів тим зручніша, що на сьогоднішній день більшість виробників технічних засобів охорони забезпечують свої продукти програмними модулями, що дозволяють організовувати взаємодію з комп'ютерами.

В даний час найбільш перспективним середовищем інтегрування технічних засобів охорони є локальна мережа об'єкта, що охороняється. Основними перевагами використання цієї технології, як бази для інтеграції технічних засобів є її повсюдна поширеність та наявність різноманітних засобів забезпечення інформаційної безпеки.

У доповіді розглядається актуальне питання побудови інтегрованої системи охорони на базі локальної мережі із застосуванням обладнання Cisco.

Cisco - найбільший в світі виробник мережного устаткування, призначеного для обслуговування мереж віддаленого доступу, сервісів безпеки, мереж зберігання даних,3 маршрутизації і комутації, а також для потреб комерційного ринку IP-комунікацій і корпоративного ринку.

Cisco є централізованим інструментом управління доступом до мережі і платформою застосування політик. Він надає централізоване управління політиками для управління доступом до мережі і політиками використання з одного розташування.

Локальна мережа збирає ключову інформацію про доступ користувача та пристрої і використовує цю інформацію для управління доступом до мережі кінцевого користувача і доступом пристрою адміністративної мережі, незалежно від типу з'єднання.

Обладнання Cisco відповідає всім вимогам безпеки, і тому його закладено в основу національної системи конфіденційного зв’язку, яка об’єднує всі міністерства та відомства України в єдину захищену мережу. Технології Cisco широко застосовуються у різних державних установах та муніципальних службах, у закладах освіти та охорони здоров’я.

Актуальність підтверджується гострою необхідністю захисту від впливу загроз на різні сфери життя та діяльності людини. Як відомо, сучасні системи охорони включають в себе системи відеоспостереження, охоронну та пожежну сигналізацію, системи контролю та управління доступом. Усі вони можуть працювати як незалежні засоби, так і разом.

Особливістю сучасних охоронних елементів, таких як IP-відеокамери, пристрої приймально-контрольні або панелі, контролери системи СКУД є те, що вони являються мережевими пристроями і передають отриману інформацію до споживачів, у кінцевому рахунку, по локальних чи глобальних мережах.

Під час охорони важливих об'єктів, де циркулює конфіденційна інформація або інформація з обмеженим доступом, виникає питання організації і реалізації політики безпеки на засобах системи охорони.

Говорячи про системи охоронного відеоспостереження, слід зазначити про їх захист: що потрібно захищати у відеоспостереженні і від чого.

Досвід показує, що найцінніше у відеоспостереженні це:

- відеоархіви і бази даних;
- канали зв'язку, що використовуються в системі відеоспостереження;
- пристрої: камери, комутатори, сервери, і інші розумні пристрої.

Якщо говорити про канали зв’язку, то тут мова йде саме про лінії зв'язку:

- з IP-камерами;
- між сервером і АРМ;
- між серверами (в розподіленій системі);
- між сервером і мережевим сховищем;
- між сервером і інтегрованою системою СКУД.

Також варто звернути увагу на шкідливе ПЗ. Всім відомі «віруси», «троянці», «шифрувальники» ... Як не дивно, незважаючи на широку популярність, дуже на багатьох об'єктах досі взагалі немає ніякого захисту від цього типу загроз.

Для досягнення необхідних результатів потрібно визначити клас захищеності об'єкта, провести огляд сучасних систем контролю управління доступом, розглянути принципи побудови охоронних систем, розробити структуру охоронної системи, програмного забезпечення для її організації, побудувати імітаційну модель запропонованої структури, розробити програмне забезпечення.

Отже, в даній роботі було розглянуто актуальність створення інтегрованих систем охорони на базі обладнання міжнародної компанії Cisco. Мережі створюються на базі програмного забезпечення і устаткування провідних виробників. Пропоновані мережеві рішення мають високу економічну ефективність, надійність і безпеку, а також мають можливість подальшої модернізації.

УДК 004,621.396

Ю.С. Макарик, студент групи ТР-14
О.В. Андреєв, к.т.н., доц., доц. кафедри біомедичної інженерії та телекомунікацій
Державний університет «Житомирська політехніка»

РОЗРОБКА БЕЗДРОТОВОЇ СЕНСОРНОЇ МЕРЕЖІ НА БАЗІ МОДУЛІВ NRF24L01

Сенсорна мережа – система розподілених сенсорних вузлів, що взаємодіють між собою, а також з іншими мережами для запитів, обробки, передачі та надання інформації, отриманої від об'єктів реального фізичного світу з метою вироблення реакції на цю інформацію. Таким чином, сенсорна мережа включає як мінімум сенсори, актуатори і комунікаційні вузли.

Основною сферою застосування сенсорної мережі є контроль та моніторинг вимірюваних параметрів фізичних середовищ та об'єктів та в деяких випадках – управління цими об'єктами. Область покриття сенсорної мережі може становити від кількох метрів до кількох кілометрів за рахунок можливості ретрансляції повідомлень від одного елемента мережі до іншого.

Сенсорна мережа має здатність до ретрансляції повідомлень ланцюжком від одного вузла до іншого, що дозволяє у разі виходу з ладу одного з вузлів організувати передачу інформації через сусідні вузли без втрати якості. Сама мережа визначає оптимальний маршрут руху інформаційних потоків.

У сенсорній мережі вузли зазвичай спілкуються за допомогою бездротового зв'язку. Зв'язок може здійснюватися за допомогою радіо, інфрачервоного випромінювання або оптичних сигналів. Основним недоліком такого зв'язку є вимога прямої видимості між відправником та отримувачем.

Максимально допустима відстань взаємодії між вузлами бездротової системи залежить від цілого ряду факторів: робоча частота, вихідна потужність передавача, ефективність антен, чутливість приймача. Перешкоди, переміщення об'єктів або вузлів і навіть атмосферні умови можуть істотно вплинути на граничну відстань між вузлами або на якість зв'язку між ними. Безумовно, одним із найважливіших питань при створенні бездротової системи є вибір її частотного діапазону. Одним з найпоширеніших варіантів радіозв'язку є використання смуг частот для промислових, наукових та медичних цілей (ISM – (англ. industrial, scientific and medical)), які визначені Сектором радіозв'язку Міжнародного союзу електрозв'язку та доступні без ліцензій у більшості країн. Основними перевагами використання радіочастот ISM є широкий спектр частот та доступність у всьому світі. Вони не прив'язані до конкретного стандарту, цим дають велику свободу для реалізації енергозберігаючих стратегій у сенсорних мережах.

У роботі розглядається можливість реалізації бездротової сенсорної мережі на базі модулів nRF24L01. Модуль має 125 частотних каналів, що розміщені у діапазоні ISM від 2,4 ГГц до 2,525 ГГц з кроком 1МГц. На одному частотному каналі одночасно можуть працювати 7 пристроїв (1 приймач і 6 передавачів) з різними адресами. Модуль використовує передавач з GFSK модуляцією та максимальною вихідною потужністю 0 dBm, антену з коефіцієнтом підсилення 2dBm. Це забезпечує дальність зв’язку до 100 м при чутливість приймача -82 dBm. До мікроконтролера сенсорного вузла модуль підключається за інтерфейсом SPI і забезпечує максимальну швидкість передачі до 2 Мбіт/с. Послідовний периферійний інтерфейс (SPI) – це синхронний протокол послідовної передачі даних, що використовується для зв'язку мікроконтролера з одним або декількома периферійними пристроями. Інтерфейс SPI відрізняється відносно високою швидкістю і призначений для зв'язку близько розташованих пристроїв. Відповідно до протоколу SPI, один із взаємодіючих пристроїв (зазвичай мікроконтролер) завжди є ведучим і контролює ведені периферійні пристрої. Як правило, всі пристрої, що взаємодіють об'єднані трьома загальними лініями: MISO (Master In Slave Out) – лінія передачі даних від веденого пристрою (Slave) до ведучого (Master); MOSI (Master Out Slave In) – лінія передачі даних від провідного пристрою (Master) до провідних (Slave); SCK (Serial Clock) – тактові імпульси, що генеруються провідним пристроєм (Master) для синхронізації процесу передачі даних. SS (Slave Select) – вивід, присутній кожному відомому пристрої. Він призначений для активізації Майстром того чи іншого периферійного устрою. Периферійний пристрій (Slave) взаємодіє з ведучим (Master) тоді, коли на висновку SS присутній низький рівень сигналу. В іншому випадку дані від Master-пристрою ігноруватимуться. Така архітектура дозволяє взаємодіяти з декількома SPI-пристроями, підключеними до однієї і тієї ж шини: MISO, MOSI та SCK.

Таким чином, функціонально радіомодуль NRF24L01 дає можливість організації сенсорної міні-мережі без підключення до інтернету.

УДК 004.42

В.В. Гордієнко, студент
Г.В. Марчук, старший викладач
Державний університет «Житомирська політехніка»

ВИБІР АРХІТЕКТУРИ ДЛЯ «СИСТЕМИ ОПТИМІЗАЦІЇ НАВЧАЛЬНОГО ПРОСТОРУ»

Для веб-систем найчастіше використовується клієнт-серверна архітектура, яка складається власне з клієнта та сервера. Клієнт представляє собою відкриту сторінку у браузері на комп'ютері або будь-якому іншому гаджеті, який виконує запити та відображає їх результати. Сервер в свою чергу – це комп'ютер або обладнання, яке виконує обробку запитів та взаємодіє з даними баз даних. Переваги використання клієнт-серверної архітектури:

- немає дублювання коду. Якби вся обробка виконувалась на стороні клієнта – кожен додаток містив би в собі код для обробки логіки, базу даних, довідники тощо;
- безпека. Усі дані знаходились би на клієнті і, відповідно, він мав би до них доступ;
- навантаження. Обробку запитів бере на себе інша машина, тому клієнт буде менш навантаженим.

До мінусів можна віднести:

- залежність від роботи сервера. Якщо не працює сервер – ніхто не буде мати доступу до функціоналу системи. Однак цю проблему можна вирішити за допомогою кластеризації сервера;
- відносно висока вартість обладнання. Чим вищі вимоги до сервера, кількості даних та користувачів – тим дорожчим буде обладнання;
- необхідність в адміністраторі. Потрібна людина, яка зможе налагоджувати несправності та управляти базою даних.

Альтернативою є мікросервісна архітектура, яка поділяє систему на частини, кожна з яких виконує свою задачу. У системі, яка управляє освітнім процесом, можна виділити лише декілька сервісів, тому недоцільно ускладнювати розробку та деплой додатку, використовуючи мікросервіси.

На серверній частині доцільно використати MVC-патерн, який розділяє дані, представлення (вигляд) та обробку дій на компоненти. MVC розшифровується як Model-View-Controller, де Model – певна модель предметної області, яка описує та обробляє дані, View – візуалізація інформації, у нашому випадку відповідає за передачу даних у JSON форматі на клієнт, Controller – пов'язує тип запиту та відповідну його обробку.

На клієнті бібліотеку-патерн Vuex, що допоможе упорядкувати сховищем, станом та керувати запитами до бази даних. Тут використовується дві основні сутності: store – сховище даних (зберігання, обробка, шляхи запису та отримання) та service – довідник, у якому прописані відповідні запити до сервера. У сховищі описуються:

- state – стан сховища, тобто поточні дані;
- actions – дії, які можна виконувати з даними (отримати, змінити, видалити);
- mutations – «мутація» поточних даних, тобто обробка їх зміни.

Було розглянуто різні архітектурні стилі та обрано клієнт-серверну архітектуру. На серверній частині вирішено застосувати MVC-патерн, а на клієнтській – Vuex (рис. 1).

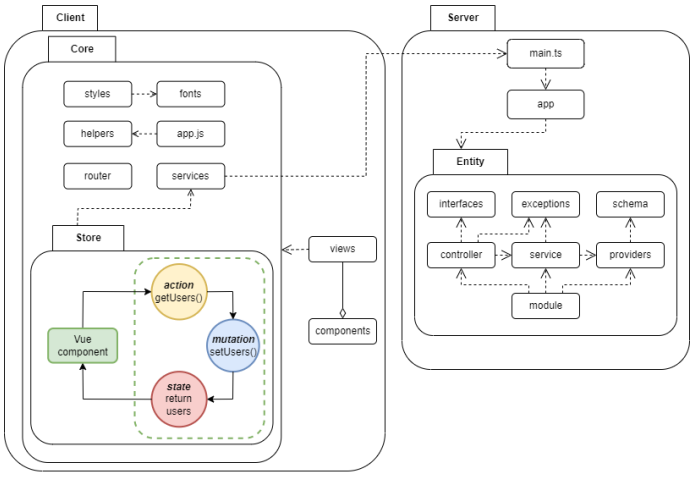

Рис. 1. Схематичне зображення MVC-патерн на серверній частині і Vuex на клієнтській

УДК 614.844

В.Г. Ципоренко, к.т.н., доц.
В.Р. Халілов, студент гр. ТР-14
Державний університет «Житомирська політехніка»

КОМБІНОВАНА СИСТЕМА ВІДЕОСПОСТЕРЕЖЕННЯ ОФІСНОГО ПРИМІЩЕННЯ

На даний момент системи відеоспостереження є найбільш поширеним способом забезпечити об’єкт від незаконного доступу сторонніх осіб на територію, що охороняється. За допомогою відеокамер є можливість одночасно контролювати декілька зон на одному об’єкті. Також завдяки таким системам можна з’ясувати особу злочинців або дізнатися їх наміри заздалегідь. Системи відеоспостереження часто використовуються для спостереження у місцях, які потребують постійного нагляду.

Система відеоспостереження (CCTV) – це комплекс обладнання та програмного забезпечення, призначення якого є спостереження за територією, діями та ситуацією. Сьогодні це – найбільш поширена система для охорони та моніторингу цілей. Системи відеоспостереження відкривають нові можливості не тільки для фіксації правопорушень, а також для їх попередження.

Камери спостереження можуть використовуватися для централізованого стеження за виробничим процесом, або у разі наявності середовища, небезпечного для людини. Системи відеоспостереження можуть знімати безперервно, або вмикатись лише за заданою подією. Досконаліші системи стеження дозволяють отримувати оповіщення та створювати записи, які зберігатимуться роками, з різною якістю та з додатковими можливостями (виявлення рухів та розпізнавання обличчя або автомобільних номерів).

Сучасна система відеоспостереження дає можливість: віддалено контролювати об’єкт, що охороняється з будь-якої точки світу; отримати доступ до архіву відеозаписів; переглядати камери з мобільного телефону або планшету; отримувати сповіщення про спрацювання датчиків руху або інших на об’єкті, що охороняється; налаштувати запис відеокамер за розкладом або при спрацюванні датчиків; налаштувати фіксацію подій та їх відправку поштою або іншим повідомленням.

Системи відеоспостереження поділяються на аналогові та цифрові.

Аналогові системи відеоспостереження передбачають використання аналогових відеокамер , принцип яких полягає у формуванні відеосигналу із світлового потоку, який проходить через лінзу об’єктиву і потрапляє на матрицю. Така система складається з відеокамер і записуючого пристрою – відеореєстратора. Зазвичай аналогові системи використовують на невеликих підприємствах.

Перевагами аналогових систем відеоспостереження є: простота користування, відпрацьовані технології монтажу, доступна ціна, висока надійність, стабільна робота. Недоліками аналогової системи є постійна потреба в обслуговуванні та обмеженість функцій.

Цифрові системи відеоспостереження містять блок цифрової обробки сигналу, вбудований веб-браузер і формують більш якісне зображення, яке можна передавати у вигляді цифрового сигналу по LAN/WAN мережам системи відеоспостереження. Цифрові камери застосовують на найбільш відповідальних ділянках системи відеоспостереження.

Перевагами цифрових систем відеоспостереження є: висока чутливість, швидкість зображення, висока роздільна здатність і деталізація. Недоліками цифрових систем є їх висока собівартість.

Цифровий інтерфейс HD-SDI спочатку з’явився в професійному телебаченні і призначався для передачі відеосигналу високої чіткості. Застосування цього інтерфейсу у CCTV є революційним кроком, завдяки якому можна передавати цифровий відеосигнал високого формату. Цифрові камери повинні бути підключені до тієї ж мережі, що і відеореєстратор (NVR), та не обов’язково безпосередньо до NVR.

Функції, характеристики і комплектація системи відеоспостереження залежать від вимог замовника до безпеки об'єкту. Як правило, мінімальна конфігурація такої системи містить: відеокамери, пристрої обробки відеосигналів [квадратори, мультиплексори тощо], записуючий пристрій [відеореєстратори, відеорекордери] та пристрої відображення відеоінформації [відеомонітори].

В роботі запропоновано комбінована система відеоспостереження офісного приміщення. Така система передбачає одночасне використання аналогових та цифрових відеокамер з формуванням єдиного цифрового інформаційного потоку. Запропонована побудова системи забезпечує її оптимізацію за критерієм точність/вартість з використанням секторів огляду різної чіткості.

Показана доцільність використання в системі стаціонарних та переносних камер, що забезпечує можливість адаптації конфігурації системи до умов її застосування і мінімізації кількості відеокамер і їх собівартості.

Для умов забезпечення контролю приміщення в нічний час запропонована комбінована структура системи, що поєднує функції відео спостереження та охоронно-пожежної безпеки.

Також запропоновані відповідні алгоритми функціонування комбінованої системи та виконано аналіз ефективності її функціонування.

УДК 004,621.396

К.О. Нестеренко, студентка групи ТР-14
О.В. Андреєв, к.т.н., доц., доц. кафедри біомедичної інженерії та телекомунікацій
Державний університет «Житомирська політехніка»

РОЗРОБКА ПРИСТРОЮ RFID ДОСТУПУ З ПЕРЕДАЧЕЮ ПОВІДОМЛЕНЬ ДО ХМАРНОГО СЕРВІСУ TELEGRAM

У зв'язку з бурхливим розвитком мереж із пакетною комутацією і насамперед Інтернету на початку 2000-х років світове телекомунікаційне співтовариство спочатку виробило, а потім і розпочало реалізацію нової парадигми розвитку комунікацій – мереж наступного покоління NGN (Next Generation Networks). Технології NGN вже пройшли еволюційний шлях розвитку від гнучких комутаторів (Softswitch) до підсистем мультимедійного зв'язку IMS (IP Multimedia Subsystem) та бездротових мереж довготривалої еволюції LTE (Long Term Evolution).

Проте останнім часом значного розвитку набули методи радіочастотної ідентифікації RFID (Radio Frequency IDentification), бездротові сенсорні мережі WSN (Wireless Sensor Network), комунікації малого радіусу дії NFC (Near Field Communication) та між машинні комунікації M2M, які інтегруючись з Інтернет, дозволяють забезпечити простий зв'язок між різними технічними пристроями («інтернет – речами»), число яких може бути величезним, а також із хмарними сервісами зберігання і обробки даних.

Радіочастотна ідентифікація – це спосіб забезпечення зберігання та передачі інформації зі зручного носія-мітки в потрібне місце за допомогою спеціальних пристроїв. Такі мітки-ідентифікатори дозволяють полегшити розпізнавання різних об'єктів: товарів в магазині, рухомих засобів при транспортуванні, можуть ідентифікувати людей і тварин, не кажучи вже про широкі можливості ідентифікації документів і майна.

Радіочастотне розпізнавання здійснюється за допомогою закріплених за об'єктом спеціальних міток, що несуть ідентифікаційну та іншу інформацію. RFID-міткам не потрібен контакт або пряма видимість, дані з пасивної мітки можуть бути отримані на порівняно невеликій відстані до кілька метрів (метро, офіси, банки, магазини). Технологія RFID вже довго і успішно використовується як електронний ключ для керування доступом до приміщень. RFID-мітки можуть бути використані як для читання, так і для запису великого обсягу інформації.

Принцип роботи RFID мітки полягає в тому що, при потраплянні у радіочастотне поле, мітка активується. Це поле генерується зчитувачем і надсилається за допомогою антени, далі мітка посилає сигнал у відповідь зчитувачу. Антена отримує сигнал у відповідь від мітки і передає його на зчитувач. Отриманий сигнал від антени обробляється за допомогою мікроконтролера у зчитувачі. І вже далі, оброблений сигнал посилається на користувальницьке програмне забезпечення. Звичайно, ця схема є дуже спрощеною і деякі її пункти можуть змінюватися залежно від технології, яка використовується, але вона демонструє суть роботи RFID та безконтактної ідентифікації.

За типом пам'яті RFID-мітки поділяються на призначені лише для ідентифікації (RO, Read Only), розроблені для зчитування блоку інформації (WORM, Write Once Read Many) і такі, що перезаписуються (RW, Read and Write). RO RFID-мітки використовуються виключно для ідентифікації – дані унікального ідентифікатора записуються під час виготовлення, тому скопіювати їх та підробити мітку практично неможливо. WORM RFID-мітки дозволяють одноразово записати будь-які дані, які згодом можна буде багаторазово зчитувати та використовувати. Це дозволяє користувачеві доповнити мітку своєю інформацією, яка буде використовуватися при зчитуванні. RW RFID-мітки містять блок пам'яті, який дозволяє багаторазово записувати та зчитувати інформацію.

У роботі пропонується реалізація системи контролю RFID – доступу у приміщення з використанням бездротової технології передачі даних у хмарний сервіс Telegram. При цьому розглядаються можливості використання RFID-міток з інтерфейсами SPI, I2C, UART та Wiegand.

У якості пристрою, який забезпечує обробку даних та підключення до точки доступу WiFi пропонується використання мікроконтролера ESP32, або ESP8266. Обговорюються особливості реалізації прототипу системи RFID – доступу на основі зчитувача RFID з модулем RC522, що живиться від напруги 3,3В і випромінює радіохвилі на частоті 13,56 МГц та підключається до мікроконтролера за інтерфейсом SPI. Такий варіант дозволяє організувати живлення безпосередньо від плати Piranha ESP32, яка була обрана для реалізації проекту.

Обговорюються алгоритми та особливості реалізації програмного коду для запису та зчитування інформації з RFID-міток, а також отримання даних про поточний час доступу з NTP – серверу. Розроблений пристрій контролю доступу передбачає можливість передачі даних на мобільний телефон користувача і є достатньо недорогим і надійним.

УДК 621.37

В.В. Ципоренко, к.т.н., доц.
П.Л. Герасимчук, студент гр. ЗТР-18
Державний університет «Житомирська політехніка»

РОЗРОБКА ШИРОКОСМУГОВОЇ АНТЕНИ РАДІОМОНІТОРИНГУ СИГНАЛІВ ДВЧ-УВЧ ДІАПАЗОНУ

Радіомоніторинг забезпечує безперервне отримання, достовірність та актуальність добутих даних. Безперервність досягається постійністю роботи засобів моніторингу, актуальність – своєчасністю отримання необхідних для прийняття рішення даних.

Станції радіомоніторингу застосовуються для рішення наступних задач: вимірювання та контроль за радіоелектронними засобами , призначеними для передавання електромагнітних хвиль різних діапазонів, отримання інформації про працюючі передавачі в певній місцевості, визначення їх типу, основних характеристик.

Структура станції повинна включати:

– широкодіапазонні ненаправлені антени різного застосування;

– набори антенних систем для автоматичного пеленгування в русі, на стоянках і для стаціонарних постів;

– набори антенних модулів з направленими властивостями для ручних пеленгаторів відкритого і скритого використання;

– перетворювачі радіосигналів для розширення робочих діапазонів частот;

– апаратуру прив'язки засобів радіомоніторингу до географічних координат.

Особливістю антен станції радіомоніторингу є те, що антена повинна бути широкосмугова. У такому випадку вона буде одна перекривати достатньо великий діапазон частот. Потрібно розробити широкосмугову антену системи радіомоніторингу. Для цього обрати тип антени, шляхом порівняльного аналізу. Провести розрахунок її геометричних розмірів. Дослідити розраховану антену у програмному середовищі MMANA-GAL. MMANA дозволяє розраховувати будь-які типи антен, які можна представити як довільний набір проводів, проводити розрахунки на будь-якій частоті, створювати або редагувати опис антени, як зазначенням цифрових координат, так і в графічному редакторі. Оптимізувати антену, гнучко налаштовуючи параметри оптимізації: Zвх, коефіцієнт стоячої хвилі (КСХ), підсилення, ширину діаграми спрямованості (ДС) випромінювання, проводити оптимізацію більше 90 параметрів антени, можливо опис спільної зміни декількох параметрів, зберігати всі кроки оптимізації у вигляді окремої таблиці для подальшого аналізу.

Будувати безліч різноманітних частотних графіків: Zвх, КСХ, підсилення, ДС, створювати таблиці для всіх змінних розрахункових даних.

Було розглянуто засоби радіомоніторингу, їх класифікацію та характеристики. Визначено що вони працюють в широкій смузі частот, тому потрібно використовувати декілька антен. Це не завжди раціонально, бо одночасне розгортання декількох антен на обмеженій території призводить до складностей в обслуговуванні. Крім того розташування на обмеженій території декількох антен призводить до виникнення взаємних перешкод. Для поста радіомоніторингу ДВЧ-УВЧ діапазону доцільно використовувати одну антену – широкосмугову, щоб усунути вище перераховані недоліки.

Широкосмугова антена – це антена, основні параметри якої не змінюються в досить широкій смузі частот, застосовується для передачі або прийому радіосигналів з широким спектром частот.

До широкосмугових антен можна віднести циліндричну спіральну антену, плоску спіральну антену, логоперіодичну антену. Найкращі діапазонні властивості мають логоперіодичні антени, тобто антени з дискретною зміною резонансних частот активних випромінювачів за логарифмічним законом. Умови збудження та взаємний вплив вібраторів такі, що в будь-якій трійці довший випромінювач поводить себе як рефлектор, коротший – як директор, а середній – як випромінювач.

Проведено розрахунок логоперіодичної антени, так як вона найбільше підходить для рішення поставлених задач. Логоперіодична антена розрахована для діапазону (100 – 500) МГц за першою та другою методиками. При другій методиці розміри антени менші порівняно з результатами першої методики. Моделювання проведенно в програмному середовищі MANNA-GAL. Коефіцієнт підсилення антени, розрахованої за першою методикою складає у середньому 7 дБ. У другому випадку –7дБ, проте при меншій кількості елементів та довжині антени.

Тому друга методика є доцільною при розрахунках, оскільки вона дозволяє зменшити габарити логоперіодичної антени при незмінному коефіцієнті підсилення. Зменшити геометричні розміри при постійних електричних.

На основі другої методики проведено розробку програми в Microsoft Visual Studio для автоматизації розрахунку геометричних розмірів логоперіодичної антени.

УДК 621.37

В.В. Ципоренко, к.т.н., доц.
В.Г. Ципоренко, к.т.н., доц.
О.В. Мельниченко, студент гр. ТР-14
Державний університет «Житомирська політехніка»

РОЗРОБЛЕННЯ КОМБІНОВАНОЇ МЕРЕЖІ ВІДЕОСПОСТЕРЕЖЕННЯ ТЦ ОЛДІ

В наші дні системи відеоспостереження виділилися в самостійну область засобів охорони, що мають власні правила і особливості експлуатації. Системи відеоспостереження – найефективніший технічний засіб забезпечення безпеки, що дозволяє швидко зафіксувати факт скоєння того чи іншого протиправного діяння, а також дає можливість контролювати якість роботи співробітників, загальну ситуацію на об'єкті.

У сучасному світі безпеку об'єкта – будь-то квартира, заміський будинок, школа або офіс – неможлива без ведення відеоспостереження. Саме відеоспостереження дозволяє вчасно виявити, попередити або припинити правопорушення. Сьогодні складно знайти об'єкт, де не було б потрібно відеоспостереження. На сьогоднішній день можна контролювати системою відеоспостереження і системою контролю доступом на віддаленій відстані за допомогою сучасних технологій передачі даних, якими є локальні мережі, Інтернет, WI-FI з'єднання. Можливий контроль над торговим, або виробничим підприємством, не виходячи з офісу.

У більшості випадків система відеоспостереження дозволяє записувати зображення на носії інформації, а також виконувати інші функції. Наприклад, повністю управляти відеокамерами, повертати об'єктив, масштабувати зображення, створювати архіви записів, переглядати і управляти ними. Крім запису відео, сучасні системи відеоспостереження можуть також сприймати аудіо інформацію, реагувати на рух і виконувати охоронні функції.

Метою розробки є розробка системи відеоспостереження для торгово-розважальному комплексу «ОЛДІ», яка призначена для забезпечення контролю правопорядку зі сторони відвідувачів та документування подій , що відбуваються на території комплексу.

Запровадження такої системи відеонагляду дозволить зменшити час реакції служби охорони на протиправні дії працівників та відвідувачів, покращити збереження матеріальних ресурсів від пошкоджень та крадіжок. Відбудеться покращення взаємодії різного роду підрозділів, що забезпечують охорону правопорядку та майна в торгівельно-розважальному центрі «ОЛДІ» за рахунок запровадження системи відео нагляду.

Для огляду прилеглих територій, фіксування проходять людей і проїжджаючих автомобілів використовують комплект відео спостережень для будівлі. Цей комплект стає хорошою системою безпеки для будівель будь-якої складності. Система відеореєстратора порівнює особи, які є в базі даних, і розпізнає номери машин. Добре розпізнає обличчя. Результат порівняння дозволяє викликати охорону або відкрити шлагбаум.

Як годиться для більшої системи відеоспостереження для першого плану входять такі характеристики: універсальність, робота при будь яких погодних умовах, функціональність. Можливість роботи в нічний час доби за допомогою інфрачервоного підсвічування нового покоління.

Таємне відеоспостереження в темних місцях. Для даного типу спостереження підійдуть спеціальні відеокамери, які мають малі розміри і оснащені інфрачервоним підсвічуванням. Його використання дозволяє домогтися непоганий освітленості, приховуючи при цьому розташування самої камери. Це основний спосіб підсвічування для камер в нічний час доби.

Бездротове спостереження це актуальний спосіб, коли необхідна мобільність і автономність. Таке спостереження використовує для передачі даних мережі GPRS, Wi-Fi, 3G. Такий підхід значно спрощує монтаж системи відеоспостереження та дозволяє розташовувати камери в самих непередбачуваних місцях. Досить популярні такі системи в інтер'єрах, де неприпустима прокладка додаткових кабелів.

Купівля системи відеоспостереження для офісу – питання безпеки майна фірми, її співробітників і клієнтів. Для початку варто визначитися з кількістю камер. Для кабінетів підійдуть ширококутні камери. Для коридорів краще взяти камери з кутом менше, вони дивляться вздовж коридору, не перекриваючи більшу частину кадру стінами. Для великих переговорним, кімнат, в яких проводять фокус-групи або тренінги камери з об'єктивом «Риб'яче око».

На вибір візьмемо два бренда виробників камер однієї цінової категорії таких як Partizan та Hikvision. Портфоліо Hikvision включає аналогові і цифрові відеокамери, відеореєстратори, мережеве та серверне обладнання, пристрої контролю доступу. Проаналізувавши дві камери можна зробити висновки, що камера бренду Hikvision набагато краща ніж Partizan оскільки за туж ціну ми отримуємо кращу картинку, більший функціонал кращу систему захисту що не менш важливо від самого відображення зйомки.

УДК 004.8

М.С. Сітайло, студент,
Г.В. Марчук, ст. викладач
Державний університет «Житомирська політехніка»

ВИКОРИСТАННЯ FACENET ДЛЯ СИСТЕМИ КОНТРОЛЮ ВІДВІДУВАНОСТІ ЗАНЯТЬ СТУДЕНТАМИ

Задача ідентифікації людини за її обличчям є дуже популярною й актуальною в наш час. Існують багато типів моделей, які показують чудові результати. Проте поряд з популярними згортковими нейронними мережами (Convolutional Neural Network, CNN) типу ResNet та Inception є особлива мережа – FaceNet [1]. Її особливість в тому, що вона являється одразу системою для підтвердження, розпізнавання особистості та пошуку схожих людей. Попри те що, архітектура цієї мережі відрізняється від звичайних, її використання на популярних наборах даних для розпізнавання людей продемонструвало чудовий результат [2], що доводить її ефективність. Універсальність цієї мережі спричинена тим, що дана модель базується та такому типі нейронних мереж як Siamese Neural Network (SNN) (рис. 1).

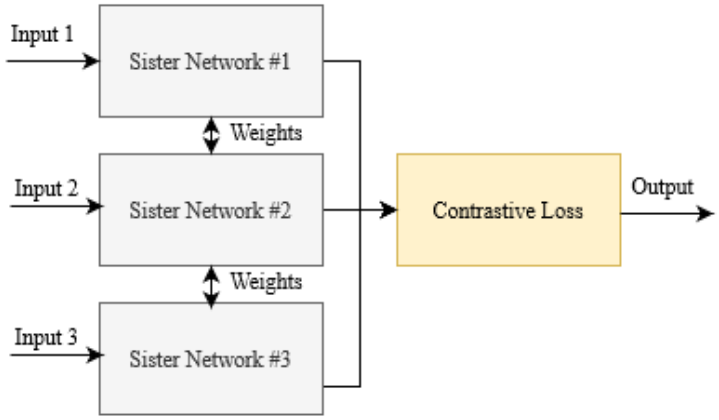

Рис. 1. Архітектура Siamese Neural Network

Назва цієї архітектури пов’язана з її основною особливістю – вона складається з декількох згорткових підмереж, які мають спільні ваги та зсуви. Кожна з цих нейронних підмереж має спеціальний шар виходу, який містить 128 вузлів та називається Embeding layer. У звичайній CNN вихід мережі складається з вузлів, кількість яких дорівнює кількості класів і значення є ймовірністю цього класу. В той же час у SNN виходом мережі є вектором 128-вимірного евклідового простору. Відповідно однією з основних відмінностей цієї архітектури від звичайних CNN є те, що вона не класифікує зображення, а генерує його вектор у багатовимірному просторі.

Навчання нейронної мережі проходить у два етапи. На першому етапі створюються триплети – набори з базового зображення, та зображень того ж класу, що і базове (Postive) та зображення з іншого класу (Negtive). Потім використовується метод triplet loss (втрата триплетів), вчимо нейронну мережу впізнавати об'єкти: відстань між зображення конкретної людини (Anchor) та зображенням схожої людини (Postive) повинна бути меншою, ніж відстань між Anchor та зображенням не схожої людини (Negtive) (рис. 2). Ідентифікатори персонажів у зразках Postive та Anchor однакові, а ідентифікатори персонажів у зразках Negtive та Anchor різні.

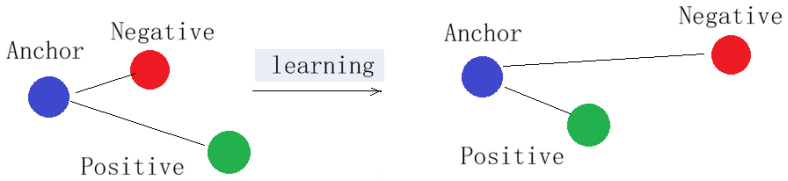

Рис. 2. Триплетна втрата. До тренування (ліворуч) та після тренування (праворуч)

Триплетна втрата – це назва функції, яка використовується для перевірки особи. Функція втрат триплетів виглядає наступним чином:

$$L = \sum_{i}^{N} \left[\left\| f\left(x_i^a\right) - f\left(x_i^p\right) \right\|_2^2 - \left\| f\left(x_i^a\right) - f\left(x_i^n\right) \right\|_2^2 + \alpha \right],$$

де i – індекс триплету;
N – кількість триплетів у батчі;
x_i^a – вектор базового зображення;
x_i^P – вектор зображення того ж класу;
x_i^n – вектор зображення іншого класу;
α – константа, яка допомагає запобігти випадку, коли f(x) = 0, при будь-яких значеннях x;
$\|f(x_i^a) - f(x_i)\|$ – евклідова відстань.

Ефективність навчання залежить від обраних пар триплетів, тому перед кожною ітерацією необхідно формувати такі набори, щоб різниця відстаней між векторами (x_i^a; x_i^P) та (x_i^a; x_i^n) була мінімальною.

На другому етапі навчання зображення, згенерованих триплетів, передаються на вхід мережі (по зображенню на кожну підмережу) й на виході отримуються три вектори. Після чого, розраховується значення функції втрат триплетів з використанням отриманих даних й синхронно оновлюються ваги і зсуви всіх підмереж, щоб кожна залишалася ідентичною іншим.

Мета дослідження – створення системи контролю відвідуваності занять студентами. Дана задача має дві основні проблеми: недостатня кількість зображень студентів для навчання класифікатора і велика можливість зміни списку студентів

Перша проблема є дуже важливою, так як наявність достатньої кількості даних кожного класу є критично необхідним для створення якісного класифікатора. В той же час, зібрати велику кількість даних, які будуть включати по декілька десятків фотографій кожного студента, їх обробити та підтримувати актуальність всього набору даних є задачею складною. Окрім цього, дане завдання потребує примусового збору даних, що не є правильним з морально-етичного боку. В розпорядженні розробників системи є зображення студентів, які зберігаються в їх особовій справі та їх студентські квитки. Отже, ми це по 1-2 фотографії студента, що являється дуже маленькою кількістю екземплярів даних для класу.

Інша проблема полягає в тому, що у випадку коли кожному студенту призначається клас, зміна його зовнішнього вигляду або зміна кількості студентів вимагає перенавчання класифікатора.

Одразу обидві проблеми вирішуються за допомогою використання SNN. Як вже відомо, на виході модель отримує набір з 128 значень. Ці значення – координати зображення в евклідовому просторі. Відстань між векторами у цьому просторі залежить від зображень, які вони представляють. Чим більша схожість зображень, тим ближче знаходяться їх вектори у просторі і навпаки.

Процес ідентифікації відбувається за методом найближчої точки. Задля покращення результатів, функція втрат базується на класифікації Large Margin Nearest Neighbors (LMNN) [3]. Її основна ідея полягає в тому, щоб збільшувати відстань між точками різних класів і зменшувати від точками одного класу під час навчання. Окрім цього, введення правильного порогу відстані між зображеннями одного класу додатково дозволяє вирішити проблему різного освітлення, позицій обличчя та відкинути незнайомих системі людей.

Отже, за допомогою згаданої нейронної мережі можна вирішити описані проблеми наступним чином:

- невеликий набір даних компенсується тим, що класифікація відбувається за допомогою пошуку найближчих сусідів. Тобто, навіть однієї фотографії може бути достатньо для коректної ідентифікації;
- при додаванні нового студента можна згенерувати вектор для його зображення й використовувати для ідентифікації без перенавчання моделі.

Список використаної літератури:

1. Schroff, Florian, Dmitry Kalenichenko, James Philbin, FaceNet: A Unified Embedding for Face Recognition and Clustering, CVPR 2015. https://doi.org/10.48550/arXiv.1503.03832.

2. Face Verification on YouTube Faces DB [Електронний ресурс]. – Режим доступу : https://paperswithcode.com/sota/face-verification-on-youtube-faces-db.

3. Large Margin Nearest Neighbors (LMNN) [Електронний ресурс]. – Режим доступу : https://pydml.readthedocs.io/en/latest/dml.lmnn.html.

УДК 004.4, 004.67

Д.Ю. Лисогор, аспірант
Ю.І. Лисогор, ст. викладач
А.В. Морозов, к.т.н., доц.
Державний університет «Житомирська політехніка»

СТВОРЕННЯ ПРОГРАМНОГО КОМПЛЕКСУ ДЛЯ АНАЛІЗУ ТА ПРОГНОЗУВАННЯ ПРОДУКТИВНОСТІ ЗЕМЕЛЬ

Стрімкий розвиток інформаційних технологій не пройшов повз агропромисловий комплекс. З їхньою появою все більшої популярності в сільському господарстві набирає точне землеробство. На сьогодні це комплексна високотехнологічна система господарювання, що впроваджує новітні досягнення в галузі інформатики й техніки, це низка рішень, які в сумі дають колосальний результат.

У комплексі точного землеробства умовно можна виділити три складові:

- техніка та обладнання;
- аналітичні дані для побудови карт завдань;
- програмне забезпечення.

Відразу впровадити весь комплекс точного землеробства складно та дорого. Виходячи з цього, простіше діяти поетапно. Спочатку потрібно провести інвентаризацію полів та скласти їх електронну карту, вивчити стан ґрунтів, а далі починати роботу з технікою.

Розглянемо системний підхід до впровадження точного землеробства. Проект можна розділити на три блоки: «Земельний банк», «Техніка та обладнання» і «Джерела даних для аналізу». З огляду на той факт, що основним активом в агровиробництві є земля, то й побудова системи управління земельним банком – це перший і один з найважливіших кроків для виживання в умовах сучасних ринкових реалій. Усі результати картографування повинні зводитися в одну карту точних контурів полів і у векторному форматі експортуватися в сервіс, розроблений для збирання й аналізу просторових даних сільськогосподарських підприємств.

Другий блок «Техніка та обладнання» розпочинається з інвентаризації технічних засобів. Якість технологічних операцій безпосередньо залежить від техніки і навісного обладнання, систем паралельного водіння і автопілотів, систем висіву та внесення добрив. Вся сільськогосподарська техніка повинна бути оснащена GPS-трекерами, що дозволяє відстежувати місце розташування всіх машин з будь-якої точки.

Корпоративна система GPS-моніторингу техніки, агрегатів та автотранспорту уможливила комплексний облік пального по ланцюжку «АЗС – бензовоз – техніка – витрата на поле», а також підключення диспетчерської служби, систем оперативного планування й облік фактичних робіт техніки. Крім GPS-приймачів комбайни обладнані датчиками врожайності й вологості, а бортовий комп'ютер дозволяє проводити процес документування, картографування врожайності. Це дає можливість побачити показники маси зерна на різних ділянках поля. Інформація зберігається у вигляді треку зі значеннями в конкретному місці на полі. Дані одночасно збираються з усіх машин і зберігаються в обліковому записі.

У третьому блоці «Аналіз даних» аналізуються супутникові знімки з оцінкою стану посівів. Супутниковий моніторинг дозволяє в режимі реального часу спостерігати за станом посівів на великій території і навіть на полях, що знаходяться на великій відстані. Користь безперервного спостереження в тому, що у разі будь-якого відхилення від норми надходить оперативне повідомлення про проблему.

Для побудови картограм внесення добрив або перегляду технологій обробітку ґрунтів проводиться аналіз історичної продуктивності. Він являє собою низку супутникових знімків і їх порівняння. У результаті у вас на руках буде інформація про закономірний розвиток біомаси протягом багатьох років. Після вивантаження даних з польового обладнання в програмне забезпечення можна проводити просторовий аналіз за будь-яким обраним показником: продуктивності полів, карти врожайності, супутникових даних, даних агрохімічного аналізу, карти рельєфу та інші.

У сільському господарстві, як і в інших галузях, збирання, зберігання й аналіз отриманої інформації відіграє важливу роль. Недостатньо мати космознімки або техніку, нехай навіть й обладнану датчиками, потрібно вміти аналізувати отримані дані, щоб ухвалювати правильні рішення.

Такий інноваційний підхід до аграрного бізнесу підвищує ефективність роботи, збільшує врожайність, а також зменшує витрати на вирощування зернових та інших культур. Відбувається це шляхом вибору правильної концепції керування сільським господарством, в основі якої лежить дослідження неоднорідностей ділянок поля.

Від реалізації програмного комплексу агрокомпанії отримають повернення інвестицій завдяки економії витрат на паливно-мастильні матеріали та добрива. Впровадження систем управління агровиробництвом оптимізує процес управління земельним банком агрокомпанії, зменшить вплив людського фактору, забезпечить прозорість виробничих ланцюжків, що в свою чергу дозволить підвищити контроль активів і ефективність управлінських рішень.

УДК 378.6.004.4

О.О. Окунькова, ст. викладач каф. комп'ютерної інженерії та кібербезпеки
Державний університет «Житомирська політехніка»

ІНСТРУМЕНТИ МОВИ PYTHON ДЛЯ АНАЛІЗУ ДАНИХ

У сучасному світі спостерігається тенденція до значного зростання обсягів інформації, що потребує її збору, ефективної обробки та збереження, а ускладнення її структури робить все більш актуальним створення комп'ютерних технологій та засобів високопродуктивного аналізу даних.

Аналіз публікацій показує, що на даний час безперечним фаворитом для масштабованої обробки даних є мова програмування Python. Вона пропонує безліч бібліотек, які застосовуються на всіх етапах аналізу даних. Найпопулярнішим сценарієм використання мови Python для аналізу даних є: пошук, обробка, моделювання та візуалізація.

Для пошуку даних використовуються бібліотеки Python Scrapy та BeautifulSoup. Scrapy – це одна з найпотужніших бібліотек, продуктивність якої надзвичайно висока. Забезпечує спільну роботу з відкритим вихідним кодом для отримання даних із вебсайтів. Основною перевагою Scrapy є те, що вона побудована на основі Twisted, асинхронної мережевої структури, що означає використання Scrapy неблокуючого механізму при надсиланні запитів користувачам. За допомогою Scrapy можна створювати програми, які збирають структуровані дані в мережі або з API. Найбільшою перевагою використання Scrapy є можливість легкого перенесення існуючого проекту в інший проект. Тому для великих та складних проектів Scrapy – найкращий вибір для розробки. Засобами BeautifulSoup здійснюється збір даних та розміщення їх у певному форматі в тому випадку коли неможливо отримати дані з API. BeautifulSoup допомагає програмісту швидко отримати дані з певної веб-сторінки. Але проблема з Beautiful Soup в тому, що вона не може виконати всю роботу самостійно, а тому потребує певних модулів для роботи. Для посилання запиту на вебсайт використовуються бібліотеки Requests або urlib2. Після завантаження даних HTML або XML на комп'ютер Beautiful Soup потрібен зовнішній аналізатор для аналізу завантажених даних. Для цього найчастіше використовуються XML-parser lxml, HTML-parser lxml, HTML5lib, html.parser.

Обробку і моделювання даних забезпечують бібліотеки NumPy, SciPy і Pandas. NumPy (Numerical Python) є універсальним інструментом для обробки масивів, що використовується для сортування великих наборів даних, спрощення виконання математичних операцій та їхню векторизацію. Бібліотека SciPy містить модулі для ефективних математичних процедур, таких як лінійна алгебра, інтерполяція, оптимізація, інтеграція та статистика. Основний функціонал бібліотеки SciPy побудований на NumPy та його масивах. Pandas розшифровується як бібліотека для аналізу даних Python. Це пакет Python з відкритим вихідним кодом, який надає високоефективні, прості у використанні структури даних та інструменти для аналізу даних. Pandas бере дані у файлі CSV або TSV або базу даних SQL і створює об'єкт Python з рядками та стовпцями, який називається кадром даних. Фрейм даних дуже схожий на таблицю у статистичному програмному забезпеченні, скажімо, Excel або SPSS. Pandas пропонує дві структури даних: Series (список елементів) та Data Frames (таблиця з декількома колонками). Ця бібліотека конвертує дані в Data Frame, дозволяючи видаляти та додавати нові колонки, а також виконувати різні операції.

Бібліотеки Matplotlib та Seaborn широко використовуються для візуалізації даних. Вони допомагають конвертувати величезні списки чисел у зручні графіки, гістограми, діаграми, теплові карти тощо. Візуалізація даних дозволяє представити їх у графічному вигляді, що сприяє більш ефективному вивченню та аналізу, ніж це можна зробити використовуючи дані представлені у звичайному форматі. Matplotlib – найкраща та найпопулярніша Python-бібліотека для цієї мети. Бібліотека Seaborn використовується для створення статистичних графіків на Python. Вона побудована на основі Matplotlib і тісно інтегрується із структурами даних Pandas. Seaborn допомагає проаналізувати та зрозуміти дані. Функції побудови графіків працюють із датасетами і виконують всі необхідні перетворення на створення інформативних графіків. Для досягнення більшого ефекту в питанні візуалізації даних доцільно скористатися можливостями інтерактивної бібліотеки Bokeh. Вона забезпечить елегантну та стислу побудову графіки в стилі D3.js та розширить цю можливість завдяки високопродуктивній інтерактивності за дуже великими або потоковими наборами даних. Bokeh може допомогти всім, хто хоче швидко та легко створювати інтерактивні сюжети, панелі моніторингу та програми для передачі даних.

Аналіз даних – важлива частина будь-якої діяльності, яка потребує автоматизованої обробки. На сьогодні мова програмування Python є однією з найкращих мов для статистики, машинного навчання, прогнозування, аналітики, а також рішення стандартних задач із обробки даних. В її арсеналі є безліч функцій, готових до використання бібліотек, вона має величезну спільноту і легко вивчається – ось, що робить мову програмування Python найкращим вибором для фахівців з аналізу даних.

УДК 612.15

К.С. Терех, студентка гр. БІ-21, IV курс
Р.О. Коломієць, к.т.н., доц. каф. БІтаТ
Державний університет «Житомирська політехніка»

РЕОГРАФ ІЗ МОСТОВИМ ПЕРЕТВОРЮВАЧЕМ

Актуальною проблемою сучасної медицини є захворювання серцево-судинної системи. Розмаїття сучасної діагностичної апаратури представлене випробуваними на практиці методами реографії, сфігмографії, ехокардіографії, оптичної та комп'ютерної капіляроскопії, радіонуклідної діагностики, ангіографії, ультразвуковими методами діагностики, лазерною доплерографією, комп'ютерною томографією (КТ), МРТ в судинному режимі (МРА), перфузійною МРТ тощо. Але найбільш інформативним методом моніторингу стану організму, експрес- та функціональної діагностики серцево-судинної системи залишається реєстрація пульсової хвилі.

Реографія (або імпедансна плетизмографія) є одним із методів дослідження серцево-судинної системи, якому властиві висока інформативність результатів, неінвазивність, відносна простота і доступність не лише діагностичним центрам, але і звичайним поліклінікам. Цей метод використовується для діагностики центральної і регіональної гемодинаміки, визначення ударного та хвилинного об'ємів крові, загального периферійного опору і дозволяє дати характеристику венозному відділу кровообігу і мікроциркуляції.

Реографічні методи дозволяють оцінити сумарне кровонаповнення органів і тканин. Крім того, важливою перевагою реографії являється можливість одночасного дослідження кровообігу кількох судинних областей, у тому числі симетричних, що дозволяє легко виявити порушення кровообігу. Слід також зазначити, що реографічні методи практично не мають протипоказань та підходять для довготривалих досліджень. Цей, далеко неповний перелік переваг реографії свідчить про те, що реографічні методи можуть надавати істотну допомогу для правильної постановки діагнозу і, особливо, для поточної оцінки змін кровообігу, у тому числі при проведенні функціональних проб.

Метою створення пристрою є можливість дослідження функцій серця та кровообігу грудного відділу тіла людини в умовах медичного закладу.

Реограф складається з електродів, генератора, мостового перетворювача, в одне з плечей якого за допомогою електродів підключений досліджуваний орган пацієнта. Живлення мосту здійснюється змінним струмом 50 кГц від генератора. Також складовими реографа є підсилювач, фільтр та реєстратор сигналу. Структурна схема представлена на рис. 1.

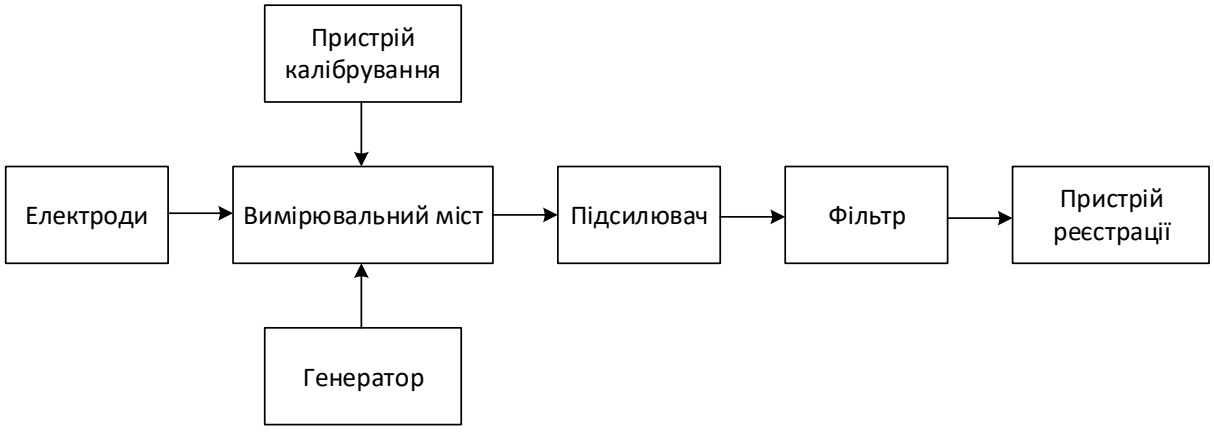

Рис. 1. Структурна схема реографа із вимірювальним мостом

За допомогою електродів сигнал від пацієнта поступає на вимірювальний міст. Для цього проекту було обрано електроди типу Skintact FS50 діаметром 5 см.

Джерелом зондуючого змінного сигналу є генератор, включений в одну діагональ вимірювального мосту (рис. 2). Властивості мостової схеми такі, що напруга U_{BD}, яка реєструється у вимірювальній діагоналі (різниця потенціалів між точками B і D) дорівнює нулю тільки в тому випадку, коли опори, включені в плечі мосту, попарно рівні ($R_{AB} = R_{AD}$ та $R_{CB} = R_{CD}$). Таким чином, якщо до одного з плечей мосту підключити вимірюваний опір (ділянка тіла пацієнта), то коливання електричного опору досліджуваного об'єкту будуть перетворені в коливання напруги, що реєструється у вимірювальній діагоналі (U_{BD}).

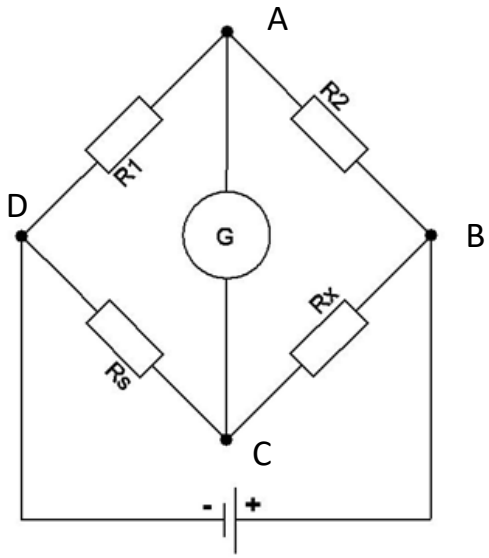

Рис. 2. Вимірювальний міст

Для встановлення кількісної відповідності між амплітудою зміни опору досліджуваного об’єкту та величиною напруги, що реєструється за допомогою вимірювального мосту у схему включають схему калібрування. Вона генерує еталонні сигнали відомої форми та амплітуди.

Перед реєстрацією сигнал з виходу вимірювальної схеми повинен бути підсилений та відфільтрований. У якості підсилювача було обрано інструментальний. Фільтрація буде відбуватися за допомогою смугового фільтра за класичною топологією Саллена-Кея.

На основі структурної схеми було розраховано основні блоки електричної принципової схеми реографа з мостовим перетворювачем (рис. 3), серед яких генераторна колах зсуву фази, вимірювальний міст, інструментальний підсилювач, смуговий фільтр (топологія Саллена-Кея).

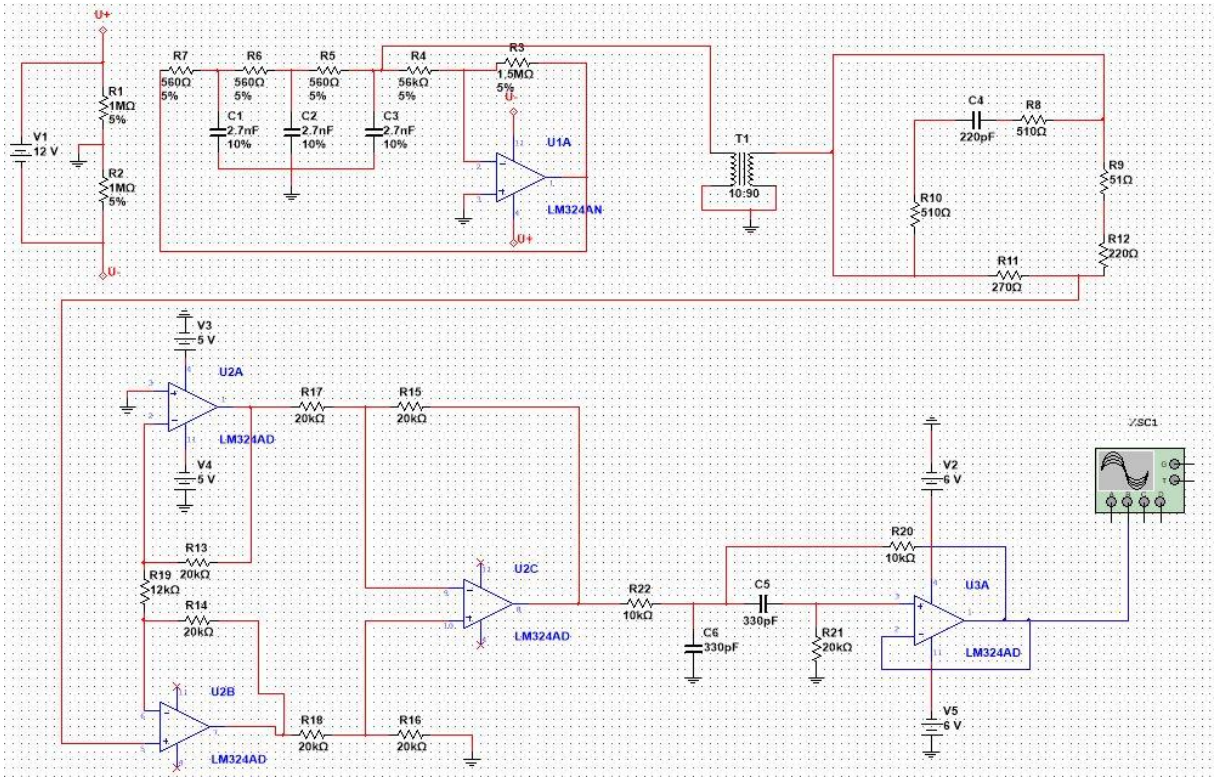

Рис. 3. Електрична принципова схема реографа із мостовим перетворювачем.

УДК 004.8

A.S. Chevkota, student
G.V. Marchuk, Senior Lecturer
T.A. Vakaliuk, Dr of Pedagogic Sciences, Full Professor,
Professor at the Department of SE
Zhytomyr Polytechnic State University

ANALYSIS OF THE FEATURES OF ARTIFICIAL INTELLIGENCE IN COMPUTER GAMES OF THE GENRE "ONLINE FIRST PERSON SHOOTER"

Artificial intelligence in the realities of the modern world is in great demand to solve problems of various types and complexities because of the technological progress of mankind. Currently, artificial intelligence (AI) can be used anywhere, for example, for surgery, for automatic driving, etc [1].

AI is even used in computer games of various genres, which is an integral part of the gameplay for most of them, as it gives players a vivid gaming experience [1]. AI is mostly used in the form of bots (computer-controlled units) and as one virtual rival of a real player, for example, in a game of chess. The most popular game genre that used AI was the real-time strategy genre. In this genre, the computer must control a large number of combat units and effectively resist real players, using all its resources and game mechanics. However, AI is now used in other genres [2].

Extensive use of AI can be seen in FPS games (first-person shooter) and Online FPS. The main difference between AI between FPS games and Online FPS games is that in the first case, AI has a pre-determined pattern of behavior when meeting a real player, while in Online FPS AI is constantly learning to confront the real player by analyzing his many previous actions (fig.1).

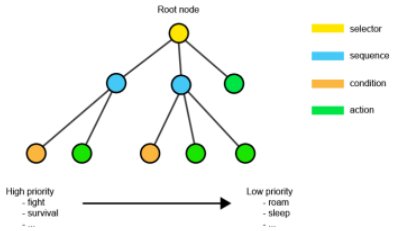

Figure 1. Simplified behavior tree

Prominent examples for comparison are games such as Call of Duty (singleplayer) and CS:GO. For example, in the game CS:GO from Valve, in a match on Faceit (game platform) servers, where two teams of five players compete against each other, there may be a situation where one or more players for some reason disconnected from the game and can't keep playing, then bots come to the rescue. Bots replace team members who have dropped out of the game, and by analyzing the previous game of their opponents, make certain decisions to confront them more effectively [3]. In Call of Duty games, bots have pre-configured templates to confront real players. The player can choose templates of confrontation of bots against themselves in the game settings, ie just choose the complexity of the game.

AI in games of the genre Online FPS has much in common with games of other genres. The main common feature of these genres is that AI analyzes the behavior of the real player and makes the most effective decisions about their next steps against him. For example, the purchase of certain equipment for combat units, if such an opportunity is provided by the game itself. CS:GO gives a certain amount of time before the round to purchase equipment (grenades, weapons, body armor, etc.), and bots, after analyzing the previous actions of a real player, can choose which equipment is best for the current round and how to use this equipment. Bots can communicate with each other, providing different information to each other, and simulate teamwork [3], because, for example, if the AI buys the same equipment for all bots, there will be no effective confrontation against the real player because the player just gets used to AI actions. The main difference between AI in this genre is the orientation in the virtual 3D space because it needs not only to analyze the positioning of bots on any map but also the correct location of the sight and some knowledge from which angle a real player can appear to harm the team. Bots must also analyze and understand when to use grenades, when to move other team members to another point on the map after analyzing all the information for the round, and so on.

In computer games of various genres, including online FPS, the developers reduce the complexity of the AI for a better gaming experience so that the player is not too difficult to resist. To do this, many parameters are introduced for AI, one of which may be, for example, the speed of AI's reaction to the actions of a real player.

References:

1. Everyone is talking about artificial intelligence. Let's explain what it is in simple words. URL: https://cutt.ly/oHNrtXR
2. History of AI Use in Video Game Design. URL: https://cutt.ly/hHNrqrK
3. Bot. URL: https://counterstrike.fandom.com/wiki/Bot

УДК 004.621.396

О.В. Андреєв, к.т.н., доц.
Т.М. Нікітчук, к.т.н., доц.
В.Л. Кушнірук, студент гр. ТР-14
Державний університет «Житомирська політехніка»

РОЗРОБКА ДИСТАНЦІЙНОЇ СИСТЕМИ МОНІТОРИНГУ ЯКОСТІ ПОВІТРЯ У ПРИМІЩЕННІ

Науково-технічний прогрес і зростання промислового виробництва призвели до суттєвого збільшення забруднення довкілля, зокрема і повітря, що сильно впливає на стан здоров'я людини. Тому контроль якості повітря є одним із досить важливих та актуальних завдань у сучасному світі.

Одним з ключових факторів впливу на стан здоров'я студентів в навчальних закладах є дотримання санітарно-гігієнічних показників мікроклімату, а саме температури, вологості повітря, концентрації вуглекислого газу та концентрації легких аероіонів.

При підвищенні температури значно збільшується потовиділення, в наслідок чого здійснюється різке порушення водного-сольового обміну, змінюються інші параметрі крові, в наслідок чого вона згущається, збільшується частота пульсу, збільшується артеріальний тиск.

Негативна дія високої температури збільшується при підвищеній вологості, тому що при цьому погіршується тепловіддача від тіла людини. Це призводить до зміни у обміні речовин, роботі серцево-судинної системи, системі дихання, порушення центральної та периферичної нервових систем.

Суттєві фізіологічні зміни в організмі здійснюються також при холодовому впливу, а саме звуження судин м'язів та шкіри, при цьому зніжується пульс, збільшується об'єм дихання і споживання кисню. Всі ці зміни безумовно відображаються на працездатності людини, концентрації уваги, рівні сприйняття інформації, якості навчання та взагалі можуть призвести до захворювань.

Тому дуже важливим напрямом досліджень є створення інформаційно-цифрового середовища, яке забезпечить вимірювання та контроль мікроклімату в приміщенні, показників стану здоров'я студентів та передачі їх на відстань для можливості контролю за вищезазначеними показниками віддалено.

Система дистанційного моніторингу стану повітря у приміщенні фактично може бути побудована на базі технології Інтернету речей. При цьому взаємодію інтернет-речей з користувачем доцільно організувати через сервер з використанням посередницької платформи даних.

Ця платформа буде здійснювати:

- прийом повідомлень від інтернет-речей та передачу їх користувачам;
- зберігання прийнятої інформації та її обробку;
- забезпечення інтерфейсу користувача з можливістю двостороннього обміну між користувачем та інтернет-річчю.

Метод централізованого сервера також надає надійні засоби зберігання та обробки інформації, дозволяє інтернет - речам використовувати хмарні сервіси.

У роботі пропонується розробка блоку моніторингу мікроклімату, який забезпечує контроль температури та вологості повітря у приміщенні.

Відображення результатів здійснюватиметься на екрані приладу, а також передбачається віддалена передача даних на сервер в форматі HTML в режимі реального часу. Для створення інтернет-речей, які можуть збирати різну інформацію та поширювати її по комунікаційних мережах, ідеально підходять недорогі модулі Wi-Fi ESP32 та ESP8266, а для виміру температури та вологості можуть бути використані датчики типу DHT11/DHT22.

Збирання даних від датчика та передавання контрольованих параметрів на сервер запропоновано здійснювати через пристрій-шлюз на базі мікроконтролера ESP8266, який надає точку доступу до мережі Інтернет.

УДК 004,621.396

Л.В. Карапет, студентка групи ТР-14
О.В. Андреєв, к.т.н., доцент кафедри біомедичної інженерії та телекомунікацій
Державний університет «Житомирська політехніка»

РОЗРОБКА ПРИСТРОЮ ДИСТАНЦІЙНОГО КОНТРОЛЮ ЗА НЕСАНКЦІОНОВАНИМ ПРОНИКНЕННЯМ ДО ПРИМІЩЕННЯ

Для того, щоб захистити свою квартиру або офіс достатньо встановити охоронну сигналізацію. Головна задача такого обладнання – швидке сповіщення власників нерухомості або спеціальної служби про несанкціоноване проникнення до приміщення.

Отже метою роботи є розробка пристрою дистанційного контролю за несанкціонованим проникненням до приміщення з передаванням сигналу про проникнення у хмарний сервіс Telegram. Як чутливий елемент системи сигналізації будемо використовувати піроелектричний інфрачервоний датчик руху (PIR), який дозволяє вловлювати рух. PIR датчики руху по суті складаються з чутливого піроелектричного елемента, який вловлює рівень інфрачервоного випромінювання. PIR датчики відмінно підходять для проектів, у яких необхідно визначати наявність або відсутність людини в межах певного робочого простору.

Система дистанційного контролю за несанкціонованим проникненням до приміщення фактично може бути побудована на базі технології Інтернету речей. Для створення інтернет-речей, які можуть збирати різну інформацію та поширювати її по комунікаційних мережах, ідеально підходять недорогі модулі Wi-Fi ESP32 та ESP8266.

Збирання даних від датчика руху та передавання сигналу тривоги на сервер запропоновано здійснювати через пристрій-шлюз на базі мікроконтролера ESP32, який надає точку доступу до мережі Інтернет.

Telegram Messenger – це хмарний сервіс обміну миттєвими повідомленнями та IP-телефонії, який може бути встановлений у смартфоні або комп'ютері. Після включення системи сигналізації мікроконтролер ESP32 у чат з ім'ям бота надсилає повідомлення про початок роботи "Bot started up", а потім при виявленні руху щоразу надходитиме повідомлення "Motion detected!" (рис. 1).

Рис. 1. Приклад повідомлень системи безпеки

Запровадження такого пристрою допоможе збільшити швидкість реакції власника будівлі на вторгнення та дистанційно наглядати за своєю приватною власністю.

УДК 681.5.08

С.І. Вознюк, студент групи ТР-14
О.Л. Коренівська, к.т.н., доц. каф. біомедичної інженерії та телекомунікацій
Державний університет «Житомирська політехніка»

СИСТЕМА ДИСТАНЦІЙНОГО КЕРУВАННЯ МІКРОКЛІМАТОМ НАВЧАЛЬНИХ АУДИТОРІЙ

Великий вплив на організм людини має мікроклімат у будівлях. До нього прийнято відносити такі фізичні параметри, як температура, відносна вологість, атмосферний тиск, рівень CO_2 у повітрі. Мікроклімат – це поєднання фізичних параметрів, які впливають на обмін теплової енергії людини з навколишнім її середовищем.

Необхідність отримання інформації про поточний стан мікроклімату будівлі виникає при контролі умов праці, виробництва та зберігання продукції в приміщеннях.

Традиційний підхід до моніторингу кліматичних параметрів за допомогою портативних переносних або настінних приладів з необхідністю фіксування показань вручну неефективний, а часто і вкрай скрутний з точки зору витрат часу з боку персоналу. До того ж ручний моніторинг не позбавлений впливу людського фактору.

Сучасні системи управління кліматом являють собою досить складні системи автоматичного регулювання, які здійснюють підтримку параметрів повітря в контрольованих об'ємах в заданих межах на підставі сигналів, що надходять з датчиків температури і вологості. У роботі описана система контролю температури і вологості в приміщенні засобами бездротової технології передачі вимірювальної інформації. Дана система віддаленого моніторингу (рис. 1) заснована на програмно-апаратних засобах середовища ARDUINO та плати ESP32.

Апаратні модулі:

– ESP32;
– DHT-22;
– MQ-135;
– Реле

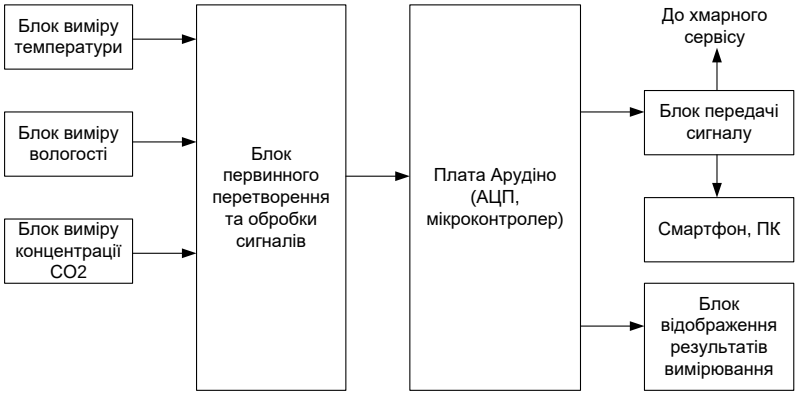

Рис. 1. Структурна схема системи моніторингу параметрів мікроклімату

ESP32 — це серія мікроконтролерів типу «система на кристалі», що мають інтегровані контролери Wi-Fi і Bluetooth (дворежимний, англ. *dual-mode*), низьке енергоспоживання і невисоку ціну. У серії ESP32 використовується мікропроцесор Tensilica Xtensa LX6 в двоядерних та одноядерних варіаціях та включає вбудовані антенні перемикачі, радіочастотний балун, підсилювач потужності, приймач з низьким рівнем шумів, фільтри та модулі керування живленням.

Давач вологості і температури DHT11 використовує таку техніку збору цифрових сигналів і технологію зондування вологи, яка дозволяє забезпечити надійність і стабільність інформації. Його чутливі елементи з'єднані з 8-бітним одночіповим комп'ютером. Кожен датчик цієї моделі є відкалібрований у точній камері калібрування, а калібрувальний коефіцієнт зберігається в типі програми в OTP-пам'яті, коли датчик виявляє, він буде цитувати коефіцієнт з пам'яті.

Датчик MQ-135 відноситься до напівпровідникових приладів. Принцип роботи датчика заснований на зміні опору тонкоплівкового шару діоксиду олова SnO2 при контакті з молекулами газу, що визначається. Чутливий елемент датчика складається з керамічної трубки з покриттям Al2O3 та нанесеного на неї чутливого шару діоксиду олова. Усередині трубки проходить нагрівальний елемент, який нагріває чутливий шар до температури, за якої він починає реагувати на газ, що визначається. Чутливість до різних газів досягається варіюванням складу домішок у чутливому шарі.

УДК 61: 621+004.78.056

Є.В. Онищенко, студентка гр. БІ-21, IV курс
О.Л. Коренівська, к.т.н., доц. каф. біомедичної інженерії та телекомунікацій
Державний університет «Житомирська політехніка»

ПРИЛАД ДЛЯ ЕЛЕКТРОСТИМУЛЯЦІЇ М'ЯЗІВ ЛЮДИНИ

Згідно наукових досліджень встановлено, що малорухливий спосіб життя призводить до появи нових захворювань через порушення обміну енергією між біологічно активними точками. Інколи малорухливість, яка веде до ослаблення і навіть атрофії м'язів, буває вимушеною, вона може бути пов'язана з наявністю захворювань, при яких фізичні навантаження протипоказані або неможливі.

Застосування електростимуляції м'язів в неврології засноване на здатності електричного струму проходити через м'язові волокна, викликаючи в них фізіологічну відповідь у вигляді скорочувальної активності або розслаблення. Особливо це важливо, коли власні нервові імпульси від центральної нервової системи не можуть досягти м'язів в результаті певних причин. Спосіб електростимуляції захищає м'язову тканину від атрофії, покращує її живлення і обмін речовин за рахунок постійної стимулюючої дії електричного струму. Є наукові дані, які свідчать про те, що при пошкодженні м'язів їх регенерація підвищується при зовнішній стимуляції.

Міостимулятор імітує потенціал дії, який виходить від центральної нервової системи. Вірно налаштувавши силу електричного сигналу, можна максимально наблизити такі скорочення до показників, властивих здоровому спортивному навантаженню. А ще рух м'язів гарантовано розганяє кров по судинах, може вплинути на вироблення молочної кислоти, поліпшити еластичність м'язів.

Для підвищення ефективності терапевтичних процедур пропонується розробка структури біотехнічної системи (рис. 1), як реалізує спосіб формування параметрів впливу міоелектростімуляції пацієнта залежно від поточного стану м'язів.

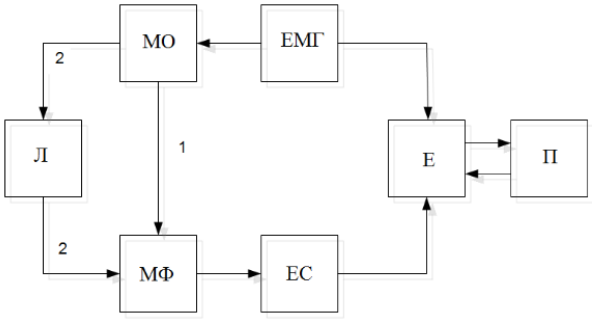

Рис. 1. Структурна схема біотехнічної системи м'язової електростимуляції

де Л – лікар; ЕМГ – модуль реєстрації електроміограми; МО – модуль обробки результатів ЕМГ; ЕС – електростимулятор; МФ – модуль формування параметрів впливу; Е – електроди; П – пацієнт.

Мікропроцесорний електростимулятор (ЕС) формує послідовність електричних імпульсів із заданими параметрами. Електродна система (Е) забезпечує, по-перше, передачу імпульсів на нервові закінчення, що призводить до активного скорочення м'язів, по-друге, реєстрацію сигналів ЕМГ. Модуль (МО) визначає основні параметри ЕМГ, що дозволяє здійснювати автоматичне коригування параметрів стимуляції (коло зворотного зв'язку 1).

В системі передбачена можливість попереднього налаштування, зміни та коригування параметрів стимуляції безпосередньо особою, яка приймає рішення (Л) (коло зворотного зв'язку 2). Додаткове коло зворотного зв'язку необхідно, насамперед, у випадках коли зміна параметрів стимуляції здійснюється внаслідок змін стану пацієнта, що не вимірюється інструментально (почервоніння шкіри, больові відчуття тощо).

Електростимулятор забезпечує стимуляцію струмами прямокутної форми з різними частотами та співвідношенням сигнал-пауза з такими параметрами:

- тривалість імпульсів: 1–5 мс;
- тривалість паузи: 2, 4, 5 мс;
- частота імпульсів: 10, 100, 200 Гц.

Прилад призначений для використання в фізіотерапевтичних кабінетах медичних закладів та побуті для профілактики атрофії м'язів та лікувального впливу при тренуванні та відновлюванні рухової активності м'язів людини уражених внаслідок різних захворювань опорно-рухового апарату та розладів центральної нервової системи.

УДК 004.4

А.О. Степурко, магістр
О.В. Власенко, ст. викладач
С.М. Кравченко, ст. викладач
Державний університет «Житомирська політехніка»

ДЛЯ ЧОГО ПОТРІБНО WEBRTC API

WebRTC (Web Real-Time Communications) – це технологія, яка дозволяє Web-додаткам та сайтам захоплювати та вибірково передавати аудіо та/або відео медіа-потоки, а також обмінюватися довільними даними між браузерами, без обов'язкового використання посередників. Набір стандартів, які включає технологія WebRTC, дозволяє обмінюватися даними та проводити пірингові телеконференції, без необхідності користувачеві встановлювати плагіни або будь-яке інше стороннє програмне забезпечення.

Оскільки WebRTC не вимагає плагінів, фреймворків або програм, все, що вам потрібно, це браузер, сумісний з цією технологією. Для кінцевого користувача програми WebRTC просто працюють прямо з коробки. Ніякого Flash, Silverlight, жодного JavaScript API, лише чисте відео, аудіо та передача даних на будь-якій вебсторінці. Крім того, оскільки WebRTC повністю залежить від браузера, ви отримуєте максимально можливу продуктивність та мінімальну затримку. Наприклад, припустимо, що користувач намагається поділитись файлом. Без WebRTC користувач повинен завантажити цей файл на сервер, а користувач-одержувач повинен завантажити цей файл. З WebRTC ці файли передаються безпосередньо через канал даних WebRTC без серверів або інфраструктури. WebRTC є невід'ємною частиною специфікації HTML5, керованої IETF та W3C. Він відображається у браузері за допомогою JavaScript.

Технологія працює, з'єднуючи два браузери через RTCPeerConnection. По-перше, браузери підключаються через сигналізацію, передаючи протокол сеансу опису (SDP). Ця сигналізація виявляє, де знаходяться два користувачі та як підключитися. Після відкриття RTCPeerConnection між двома браузерами можна передавати відео, аудіо та дані. Для роботи необхідно два веббраузери і спосіб передачі SDP між ними. SDP містить інформацію про ваш комп'ютер, що підтримуються вами аудіокодеки, способи передачі даних між комп'ютерами і доступні на вашому комп'ютері порти, до яких ви можете підключитися.

Найбільш популярним є передача аудіо і відео потоку в режимі реального часу. Коли користувач починаєте аудіо або відеодзвінок WebRTC, технологія має встановити з'єднання з усіма іншими пристроями, які будуть підключені до дзвінка. Перш ніж можна буде встановити з'єднання WebRTC, программа має пройти через ваш брандмауер та NAT. Брандмауери та пристрої NAT працюють, встановлюючи загальнодоступну IP-адресу для комп'ютера користувача, який транслюється у зовнішній світ і маскує приватну IP-адресу. Комп'ютер знає лише вашу приватну IP-адресу. Таким чином, програма WebRTC зв'язується з сервером STUN (Session Traversal Utilities for NAT), щоб отримати загальнодоступну IP-адресу. Таким чином, програма WebRTC може направити вхідне з'єднання на правильну IP-адресу. Як тільки загальнодоступна IP-адреса користувача буде отримана з сервера STUN, WebRTC отримає загальнодоступну IP-адресу для інших пристроїв, які будуть підключатися до дзвінка. Як тільки програма дізнається всі необхідні IP-адреси, вона створює список потенційних конфігурацій підключення, також званих кандидатами ICE (Interactive Connectivity Establishment), і вибирає найефективнішу конфігурацію. Потім програма WebRTC використовує цю конфігурацію підключення для відкриття приватного каналу даних, де всі пристрої, що беруть участь у викликі WebRTC, можуть обмінюватися аудіо та відео в режимі реального часу. А оскільки лише пристрої, що беруть участь у дзвінку, знають конфігурацію з'єднання, з'єднання є приватним і не може бути доступним нікому, хто не бере участь у дзвінку.

Канал даних WebRTC додає ще один унікальний вимір у програмі WebRTC. Передача даних між двома користувачами в сучасному світі браузерів — складний процес із JavaScript, і більшість розробників покладаються на сервер як посередник. WebRTC API каналу даних дозволяє передавати довільні дані по з'єднанню. Це дозволяє широкомасштабний обмін файлами, швидкі розраховані на багато користувачів ігри і навіть програми для віддаленого управління.

Отже, WebRTC API дає можливість розробникам легко створювати одноранговий зв'язок між користувача та обмінюватися даними між ними в режимі реального часу в веб-додатках з великою підтримкою даної технології.

Список використаної літератури:

1. Офіційна документація по WebRTC [Електронний ресурс]. – Режим доступу : https://webrtc.org/getting-started/overview.
2. Що таке WebRTC і чому розробники та компанії полюбляють цю мережу технологію [Електронний ресурс]. – Режим доступу : https://senior.ua/articles/chto-takoe-webrtc-i-pochemu-razrabotchiki-i-kompanii-lyubyat-etu-setevuyu-tehnologiyu.

УДК 004.4

А.О. Степурко, магістр
О.В. Власенко, ст. викладач
С.М. Кравченко, ст. викладач
Державний університет «Житомирська політехніка»

РІЗНИЦЯ МІЖ ПРОТОКОЛАМИ TCP І UDP ТА ЇХ ВИКОРИСТАННЯ

Обчислювальне програмування повне протоколів. Все, що потрібне вашому комп'ютеру, обробляється ними. Більшість завдань навіть мають набір різних протоколів обробки певних частин завдання. Найбільш поширеним прикладом цього є підключення до Інтернету. Багато хто може припустити, що IP або інтернет-протокол є всеосяжним протоколом для обробки інтернет-трафіку та підключень. Однак є безліч різних протоколів, що діють одночасно. У прикладі з комп'ютером, підключеним до Інтернету, є TCP/IP і UDP.

TCP, або протокол управління передачею, є найпоширенішим мережевим протоколом Інтернету. TCP надзвичайно надійний і використовується для всього: від перегляду веб-сторінок (HTTP), надсилання електронних листів (SMTP) та передачі файлів (FTP). Воно використовується в ситуаціях, коли необхідно, щоб усі дані, що надсилаються одним пристроєм, були отримані іншим у цілості та безпеці. Наприклад, коли ви відвідуєте веб-сайт, TCP використовується, щоб гарантувати отримання всього, починаючи з тексту, зображень та коду, необхідного для відображення сторінки. Без цього протоколу зображення або текст може бути відсутнім або надходити в неправильному порядку, що призведе до розриву сторінки.

TCP – це протокол, орієнтований встановлення з'єднання. Це означає, що він встановлює з'єднання між двома пристроями перед передачею даних та підтримує це з'єднання протягом усього процесу передачі.

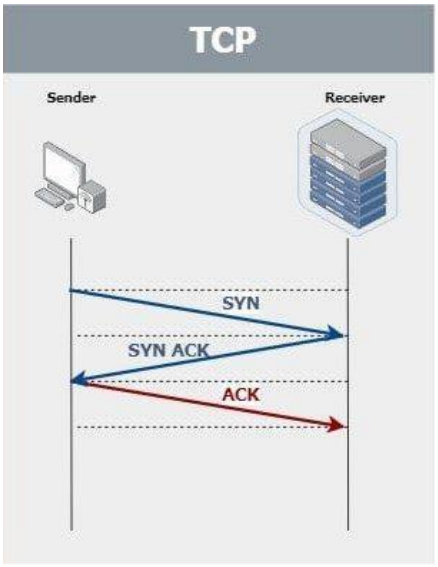

Рис. 1. Робота TCP протоколу.

Наприклад, щоб користувач прочитав повідомлення, його пристрій спочатку повідомлення на сервер під назвою SYN (Synchronize Sequence Number). Після сервер відправив підтверджуюче повідомлення, зване SYN-ACK. Коли пристрій користувача отримав SYN-ACK від серверу, пристрій відправляє назад повідомлення підтвердження ACK, яке встановлює з'єднання. Після встановлення TCP-з'єднання між двома пристроями протокол гарантує передачу всіх даних.

UDP, або протокол дейтаграм, є ще одним з основних протоколів, що складають набір інтернет-протоколів. Цей протокол менш надійний, ніж TCP, але набагато простіший. Його використовують в ситуаціях, коли допустима деяка втрата даних, наприклад, відео/аудіо в реальному часі, або коли швидкість є критичним фактором, наприклад, онлайн-ігри.

Хоча UDP схожий на TCP в тому, що він використовується для надсилання та отримання даних в Інтернеті, є кілька ключових відмінностей. По-перше, UDP це протокол без встановлення з'єднання, що означає, що він не встановлює з'єднання заздалегідь, як це робить TCP з триетапним рукостисканням. Далі UDP не гарантує, що всі дані будуть успішно передані. За допомогою UDP дані відправляються на будь-який пристрій, що прослуховує, але йому все одно, якщо деякі з них будуть втрачені по шляху. Це одна з причин, чому UDP також відомий як протокол «запустив і забув».

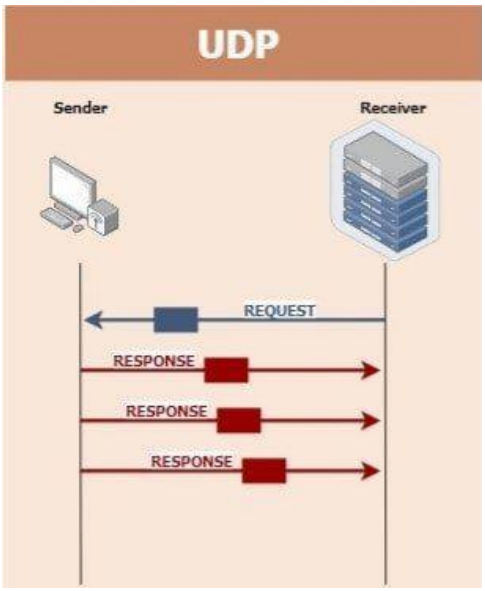

Рис. 2. Робота UDP протоколу.

UDP набагато простіше і не намагається встановити з'єднання між пристроями перед відправкою даних або перевірити, чи всі дані взагалі прибутку. Він просто надсилає дані на будь-який пристрій, який їх запитує, і продовжує робити це доти, доки інший пристрій не відключиться або залишиться даних для відправки.

TCP необхідний у ситуаціях, коли важливо, щоб усі пакети даних надсилалися по порядку та щоб усі пакети надходили. Мережа просто не працювала б без TCP. Він працює повільніше через те, як він встановлює з'єднання, а також через перевірку відсутності пакетів, він все ж таки може працювати блискавично використовуючи буферизацію. Наприклад на майданчиках для перегляду відео / аудіо матеріалів використовується TCP протокол, щоб не втратити частину матеріалу при транслюванні.

UDP – найкращий вибір для живого відео та аудіо або онлайн-ігор, де швидкість важливіша за потенційну втрату даних. Коли користувачі використовують сервіси для створення відео-телефонної зв'язку, відео та аудіо передаються за протоколом UDP. Якщо деякі пакети будуть втрачені на шляху, це буде виглядати як невелика затримка або обрізання відео / аудіо.

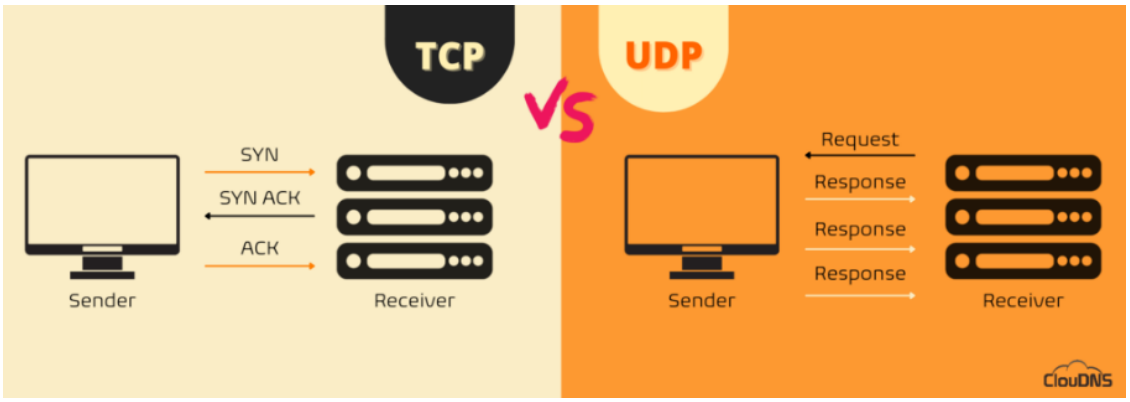

Рис. 3. Відмінність роботи TCP та UDP протоколів.

Отже, різниця між протоколами TCP і UDP укладаються, що TCP протокол не втрачає пакетів, а чекає відповіді на відісланий пакет, а UDP протокол відправляє пакети не чекаючи відповіді, того він більш швидший але може втрачати інформацію. Обидва протоколи використовуються виходячи з сценарію.

Список використаної літератури:

1. Інформація о протоколі TCP [Електронний ресурс]. – Режим доступу : https://networkguru.ru/protokol-transportnogo-urovnia-tcp-chto-nuzhno-znat/.
2. Різниця між TCP і UDP протоколами [Електронний ресурс]. – Режим доступу : https://uk.living-in-belgium.com/difference-between-tcp-and-udp-350.

УДК 004.4

І.В. Ковтонюк, магістр
Г. В. Марчук, ст. викладач
Державний університет «Житомирська політехніка»

CROSS-PLATFORM РОЗРОБКА У ПОРІВНЯННІ З NATIVE

Мобільні програми стали незмінним супутником сьогоднішнього життя. З їхньою допомогою можна не тільки розважатися, здійснювати покупки або замовляти ті чи інші послуги онлайн, але й просувати свій бізнес, збільшувати клієнтську базу, а відтак і множити прибуток.

Вже протягом багатьох років серед розробників ведуться суперечки з приводу цілісності використання крос-платформ розробки для мобільних додатків у порівнянні з нативною розробкою.

Головний принцип, що лежить в основі крос-платформних рішень – поділ коду на дві частини:

- крос-платформну, що живе у віртуальному оточенні та має обмежений доступ до можливостей цільової платформи через спеціальний міст;
- натив, який забезпечує ініціалізацію програми, керує життєвим циклом ключових об'єктів і має повний доступ до системних API.

Приклади нативних додатків представлені на рис. 1.

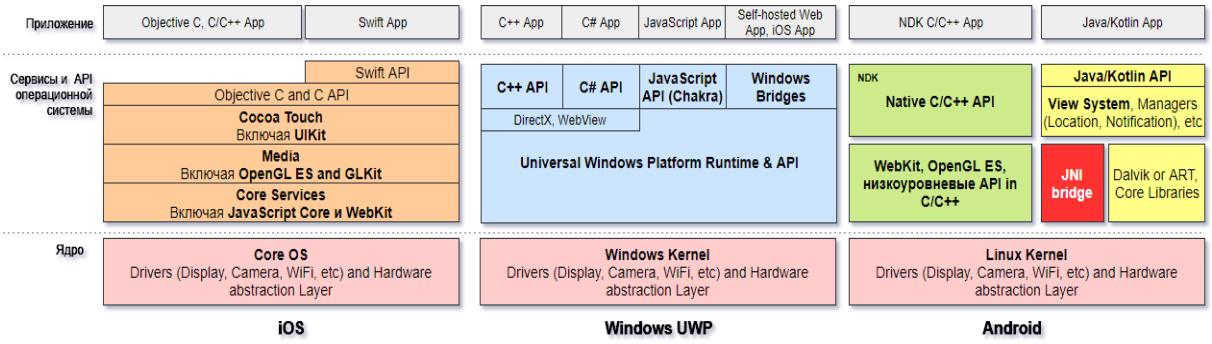

Рис. 1. Нативні додатки [4]

Нативними вони називаються тому, що для їх написання була використана «рідна» для них мова програмування. Наприклад, для Android це Java або відносно молода мова Kotlin, для IOS – це Objective-C та Swift.Додатки інсталюються напряму з магазинів, які належать до конкретної платформи, вони можуть використовувати весь доступний телефону функціонал з вбудованих можливостей, як – камеру, GPS-датчик, акселерометр, компас, список контактів тощо.

Переваги нативних додатків:

- швидкодія та продуктивність;
- захищеність;
- широкий інтерфейс можливостей;
- здатність працювати оффлайн;
- максимальна зручність для користувача

Недоліки нативних додатків:

- тривалість розробки;
- висока вартість розробки;
- необхідність постійно оновлювати додаток у косметичних цілях

Для зв'язування між собою нативного та крос-платформного світів, необхідно використовувати спеціальний функціонал, який називають міст «bridge» саме він буде надавати певний функціонал нашому додатку та обмежувати його роботу, якщо це знадобиться. Саме міст конвертує команди та викликі API та бібліотек і при великому навантаженні його продуктивність може зменшуватись.

Крос-платформні програми пишуться відразу для декількох платформ однією мовою, відмінною від нативної. Який код може працювати на різних пристроях? Тут також є два підходи:

- Перший полягає в тому, що на етапі підготовки до публікації він перетворюється на нативний для певної платформи за допомогою транспілера. Фактично одна крос-платформна мова програмування «перекладається» на іншу.
- Другий полягає у тому, що весь код потрапляє в спеціальну обгортку, яка виконуючи код передає команди напряму до нативних функцій системи.

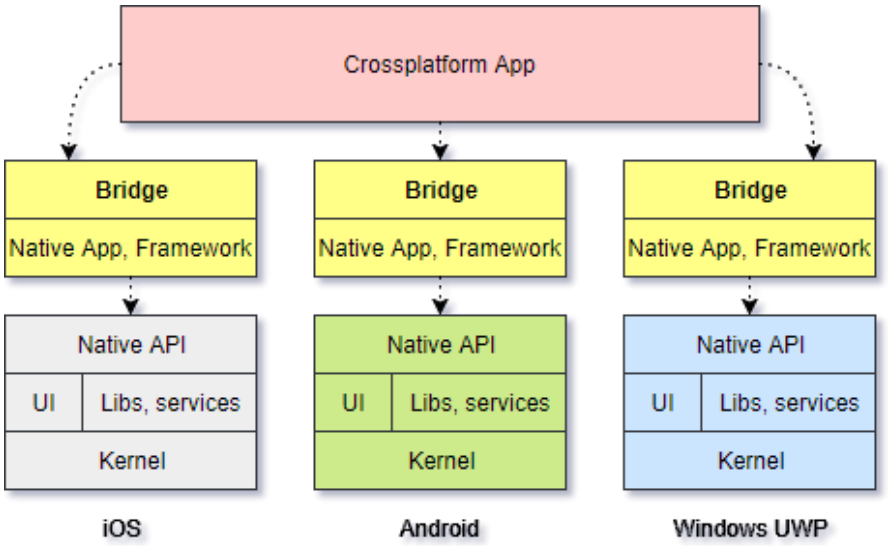

Рис. 2. Крос-платформний додаток[4]

Передбачається, що більша частина такого коду може переноситься між платформами – очевидно, що, наприклад, логіка здійснення покупок, збереження товару в кошик, прорахунок маршруту таксі, написання повідомлення в месенджер не змінюється залежно від того, Android у клієнта або iOS. Потрібно лише доопрацювати UI та UX для платформ, але зараз, у певних межах, навіть це можна об'єднати – наприклад, меню-гамбургер активно використовується як на Android, так і на iOS. Так що навіть внесення виправлення в інтерфейс для того, щоб програма відповідала духу і букві потрібної платформи – питання бажання, необхідної швидкості та якості розробки.

Переваги:

– Значно менша тривалість розробки та затрати на розробку
– При написанні можна створити свою бібліотеку компонентів, яку потім можна буде використати у інших проєктах.

Недоліки:

– проблеми у реалізації складних функцій чи можливі проблеми роботи навіть із простими процедурами через помилки самих фреймворків розробки. Крос-платформне середовище лише транслює запити до системних викликів та інтерфейсів у розуміється нею, системою, формат, і тому на цьому етапі можливі як складнощі з розумінням, так і виникнення помилок усередині самого фреймворку;
– швидкість роботи.

Оскільки крос-платформне середовище є «надбудовою» над кодом (не завжди, але в певних ситуаціях), у ньому виникають свої затримки та паузи у відпрацюванні дій користувача та виведенні на екран результатів. Це було особливо помітно кілька років тому на смартфонах, мало потужніших щодо сьогоднішніх, проте зараз, зі зростанням продуктивності мобільних пристроїв, це вже можна знехтувати.

Можна зробити висновки: ці два методи практично є дзеркальним відображенням одна одної – те, що є перевагами у нативної розробки додатків, недоліки у крос-платформної, і навпаки. Отже, все залежить від завдання. Якщо потрібно написати прототип програми для декількох платформ або мобільну версію сайту, то можна подивитися у бік крос-платформних фреймворків.

З іншого боку, універсальність крос-платформних додатків має чимось компенсуватися. Десь спливає «нерідний» елемент інтерфейсу, десь гірше відбувається взаємодія із системою, десь просідає швидкість роботи тощо. Незважаючи на те, що нативна розробка вимагає більше ресурсів, багато компаній віддають перевагу саме її, тому що на виході виходить більш стабільний продукт.

Список використаної літератури:

1. Офіційна документація Adroid Developer [Електронний ресурс]. – Режим доступу : https://developer.android.com.
2. Офіційна документація Flutter [Електронний ресурс]. – Режим доступу : https://flutter.dev/.
3. Офіційна документація React Native [Електронний ресурс]. – Режим доступу : https://reactnative.dev/.
4. Нативно чи ні? Чотири міфи про крос-платформну розробку [Електронний ресурс]. – Режим доступу : https://lingvabona.

УДК 621.385.69

М.О. Михаленко, студент гр. ТР-14
В.Б. Бенедицький, ст. викладач кафедри БІтаТ
Державний університет «Житомирська політехніка»

СИСТЕМА ВИМІРЮВАННЯ ПІКОВОЇ ПОТУЖНОСТІ ЕФІРНОГО ТЕЛЕБАЧЕННЯ СТАНДАРТУ DVB-T2

Цифрове радіомовлення – це технологія радіомовлення, яка базується на передачі аудіовізуальної медіа інформації за допомогою потоків бітів. Радіомовний сигнал складається з відео- і аудіо даних. Крім того, передаються описові та технічні метадані для ідентифікації програм та вибору конфігурації приймача (наприклад, відомості про радіомовну станцію, застосовувані системи стиснення відео- та аудіоданих, розташування звукових каналів або керуючих даних для інтерактивних функцій, формати кадру та багато інших відомостей).

Зараз на ринку існують системи вимірювання пікової потужності ефірного телебачення стандарту DVB-T2. Основним їх недоліком є велика собівартість та низькій рівень якості, при мінімальному функціоналу. Після ознайомлення з методами відстеження рівня цифрового сигналу типу DVB-T2 було прийнято рішення побудувати дану систему аналізу пікової потужності на мікроконтролері ADUC845 та детекторі ADL5502.

При роботі з цифровими сигналами важливо враховувати швидкість передачі даних, вид сигналу, дальність передачі, завадозахищеність та точність. Формат DVB-T2 є покращеним та функціонально розширеним послідовником формату DVB-T. DVB-T2 принципово відрізняється як архітектурою системного рівня (MAC-рівня), так і особливостями фізичного рівня.

У DVB-T2 використовується OFDM-модуляція з великою кількістю піднесучих, що забезпечує стійкий сигнал. Подібно DVB-T, DVB-T2 передбачає велику кількість різних режимів, це робить DVB-T2 дуже гнучким стандартом. Для виконання корекції помилок в DVB-T2 застосовується таке ж кодування, яке було вибрано для DVB-S2. Поєднання кодування з низькою щільністю перевірок на парність (LDPC) і кодування Боуза-Чоудхурі-Хоквінгема (BCH) забезпечує дуже стійкий сигнал і чудову якість в умовах з високим рівнем шумів і перешкод, структурна схема принципу роботи сигналу зображена на рис. 1.

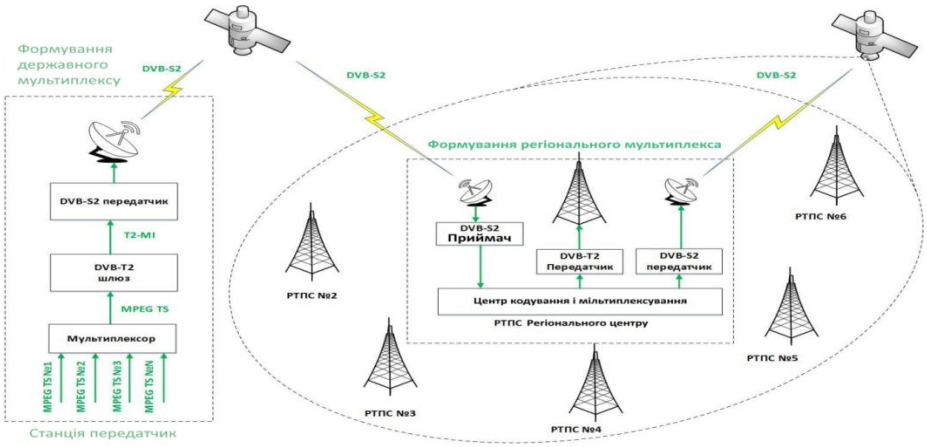

Рис.1. Структурна схема цифрового радіомовлення DVB-T2

ADL5502 являє собою комбінацію детектора потужності, що реагує на середнє (середньоквадратичне) значення сигналу і детектора огинання, призначеного для точного визначення хрест-фактора модульованих сигналів. Даний компонент може бути використаний у сигнальному тракті високочастотних передавачів і приймачів на частотах від 150 кГц до 6000 МГц при ширині смуги огинання більше 10 МГц. Працюючи від однієї напруги живлення в діапазоні від 2,5 до 3,3 В, детектор споживає менше 3 мА.

Основними перевагами запропонованої системи над існуючими є :

- низька собівартість кінцевих пристроїв;
- швидкодія (в порівнянні з аналогами на ринку);
- діапазони частот;
- відкритий стандарт;
- система буде стійка до шумів і перешкод.

Проведено дослідження системи вимірювання пікової потужності ефірного телебачення стандарту DVB-T2. Розроблено систему для дослідження рівня сигналу в конкретному діапазоні роботи відповідного стандарту мовлення ефірного телебачення.

УДК 004.056.53

В.С. Харчук, студент гр.ТР-14,
В.Б. Бенедицький, ст. викладач кафедри БІтаТ
Державний університет «Житомирська політехніка»

СИСТЕМА IP-ВІДЕОСПОСТЕРЕЖЕННЯ ДЛЯ ЗАБЕЗПЕЧЕННЯ КОНТРОЛЮ ПРАВОПОРЯДКУ

З розвитком науки і техніки життя людини все більше полегшується, але поряд із появою нових технологій йдуть не лише позитивні зміни. Завжди є ризик того, що нові технології будуть використанні проти безпеки людей і тому ми вважаємо, що поряд із модернізацією і видозміненням способів вчинення злочинів, повинна йти обов'язкова розробка та впровадження нових технологій для протидії злочинності. Одним із гострих питань розслідування злочинів є швидке реагування на вчинений злочин і затримання правопорушника по гарячих слідах, але це не завжди вдається в виду того, що дуже часто сам факт вчинення злочину виявляється значно пізніше його фактичного вчинення. І задля покращення реагування правоохоронних органів на злочини слід звернути увагу на системи відеоспостереження. Інформація, отримана з камер відеоспостереження, часто стає доказом при розслідуванні кримінальних правопорушень. Варто приділити увагу відеоспостереженню, що працює в «реальному часі».

Відеоспостереження – це невід'ємна частина сучасних систем безпеки. Без камер відеоспостереження важко собі уявити надійну систему безпеки.

Керування відеокамерами і відеопотоками стало значно легше. Спектр підтримуваних сучасних функцій відеоспостереження постійно розширюється. На ринку є широкий вибір програмного забезпечення для самих різних систем відеоспостереження, починаючи від невеликих систем, які нараховують декілька відеокамер встановлених в магазинах, і закінчуючи великими системами, в складі яких входить сотні відеокамер, встановлених зазвичай на декількох об'єктах, географічно віддалених один від одного.

Головні відмінності інтелектуальної відеокамери від звичайної перебувають у двох аспектах. Перший в архітектурі камери. Інтелектуальна камера зазвичай включає у себе спеціальний вузол обробки зображень, до складу якого входять один або декілька мікропроцесорів для виконання інтелектуальних алгоритмів обробки інформації, орієнтованих на конкретне спеціальне програмне забезпечення.

Основне завдання такого блоку є не тільки покращення зображення отриманих кадрів, а і у вилучені інформації. Апаратна частина звичайних камер простіше та у більшості своїй орієнтована на покращення якості знімків сцени. Другий аспект – в тієї інформації, яку видає та чи інша камера. Інтелектуальна відеокамера орієнтована на отримання та передачу інформації (метадані), яка відокремлюється від зображень сцени та у подальшому використовується автоматизованою системою.

Система може ідентифікувати та фіксувати викрадені автомобілі, розпізнавати номер, марку, модель, колір автомобіля, навіть машину, на якій встановлено номер іншого авто. Може реагувати на нетипові рухи транспорту – наприклад проїзд на червоне світло або виїзд на зустрічну смугу. Окрім зазначеного, ця система може розпізнавати обличчя навіть якщо людина спробує змінити зовнішність, наприклад відростивши вуса або надівши окуляри.

У розвинених країнах з подібними системами вдається вдало виявляти злочинців яким тривалий час вдається переховуватись від правоохоронних органів. Яскравим прикладом ефективності роботи систем відеоспостереження є розпізнавання та затримка братів Царнаєвих, які підозрюються в організації вибухів на фінішній лінії бостонського марафону.

Також можливий аналіз вже отриманих відеозаписів з метою встановлення місця знаходження особи в певний проміжок часу. Новітні камери відеоспостереження фіксують яскраві спалахи або гучні звуки, вибухи, постріли, удари та миттєво сповіщає поліцію.

Слід також звернути увагу на те, що впровадження таких технологій повинно розпочатись перш за все у розроблені програмного забезпечення та механізмів модернізації вже існуючих відеокамер встановлених в магазинах, банкоматах тощо.

Метою роботи є розробка системи відеоспостереження анонімної фірми, яка призначена для забезпечення контролю правопорядку зовнішньої території навколо об'єкту.

Основними проблемами реалізації цього проекту ми вбачаємо у високій вартості обладнання, але ніякі матеріальні витрати не зрівняються з тим підвищенням рівня безпеки громадян, який ми отримаємо в результаті.

Тож, з огляду на все вищесказане вважаємо за необхідність впровадження сучасних передових технологій у роботу поліцейських з метою полегшення виявлення та розслідування злочинів, а також забезпечення безпеки людей та громадян.

УДК 004

І.Д. Лімінович, магістр, гр. ІПЗм-21-1, ФІКТ
Д.Ю. Лисогор, аспірант, ФІКТ
Т.М. Локтікова, ст. викладач кафедри ІПЗ, ФІКТ
Державний університет «Житомирська політехніка»

ПРОГРАМНИЙ КОМПЛЕКС ДЛЯ АНАЛІЗУ СТАТИСТИКИ ФУТБОЛЬНИХ МАТЧІВ ТА ПРОГНОЗУВАННЯ РЕЗУЛЬТАТІВ НА ОСНОВІ МАШИННОГО НАВЧАННЯ

У наш час усі сфери людського життя описуються у вигляді статистики. Спорт є однією з найпоширеніших розваг, тому статистика виступів спортсменів, результати змагань та інші дані цікавлять глядачів звідусіль. Футбол, як найпопулярніший вид спорт, у тому числі. На основі статистики здійснюються передбачення на окремі матчі або, навіть, футбольні сезони. Такі прогнози можуть виконуватися як людиною, так і автоматизовано, за допомогою комп'ютера.

Прогнози, зроблені людиною, мають свої переваги та недоліки. Перевагою є те, що людина окрім цифр бачить показники, які комп'ютер може не враховувати. Наприклад, атмосферу в команді та фізичну форму окремих гравців, які можуть створювати різницю на футбольному полі. Проте, людина може здійснювати прогноз, керуючись емоціями й особистими очікуванням від матчу, що безсумнівно є недоліком.

Автоматизовані комп'ютерні прогнози постійно розвиваються та стають все точнішими, враховуючи більшу кількість факторів із кожною новою системою. Це тісно пов'язано і з розвитком футбольної статистики. З'являються нові показники, які дозволяють підвищити точність оцінки як команди, так і окремих гравців.

Останніми роками було створено декілька автоматизованих комп'ютерних систем, які передбачали результати різних футбольних сезонів. Зокрема, було оглянуто та проаналізовано систему аналізу від BT Sport, «суперкомп'ютер» talkSPORT і «суперкомп'ютер» Mirror Football. Однією з найкращих можна вважати систему, яку в 2020 році представила британська радіокомпанія talkSPORT. Система, названа «суперкомп'ютером», зробила прогноз на сезон Англійської Прем'єр Ліги (АПЛ) 2020/2021. Було передбачено, що перше місце у лізі займе Манчестер Сіті, другим фінішує Ліверпуль, а четвірку лідерів замкнуть Челсі та Манчестер Юнайтед відповідно. Порівняємо цей прогноз з реальним результатом турніру (рис. 1).

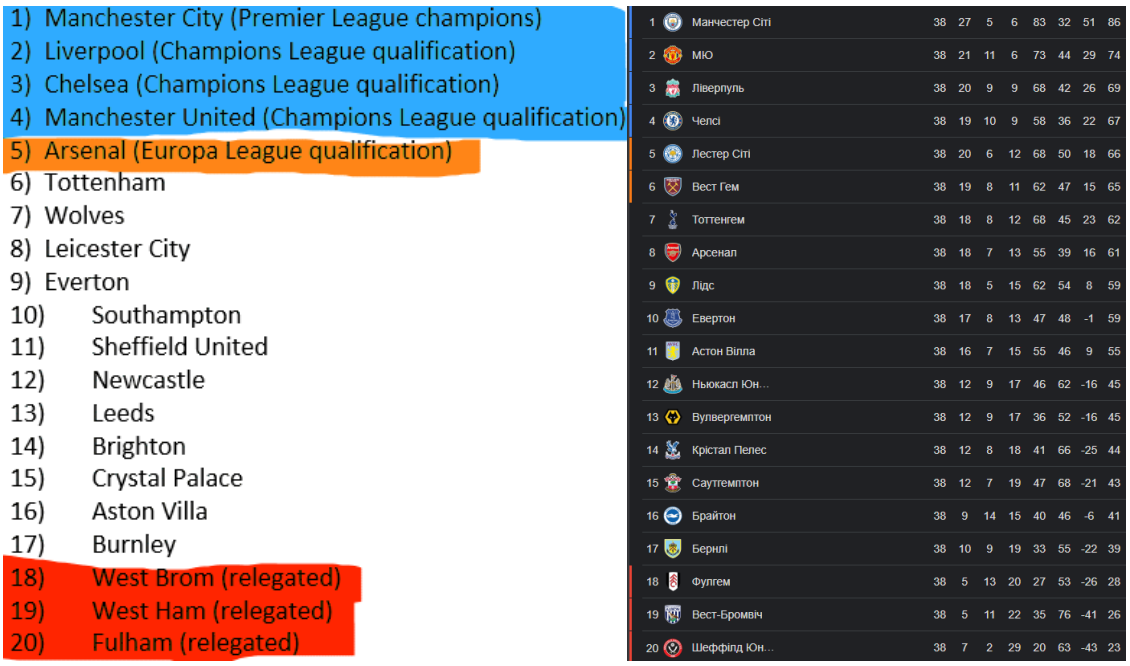

Рис. 1. Прогнозована (зліва) та реальна (справа) таблиці АПЛ 2020 / 2021

Як бачимо, чемпіона країни було вгадано вірно. Загалом, якщо не зважати на точне розташування команд, першу четвірку турнірної таблиці також було передбачено правильно, як і дві з трьох команд, які покидають турнір. Проте мають місце й такі грубі неточності, як передбачення вильоту для Вест Гему, який в результаті зайняв досить високе 6 місце.

На сьогодні розроблено велику кількість додатків для прогнозування результатів футбольних матчів на основі статистики. Найбільш поширеними є Bet-Plus, FootBet, FlashScore, Robo-Win. Було проведено аналіз вищезгаданих додатків та виділено їх переваги та недоліки (табл. 1).

Таблиця 1

Порівняльна характеристика додатків для прогнозування результатів футбольних матчів

	Bet-Plus	FootBet	FlashScore	Robo-Win
Наявність власних алгоритмів	+	+	-	+
Кросплатформенність	-	-	+	-
Зручний інтерфейс	-	+	+	+
Заявлена точність прогнозів	85 %	70 %	-	83 %
Доступність	-	+	+	-
Мультимовність	-	-	+	+
Можливість налаштування даних для аналізу	+	-	-	-
Наявність детальної статистики команд, гравців, турнірів, доступної для перегляду	-	-	+	-
Використання машинного навчання для аналізу даних та прогнозування результатів матів	-	-	-	-

Порівнявши існуючі додатки для передбачення результатів футбольних матчів, можна оцінити точність прогнозів, які вони здійснюють, та побачити, що жоден з них не використовує машинне навчання в своїй роботі.

Для розробки пропонованої системи аналізу було обрано метод контрольованого навчання. Контрольоване навчання – це задання вивчення функції, яка перетворює вхідні дані у вихідні на основі прикладів пар «вхід–вихід». У нашому випадку потрібно передбачити категорію результатів (перемога вдома / нічия / перемога на виїзді) або кількість голів, забитих командою (постійну кількість). Це й зумовило вибір контрольованого методу машинного навчання.

Було розглянуто різні методи аналізу футбольної статистики, а саме: система рейтингів, метод експертних оцінок, метод послідовних порівнянь, метод парних порівнянь, залежний від часу ланцюг Маркова Монте-Карло та метод VAEP.

У системі використано VAEP (Valuing Actions by Estimating Probabilities) метрику. Ця метрика побудована на моделі машинного навчання, яка оцінює кожну дію футболіста на полі, обчислюючи те, яким чином змінилася би можливість забити і пропустити гол в результаті певної дії. Якщо стисло, то оцінка дії гравця +0,05 свідчить про те, що в результаті тактико-технічної дії гравця ймовірність забити гол збільшилася на 0,05. Відповідно, оцінка -0,05 означає, що відповідна дія збільшує шанси суперника забити гол на цей же коефіцієнт. На підставі таких оцінок визначається рейтинг футболістів VAEP. У залежності від середнього рейтингу футболістів можна розрахувати рейтинг команди та на основі цих даних виконувати прогноз на результат матчу. VAEP для кожної конкретної дії визначається як сума атакуючих та оборонних дій. Нижче наводиться формула визначення VAEP дії.

$$V(a_i, x) = \Delta P_{scores}(a_i, x) + (-\Delta P_{concedes}(a_i, x)),$$

$$\Delta P_{scores}(a_i, x) = P_{scores}(S_i, x) - P_{scores}(S_{i-1}, x),$$

$$\Delta P_{concedes}(a_i, x) = P_{concedes}(S_i, x) - P_{concedes}(S_{i-1}, x),$$

де $V(a_i, x)$ – VAEP для дії a гравця x,

$\Delta P_{scores}(a_i, x)$ – зміна вірогідності забити гол в результаті дії a гравця команди x,

$\Delta P_{concedes}(a_i, x)$ – зміна вірогідності пропустити гол в результаті дії a гравця команди x,

$P_{scores}(S_i, x)$ – вірогідність забити гол командою x за 10 наступних дій, залежно від поточного стану гри (СГ) S,

$P_{scores}(S_{i-1}, x)$ – вірогідність забити гол командою x за 10 наступних дій, відносно попереднього СГ,

$P_{concedes}(S_i, x)$ – вірогідність пропустити гол командою x за 10 наступних дій, залежно від поточного СГ,

$P_{concedes}(S_{i-1}, x)$ – вірогідність пропустити гол командою x за 10 наступних дій, відносно попереднього СГ.

Було розроблено комп'ютерну програму, яка врахувала відзначені недоліки як людського, так і комп'ютерного прогнозів.

Для зручної візуалізації даних також було розроблено сайт, який враховує всі сучасні вимоги до інтернет ресурсів, а саме мультимовність, адаптивність тощо.

УДК 004.8

В.О. Юрченко, магістр, гр. ІПЗм-21-1, ФІКТ
Н.О. Кушнір, асистент кафедри ІПЗ, ФІКТ
Т.М. Локтікова, ст. викладач кафедри ІПЗ, ФІКТ
Державний університет «Житомирська політехніка»

ШТУЧНІ НЕЙРОННІ МЕРЕЖІ В ЗАДАЧАХ АНАЛІЗУ ТА КЛАСИФІКАЦІЇ ЗОБРАЖЕНЬ

Штучні нейронні мережі (ШНМ) – один із перспективних напрямів у розробці штучного інтелекту, які з кожним роком знаходить все більше галузей застосування. За їх допомогою можна ефективно вирішувати низку різноманітних задач, наприклад: класифікація сигналів, розпізнавання об'єктів, оцінювання та прогнозування даних, та, зокрема, задач аналізу та класифікації зображень. У таких задачах потрібно оброблювати велику кількість даних, через що нейронні мережі досить часто складаються з великої кількості нейронів та шарів. Це зумовлює дві проблеми: по-перше, вибору оптимальної моделі нейронної мережі та, по-друге, побудування ефективного алгоритму її навчання.

Штучні нейронні мережі – це обчислювальні математичні моделі, які дозволяють із сукупності вхідних даних отримати необхідні вихідні дані. Вони імітують біологічні процеси, що відбуваються в нервовій системі людини. Ключовими елементами ШНМ є штучні нейрони. У класичному представленні вони складаються зі вхідних сигналів, вагових коефіцієнтів, функції активації та вихідного сигналу.

Функція активації обчислює вихідний сигнал штучного нейрона в залежності від вхідних сигналів, які промасштабовано згідно їх вагових коефіцієнтів. Вибір функції активації залежить від необхідних вихідного сигналу та швидкодії, а також визначається вирішуваною задачею. Прикладом найпростішої активаційної функції є функція Гевісайда, яка за від'ємних вхідних значень дорівнює 0, за додатних – 1. Частіше використовується сигмоїдальна функція, яка є нелінійною та аналоговою і вдало підходить до задач класифікації об'єктів зображень. Також, досить поширеною є активаційна функція «ReLU» (rectified linear unit), яка повертає вхідне значення у випадках, якщо воно додатнє і 0 – якщо від'ємне.

Існує велика кількість варіантів побудови штучних нейронних мереж. Вони відрізняються структурами – моделями зв'язків нейронів. Розрізняють ієрархічні, рекурентні та конкурентні структури. Загалом, усі моделі штучних нейронних мереж побудовані подібним чином. Нейрони розподіляються в мережі по шарам. Спочатку інформація надходить на нейрони вхідного шару. Вони передають її далі – до нейронів так званого прихованого шару. У прихованих шарах здійснюється основна обробка даних, після чого інформація надходить в останній шар – вихідний. Кількість нейронів та прихованих шарів обираються в залежності від конкретної задачі, яку вирішує нейронна мережа, обсягу даних та доступних обчислюваних ресурсів. Першою штучною нейронною мережею вважають перцептрон Розенблата, основою якого є модель роботи мозку при розпізнаванні оптичних образів [1]. Структурно – це проста рефлекторна мережа. За сучасною термінологією така ШНМ належить до одношарових із ієрархічною структурою. При побудові нейронної мережі важливе значення має її навчання. Чим більшою буде кількість даних, використовуваних при навчанні, тим ефективнішим буде його результат. Дані можливо отримати ручним або автоматичним методом. Вручну зібрані дані хоч і є точнішими, але, враховуючи потрібну їх кількість для якісного навчання ШНМ, зазвичай являють собою непосильну задачу. Частіше використовують автоматичний збір даних. Досить розповсюдженою практикою є створення іншої ШНМ, яка підготовлюватиме дані та «змагатиметься» з першою. Правильний збір даних – це одна з найскладніших та найоб'ємніших робіт для реалізації навчання нейронної мережі. Існують три основних підходи до навчання нейронної мережі: навчання зі вчителем, навчання без вчителя та навчання з підкріпленням. При навчанні зі вчителем потрібно заздалегідь підготувати вибірку даних для навчання із множини пар, кожна з яких складається із даних, які надходитимуть у вхідний шар ШНМ, та ідеального значення для вихідного шару – «правильної відповіді». Таке навчання спрямоване на досягнення такого стану нейронної мережі, щоби за заданих вхідних даних максимально наблизитися до ідеальних вихідних. Для досягнення мети при навчанні без вчителя необхідно постійно модифікувати внутрішній стан нейронної мережі, тобто вагові коефіцієнти, згідно оцінки вхідних та набутих у ході навчання даних. Бажані значення порівнюються з поточними та виконується корекція за допомогою зворотного зв'язку. При навчанні з підкріпленням нейронній мережі не вказується точного значення бажаного виходу, але після отримання цього виходу їй виставляється оцінка – відповідний коефіцієнт відпрацювання ШНМ. Модель нейронної мережі, її шари, активаційні функції, алгоритм навчання потрібно обирати згідно поставленої задачі. Для побудови пропонованої нейронної мережі було обрано класичну задачу – класифікацію об'єктів на зображенні. Це зумовлено тим, що вже існує вдалий набір даних для навчання. Цей набір складається з 12500 зображень котів та такої ж кількості зображень собак [2]. На виході ШНМ визначить, кішка чи собака в завантаженому на її вході зображенні. Зважаючи на формат вхідних даних (масив значень пікселів), використовувати традиційні повнозв'язні нейронні мережі недоцільно через необхідність величезної кількості нейронів вхідного шару. Найкращим вибором буде згорткова нейронна мережа, яка саме завдяки згортці дозволяє зменшити кількість інформації, що зберігається у пам'яті, а також ієрархічно виділити та агрегувати ознаки вхідних даних. Завдяки цьому збільшується

обчислювальна потужність нейронної мережі та здатність моделювати більш складні залежності. Згорткові нейронні мережі – це ШНМ такої архітектури, яка побудована на основі багатошарового перцептрону, модифікованого таким чином, аби підготовка вхідних даних була мінімальною. Такі нейронні мережі найчастіше застосовуються для розпізнавання та класифікації об'єктів зображень, у галузі комп'ютерного зору. Створення згорткової ШНМ спонукалось біологічним процесом з'єднання нейронів зорової кори тварин. Нейрони кори головного мозку реагують на вхідний сигнал лише в області свого зорового поля, яке має назву рецептивного поля. Всі рецептивні поля можуть перекриватися один одним, але в результаті складаються так, щоби покрити всю область зорового поля. За такого підходу зображення оброблятимуться набагато швидше порівняно з класичними багатошаровими перцептронами. При цьому загальна структура у них схожа. Згорткова нейронна мережа також складається з шарів входу, виходу та декількох прихованих шарів, але в згорткових ШНМ приховані шари включають згорткові, агрегувальні, повнозв'язні та шари нормалізації.

У згортковій нейронній мережі кожен шар відповідає певній властивості зображення. У перших шарах містяться основні ознаки: контури, грані. Після їх обробки можливо розпізнати текстури, частини об'єктів. Вихідні шари міститимуть результат класифікації зображення або виокремлений об'єкт чи певна властивість зображення. Для розглядуваної задачі це буде результат класифікації об'єкту зображення: якщо обчислене вихідним нейроном значення є ближчим до 0, то нейронна мережа вирішила, що об'єктом зображення є кіт, інакше, якщо це значення є ближчим до 1, то – собака.

Для побудови пропонованої нейронної мережі було обрано «TensorFlow». Це – бібліотека з відкритим кодом, яка призначена для побудови та навчання нейронних мереж, що розроблена, розвивається та підтримується компанією «Google» [3]. Для зручності розробки ШНМ, додатково було використано високорівневий API «Keras». Як середовище розробки було обрано додаток «Google Colaboratory». Цей вибір було зумовлено тим, що він надає можливість писати та компілювати розроблюваний код блоками напряму у веб-переглядачі без попередніх налаштувань, завантажень бібліотек та синхронізації їх версій. Недоліком додатка можна вважати те, що код виконується на віддалених серверах «Google», а це, в свою чергу, дається взнаки на швидкодії, яка могла би бути вищою при виконанні коду на локальному комп'ютері. Однак використання додатку дозволяє швидко побудувати, налаштувати та навчити нейронну мережу, а завдяки застосуванню API «Keras» перенести код в подальшому на локальний комп'ютер буде не складно. Спершу потрібно підготувати набір зображень для навчання ШНМ [2]. Для кожного зображення було встановлено розміри до 200 пікселів у висоту, таку ж кількість в ширину, без збереження пропорцій. З підготовленого набору зображень 75 % були виділені для навчання нейронної мережі, решта – для її тестування. Також, для передачі до вхідного шару ШНМ, зображення були перетворені в масив значень від 0 до 1.

Для визначення загальних властивостей зображень першими шарами нейронної мережі було обрано 3 блоки, які складаються відповідно з 32, 64 та 128 згорткових шарів розмірами 3 на 3 пікселя та одного агрегувального шару. Наступним є шар вирівнювання. Далі, для визначення ознак, притаманних саме котам чи собакам, було побудовано 128 шарів звичайних повнозв'язних нейронів. Вихідний шар – один, який являє собою повнозв'язний нейрон. Пороговою активаційною функцією для всіх нейронів, окрім вихідного, було обрано вищезгадувану функцію «ReLU». Це дозволяє витрачати якомога менше ресурсів та не обраховувати значення, менші 0. Активаційною функцією вихідного шару є сигмоїдальна. Схематична модель побудованої нейронної мережі представлена на рис. 1.

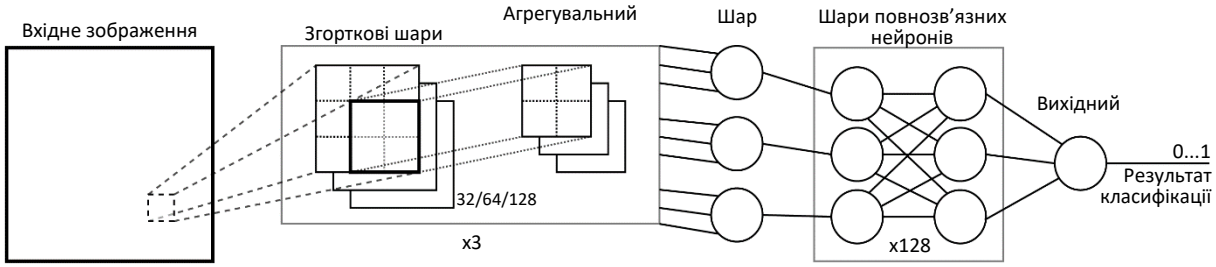

Рис. 1. Схематична модель побудованої згорткової ШНМ для класифікації об'єктів зображень

Навчання нейронної мережі проходило в 20 епох. Точність класифікації об'єктів зображень в останню епоху перевищила 87 %.

Список використаної літератури:

1. Rosenblatt F. The perceptron: a probabilistic model for information storage and organization in the brain / Frank Rosenblatt // Psychological Review. – 1958. – № 65.6. – С. 386–408.

2. Kaggle Cats and Dogs Dataset // Microsoft [Електронний ресурс]. – Режим доступу : https://www.microsoft.com/en-us/download/details.aspx?id=54765.

3. TensorFlow // Google [Електронний ресурс]. – Режим доступу : https://www.tensorflow.org/.

УДК 004

В.О. Хребтань, студент IV курсу
М.С. Граф, PhD
Державний університет «Житомирська політехніка»

АНАЛІЗ НЕОБХІДНОСТІ СТВОРЕННЯ ВЕБ-РЕСУРСУ КІБЕРСПОРТИВНИХ ЗМАГАНЬ

Зміна світогляду та способу існування сучасної людини, зокрема автоматизація та комп'ютерізація різних сторін життя, більш глибоке впровадження ІТ-технологій в побут пересічного мешканця та розвиток ІТ-сфери самої по собі, зумовлюють зростання популярності кіберспорту в світі.

За останні п'ять років кіберспортивна аудиторія зросла з 270 до 495 млн. глядачів, До того ж у 2021 році в Азії налічувалося близько 1,48 мільярда геймерів, а Європа посіла друге місце з ігровою аудиторією 715 мільйонів. Загалом у світі налічується 3,24 мільярда геймерів. Кіберспортивна спільнота України зростає з року в рік, чому в великій мірі сприяло офіційне визнання кіберспорту та надання 21 липня 2021 року створеній в 2017 році в Дніпрі Федерації кіберспорту України (Ukrainian Esport Federation, UESF) національного статусу.

Досягнення кіберспортсменів України, а саме: в далекому 2002 році кіберспорт України отримав першу престижну міжнародну нагороду – бронзову медаль чемпіонату світу з кіберспорту в парній дисципліні Quake 3, через два роки Роман Веренко завоював ще одну бронзу WCG в дисципліні Unreal Tournament, третью бронзову нагороду WCG для України виборов Михайло Новопашин в дисципліні WarCraft 3 в 2005 році, золота медаль з'явилася в 2007 році, коли Михайло Новопашин та Олег Хмара на чемпіонаті Європи отримали перше місце в дисциплінах WarCraft 3 і FIFA, а також третє місце київської команди A-Gaming на WCG 2007 в дисципліні CS:1.6; золото Михайла Новопашина в WarCraft 3 і серебро Олега Хмари в FIFA на World Cyber Games 2008; перше місце української команди NAVI (Natus Vincere) в CS: 1.6 на Intel Extreme Masters, ESWC та World Cyber Games у 2010 році, не лише вселяють гордість, але й залучають все більше прихильників починаючи з дитячого віку.

Не можна не помітити, що після створення у 2010 році турніру The International, у якому призовий фонд формується за рахунок учасників Valve Corporation вивела кіберспорт усього світу на новий рівень. В теперішній час призові фонди, що розігруються, можуть досягати декількох мільйонів доларів США. Турнір з Dota 2 The International кілька разів бив рекорди з виплат: так, у 2017 було розіграно $25 млн, у 2018 – $ 26 млн, у 2019 – $ 34 млн. Отже, можна стверджувати про велику економічну привабливість участі в турнірах для організаторів, учасників, рекламодавців, виробників обладнання для геймінгу та інших.

В той же час, не зважаючи на величезну кіберспортивну аудиторію та збільшення кількості турнірів, що проводять в усьому світі, кількість платформ для організації подібних змагань, залишається невеликою, маловідомою та має, з позицій гравця, ряд недоліків, наприклад, обмежений вибір доступних ігор – більшість відомих ресурсів призначена для змагань в CS, DOTA2, іноді LOL, обмеження форматів змагань, користувачі можуть не встановлювати античит, доступ тільки платний, системи карми, яка дозволяє спільноті самостійно карати гравців та інше.

Розвиток великої кількості кібердисциплін різного напряму, а також залучення великої кількості гравців різного рівня ігрових навичок, темпераменту та моральних якостей, крім того монетизація кіберзмагань, пояснюють необхідність створення платформи, яка вирішувала б наступні завдання:

- ✓ надання доступу до змагань гравцям будь-якого рівня
- ✓ збір персональної статистики гравців
- ✓ відбір та/або допомога у формуванні команд згідно зібраної статистики
- ✓ автоматизоване проведення турнірів
- ✓ забезпечення призових фондів і збір коштів на їх формування
- ✓ забезпечення чесної гри
- ✓ коментування та трансляція змагань зацікавленій аудиторії

Таким чином, враховуючи вищесказане, можна стверджувати, що створення веб-платформи для проведення кіберспортивних змагань сприятиме зростанню популяризації кіберспорту в Україні та світі, покращенню іміджу України на світовій арені, а також, що економічна привабливість подібних проектів є своєчасною та корисною ініціативою.