МІНІСТЕРСТВО НАУКИ ТА ОСВІТИ УРАЇНИ

УНІВЕРСИТЕТ "УКАРАЇНА"

Інститут комп’ютерних технологій

КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ: ОСВІТА І НАУКА

Тези доповідей

XV всеукраїнської конференції

м. Київ, 5-6 червня 2024 року

МІНІСТЕРСТВО НАУКИ ТА ОСВІТИ УРАЇНИ

УНІВЕРСИТЕТ "УКАРАЇНА"

Інститут комп’ютерних технологій

КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ: ОСВІТА І НАУКА

Тези доповідей

XV всеукраїнської конференції

м. Київ, 5-6 червня 2024 року

Київ - 2024

Затверджено до друку
Вченою радою Інституту комп`ютерних технологій
Відкритого міжнародного університету розвитку людини «Україна»
(протокол № 3 від 07.06.2024 р.)

Відповідальний за випуск: Наталія ОДРІБЕЦЬ
Редакційна група Відкритого міжнародного університету розвитку людини «Україна»: Таланчук П.М. (головний редактор), Давиденко Г.В., Одрібець Н.В., Забара С.С., Додонов О.Г., Дуднік А.С., Писарчук О.О., Зеленський К.Х., Зайцев В.Г., Поліновський В.В., Тимошенко А.Г., Павленко В.І., Кіт Г.В.

Комп'ютерні технології: освіта і наука: тези доповідей XV Всеукраїнської конференції, (м. Київ, 5-6 червня 2024 р.). К. : Університет «Україна», 2024. 72 с.

У збірнику вміщено тези доповідей XV Всеукраїнської конференції «Комп'ютерні технології: освіта і наука», в яких відображено сучасні тенденції у сфері комп’ютерних наук, інформаційних технологій та інших суміжних галузей. Інноваційні підходи в освіті та науці, актуальні проблеми інфокомунікаційних та комп’ютерних технологій, роль технологій у сучасному навчанні та дослідженнях, вплив інформаційних технологій на суспільство та бізнес.

Конференція відбулась в рамках реалізації наукових досліджень: «Метод захисту неструктурованої інформації на мобільних простоях що використовуються в адаптивних кейс-менеджмент системах» № 0124U000025 та «Імітаційна модель навігації та дешифрування мап з дронів для точних геоінформаційних додатків» № 0124U000036.

ISBN 978-966-388-707-4

DOI https://doi.org/10.36994/978-966-388-707-4-2024-71

Програмний комітет конференції:

Голова:
Таланчук П.М. – д.т.н., проф., академік АПН України;

Члени:
Давиденко Г.В. - д.п.н., професор, проректор з наукової і міжнародної діяльності Університету «Україна»;
Одрібець Н.В. – к.ф.-м.н., доцент, директор Інституту комп'ютерних технологій Університету «Україна»;
Забара С.С. – д.т.н., професор, почесний директор Інституту комп'ютерних технологій Університету «Україна»;
Додонов О.Г. - д. т. н., професор, Інститут проблем реєстрації інформації НАН України;
Дуднік А.С. - д. т. н., професор, Київський національний університет імені Тараса Шевченка;
Писарчук О.О. – д. т. н., професор, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»;
Зеленський К.Х. – д. т. н., професор, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»;
Зайцев В.Г. - д. т. н., професор, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»;
Поліновський В.В. - к.т.н., доцент, CEO академії GoITeens.
Тимошенко А.Г. – к.т.н., професор Університету «Україна»;
Павленко В.І. – к.ф.-м.н., доцент Університету «Україна»;
Кіт Г.В. – к.т.н., директор Івано-Франківської філії Університету «Україна»;

Організаційний комітет конференції:

Голова комітету:
Кучерявий І.Т. – д.ф.н., перший проректор Університету «Україна»;

Заступник голови комітету:
Одрібець Н.В. – к.ф.-м.н., директор Інституту комп'ютерних технологій;

Члени комітету:
Дуднік А.С. - д. т. н., професор, Київський національний університет імені Тараса Шевченка;
Морозова І.В. – в.о. завідувача кафедри комп'ютерної інженерії;
Веденєєва О.А. – в.о. завідувача кафедри інформаційних технологій та програмування;
Павленко В.І. – к.ф.-м.н., доцент Університету «Україна»;
Самарай В.П. – к.т.н., доцент Університету «Україна»;
Тимошенко А.Г. – к.т.н., професор Університету «Україна»;
Ізварін І.В. - к.т.н., доцент Університету «Україна»;

Авдалов Г.В. – ст.викл. Університету «Україна»;
Павленко О.Ю. – інженер-дослідник Університету «Україна»;
Поліновський В.В. - к.т.н., доцент, CEO академії GoITeens.
Сукенніков О. В. – керівник управління освіти Святошинської районної в місті Києві державної адміністрації.

ЗМІСТ

ВСТУПНЕ СЛОВО

Шановні колеги

Вітаю всіх учасників та організаторів XV Всеукраїнської конференції «Комп'ютерні технології: освіта і наука»!

Роль комп'ютерних технологій для розвитку України була і залишається вкрай важливою. Інформаційні технології нерозривно пов'язані з комп'ютером. Комп'ютерна техніка та системи зв'язку використовуються для збирання, передавання, отримання, пошуку, опрацювання та поширення інформації. Інформаційні технології відкрили нові можливості для навчання, роботи й відпочинку; надали доступ до великого обсягу інформації, сприяли виникненню сучасних способів спілкування, полегшили працю людей, ставши невід'ємною частиною нашого життя.

Особливо важливими комп'ютерні технології стали для України під час війни – для перемоги над рашистами. Вона, війна, створює серйозні виклики і перешкоди для ефективного розвитку країни, однак поєднання інформаційних технологій і високоточної зброї дасть можливість невеликим мобільним угрупуванням так званого "швидкого реагування" вирішувати будь-які стратегічні завдання.

Що ж входить в арсенал "інформаційної" війни? Це супутники-шпигуни і мініатюрні безпілотні літаки, які здатні розрізняти на землі предмети розміром менше метра. Це могутні суперкомп'ютери, здатні швидко проаналізувати і оцінити ситуацію, допомогти ухвалити вірні рішення. І, нарешті, це комп'ютерні віруси, здатні проникнути в телекомунікаційні мережі і системи управління супротивника та паралізувати їх дію.

Така комп'ютерна "вірусна" війна відбувається вже сьогодні. Її під час повномасштабної війни в Україні ведуть хакери – зломщики комп'ютерних мереж – з обох боків.

Також цікавим прикладом є більш досконала зброя з оптичними прицілами, прилади нічного бачення, управління з особистого комп'ютера з самонаведенням при програмуванні; управління голосом, що дозволяє відстежувати місце знаходження солдата, зв'язуватися з командиром за допомогою супутників і літаків - розвідників та своєчасно дізнаватися про маневри супротивника. Скоро кожен солдат-піхотинець виконуватиме роль оператора персонального мультимедійного комп'ютера розміром з середню книгу.

У винищувачах нового покоління є цифрові дисплеї, на яких пілот може бачити всю основну пілотажну інформацію. Додатково важлива бойова і пілотажна інформація передаватиметься на лобове скло шолома пілота. Це позбавить його від необхідності безперервно дивитися на прилади перед собою. Він зможе повертати голову і оцінювати ситуацію ще і візуально. Надалі роль пілота в пілотуванні літаком стане менша: комп'ютер вирішуватиме, з якою швидкістю і на яких режимах бойова машина виходитиме на мету та в який момент дозволити льотчикові застосувати зброю.

Шановні колеги! Як бачите, вже зараз іде війна нового покоління з використанням новітніх технологій. І сьогодні, на нашій конференції, що

триватиме два дні, науковці об'єдналися на пленарному засіданні, де буде представлено доповіді присвячені різним вимірам розвитку Української держави в умовах воєнного стану, сучасної освіти та науки в контексті використання комп'ютерних технологій, освіти і науки.

Інтерактивні платформи об'єднають дослідників в обговоренні актуальних і дискусійних проблем сучасної науки, нових комп'ютерних технологій, які виступають каталізаторами задля забезпечення в Україні більшої безпеки та її перемоги. Для українських науковців це є надзвичайно важливою складовою, оскільки якщо міжнародні партнери та українські науковці не будуть сьогодні пропонувати та використовувати найкращі комп'ютерні технології – ми усі будемо знаходитися в зоні величезної небезпеки.

Переконаний, що таке обговорення буде важливою складовою спільної боротьби українців за перемогу.

Щиро зичу успіхів у роботі нашої конференції. Бажаю ніколи не втрачати віру в переможну силу наукового знання. І, найголовніше, – в перемогу України.

Слава Україні!

Петро ТАЛАНЧУК
доктор технічних наук, професор,
дійсний член Академії педагогічних наук України,
заслужений діяч науки і техніки України,
Президент Університету «Україна»

МАШИНИЙ ЗІР В РОЗМІНУВАННІ: ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ТА БЕЗПЕКИ

Батрак О.Г.
аспірант кафедри комп'ютерної інженерії, Відкритий міжнародний університет розвитку людини «УКРАЇНА»
https://orcid.org/0009-0007-8248-5935
Науковий керівник: професор, доктор технічних наук Зайцев В.Г.,
Відкритий міжнародний університет розвитку людини «УКРАЇНА»

Ключові слова: машинний зір, розпізнавання цілей, розмінування, алгоритми розпізнання, нейронні мережі, магнітометр.

В сучасному світі проблема мін та нерозірваних вибухових пристроїв (НВП) залишається однією з найбільш актуальних та небезпечних. Негативні наслідки від їхнього існування можуть бути надзвичайно тяжкими, забираючи людські життя та спричиняючи серйозні травми. У такій обстановці виникає потреба у розвитку та впровадженні ефективних технологій для виявлення та нейтралізації цих небезпечних об'єктів. Машинний зір, що є однією з ключових галузей штучного інтелекту, виявляється надзвичайно потужним інструментом у цьому процесі.

Перш за все, детально розглянемо алгоритми виявлення мін, які є серцевиною систем машинного зору для розмінування. Серед них можна виділити такі, як Convolutional Neural Networks (CNN), You Only Look Once (YOLO) та Single Shot MultiBox Detector (SSD). Ці алгоритми використовуються для автоматичного виявлення та класифікації небезпечних об'єктів на мінному полі з високою швидкістю та точністю. Для оцінки їхньої ефективності, проведемо аналіз результатів тестування, включаючи таблиці з даними щодо точності, чутливості та специфічності кожного з алгоритмів на різних наборах даних [1].

Далі, розглянемо використання нейронних мереж у розмінуванні. Завдяки своїй здатності до автоматичного виявлення складних закономірностей у великих обсягах даних, нейронні мережі стають ефективним інструментом у виявленні мін та НВП. В створенні моделі для дослідження розпізнавання планується використання різних архітектур нейронних мереж, таких як згорткові нейронні мережі (CNN), рекурентні нейронні мережі (RNN) та їхні комбінації для досягнення кращих результатів у виявленні небезпечних об'єктів. Порівняння алгоритмів наведено в таблиці 1, де точність (%) - це відсоток правильно класифікованих об'єктів (мін або інших небезпечних об'єктів) відносно загальної кількості об'єктів у тестовому наборі даних. Чутливість (%) вказує на відсоток правильно виявлених позитивних випадків (мін або небезпечних об'єктів) серед усіх дійсно позитивних випадків у тестовому наборі. Специфічність (%) - відсоток правильно визначених негативних випадків (відсутність мін або небезпечних об'єктів) серед усіх дійсно негативних випадків у тестовому наборі. Ці метрики є стандартними мірками ефективності моделей класифікації у машинному навчанні та дозволяють оцінити їхню точність та надійність в розпізнаванні мін та інших небезпечних об'єктів [2].

Алгоритм	Точність,%	Чутливість,%	Специфічність,%
CNN	95.2	92.1	96.5
YOLO	93.8	91.5	94.2
SSD	94.5	93.2	95.8

Таблиця 1. Порівняння алгоритмів для розпізнавання мін

Для різних типів мін було отримано такі результати (табл. 2)

Тип міни	Алгоритм	Точність,%
Протипіхотна	CNN	96.3
Протитанкова	SSD	95.1

Таблиця 2. Результати роботи алгоритмів

Сама модель для досліджень базується на використанні:

- дрону 10” (несуча платформа для сенсорів)
- магнітометру (складання карти відхилень магнітного поля досліджуваної поверхні та перетворення їх в спектральні зображення)
- відеокамери (для розпізнавання вибухонебезпечних об’єктів. Планується використання фото різних поширених типів вибухівки для навчання та використання машинного зору)

Ймовірні інші сенсори. На поточному етапі не розглядаються.

Використання магнітометру вважаю дуже ефективним методом:

1. 3 саперів з металошукачем: 60 хв. виявлення, 100 хвилин очищення.
2. 3 сапери та 2 дрони з магнітометром: сканування дроном 2 хв, виявлення саперами 10 хв, очищення 100 хвилин

Зменшення часу на очистку території 112 хв проти 160. Ефективність 30% [3].

Окремо варто зупинитися на важливості акустичного та радіо-лазерного сканування в розмінуванні. Ці методи, що базуються на вимірюваннях звукових або радіо-лазерних сигналів, можуть доповнювати зображення, отримані з візуальних сенсорів, та забезпечити додаткові дані для точнішого виявлення небезпечних об'єктів у різних умовах, включаючи обмежені видимість або утруднення на мінному полі [4].

Отже, використання машинного зору в розмінуванні відкриває широкі можливості для покращення безпеки та ефективності операцій на мінному полі. Однак існують деякі проблеми, що потребують уваги. Наприклад, точність виявлення вибухонебезпечних об'єктів, розрізнення між реальними загрозами та незначними об'єктами, а також проблеми з надійністю та стійкістю систем у різних умовах. Наступним кроком досліджень і буде покращення в алгоритмах машинного зору, збільшення точності і швидкості виявлення, розробка більш адаптивних систем до різних умов довкілля та забезпечення надійності.

Список використаних джерел:

1. Маковейчук О.М., Занфіров Р.Р., Науменко А.В., Гайовий О.О., Вияснівський В.А. Приклад використання згорткової нейронної мережі для розпізнавання номіналу банкнот. Науковий журнал «IT SYNERGY», 2022, випуск 1 (2)

2. T.Hutsul, M.Khobzei, V.Tkavch, O.Krulikovskyi, O.Moisiuk, V.Ivashko, A.Samila. «Review of approaches to the use of unmanned aerial vehicles, remote sensing and geographic information systems in humanitarian demining: Ukrainian case».

3. Розмінування в Україні за допомогою магнітометра від фонда Поступ: як працює (https://thepage.ua/economy/razminirovanie-v-ukraine-tehnologii-obnaruzheniya-min)

4. Сергієнко О.Ю. Розвиток теорії та удосконалення систем автономної навігації мобільних наземних роботів у недетермінованих середовищах. УДК 681.5+621.375.826; 656.052.1

РОЛЬ СИСТЕМ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Близнюк А.В.
аспірант, група КІ-23-1, спеціальність 123 «Комп'ютерна інженерія»,
Відкритий міжнародний університет розвитку людини «УКРАЇНА»
https://orcid.org/0009-0007-4461-5823
Науковий керівник: Писарчук О.О. доктор технічних наук, професор,
Відкритий міжнародний університет розвитку людини «УКРАЇНА»

Анотація. Сучасні інформаційно-телекомунікаційні системи державного сектору потребують підвищеної уваги до кібербезпеки через зростання кількості кібератак. Витоки конфіденційної інформації можуть серйозно вплинути на національну безпеку та економічну стабільність. Системи підтримки прийняття рішень (СППР) є інтегрованими системами, які використовують дані та моделі для підтримки процесу прийняття рішень у сфері кібербезпеки. Вони допомагають аналізувати загрози, прогнозувати атаки і вибирати оптимальні заходи захисту. Використання СППР дозволяє передбачати та запобігати кібератакам, оптимізувати ресурси, автоматизувати процес прийняття рішень та знижувати ризики. Інтеграція СППР з DLP системами підвищує загальний рівень кібербезпеки організації, забезпечуючи багаторівневий захист.

Abstract. Modern information and telecommunication systems in the public sector require increased attention to cybersecurity due to the growing number of cyberattacks. Leaks of confidential information can significantly impact national security and economic stability. Decision Support Systems (DSS) are integrated systems that use data and models to support decision-making processes in cybersecurity. They help analyze threats, predict attacks, and select optimal protective measures. Using DSS allows predicting and preventing cyberattacks, optimizing resources, automating decision-making processes, and reducing risks. Integrating DSS with DLP systems enhances the overall level of an organization's cybersecurity, providing multi-layered protection.

Сучасні інформаційно-телекомунікаційні системи державного сектору все частіше стають об'єктами кібератак, що вимагає підвищеної уваги до питань кібербезпеки. Витоки конфіденційної інформації можуть мати серйозні наслідки для національної безпеки та економічної стабільності. Таким чином, розробка ефективних систем підтримки прийняття рішень (СППР), які здатні вчасно виявляти та блокувати потенційні канали витоку інформації, є надзвичайно важливою задачею.

Система підтримки прийняття рішень (СППР) - це інтегрована система, яка використовує дані та моделі для підтримки процесу прийняття рішень у різних сферах діяльності. У контексті кібербезпеки, СППР аналізує інформацію про загрози та вразливості, прогнозує можливі атаки і допомагає у виборі оптимальних заходів захисту.

СППР забезпечує комплексний підхід до управління кібербезпекою, пропонуючи наступні переваги:

1. Проактивний захист: СППР дозволяє передбачити і запобігти можливим кібератакам ще до їхнього виникнення.
2. Оптимізація ресурсів: Використання СППР дозволяє ефективно розподіляти ресурси та знижувати витрати на кібербезпеку.
3. Підвищення швидкості реагування: СППР автоматизує процес прийняття рішень, що дозволяє швидко реагувати на інциденти.
4. Зниження ризиків: СППР допомагає ідентифікувати потенційні загрози і вразливості, знижуючи ймовірність успішних атак.

Є декілька основних підходів до побудови СППР. Морфологічний підхід, який застосовується для вибору оптимальних варіантів захисту інформаційних систем. Він передбачає використання морфологічних матриць для генерації варіантів комплексів захисту з урахуванням апаратно-програмної сумісності.

Моделі машинного навчання (ML): Використовуються для автоматичного виявлення аномалій та потенційних загроз на основі аналізу великих обсягів даних, наприклад, від DLP (Data Loss Prevention) систем. Інтелектуальні системи: Включають в себе експертні системи та методи нечіткої логіки для оцінки ризиків і прийняття рішень.

Інтеграція СППР з DLP системами дозволяє створити багаторівневу систему захисту, що включає в себе моніторинг та аналіз даних. DLP системи забезпечують збір даних про можливі витоки інформації, які СППР аналізує для виявлення загроз.

Також можна інтеграція реалізовує автоматичне реагування, оскільки СППР може автоматично блокувати канали витоку на основі даних від DLP систем. Зокрема і підвищується ефективність роботи захисту, бо використання СППР разом з DLP системами дозволяє швидко і точно виявляти та блокувати загрози, підвищуючи загальний рівень кібербезпеки організації.

Тому використання СППР у кібербезпеці державних інформаційно-телекомунікаційних систем дозволяє суттєво знизити витрати на засоби захисту та підвищити ефективність управління захистом інформації.

Список використаної літератури

1. Development of a support system for managing the cyber security / V. A. Lakhno // Радіоелектроніка, інформатика, управління. - 2017. - № 2. - С. 109-116. - Режим доступу: http://nbuv.gov.ua/UJRN/riu_2017_2_14.

2. Технологія колективної розробки системи підтримки прийняття рішень керівника аптечної мережі / О. О. Писарчук, Д. В. Котенко, Д. О. Ткачук, І. М. Ганношина // Наукоємні технології. - 2018. - № 4. - С. 423-427. - Режим доступу: http://nbuv.gov.ua/UJRN/Nt_2018_4_7.

МАСШТАБУВАННЯ МІКРОСЕРВІСНОГО ЗАСТОСУНКУ: ПРАКТИЧНИЙ ДОСВІД

Богуцький Андрій, аспірант програми «Комп'ютерна інженерія»,
Відкритий міжнародний університет розвитку людини «Україна» (Україна),
Інститут комп'ютерних технологій, bohutskyi_ak22@nuwm.edu.ua,
https://orcid.org/0009-0006-9458-8838
Павленко Володимир, к.ф.-м.н., https://orcid.org/0000-0002-3958-0415
Тимошенко Оксана, к.ф.-м.н.,https://orcid.org/0009-0003-4331-1706

Анотація

На сьогоднішній день мікросервісна архітектура набула широкої популярності серед розробників програмного забезпечення як інструмент швидкого та якісного вирішення бізнес-завдань. Станом на зараз знання розробника можуть обмежуватися набором бібліотек у рамках однієї мови програмування, і цього буде цілком достатньо для розгортання повноцінних застосунків. Проте з плином часу склад команди розробників змінюється, і якщо на початковому етапі розробки застосунку кількість мікросервісів можна порахувати на пальцях однієї руки, то згодом ця кількість виростає до кількох десятків, а іноді і сотень. Тому виникає необхідність систематизувати та узагальнити загальні підходи до покращення роботи команди при збільшенні кількості її працівників та обсягу завдань.

Abstract

Today, microservice architecture has gained wide popularity among software developers as a tool for solving business problems quickly and efficiently. Up to this point, a developer's knowledge can be limited to a set of libraries within one programming language, and it is enough to deploy full-scale applications. However, over time, the composition of the development team changes, and if at the initial stage of application development, the number of microservices can be counted on the fingers of one hand, then later this number grows to several dozen, and sometimes hundreds. Therefore, there is a need to systematize and generalize common approaches to improving team performance as the number of employees and the scope of tasks increase.

Методологія

Методологія включає аналіз існуючих підходів до масштабування мікросервісів, в тому числі вивчення літератури з контейнеризації (Docker) та командної співпраці (Scrum). Практичний аналіз: реалізація та тестування архітектурних патернів і технологій в реальних умовах. Критичний аналіз: оцінка переваг та недоліків кожного підходу з точки зору продуктивності, надійності та масштабованості для визначення сучасних практик та тенденцій масштабування мікросервісних додатків.

Результати

При розробці нового мікросервісу з нуля розробники постають перед цілою низкою питанн:

- Основні цілі, функції та потреби користувачів застосунку.

- Структура та залежності у базах даних, їх кількість та тип.
- Архітектура та модульність застосунку.
- Вибір технологій та бібліотек.
- Модульне та інтеграційне тестування [1].

Іноді бізнес може поставити завдання, з яким ця команда зможе впоратись за час, який є явно більшим ніж того вимагає завадання. На цьому етапі, технічний лідер команди має бути добре проінформований кількісно-якісним складом команди та повинен опиратися на попередній досвід у прийнятті рішень щодо можливості чи неможливості виконання завдання в зазначені терміни.

Збільшення чисельності команди неодмінно призводить або до тимчасового зниження продуктивності команди або до збільшення навантаження на його членів, оскільки частина працівників буде займатись адаптацією нових членів команди. Якщо команда знаходиться в стані активної розробки нового функціоналу, і уникнути збільшення її штату неможливо, варто розподілити роботу так, щоб віддати прості завдання чи виправлення помилок для новачків, а вже досвідченні члени команди, мають займатися осоновними, великими задачами.

З часом краще розділяти команди на менші, при чому закріпити за кожною з них саме ті мікросервіси, над якими його члени мають найкращі знання. Меншими за чисельністю командами значно легше керувати, крім того вони можуть показувати кращі результати порівняно з великими, оскільки значно менше часу витрачається на зустрічі, які часто не мають значого впливу на результат.

Введення строгих правил проектування значно спрощує розробку застосунку. При маніпуляції одразу кількома мікросервісами розробник зможе швидко внести до них зміни. Крім того знайомство з новим мікросервісом не займе багато часу, оскільки розробник вже фактично бачив ті ж самі патерни проектування на попередніх застосунках, і він вже розуміє яку функцію може виконувати той чи інший сервіс [2].

Використовуючи сучасні інструменти розробки, перевірки, тестування та керування командою можна досягати кращих результатів витрачаючи при цьому менше коштів. Добре себе зарекомендували методи розділення великих команд на менші керування якими відбувається з використанням методології принципів та практик Scrum. З огляду на сучасні виклики, мікросервісна архітектура продовжує еволюціонувати як практичний засіб для вирішення проблем бізнесу і людей.

Література

1. Про архітектуру додатків [Електронний ресурс] – URL: https://foxminded.ua/arkhitektura-zastosunku/. (дата звернення 09.05.24)

2. What is SOLID? Principles for Better Software Design [Електронний ресурс] – URL: https://www.freecodecamp.org/news/solid-principles-for-better-software-design/. (дата звернення 25.05.24)

ПРОБЛЕМИ ЗАХИСТУ ВІД DDOS АТАК НА РІВНІ МЕРЕЖІ

Борисенко Олександр Сергійович
ІІ курс аспірантури, група КІ-22-1, спеціальність “Комп’ютерна інженерія”
Інститут комп’ютерних технологій Університету “Україна”
https://orcid.org/0009-0001-3738-5878
Науковий керівник: Тимошенко А.Г., к.т.н., проф.

Анотація. *Ця доповідь розглядає типи DDoS атак на рівні мережі і проблеми захисту від них. Найбільш поширені типи DDoS атак включають UDP Reflection та SYN-флуд атаки. Ці атаки можуть перевантажити мережу або системні ресурси, такі як сервери та фаєрволи. Ефективний захист вимагає впровадження механізмів, як-от SYN-куки та перевірку адреси джерела (SAVE), для запобігання виснаженню ресурсів.*

Annotation. *This article examines types of DDoS attacks at the network level and the challenges of defending against them. The most common types of DDoS attacks include UDP Reflection and SYN flood attacks. These attacks can overwhelm network or system resources such as servers and firewalls. Effective defense requires implementing mechanisms such as SYN cookies and Source Address Validation Everywhere (SAVE) to prevent resource exhaustion.*

DDoS (Distributed Denial of Service) атака – це зловмисний спосіб виведення з ладу інтернет-сервісу, веб-сайту або мережі шляхом перенавантаження системи великим обсягом шкідливого трафіку. Мета атаки полягає у блокуванні доступу легітимним користувачам до ресурсів.

Як працюють DDoS атаки

DDoS атака зазвичай виконується з використанням ботнетів – мереж заражених комп'ютерів (ботів), які зловмисники контролюють дистанційно. Ці боти одночасно відправляють величезну кількість запитів до цілі, перевантажуючи її ресурси (наприклад, процесор, пам'ять або смугу пропускання).

Найпоширенішими DDoS-атаками є атаки на основі протоколу User Datagram Protocol (UDP) і SYN-флуди, які відносяться до атак на інфраструктурному рівні. Ці атаки генерують великий обсяг трафіку, який може перевантажити мережу або використовувати ресурси систем, таких як сервери, фаєрволи, системи запобігання вторгнень (IPS) або балансувальники навантаження. Ефективне пом'якшення таких атак потребує мережі або систем, здатних швидко збільшити пропускну здатність.

UDP Reflection Атаки

Атаки відбиття UDP використовують те, що UDP є не сесійним протоколом. Зловмисники можуть створити запит UDP з IP-адресою цілі як IP-джерело, тобто підробити пакет запиту. Цей пакет надсилається до проміжного сервера, який відповідає на підроблену адресу, тим самим перенаправляючи відповідь на IP жертви. Проміжний сервер генерує відповідь, яка в кілька разів більша за запит, тим самим підсилюючи атаку.

Коефіцієнт посилення залежить від використовуваного протоколу, наприклад, DNS, NTP, SSDP, CLDAP, Memcached, CharGen або QOTD. Наприклад, коефіцієнт посилення для DNS може становити від 28 до 54 разів. Отже, запит

розміром 64 байти може генерувати більше 3400 байт шкідливого трафіку до цільової IP-адреси.

Слід зазначити, що атаки відбиття, хоча і надають зловмисникам "безкоштовне" посилення, потребують можливості підробки IP-адрес. Зі зростанням кількості провайдерів, які впроваджують повсюдну перевірку адреси джерела (SAVE) або BCP38, ця можливість зникає. Це змушує провайдерів DDoS-атак припиняти атаки відбиття або переміщуватися до дата-центрів і провайдерів, які не впроваджують перевірку адреси джерела.

Атаки SYN Flood

Як працюють атаки SYN Flood

Коли користувач підключається до сервісу TCP, такого як веб-сервер, його клієнт відправляє пакет SYN. Сервер відповідає пакетом SYN-ACK, а клієнт завершує з'єднання пакетом ACK, створюючи трьохстороннє рукостискання.

Механізм атаки

В атаці SYN Flood зловмисник надсилає велику кількість пакетів SYN, але ніколи не надсилає завершальних пакетів ACK. Сервер залишається в очікуванні відповіді на напіввідкриті TCP-з'єднання, що призводить до вичерпання ресурсів сервера для нових з'єднань.

Захисні механізми

Сучасні операційні системи використовують SYN-куки, щоб запобігти вичерпанню таблиці станів від атак SYN Flood. Коли черга SYN досягає певного порогу, сервер відповідає SYN-ACK з спеціально сформованим початковим порядковим номером без створення запису в черзі SYN. Якщо сервер отримує ACK з правильним номером підтвердження, він додає запис у свою таблицю станів і продовжує роботу як звичайно.

Вплив атак

Основний вплив атак SYN Flood проявляється у виснаженні пропускної здатності мережі та ресурсів процесора. Проміжні пристрої, такі як фаєрволи або механізми відстеження з'єднань у групах безпеки EC2, можуть також постраждати від вичерпання таблиці станів TCP і почати відхиляти нові з'єднання.

Ми розглянули найпоширеніші типи DdoS атак на рівні мережі. До них належать UDP Reflection і SYN flood атаки. UDP Reflection атаки використовують безсесійні протоколи для підсилення трафіку, а SYN flood атаки експлуатують процеси TCP-з'єднань для виснаження ресурсів серверу. Ефективне пом'якшення вимагає механізмів, таких як SYN-куки і перевірка адреси джерела, щоб запобігти виснаженню ресурсів.

АДАПТИВНА СИСТЕМА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА МОБІЛЬНИХ ПРИСТРОЯХ

Бровченко Євген Миколайович
ІІІ курс, група КІ-22-1, спеціальність «Комп'ютерна інженерія»
Інститут комп'ютерних технологій Університету «Україна»
https://orcid.org/0000-0002-1416-0385
Науковий керівник: Самарай В. П., к.т.н., с.н.с., доцент
Інститут комп'ютерних технологій Університету «Україна»

Анотація. Робота присвячена проблемі використання мобільного пристрою в умовах активного впливу та захист неструктурованої інформації. Увага приділена використанню мобільного пристрою як частини інформаційної системи та можливі заходи щодо захисту інформації від протиправних дій. Була проведена робота по вивченню проблеми в реальних умовах використання та взаємодії. Пропонується модель алгоритму адаптивного захисту інформації. В основу моделі покладена ідея динамічної адаптації системи.

Ключові слова: мобільній пристрій; захист інформації; неструктурована інформація; кібербезпека.

ADAPTIVE INFORMATION SECURITY SYSTEM ON MOBILE DEVICES

Annotation. The work is devoted to the problem of using a mobile device in conditions of active influence and protection of unstructured information. Attention is paid to the use of a mobile device as part of an information system and possible measures to protect information from illegal actions. Work was carried out to study the problem in real conditions of use and interaction. A model of the adaptive information protection algorithm is proposed. The model is based on the idea of dynamic adaptation.

Key words: mobile device; security; information protection; user interaction with a mobile device; adaptive security.

Мобільний пристрій містить багато різноманітної інформації чи даних. Природа та важливість цієї інформації може бути різною, але захист має пріоритетне значення. Враховуючи динаміку розвиту та невизначеність деяких процесів, перед інженерами та розробниками стоїть важке та важливе завдавання по захисту інформаційних систем та забезпеченню надійної роботи. Мобільний пристрій можна вважати найбільш проблематичною складовою. Цей пристрій має ряд переваг та особливостей. Робота присвячена проблематиці використання мобільних пристроїв та захисту неструктурованої інформації. Неструктурована інформація може бути у вигляді текстових документів, електронних листів, фотографій, відео, записів голосу та іншого контенту, який зберігається на мобільних пристроях. До основних проблем можна віднести: втрата або крадіжка мобільного пристрою; вразливості операційної системи та програмного забезпечення; недостатній рівень шифрування та недостатній рівень складності паролів; нехтування кібергігієною. Існуючи інженерно-архітектурні рішення не завжди виконують поставлену задачу та можуть мати проблеми з інтеграцією. Аналіз прикладної області та результати дослідження говорять про те що є попит на швидкі та ефективні рішення щодо безпеки інформаційних систем в цілому та

мобільного пристрою зокрема. Лише комплексний підхід може забезпечити ефективне рішення. Адаптивний захист передбачає використання різних методів і технологій, таких як шифрування, біометричні ідентифікатори, інтелектуальні системи виявлення загроз. Включає в себе постійне оновлення і покращення методів захисту, оскільки загрози постійно еволюціонують, і необхідно підлаштовувати захисні механізми під нові виклики. Користувачі мобільних пристроїв повинні бути активно включені в процес адаптивного захисту, слідкувати за оновленнями, використовувати паролі, підтримувати резервне копіювання і відповідати на попередження щодо безпеки. Розробники програмного забезпечення для мобільних пристроїв мають велику відповідальність щодо забезпечення безпеки інформації, і вони повинні включати адаптивні захисні механізми в свої додатки і платформи. Процес вимагає поєднання технічних, організаційних та освітніх заходів для досягнення максимальної ефективності. Забезпечення адаптивного захисту інформації на мобільних пристроях є ключовою умовою для збереження приватності і безпеки користувачів у цифровому світі. Може бути покращений завдяки співпраці між виробниками, науковцями, законодавцями та споживачами для розвитку більш безпечних інформаційних середовищ.

Захист інформації на мобільному пристрої засновано на поєднанні технологічних нововведень та підвищенні обізнаності користувачів з питань кібербезпеки. Деякі напрямки розвитку включають застосування штучного інтелекту (AI) та машинного навчання. AI може допомогти в розробці розширених механізмів захисту, що автоматично виявляють аномальні або підозрілі дії та блокують потенційні загрози. Біометрична автентифікація, покращення технологій біометричної автентифікації, таких як розпізнавання обличчя, відбитків пальців, можуть забезпечити більш надійний захист інформації. Застосування блокчейн-технологій, блокчейн може відігравати важливу роль у забезпеченні безпеки інформації, оскільки він дозволяє зберігати дані розподіллено та захищено від змін. Розвиток квантово-стійких алгоритмів шифрування, з розвитком квантових комп'ютерів створюється потреба в нових алгоритмах шифрування, які можуть витримати потужність квантового злому. Приватність за замовчуванням (Privacy by Design), проектування мобільних пристроїв та застосунків з врахуванням приватності користувачів сприятиме захисту інформації на мобільних пристроях. Освіта та обізнаність користувачів, підвищення обізнаності користувачів щодо кібербезпеки та навчання їх ефективним методам захисту інформації на мобільних пристроях допоможе зменшити ризик виникнення інцидентів, пов'язаних з безпекою. Розвиток законодавства та нормативної бази, вдосконалення законодавства та нормативної бази у галузі кібербезпеки сприятиме створенню надійного середовища для захисту інформації. Захист інформації на мобільних пристроях спиратиметься на комбінації технологічного прогресу, навчання користувачів та співпраці між різними сторонами, такими як розробники, постачальники послуг та законодавці. Забезпечення безпеки та приватності даних в цифровому світі залишається пріоритетом, оскільки кількість мобільних пристроїв та їх використання продовжують зростати.

Сучасній користувач мобільних пристроїв має певні вимоги що спарюються на ергономіку та рівень інформаційної обізнаності. Розвиток галузі в цілому

вимагає швидких, надійних та ефективних рішень що потрапляють не лише в економічну площину а й площину кібербезпеки. Використання мобільних пристроїв може адаптуватися до швидких сучасних потреб безпеки організації та може бути легко налаштований відповідно до конкретних вимог. Мобільний пристрій є зручним і доступним для багатьох користувачів, він зазвичай знаходиться поруч з користувачем і може використовуватися як додатковий елемент безпеки.

Список використаних джерел:

1. Бровченко, Є. М., Самарай, В. П., Даценко, І. П., Павленко, В. І., Середа А.В. Захист неструктурованої інформації на мобільному пристрої. Інфокомунікаційні та комп'ютерні технології, No 1(05). Київ, 2023. с. 194–200.

МОДЕЛЮВАННЯ ЕЛЕКТРОМЕРЕЖ З ВИКОРИСТАННЯМ МАШИННОГО НАВЧАННЯ. МОДЕЛІ, ДАНІ І ВИКЛИКИ

Войтех Д.В.
І курс, група КІ-23-1 phd, спеціальність «Комп`ютерна інженерія»,
Інститут комп'ютерних технологій Університету «Україна».
https://orcid.org/0009-0003-8997-5495
Науковий керівник: Тимошенко А.Г., к.тех.н., доцент,
Інститут комп'ютерних технологій Університету «Україна»

Анотація: Дана робота презентує дослідження найбільш актуальних задач у галузі моделювання енергомереж, для вирішення яких є доцільним використання методів машинного навчання. У ній розглядається, як машинне навчання може сприяти оптимізації функціонування мереж та відігравати ключову роль у модернізації енергетики. Аналізуються такі проблеми, як задача оптимального розподілу потужності, оцінки стану системи, прогнозування попиту та генерації тощо. Також досліджуються різні типи даних, що використовуються для навчання моделей, сформовано практичні поради щодо їх обробки. Наведено сценарії застосування і категоризацію різних методів машинного навчання а також оцінку майбутніх перспектив цієї сфери. Крім цього, робота включає прикладний аналіз загальноєвропейського мережевого набору даних від GridKit.

Abstract: This study presents research on the most topical tasks in the field of energy grid modeling, for which the use of machine learning methods is appropriate. It examines how machine learning can contribute to optimizing network operations and play a key role in the modernization of energy systems. The study analyzes problems such as optimal power distribution, system state estimation, demand and generation forecasting, among others. It also explores various types of data used for training models, providing practical advice on their processing. Scenarios for application and categorization of different machine learning methods, as well as an assessment of future prospects in this field, are presented. Additionally, the work includes an applied analysis of the pan-European network dataset from GridKit.

Перед людством на сьогоднішній день постає ряд складних викликів, серед яких зменшення кількості викидів парникових газів та прискорення процесу енергетичної трансформації спрямованої на децентралізацію енергосистеми. Класичні методи аналізу та моделювання енергосистем вже сьогодні на практиці виявляються недостатньо ефективними оскільки враховують невизначеність розподільчої електромережі пов'язану лише зі споживанням і те, що електроенергія потрапляє у мережу розподілу переважно з мережі передачі. Відповідно до сучасних реалій енергосистеми, де відновлювані джерела електроенергії з мінливою генерацією становлять суттєву частку а можливості щодо контролю і моніторингу самої мережі розподілу є досить обмеженими, вже зараз існує потреба в більш комплексних інструментах моделювання які дозволять врахувати вищезгадані фактори [1].

Модель енергосистеми описує фізичне розташування та з'єднання усіх її компонентів, зазвичай у вигляді графа, що складається з вузлів (генератори,

навантаження, підстанції) та ребер (лінії електропередачі). Залежно від задачі моделювання, топологія енергосистеми може бути орієнтованим або неорієнтованим графом. Формалізується модель у вигляді системи рівнянь, які описують взаємозв'язки між змінними та враховують вплив різних компонентів. Традиційні підходи засновані на складних фізичних моделях, але через масштаб сучасних енергосистем часто застосовуються певні спрощення. Технології у сфері штучного інтелекту та зокрема машинного навчання швидко розвиваються в тому числі завдяки регулярній появі нових великих наборів даних, регулярному вдосконаленню обчислювальних систем а також появою нових архітектур моделей глибинного навчання [2]. Відповідно, методи машинного навчання можуть використовуватися як високоякісні апроксиматори з кращими можливостями адаптації до змін у поведінці системи.

Ключовою вимогою стабільного функціонування енергосистеми і також ціллю моделювання є підтримання балансу виробництва та споживання електроенергії, що забезпечується в тому числі сталою частотою (50 або 60 Гц залежно від країни). Будь-який дисбаланс призводить до зміни частоти. Історично підтримання енергобалансу досягалося за допомогою планування та маневрування потужністю у режимі реального часу контрольованих генераторів, таких як теплові (вугільні та газові) електростанції. В основі моделювання цих процесів лежить задача оптимального розподілу потужності (optimal power flow, OPF) [3].

Для моделювання сучасних енергосистемах використовується широкий спектр різноманітних джерел даних, в тому числі від систем SCADA, метеорологічні дані, мережеві вимірювальні пристрої (PMU та розумні лічильники), а також історичні часові ряди та параметри генераторів, мережевих ліній і споживачів, що надаються і обліковуються операторами енергосистем [4].

В рамках дослідження було проведено аналіз використання машинного навчання в енергетиці. До переліку входять основні сценарії і прикладні задачі для таких сімейств методів як навчання з учителем, без учителя, навчання з підкріпленням, а також окремо виділено останні напрямки досліджень, включаючи графові нейромережі та великі мовні моделі. Крім цього, у роботі було оброблено набір даних загальноєвропейської енергосистеми від GridKit і проведено його статистичний та мережевий аналіз, що дає можливість адресувати такі задачі як виявлення потенційно ненадійних мережевих зв’язків, оцінка пропускної здатності мережі у випадку відмов різного ступеня тощо [5].

Підсумовуючи, моделювання з використанням методів машинного навчання стає все більш розповсюдженим у контексті сучасних викликів в енергосистемах, зокрема необхідності інтеграції відновлюваної генерації та забезпечення стабільності мережі. Проведений аналіз наборів даних, методів та їх застосування до конкретних задач відкриває перспективу для проведення подальших досліджень з навчання і адаптації моделей машинного навчання.

Список використаних джерел

1. Sinsel, S. R., Riemke, R. L., & Hoffmann, V. H. (2020). Challenges and solution technologies for the integration of variable renewable energy sources—a review. *Renewable Energy, 145*, 2271-2285. DOI: https://doi.org/10.1016/j.renene.2019.06.147

2. Caviglione, L., Comito, C., Guarascio, M., & Manco, G. (2023). Emerging challenges and perspectives in Deep Learning model security: A brief survey. *Systems and Soft Computing, 5*, 200050. DOI: https://doi.org/10.1016/j.sasc.2023.200050
3. ScienceDirect. Optimal power flow. [Електронний ресурс] - Режим доступу: https://www.sciencedirect.com/topics/engineering/optimal-power-flow
4. Ledesma, P., Arredondo, F., & Moreno, M. Á. (2023). Adapting ENTSO-E network data for power system simulation. In *2023 IEEE International Conference on Environment and Electrical Engineering and 2023 IEEE Industrial and Commercial Power Systems Europe (EEEIC / I&CPS Europe)* (pp. 1-5). DOI: https://doi.org/10.1109/EEEIC/ICPSEurope57605.2023.10194624
5. GridKit: European and North-American extracts. [Електронний ресурс] - Режим доступу: https://zenodo.org/records/47317

ПОРІВНЯННЯ МЕТОДІВ МАШИННОГО НАВЧАННЯ ДЛЯ КЛАСИФІКАЦІЇ ФЕЙКОВИХ НОВИН

Джоші Артур
Відкритий міжнародний університет розвитку людини "Україна", Інститут комп'ютерних технологій, Київ, Україна.
https://orcid.org/0009-0003-7487-2354
Науковий керівник: Павленко В.І.., к.ф.-м.н., доцент,
Інститут комп'ютерних технологій Університету «Україна»

Анотація: *У роботі розглянуто ефективність різних моделей машинного навчання для класифікації фейкових текстових новин. Особлива увага приділяється впливу попередньої обробки даних, а саме оверсемплінгу та використанню різних векторизаторів на продуктивність моделей. Результати дослідження надають важливу інформацію про оптимальні налаштування та підходи до попередньої обробки даних для покращення точності класифікації новин на достовірність.*

Abstract: *The paper examines the effectiveness of various machine learning models for classifying fake text news. Particular attention is paid to the impact of data preprocessing, namely oversampling and the use of different vectorizers on the performance of the models. The results of the study provide important information about the optimal settings and approaches to data preprocessing to improve the accuracy of news classification for reliability.*

У сучасному інформаційному просторі фейкові новини стали серйозною проблемою, особливо в Україні, де дезінформація може мати далекосяжні наслідки як для суспільства, так і для держави. У цьому контексті машинне навчання виступає потужним засобом для автоматизованого аналізу та розпізнавання неправдивої інформації.

Для порівняння ефективності різних моделей машинного навчання використовуються різноманітні метрики. Найпростішою метрикою є точність – доля правильних відповідей алгоритму в цілому. Більш репрезантативними метриками є прецизійність (precision) по кожному класу окремо та повнота. Прецизійність є долею елементів, що були класифіковані до певного класу і при цьому дійсно є елементами цього класу. Повнота показує яку долю елементів класу знайшла модель. Для об'єднання обох метрик в одну агреговану метрику використовується f-міра [1].

Задачею даного дослідження є проведення експерименту задля оцінки впливу попередньої обробки вхідних даних і власних параметрів на ефективність моделей класифікації текстових новин українською мовою. В якості вхідних даних взято 10735 текстових новин з інформаційних телеграм каналів, які розміщені на веб-ресурсі Kaggle [2]. Даний набір даних містить в собі 8237 достовірних новин і 2498 фейкових новин. Вхідний набір даних містить в собі необроблені дані в оригінальному вигляді. Задля покращення ефективності класифікаційних моделей, до вхідних даних було застосовано наступні техніки: фільтрація стоп-слів, лематизація та стемінг.

Важливою технікою попередньої обробки даних є оверсемплінг – метод боротьби з дисбалансом класів у наборах даних для машинного навчання. Наступним кроком попередньої обробки вхідних текстових даних є векторизація – процес перетворення текстових даних у числові вектори, що можуть бути оброблені алгоритмами машинного навчання.

Таблиця 1. Вплив попередньої обробки даних на ефективність моделей

		З оверсемпінгом	Без оверсемплінгу	CountVectorizer	TFIDF Vectorizer
Наївний Баєс	Точність	78,80%	72,60%	77,80%	77,80%
	Прецизійність (фейкові)	53,80%	44,20%	52,20%	52,20%
	Повнота (фейкові)	54,60%	71,80%	49,80%	50,80%
	F-міра (фейкові)	54,20%	54,80%	51,00%	51,40%
	Прецизійність (достовірні)	86,40%	89,60%	85,00%	85,00%
	Повнота (достовірні)	85,60%	72,60%	86,40%	85,80%
	F-міра (достовірні)	86,20%	80,20%	86,00%	85,60%
Метод k найближчих сусідів	Точність	74,00%	77,20%	58,60%	74,60%
	Прецизійність (фейкові)	35,40%	58,40%	32,80%	35,80%
	Повнота (фейкові)	14,60%	0,80%	44,60%	14,40%
	F-міра (фейкові)	21,00%	1,60%	29,20%	20,60%
	Прецизійність (достовірні)	78,00%	77,20%	80,20%	79,00%
	Повнота (достовірні)	91,80%	100,00%	63,60%	92,00%
	F-міра (достовірні)	84,40%	87,00%	64,40%	85,00%
Метод опорних векторів	Точність	83,20%	80,00%	84,40%	83,80%
	Прецизійність (фейкові)	88,60%	98,60%	92,20%	89,00%
	Повнота (фейкові)	33,80%	15,40%	37,60%	35,80%

	F-міра (фейкові)	49,20%	26,80%	53,20%	50,60%
	Прецизійність (достовірні)	82,80%	79,20%	83,60%	83,20%
	Повнота (достовірні)	98,60%	100,00%	99,00%	98,60%
	F-міра (достовірні)	89,80%	88,20%	90,60%	90,40%
Випадковий ліс	Точність	91,20%	90,80%	90,80%	91,20%
	Прецизійність (фейкові)	90,20%	95,00%	91,40%	89,20%
	Повнота (фейкові)	70,20%	63,00%	68,60%	68,80%
	F-міра (фейкові)	79,00%	75,80%	78,40%	77,80%
	Прецизійність (достовірні)	91,40%	89,80%	91,00%	91,40%
	Повнота (достовірні)	97,80%	99,00%	98,00%	97,60%
	F-міра (достовірні)	94,40%	93,80%	94,60%	94,40%

З результатів, поданих в таблиці, можна зробити наступні висновки:

- Для всіх моделей, окрім методу k найближчих сусідів, оверсемплінг підвищує загальну точність на 0,4-6,2%.
- Оверсемплінг має позитивний вплив на прецизійність та повноту моделі наївного Баєса.
- Модель k найближчих сусідів практично не здатна знаходити фейкові новини за умови відсутності оверсемплінгу.
- Оверсемплінг позитивно впливає на пошук фейкових новин використовуючи модель опорних векторів.
- Прецизійність та повнота моделі випадкового лісу практично не зазнає впливу оверсемплінгу.
- Обидва векторизатори мають приблизно однакові результати для моделі наївного Баєса, опорних векторів та випадкового лісу.
- Використання TFIDF векторизатору для методу k найближчих сусідів значно підвищує точність та повноту пошуку саму достовірних новин.

Також варто проаналізувати вплив власних параметрів моделей на їх ефективність. Наприклад, параметр α в наївному Баєсі використовується для додаткової регуляризації (зглажування).

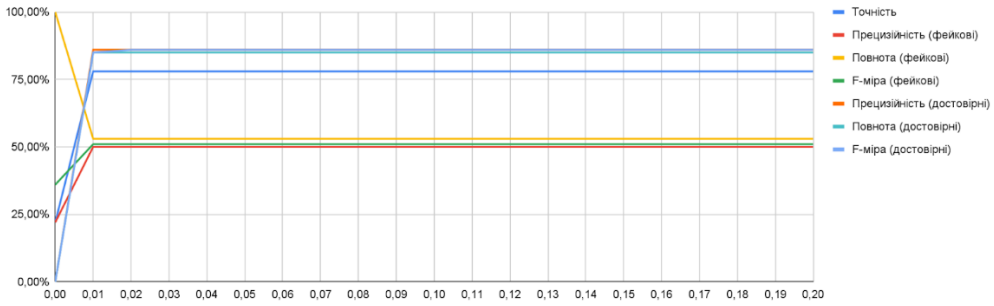


Рис. 1. Вплив регуляризації на ефективність моделі наївного Баєса

На діаграмі показана залежність метрик ефективності моделі наївного Баєса від параметру альфа. З графіку випливає, що при значенні альфа, що дорівнює 0, модель класифікує всі елементи набору даних як фейкові. Використавши навіть невелике ненульове значення alpha можна привести модель до робочого стану.

Модель k-найближчих сусідів має ряд параметрів, одна з них це k – кількість найближчих точок до яких рахується відстань.

З графіку можна помітити, що після $k = 5$ відзначається різке зменшення якості класифікації фейкових новин. Також експерименти не показали, що використання манхетенської відстані замість евклідової, або пропорційні вагові коефіцієнти суттєво позитивно впливають на якість класифікації.

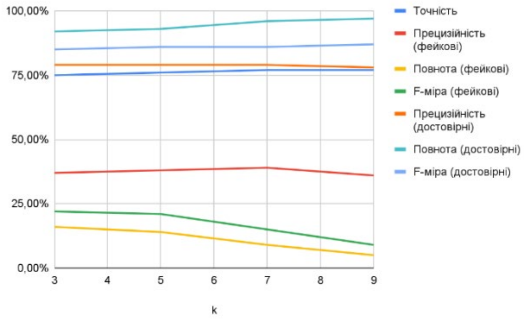


Рис. 2. Вплив параметру k на ефективність моделі k найближчих сусідів

Ефективність моделі опорних векторів має високу залежність від відображення, що використовується при переході між векторними просторами. З наступного графіку можна помітити, що для задач класифікації текстових новин найкраще підходить сигмоїдна функція.

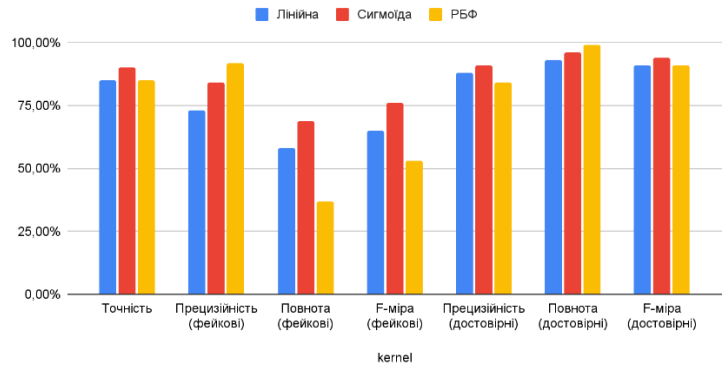


Рис. 3. Залежність ефективності моделі опорних векторів від обраного перетворення

Ефективність моделі випадкового лісу в значній мірі залежить від кількості дерев, що входять до його складу. З графіку нижче можна зробити висновок, що 50 дерев є оптимальною кількістю для даної задачі.

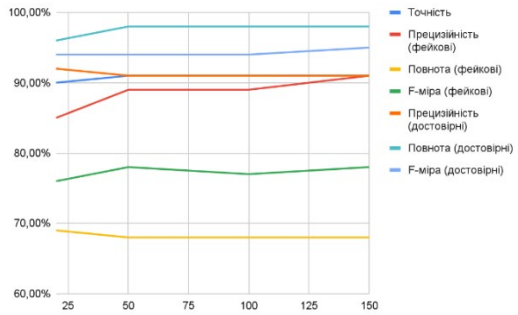


Рис. 4. Залежність ефективності моделей від кількості дерев в моделі випадкового лісу

Висновки

В рамках дослідження було проведено огляд моделей машинного навчання для класифікації текстових новин на предмет достовірності. Проведено аналіз впливу оверсемплінгу та векторизації на якість класифікації, а також вплив власних параметрів моделей на їх ефективність. Також було визначено наступне:

1. Найефективнішими моделями для класифікації фейкових новин є модель випадкового лісу на наївний Баєс. Найбільш значний вплив оверсемплінгу прослідковується для моделі наївного Баєса. Вплив оверсемплінгу на модель випадкового лісу незначний.
2. Використання TFIDF векторизатора в порівнянні з простим CountVectorizer несуттєво впливає на ефективність усіх моделей окрім моделі k найближчих сусідів за рахунок зменшення ваги часто вживаних слів.
3. Додаткова регуляризація є обов'язковою для моделі наївного Баєса, хоча і не вимагаються високі значення цього параметру.
4. Модель k найближчих сусідів не демонструє росту ефективності при збільшенні кількості точок, що беруть участь у класифікації. Найвищу ефективність дана модель показує при досить невисоких значеннях k.
5. Сигмоїда показала найкращі показники ефективності в якості відображення для моделі опорних векторів.
6. Модель випадкового лісу демонструє оптимальні показники ефективності при досить невисоких значеннях кількості дерев. Так, при класифікації набору даних обсягом біля 10000 новин, випадковий ліс з 50 дерев показує достатню ефективність.

Література

1. Ahmed H. Aliwy, Esraa H. Abdul Ameer. Comparative Study of Five Text Classification Algorithms with their Improvements. *International Journal of Applied Engineering Research* Vol. 12, 2017, Number 14, ISSN 0973-4562. pp.
2. Набір даних фейкових та достовірних українських новин. URL: https://www.kaggle.com/datasets/zepopo/ukrainian-fake-and-true-news

References

1. Ahmed H. Aliwy, Esraa H. Abdul Ameer. Comparative Study of Five Text Classification Algorithms with their Improvements. *International Journal of Applied Engineering Research* Vol. 12, 2017, Number 14, ISSN 0973-4562. pp. 4309-4319
2. Ukrainian fake and true news dataset. URL: https://www.kaggle.com/datasets/zepopo/ukrainian-fake-and-true-news

МЕТАВСЕСВІТИ ТА ЇХ ПОТЕНЦІАЛ ДЛЯ РЕВОЛЮЦІЇ В ОСВІТІ

Ємець Максим Ігорович
Аспірант ІІ курсу, група КІ-22-1, спеціальність 123 «Комп'ютерна інженерія»
https://orcid.org/0009-0006-6661-9672
Відкритий міжнародний університет розвитку людини «Україна», м. Київ
Науковий керівник: Даценко І. П., к.т.н.
Відкритий міжнародний університет розвитку людини «Україна», м. Київ

Вступ

Метавсесвіт — це віртуальний простір, де користувачі взаємодіють через аватари в реальному часі. Метавсесвіт може значно змінити освіту, забезпечуючи інтерактивні та динамічні формати навчання. У часи дистанційного навчання він пропонує нові можливості для залучення учнів/студентів і покращення освітнього процесу.

Поняття та розвиток метавсесвітів

Метавсесвіт — це цифровий простір, що об'єднує віртуальну та доповнену реальність, де користувачі можуть взаємодіяти через аватари. Концепція метавсесвіту бере свій початок з наукової фантастики 1990-х років, але значного розвитку набула з появою потужних VR та AR технологій у 2010-х роках. До основних гравців належать компанії Meta (Facebook), Microsoft, Epic Games та Roblox, які активно розробляють та впроваджують метавсесвітні технології.

Переваги метавсесвітів для освіти

Метавсесвіти забезпечують високу інтерактивність, що сприяє більшому залученню студентів у навчальний процес через ігрові елементи та віртуальні симуляції. Викладачі можуть створювати віртуальні класи та лабораторії, де студенти проводять експерименти та взаємодіють із навчальними матеріалами у безпечному середовищі. Метавсесвіти дозволяють студентам взаємодіяти з викладачами та ресурсами з усього світу, розширюючи їхній доступ до знань та експертів у різних галузях.

Технології, що підтримують метавсесвіти

VR та AR технології дозволяють створювати іммерсивні віртуальні середовища, які відтворюють реальний світ або створюють нові, динамічні для навчання та взаємодії. AI використовується для аналізу даних про навчальний процес та студентів з метою персоналізації навчання, адаптації матеріалів до потреб кожного учня та надання індивідуальних рекомендацій. Блокчейн використовується для забезпечення безпеки та недоторканості даних у метавсесвітах, а також для створення довірених систем сертифікації та відстеження успішності студентів.

Виклики та ризики впровадження метавсесвітів в освіту

Не всі навчальні заклади мають достатньо розвинуту технічну інфраструктуру для підтримки метавсесвітів, що може стати перешкодою у їх впровадженні. Використання метавсесвітів може поглибити цифрову нерівність, оскільки не всі студенти мають доступ до необхідного обладнання та інтернету для взаємодії з цими технологіями. Збільшений обсяг особистих даних, що збираються у метавсесвітах, може стати об'єктом зловживання та порушень конфіденційності.

Для успішного впровадження потрібні надійні системи захисту даних та конфіденційності.

Практичні приклади та кейси

VirBELA: Платформа для віртуальних конференцій та навчання, що надає можливість віртуального спілкування та співпраці для студентів та викладачів.

AltspaceVR: Використовується для проведення віртуальних уроків та навчальних ігор, що сприяє активній участі студентів у процесі навчання.

Mozilla Hubs: Платформа для створення та спільного відвідування віртуальних просторів, яка може бути використана для організації навчальних заходів та проектів. Labster: Віртуальна лабораторія, де студенти можуть виконувати реальні наукові експерименти у віртуальному середовищі, що дозволяє їм отримати практичний досвід без необхідності доступу до фізичного обладнання.

Досвід окремих закладів освіти та програм. Harvard University: За допомогою VR технологій вивчаються історичні події та архітектурні об'єкти для збільшення інтерактивності та залучення студентів. University of California, Berkeley: Використання VR та AR для вивчення біології, географії та інших наукових дисциплін.

Огляд найбільш перспективних проєктів та платформ. Facebook Horizon: Платформа від Meta для створення та відвідування віртуальних світів, що може бути використана для навчання. Microsoft Mesh: Платформа для спільної роботи та навчання у віртуальному просторі, що поєднує VR, AR та хмарні технології.

Перспективи та майбутнє метавсесвітів в освіті

Зростаючі технології VR, AR та AI приведуть до подальшого розвитку метавсесвітів у навчанні. Прогрес у цих областях дозволить створювати більш реалістичні, інтерактивні та персоналізовані освітні середовища, що сприятимуть кращому засвоєнню матеріалу та підвищенню мотивації студентів.

Можливі сценарії інтеграції метавсесвітів у традиційну систему освіти.

1. Віртуальні класи та лекції: Використання метавсесвітів для проведення занять та лекцій, що розширює доступ до освіти та створює нові можливості для взаємодії між студентами та викладачами.
2. Віртуальні практичні заняття: Створення віртуальних лабораторій та симуляцій для набуття практичних навичок та експериментів без необхідності фізичного обладнання.
3. Глобальний доступ до ресурсів: Використання метавсесвітів для співпраці та обміну знаннями зі спеціалістами та студентами з усього світу.

Метавсесвіти мають значний потенціал для перетворення освіти, забезпечуючи інтерактивні, залучаючі та персоналізовані навчальні середовища. Завдяки постійному розвитку технологій та поширенню доступу до них, метавсесвіти обіцяють стати невід'ємною складовою сучасної освіти, яка сприятиме підвищенню якості та доступності освіти для всіх.

Висновки. Метавсесвіти пропонують інтерактивне та персоналізоване навчання, розширюючи можливості освіти. Їх розвиток відкриває нові перспективи для трансформації навчального процесу. Важливо продовжувати дослідження та впроваджувати нові технології з метою покращення якості освіти та забезпечення доступності для всіх.

РОЗРОБКА АРХІТЕКТУРИ ЕФЕКТИВНОЇ CI/CD СИСТЕМИ ДЛЯ ПРОГРАМНИХ РІШЕНЬ ЗАСНОВАНИХ НА МІКРОСЕРВІСНІЙ АРХІТЕКТУРІ.

Загорулько А.В.
І курс, група КІ-23-1 phd, спеціальність «Комп'ютерна інженерія»
Інститут комп'ютерних технологій Університету «Україна»
https://orcid.org/0009-0004-9478-5642
Науковий керівник: Тимошенко О.М., к.ф-м.н., доцент

Анотація

Мікросервісна архітектура (MSA) здобула популярність завдяки своїй гнучкості, масштабованості та ефективності, але її впровадження є складним та ресурсоємним процессом. Основні виклики включають зростання кількості сервісів, інфраструктурні витрати та керування залежностями між сервісами. В цьому дослідженні пропонується архітектура ефективної системи неперервної збірки та розгортання (CI/CD), яка вирішує ці проблеми та якісно покращує весь цикл розробки програмного забезпечення (SDLC). Основні принципи включають модульність, використання відкритого API та формування потоку подій, що дозволяє застосовувати методи машинного навчання для аналізу масива подій розробки продукту для локалізації помилок, прогнозування ресурсів, планування наступного циклу розробки, тощо. Потік подій є ключевою особливістю запропонованої архітектури, що забезпечує нові конкурентні переваги серед наявних CI/CD систем.

Abstract

Microservice architecture (MSA) has gained popularity due to its flexibility, scalability, and efficiency, but its implementation is complex and resource-intensive. The main challenges include the growth in the number of services, infrastructure costs, and managing dependencies between services. This study proposes an efficient continuous integration and deployment (CI/CD) system architecture that addresses these issues and significantly improves the entire software development lifecycle (SDLC). The key principles include modularity, the use of an open API, and event stream formation, which allows the application of machine learning methods for analyzing the development event stream to localize errors, forecast resources, plan the next development cycle, and more. The event stream is a key feature of the proposed architecture, providing new competitive advantages among existing CI/CD systems.

Мікросервісна архітектура (MSA) побудови програмних рішень набула популярності в останні десятиліття завдяки гнучкості в питаннях масштабування та продуктивності, швидкості розробки нового та зручності розширення існуючого функціоналу, ефективного використання апаратних ресурсів та переходу до розгортання у хмарних середовищах.

Процес впровадження MSA є досить складним та ресурсоємним[1], при цьому виникають складнощі, обумовлені збільшенням

- кількості сервісів та репозиторіїв коду;
- інфраструктур та витрат на їх розгортання та керування;

та необхідністю

- підтримки конфігурацій сервісів відповідно до кожного оточення розгортання;

- керування залежностями між сервісами та спільними бібліотеками;

- використання гетерогенних сервісних платформ в рамках одного продукту (наприклад, AWS лямбди та Kubernetes сервіси)[2].

Ефективна система неперервної збірки та розгортання (CI/CD) дозволяє подолати проблеми перелічені вище[3].

Принципи архітектури ефективної CI/CD системи:

- модульність;

- базування на відкритому набору специфікацій (API);

- формування потоку подій.

Поєднання модульності та підтримки відкритого API надає можливість:

- використання сторонніх модулів системи;

- комбінування модулів від різних виробників, що дозволяє підвищити надійність та гнучкість системи в цілому.

Під потоком подій розуміємо інформацію, що продукується компонентами CI/CD системи в момент виконання відповідних задач та охоплює весь життєвий цикл продукту для поточного та ретроспективного аналізу стану продукту. Потік подій із залученням методів машинного навчання дозволяє будувати якісні метрики, систему реагування у випадку надзвичайних ситуацій, локалізувати помилки, прогнозувати ресурси та строки поставки нових версій у виробництво, тощо [3,4].

Запропонована модульна архітектура ефективної CI/CD системи на базі відкритого API із залученням методів машинного навчання переводить процес розробки та підтримки MSA програмних рішень на якісно новий рівень, підвищуючи швидкість та якість випуску нових версій, спрощуючи процеси оновлення та міграції на нову інфраструктуру. Потік подій є ключевою особливістю запропонованої архітектури, що забезпечує нові конкурентні переваги серед наявних CI/CD систем.

Список літератури.

1. Newman S., Building Microservices, 2nd Edition / Sam Newman. – O'Reilly Media, Inc., 2021. – 617 p.

2. Davis A., Bootstrapping Microservices with Docker, Kubernetes, and Terraform / Ashley Davis. – New York, USA: Manning Publications, 2021. – 440 p.

3. Eramo R., Muttilo V., Berarrdinelli L., Bruneliere H., AIDOaRt: AI-augmented Automation for DevOps, a Model-based Framework for Continuous Development in Cyber-Physical Systems. [Electronic resource] / Conference: 24th Euromicro Conference on Digital System Design (DSD 2021), Palermo, Itally – Mode of access : https://www.researchgate.net/publication/353268043_AIDOaRt_AI-augmented_Automation_for_DevOps_a_Model-based_Framework_for_Continuous_Development_in_Cyber-Physical_Systems

4. Sabharwal N., Bhardwaj G., Hands-on AIOps Best Practices Guide to Implementing AIOps / Navin Sabharwal, Gaurav Bhardwaj. – New York, USA: Apress, 2022. – 259 p.

ІНФОРМАЦІЙНА МЕРЕЖА НА ОСНОВІ ПРИНЦИПУ SOCIAL IMPACT

Касілов Д.В.
аспірант, група КІ-23-1, спеціальність 123 «Комп'ютерна інженерія»,
Відкритий міжнародний університет розвитку людини «УКРАЇНА»
https://orcid.org/0009-0001-9314-5019
Науковий керівник: Писарчук О.О. доктор технічних наук, професор,
Відкритий міжнародний університет розвитку людини «УКРАЇНА»

Анотація. Розглянуто проблематику існуючих універсальних соціальних мереж, які не мають інструментів для вирішення специфічних завдань волонтерських та соціально відповідальних ініціатив. Запропоновано бачення необхідної спеціалізованої інформаційної мережі. Основним принципом інформаційної платформи є Social Impact, який сприяє просуванню соціальних проєктів та зменшенню негативного впливу на когнітивне та ментальне здоров'я користувачів.

Ключові слова: соціальні мережі, розподілені інформаційні системи (РІС), волонтерські ініціативи, Social Impact.

INFORMATION NETWORK BASED ON THE PRINCIPLE OF SOCIAL IMPACT

Kasilov D.V.
graduate student, group KI-23-1, specialty 123 "Computer Engineering",
Open International University of Human Development "UKRAINE"
https://orcid.org/0009-0001-9314-5019
Academic supervisor: Pisarchuk O.O. Doctor of Technical Sciences, Professor
Open International University of Human Development "UKRAINE"

Abstract. The problems of existing universal social networks, which do not have tools for solving specific tasks of volunteer and socially responsible initiatives, are considered. The vision of the necessary specialized information network is proposed. The main principle of the information platform is Social Impact, which promotes the promotion of social projects and reduces the negative impact on the cognitive and mental health of users.

Keywords: social networks, distributed information systems (DIS), volunteer initiatives, Social Impact.

Універсальні соціальні мережі, такі як Facebook, Instagram та інші, орієнтовані на масову аудиторію і надають інструменти для загальної соціальної взаємодії, але не орієнтовані на вирішення специфічних потреб окремих груп користувачів, зокрема громадських організацій, благодійних фондів, волонтерів та соціально відповідальних громадян. В сучасних умовах війни в Україні зростає кількість соціальної активності громадян, що сигналізує про необхідність створення спеціалізованої інформаційної платформи, яка б забезпечувала інструменти для координації дій, планування заходів, збору коштів та ресурсів, а

також прозорого обміну інформацією для ефективної діяльності соціальних ініціатив.

Основним принципом побудови нової спеціалізованої інформаційної мережі є концепція Social Impact [2]. Він сприяє просуванню соціально відповідальних проєктів та людей, які займаються благодійністю, волонтерством та вирішенням суспільно важливих питань.

Така платформа має надавати інструменти для точної верифікації користувачів, безпечної комунікації, можливості організації обговорення суспільно важливих питань, підготовки і проведення благодійних та суспільно значущих заходів, об'єднувати унікальну репутаційну систему і широкі можливості для бізнеса.

Така мережа також має запобігти впливу різного роду ІПСО, оскільки вони часто спричиняють підвищену тривожність, соціальну ізоляцію та депресію через негативний контент [1]. За рахунок алгоритмів, що сприяють підвищенню соціальної згуртованості та підтримки, ця мережа сприятиме здоровій комунікації та створенню безпечного інформаційного простору.

Для побудови такої розподіленої інформаційної системи (РІС) необхідна масштабована архітектура [3] та апаратна частина, для проєктування яких слід використовувати науковий підхід, заснований на багатофакторних математичних моделях [4], що враховують обсяг даних, швидкість обробки запитів, навантаження на сервери, потреби користувачів та інші фактори. Такий підхід є універсальним і в подальшому дозволить синтезувати оптимальну інформаційну архітектуру для будь-якої корпоративної соціальної мережі, яка базується на принципі Social Impact.

Список використаних джерел:

1. Darshana Sedera. Human Degradation and Social Media Use Human Degradation with the use of Social Media: A Theological Perspective / Darshana Sedera, Sachithra Lokuge, Dharshani Chandrasekara // The International Conference on Information Systems ICIS 2017At: Seoul Korea – 2017 – С. 1-9.
2. Deepa Lakshmi N. Innovative Models in Social Entrepreneurship: Balancing Profit with Social Impact / Deepa Lakshmi N // Library Progress International| Vol.44 No.3 – Jul-Dec 2024 – С. 14056-14062.
3. С.Д. Приходченко. Обґрунтування вибору мікросервісної архітектури в порівнянні з монолітною / С.Д. Приходченко, К.С. Родна, Р.В. Поштак // Україна, Дніпро, НТУ «Дніпровська політехніка» – 2018 – С. 70-73.
4. О.О. Писарчук. Багатокритеріальна математична модель структурного та параметричного синтезу складної інформаційної системи / О.О. Писарчук. // В. Даля – 2010 – С. 38-44.

КАТЕГОРІЇ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЛЯ БАГАТОФАКТОРНОГО ОЦІНЮВАННЯ СТАНУ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ЗА ДАНИМИ ВІД SIEM-СИСТЕМ

Кошара А.В.
аспірант, група КІ-23-1, спеціальність 123 «Комп'ютерна інженерія»,
Відкритий міжнародний університет розвитку людини «УКРАЇНА»
https://orcid.org/0009-0000-8468-2704
Науковий керівник: Писарчук О.О. доктор технічних наук, професор,
Відкритий міжнародний університет розвитку людини «УКРАЇНА»

Анотація. *Розглядається актуальна проблема зростання кіберзагроз у світі, що посилюється з розвитком технологій штучного інтелекту. Особлива увага приділяється впливу цих загроз на державний сектор. Кіберзагрози класифікуються на три рівні: соціальна інженерія, мережевий рівень і рівень кінцевих точок, з детальним описом індикаторів для кожного з них. Підкреслено важливість аналізу індикаторів ризиків інформаційної безпеки та окреслено перспективи майбутніх досліджень, спрямованих на формалізацію системи індикаторів загроз і багатофакторне оцінювання.*

Ключові слова: *SIEM, індикатори, ризики, інформаційна безпека, багатофакторне оцінювання, державний сектор, аналіз.*

CATEGORIES OF INFORMATION SECURITY THREATS FOR MULTIFACTOR ASSESSMENT OF THE SECURITY STATE OF INFORMATION AND TELECOMMUNICATION SYSTEMS ACCORDING TO DATA FROM SIEM SYSTEMS

Koshara A.V.
graduate student, group KI-23-1, specialty 123 "Computer Engineering", Open International University of Human Development "UKRAINE"
https://orcid.org/0009-0000-8468-2704
Academic supervisor: Pisarchuk O.O. Doctor of Technical Sciences, Professor, Open International University of Human Development "UKRAINE"

Abstract. *Under consideration the current issue of increasing cyber threats worldwide, exacerbated by the development of artificial intelligence technologies, is being examined. Special attention is given to the impact of these threats on the public sector. Cyber threats are classified into three levels: social engineering, network level, and endpoint level, with a detailed description of the indicators for each. The importance of analyzing information security risk indicators is emphasized, and the prospects for future research aimed at formalizing the threat indicator system and multifactor assessment are outlined.*

Key words: *SIEM, indicators, risks, information security, multi-factor assessment, public sector, analysis.*

Паралельно з швидким розвитком комп'ютерних систем розширюється і коло можливих загроз. У зв'язку з недавнім "бумом" технологій штучного інтелекту (ШІ)

тенденція збільшення впливу кіберзагроз у найближчі десять років тільки посилюватиметься.

Варто розуміти, що загрози інформаційної безпеки є комплексним поняттям, яке характеризується різними індикаторами (факти, ризики, потенції). Тип загроз та їхній рівень (severity) визначаються залежно від поєднання цих індикаторів. Для оцінки рівня захищеності ІТС за даними від SIEM, на основі таких індикаторів, необхідно розробити інфологічну модель факторів. Ця модель дозволить визначити чинники, що впливають на стан захищеності ІТС державного сектору за даними від SIEM та їхній взаємозв'язок.

В кожен проміжок часу, перелік індикаторів та загроз може змінюватися, що спонукає до проведення інтелектуального аналізу даних. Інтелектуальний аналіз даних є складним процесом обробки та аналізу великих обсягів інформації з метою виявлення прихованих закономірностей, трендів і потенційних ризиків. Системи управління безпекою інформаційних подій (SIEM) застосовують цей вид аналізу для забезпечення ефективного моніторингу, аналізу та оцінки подій, пов'язаних з інформаційною безпекою, в інформаційно-телекомунікаційних системах. Завдяки цьому підходу вдається своєчасно виявляти потенційні загрози, що дозволяє вжити необхідних заходів для захисту критичної інформаційної інфраструктури.

Сучасні загрози інформаційно-телекомунікаційним системам, особливо в контексті кібервійн, можна класифікувати на три основні категорії або рівні. Перший рівень - соціальна інженерія, до прикладів якої належить фішинг. Другий рівень - мережевий, що включає загрози, пов'язані з проникненням у мережеву інфраструктуру. Третій рівень - кінцеві точки, де загрози спрямовані на індивідуальні пристрої користувачів.

Майбутні дослідження має бути спрямовано на математичну формалізацію взаємовідносин описаних факторів\індикаторів з подальшим застосуванням методів багатофакторного оцінювання. Результатом майбутніх досліджень повинна стати інтегрована оцінка загроз, величина якої буде пропорційна їхньому рівню, а зміст індикаторів відповідатиме їхньому типу. Це означає, що кожен індикатор буде точно відображати специфіку відповідної загрози, що дозволить отримати більш точні та релевантні результати оцінки.

Список використаної літератури

1. О.О Писарчук, Миронов Ю.О. Інфологічна модель факторів, показників та ознак, що характеризують хромосомні патології за результатами аналізу зображень каріограм пацієнта MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES, (1), 198–205.

2. Моніторинг об‘єктів в умовах апріорної невизначеності джерел інформації : [монографія] / Ю. Я. Бобало, Ю. Г. Даник, Л. О. Комарова, О. О. Лук‘янов, В. М. Максимович, О. О. Писарчук, В. В. Ріппенбейн, Р. Т. Смук, В. С. Стогній, Ю. Б. Сторонський, Б. М. Стрихалюк. – Львів, 2015. – 360 с. – Бібліографія: с. 351–359 (130 назв)

3. Писарчук О. О. Оцінювання ефективності інформаційних систем за вектором критеріїв // Збірник наукових праць ЖВІ НАУ. Випуск 3. – 2010. – С. 117–123.

4. Писарчук О. О. Розроблення багатокритеріальної методики ситуаційного управління структурою і параметрами системи забезпечення інформаційної безпеки / О. О. Писарчук, К. О. Соколов, О. П. Гудима // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. - 2016. - № 3. - С. 24-32.

МЕТОДИ ПОБУДОВИ МІКРОСЕРВІСНОЇ АРХІТЕКТУРИ В ХМАРНИХ СХОВИЩАХ

Михайленко О.О.
ІІ курс, група КІ-22-1, спеціальність «Комп'ютерна інженерія»,
Інститут комп'ютерних технологій Університету «Україна».
https://orcid.org/0009-0009-9320-8292

Анотація

У сучасному інформаційному світі проблема проектування та створення якісного програмного забезпечення є надзвичайно важливою. Під час розвитку ІТ-індустрії було знайдено багато різних методів та способів будування складних програмних систем. Одним з показників гарно побудованої програми є її архітектура, вона повинна вірно описувати предметну область та бути формальною моделлю системи. Можна вважати архітектурою програмної системи набір певних структурних компонентів зв'язаних між собою, що задають поведінку усієї системи. Основною задачею архітектури є управління складністю, елегантне та доцільне відображення предметної області.

In today's information world, the problem of designing and creating quality software is extremely important. During the development of the IT industry, many different methods and ways of building complex software systems were found. One of the indicators of a well-built program is its architecture, it should accurately describe the subject area and be a formal model of the system. The architecture of a software system can be considered a set of certain structural components connected to each other that determine the behavior of the entire system. The main task of architecture is complexity management, elegant and expedient representation of the subject area.

Об'єкт дослідження

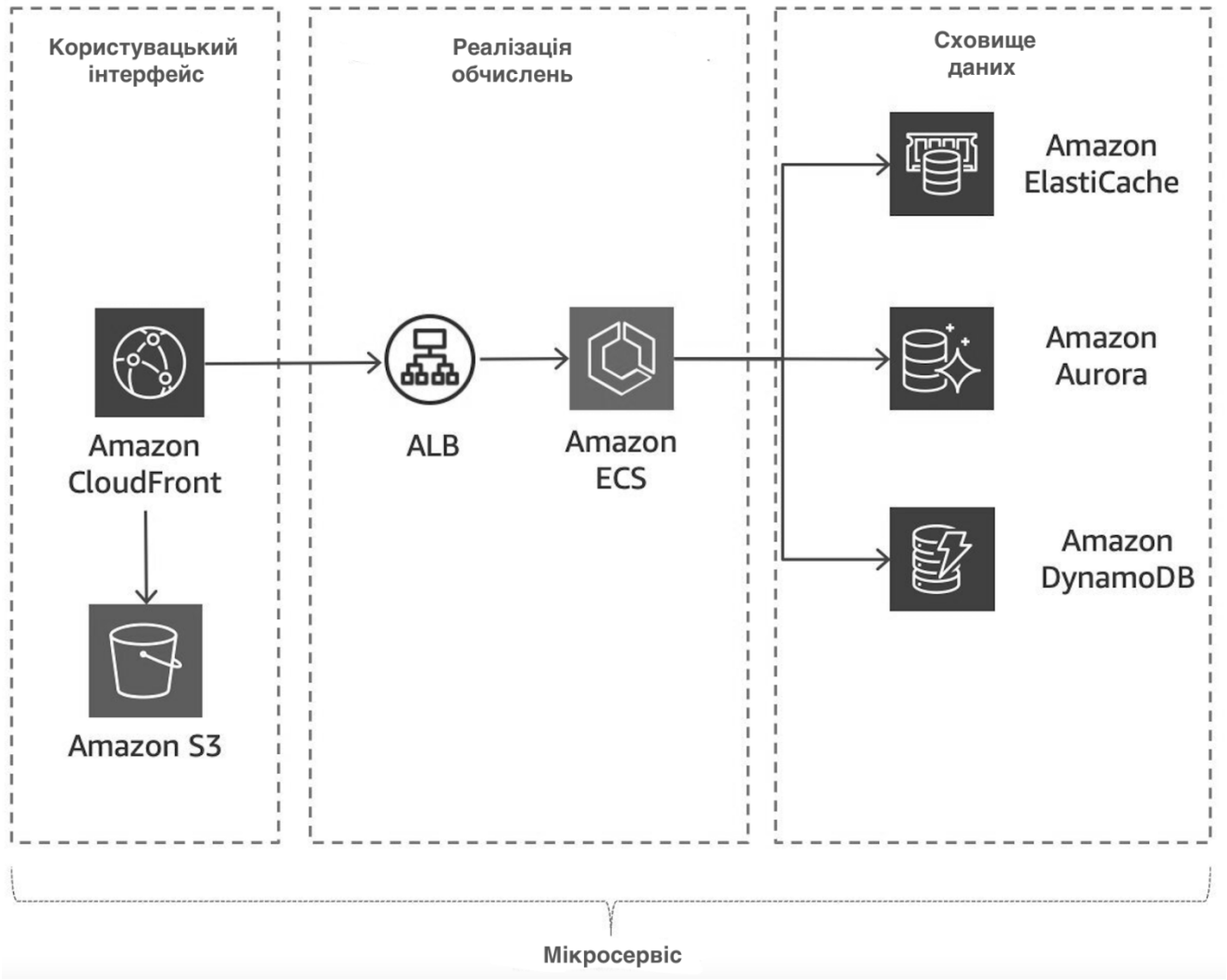
Мікросервіси представляють архітектурний стиль, в якому складні додатки створені як сукупність маленьких, легких, самодостатніх, незалежних, нетісно-зв'язаних сервісів, кожен з яких відповідальний за конкретний процес. Такий стиль протиставляється монолітному стилю, згідно з яким додатки будуються як єдине ціле. Мікросервіси співпрацюють один з одним на основі потреби виконання певної дії. Вони «спілкуються» через API, для яких не має значення мова програмування. Мікросервіси поєднують успішні та перевірені концепції з різних областей, таких як:

- Гнучка розробка програмного забезпечення
- Сервісно-орієнтовані архітектури
- API дизайн
- Безперервна інтеграція/безперервна доставка (CI/CD)

Хоча мікросервіси пропонують багато переваг, життєво важливо оцінити унікальні вимоги вашого сценарію використання та пов'язані з цим витрати. Мікросервісна архітектура стає дійсно зручною, якщо система буде розгортатися в хмарі. В якості хмари буде використовуватися AWS - Amazon Web Services.

Проста архітектура мікросервісів на AWS

Типові монолітні програми складаються з різних шарів: презентаційного



рівня, прикладного рівня та рівня даних. Архітектури мікросервісів, з іншого боку, розділяють функціональні можливості на цілісні *вертикалі* відповідно до конкретних доменів, а не технологічних рівнів. На малюнку показано еталонну архітектуру для типової програми мікросервісів на AWS.

Інтерфейс користувача

Сучасні веб-програми часто використовують фреймворки JavaScript для розробки односторінкових програм, які взаємодіють із серверними API. Ці API зазвичай створюються з використанням Representational State Transfer (REST) або RESTful API, або GraphQL API.

Впровадження мікросервісів

API вважаються *вхідними дверима* мікросервісів, оскільки вони є точкою входу для логіки програми. Зазвичай використовуються API веб-служб RESTful або API GraphQL. Ці API керують і обробляють клієнтські виклики, обробляючи такі функції, як керування трафіком, фільтрація запитів, маршрутизація, кешування, автентифікація та авторизація. AWS пропонує будівельні блоки для розробки мікросервісів, включаючи Amazon ECS і Amazon EKS як вибір механізмів

оркестровки контейнерів, а також AWS Fargate і EC2 як варіанти розміщення. AWS Lambda — це ще один безсерверний спосіб створення мікросервісів на AWS. Вибір між цими варіантами хостингу залежить від вимог замовника щодо керування основною інфраструктурою. AWS Lambda дозволяє завантажувати ваш код, автоматично масштабувати та керувати його виконанням із високою доступністю. Це усуває потребу в управлінні інфраструктурою, тому ви можете швидко рухатися та зосередитися на своїй бізнес-логіці. Lambda підтримує кілька мов програмування та може запускатися іншими службами AWS або викликатися безпосередньо з веб- чи мобільних додатків.

ДОСЛІДЖЕННЯ МАШИННОГО НАВЧАННЯ НА ОСНОВІ РЕКОМЕНДАЦІЙНИХ СИСТЕМ

Мойсеєнко Олег Вячеславович
аспірант
Відкритий міжнародний університет розвитку людини «Україна»
м. Київ, Україна
nickcambel5@gmail.com, https://orcid.org/0009-0003-2488-287X

Анотація: У реаліях інформаційного перенасичення, рекомендаційні системи стають ключовим інструментом для ефективного відбору контенту, враховуючи індивідуальні потреби користувачів. Дане дослідження спрямоване на розробку рекомендаційної системи з використанням методів машинного навчання, з фокусом на адаптації до унікальних вподобань користувачів. Розроблена система, заснована на машинному навчанні, відзначається високою ефективністю у персоналізації контенту. Обговорення включає порівняння з існуючими системами та визначення переваг запропонованого підходу. Дослідження підтверджує актуальність розробки рекомендаційних систем у сучасних умовах. Розроблена система на основі машинного навчання виявляється ефективною у задоволенні індивідуальних потреб користувачів.

Abstract: In the realities of information overload, recommendation systems become a key tool for effective content selection, considering individual user needs. This study aims to develop a recommendation system using machine learning methods, focusing on adaptation to users' unique preferences. The developed system, based on machine learning, demonstrates high efficiency in content personalization. The discussion includes a comparison with existing systems and the identification of the advantages of the proposed approach. The study confirms the relevance of developing recommendation systems in modern conditions. The developed machine learning-based system proves effective in meeting individual user needs.

Вступ/Introduction. У сучасних умовах інформаційного перенасичення, рекомендаційні системи відіграють критичну роль у допомозі користувачам знаходити релевантний контент. Враховуючи значне зростання кількості мобільних додатків та ігор, особливо актуальним стає питання розробки ефективних систем рекомендацій.

Мета дослідження/Aim. Ця робота має на меті дослідження та розробку рекомендаційної системи з використанням методів машинного навчання. Основна увага приділяється адаптації системи до унікальних вподобань користувачів.

Методи/methods. Для розробки рекомендаційної системи використовувались методи машинного навчання, зокрема алгоритми колаборативної фільтрації та методи обробки великих даних. Програмування здійснювалось за допомогою мови Python та бібліотек TensorFlow і Scikit-learn.

Результати та обговорення/Results and discussion. Розроблена система демонструє високу ефективність у персоналізації контенту для користувачів.

Порівняння з існуючими системами показало, що запропонований підхід забезпечує більш точні та релевантні рекомендації.

Висновки/Conclusions. Дослідження підтвердило важливість розробки рекомендаційних систем у сучасних умовах. Розроблена система, заснована на машинному навчанні, виявилась ефективною у задоволенні індивідуальних потреб користувачів.

ПРО МЕРЕЖЕВІ АТАКИ НА БЕЗПЕКУ В ІНТЕРНЕТІ РЕЧЕЙ

Остапенко В. І.
І курс, аспірантура, спеціальність «Комп'ютерна інженерія»,
Інститут комп'ютерних технологій Університету «Україна».
https://orcid.org/0009-0002-7394-5307
Науковий керівник: Дуднік А. С., д.т.н., доцент,
Інститут комп'ютерних технологій Університету «Україна»

Концепція Інтернету речей (IoT) впливає на різні сфери життя, такі як медицина, транспорт, торгівля та інші. Проте широке різноманіття застосування IoT призводить до актуалізації питань безпеки у цій галузі. У роботі розглядаються найбільш поширені загрози безпеці в IoT із точки зору мережевих технологій. Підкреслюється необхідність завчасного виявлення потенційних атак на IoT-пристрої для запобігання кіберзлочинам.

The concept of the Internet of Things (IoT) impacts various spheres of life, such as healthcare, transportation, commerce, and others. However, the wide variety of IoT applications leads to the actualization importance of security issues in this field. The paper discusses the most common security threats in IoT from the perspective of networking technologies. Emphasis is placed on the necessity of timely detection of potential attacks on IoT devices to prevent cybercrime.

Концепція Інтернету речей невпинно проникає у численні сфери людського життя, такі як медицина, освіта, державне управління та ін. Можна виділити такі поширені застосування розумних пристроїв: розумні будинки (додатки дозволяють управляти освітленням, системами безпеки, розумними замками, камерами тощо); розумні автомобілі (підвищують безпеку водіння, сповіщають про дорожні інциденти та ін.); розумні носимі технології (відстеження фізичної активності та стану здоров'я, допомога, щодо виявлення хвороби на початкових стадіях); розумні технології в енергомережах (забезпечення моніторингу споживання енергії, покращення ефективності її передачі, взаємодія із відновлювальними джерелами енергії); промисловий Інтернет речей (IIoT) (підключення виробничого обладнання у промислових умовах, дозволяє збирати та аналізувати дані для покращення операційної ефективності та надійності); охорона здоров'я (збирання даних про здоров'я пацієнтів, що надалі може бути використано для діагностики); технології роздрібної торгівлі (IoT оптимізує процеси покупки, оптимізація розміщення товарів та створення магазинів без касирів); технології у сільському господарстві (IoT допомагає фермерам покращувати виробничі практики, збільшувати врожайність, відстежуючи стан ґрунту, використовуючи аналітику про погодні ризики) [1].

Можна зазначити, що у 2013 році було зафіксовано перший ботнет, який включав смартпристрої, такі як телевізори та радіоняні. Це стало сигналом про нову еру кіберзагроз, де не тільки комп'ютери та сервери, але й побутові пристрої можуть бути використані для атак. У 2016 році багато відомих вебсайтів, включаючи Netflix, Twitter та New York Times, стали недоступними через масовану атаку типу DDoS (розподілене відмовлення в обслуговуванні). Ця атака була здійснена за допомогою смартпристроїв, які були заражені шкідливим програмним

забезпеченням і використані для перевантаження серверів цих вебсайтів. Цей інцидент підкреслив важливість забезпечення безпеки IoT-пристроїв, щоб запобігти їх використанню в кіберзлочинах [2].

Щодо можливих мережевих атак в IoT можна виділити: атаки аналізу трафіку (зловмисник перехоплює та аналізує повідомлення для отримання інформації про мережу); підробка RFID (фальсифікуються сигнали RFID через запис інформації, що передається з RFID-мітки); атаки спуфінгу (зловмисник надає неправильну інформацію, яка маскується під правильну та приймається системою); клонування RFID (зловмисник копіює дані з існуючої мітки RFID на іншу, можливо, вставляючи неправильні дані або контролюючи передачу даних через клонований вузол); несанкціонований доступ RFID (у випадку відсутності належної автентифікації в системах RFID, зловмисник може спостерігати, змінювати або видаляти інформацію на вузлі); атака типу "Воронка" (зловмисник компрометує вузол всередині мережі та використовує його для здійснення атаки, привертаючи трафік та змінюючи дані); атака "людина посередині" (зловмисник через Інтернет перехоплює комунікацію між двома вузлами, отримуючи конфіденційну інформацію шляхом підслуховування); відмова в обслуговуванні (зловмисник переповнює мережу великим трафіком, що призводить до недоступності послуг для користувачів); атаки на інформацію про маршрутизацію (зловмисник може ускладнити мережу, змінюючи або відправляючи хибну інформацію про маршрутизацію, що може призвести до відхилення або втрати пакетів, надсилання невірних даних або розділення мережі); атака Сивілли (у цьому типі атаки зловмисний вузол приймає ідентичність декількох вузлів і діє від їх імені, що може призвести до несанкціонованого впливу в мережі) [2].

Проте вище згаданий перелік типів атак не є вичерпним. Нові атаки можуть легко уникнути наявних методів виявлення на основі сигнатур, і їх надзвичайно важко виявити. Тому виявлення та класифікація мережевих атак також має важливе значення для підвищення надійності пристроїв в сфері Інтернету речей.

Список використаних джерел

1. Kaustubh Dhondge // Lifecycle IoT Security for Engineers. Artech, 2021.
2. Yang, Y., Wu, L., Yin, G., Li, L. Zhao, H., // A Survey on Security and Privacy Issues in Internet-of-Things. 2017. IEEE Internet of Things Journal. Volume 4, № 5, pp. 1250-1258.
3. Buczak, A. Guven, E. // A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. 2016. IEEE Communications Surveys & Tutorials. Volume 18, № 2, pp. 1153-1176.

СУЧАСНІ ТЕХНОЛОГІЇ НАВЧАННЯ У ВИЩИХ НАВЧАЛЬНИХ ЗАКЛАДАХ

Помазун Олена Олександрівна
асистент кафедри інформаційних технологій та туризму
Луцький інститут розвитку людини Університету "Україна"
https://orcid.org/0009-0003-0803-6307

Анотація. Технології значно змінюють сучасне навчальне середовище, впливаючи на методи викладання, доступ до освітніх ресурсів та ефективність навчального процесу. У статті розглядаються сучасні технології навчання, що застосовуються у вищих навчальних закладах. Описуються інноваційні підходи та методи, які сприяють підвищенню ефективності освітнього процесу. Висвітлюються переваги використання цифрових технологій, інтерактивних методів навчання, онлайн-курсів та дистанційного навчання. Також обговорюються труднощі, з якими стикаються викладачі та студенти при впровадженні новітніх технологій, та надаються рекомендації щодо їх подолання.

Abstract. Technologies are significantly changing the initial environment, affecting investment methods, access to natural resources and the efficiency of the initial process. The statistics look at current technologies that will be used in greater initial applications. Innovative approaches and methods that increase the efficiency of the lighting process are described. The advantages of using digital technologies, interactive learning methods, online courses and distance learning are highlighted. Also, the difficulties faced by students with the introduction of new technologies are discussed, and recommendations are made for their implementation.

Сучасний світ стрімко розвивається, і вища освіта не залишається осторонь від цих процесів. Технології дуже швидко перетворюють наше життя, і освіта не виключення. У вищій освіті вони грають все більш важливу роль, дозволяючи нам навчатися ефективніше та зручніше.

Однією з найбільш відомих і корисних інновацій у сучасній освіті є онлайн-курси та платформи. Цифрові технології стали невід'ємною частиною сучасного навчання. Вони включають використання комп'ютерів, планшетів, смартфонів та інших пристроїв для доступу до освітніх матеріалів. Серед найпоширеніших цифрових технологій можна виділити:

– *Онлайн-курси та платформи:* ресурси, такі як Coursera, edX та інші, пропонують широкий спектр курсів від провідних університетів світу. Це дозволяє студентам отримувати знання у зручний для них час та місце.

– *Мобільні додатки:* спеціалізовані додатки допомагають студентам організовувати навчальний процес, знаходити необхідну інформацію та виконувати завдання.

– *Хмарні технології:* використання хмарних сервісів для зберігання та обміну даними спрощує спільну роботу над проектами та доступ до навчальних матеріалів.

Інтерактивні методи навчання сприяють активній участі студентів у освітньому процесі. Вони включають:

– *Віртуальні лабораторії:* дозволяють студентам проводити експерименти в онлайн-середовищі, що зменшує витрати на обладнання та матеріали.

– *Симулятори та моделювання:* використовуються для навчання в складних або небезпечних умовах, таких як медицина чи інженерія.

– *Гейміфікація:* включення ігрових елементів у навчальний процес підвищує мотивацію та залученість студентів.

Дистанційне навчання стало особливо актуальним у зв'язку з пандемією COVID-19 та війною. Воно передбачає проведення занять через інтернет із використанням відеоконференцій, онлайн-лекцій та інших дистанційних форм навчання. Основні переваги дистанційного навчання:

– *Гнучкість:* студенти можуть навчатися з будь-якого місця та у зручний для них час.

– *Доступність:* освіта стає доступнішою для людей з обмеженими можливостями та тих, хто живе у віддалених регіонах.

– *Економія часу та коштів:* відсутність потреби у фізичному перебуванні в університеті зменшує витрати на проїзд та проживання.

Незважаючи на численні переваги, впровадження сучасних технологій у вищій школі стикається з низкою питань:

– *Технічні проблеми:* недостатня інфраструктура та технічна підтримка можуть ускладнити використання новітніх технологій.

– *Підготовка викладачів:* викладачі потребують додаткового навчання для ефективного використання цифрових та інтерактивних методів.

– *Залученість студентів:* підтримання високого рівня залученості студентів у дистанційному форматі є складним завданням.

Для вирішення цих питань рекомендується:

– *Інвестувати в інфраструктуру:* забезпечити надійний доступ до інтернету та сучасного обладнання.

– *Проводити навчання для викладачів:* організовувати курси підвищення кваліфікації з використання сучасних технологій у навчанні.

– *Розробляти інтерактивні та залучаючі матеріали:* використовувати мультимедійний контент, інтерактивні завдання та гейміфікацію для підвищення залученості студентів.

Сучасні технології відкривають нові можливості для вищої освіти, роблячи її більш ефективною, доступною та гнучкою. Використання цифрових технологій, інтерактивних методів та дистанційного навчання дозволяє створити інноваційне освітнє середовище, яке відповідає потребам сучасного суспільства. Проте для максимального ефекту необхідно долати технічні та організаційні труднощі, забезпечуючи якісну підготовку як для викладачів, так і для студентів.

Література

1. Арабаджиєв Д. Ю., Сергієнко Т. І. Особливості розвитку сучасного інформаційного суспільства в Україні в умовах політичної конфліктності. The 2 nd International scientific and practical conference «Scientific achievements of modern

society» (October 9-11, 2019). Cognum Publishing House, Liverpool, United Kingdom. 2019. С. 74–79.

2. Сергієнко Т. І. Інформаційні технології в освіті. Українські студії в європейському контексті. 2023. № 6. С. 121–126.

3. Шаров С. В., Лубко Д. В., Осадчий В. В. Інтелектуальні інформаційні системи: навч. посіб. Мелітополь: Вид-во МДПУ ім. Б. Хмельницького 2015. 144с.

ОПТИМІЗАЦІЯ ІНФРАСТРУКТУРИ БАЗ ДАНИХ НА ОСНОВІ AWS I3: ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ТА ЗНИЖЕННЯ ВИТРАТ

Рожков Сергій Миколайович
І І курс аспірантури, група КІ-22-1, спеціальність “Комп’ютерна інженерія”
Інститут комп’ютерних технологій Університету “Україна”
https://orcid.org/0009-0004-2972-7163
Науковий керівник: Павленко В.І., д.т.н., проф.

Анотація. Запропоновані зміни в архітектурі баз даних на основі AWS i3 інстансів спрямовані на оптимізацію використання ресурсів, підвищення продуктивності та зменшення витрат шляхом додавання третього вузла бази даних з локальним 'ефемерним' сховищем для оптимізації ***навантаження*** *читання, перенесення частини резервного вузла на менш потужну інстанцію та використання ефемерних реплік для забезпечення високої доступності та автоматичного перемикання між ними, що сприятиме підвищенню ефективності та надійності інфраструктури.*

Annotation. *The proposed changes in the database architecture based on AWS i3 instances aim to optimize resource utilization, enhance performance, and reduce costs by adding a third database node with local 'ephemeral' storage to optimize read workload, moving part of the standby node to a less powerful instance, and utilizing ephemeral replicas to ensure high availability and automatic failover between them, thus improving the efficiency and reliability of the infrastructure.*

Використання AWS i3 інстансів для read replica

Для зменшення витрат на EBS і EC2 та покращення обслуговування запитів лише для читання та OLAP, (англ. online analytical processing, аналітична обробка у реальному часі) , високонавантажені бази даних (наприклад для застосунків що використовуються для торгівлі на ринках цінних паперів і тд) та торгівлі гарним тоном є використання реплік для читання(read only replica) що зменшує навантаження на основний сервер(primary) що дозволяє значно підвищити продуктивність запитів, що є інтенсивними щодо вводу-виводу, та знизити загальні витрати на інфраструктуру.

Розглянемо стандартну архітектуру:

- 2 вузли бази даних (primary + standby)
- 1 резервний вузол (для BCP та DR)

Бази даних однієї платформи асинхронно реплікуються між двома зонами доступності AWS, забезпечуючи можливості відновлення після катастроф (DR). DR репліка також використовується як джерело лише для читання для SAS та подібних систем.

Запропоновані зміни:

Master DB залишається без змін.

- Додавання третього вузла бази даних з родини i3 з ‘ефемерним’ сховищем (інстанс має додатковий розділ диску який є дуже швидким так как працює в на локальних NVMe-SSD дисках, але при рестарті такого типу інстансу данні не зберігаютья).

- Перенесення навантаження лише для читання (RO) на цей "ефемерний" резервний вузол.
- Зменшення розміру резервного вузла DR до мінімально робочого.

Ці зміни дозволять зробити вузол для читання значно продуктивнішим та зменшать загальні витрати на інфраструктуру. Впровадження четвертого вузла бази даних на іншосу інстансі i3 в іншій зоні доступності (AZ) додатково підвищує надійність та відмовостійкість системи.

Загальний огляд:

- Master DB: велика інстанція m6 з великою потужністю та багатьма PIOPS EBS томами.
- Replica DR: мала інстанція m6, без автоматичного переходу, перемикання здійснюється вручну.
- Ephemerial replica: два інстанси сімейства i3 в різних зонах.

Ефемерні репліки знаходяться у кластері Keepalived, який перевіряє працездатність служби Postgres і здійснює перехід у разі непрацездатності. Ефемерні репліки ніколи не повинні бути підвищені до основних. Перехід перемикає DNS псевдонім standby.replica на іншу репліку.

Процедури переходу реплік:

- Автоматичні.
- Сповіщення для перевірки інженером.
- Репліка завантажується з іншої репліки.
- Репліка реплікується з поточного первинного вузла.

У разі рестарту обох реплік, їх потрібно буде завантажити з первинної або резервної репліки. Звичайне завантаження можна здійснити автоматично через crontab використовуючи ansible:

[root@i3.db03 ~]# crontab -l | grep reboot

@reboot ansible-playbook -b restart-setup 1>/root/ansible.log 2>&1

Playbook викликає ролі максимально автоматизовано:

- hosts: localhost roles: - postgres_ephemeral_ro_standby_setup

Це рішення дозволяє оптимізувати витрати на інфраструктуру, підвищити продуктивність системи та забезпечити надійне обслуговування запитів лише для читання.

ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В АВТОМАТИЗОВАНИХ СИСТЕМАХ УПРАВЛІННЯ СКЛАДСЬКОЮ ЛОГІСТИКОЮ

Рубаняк Т. М.
ІІ курс аспірантури, група КІ-22-1а, спеціальність “Комп’ютерна інженерія”
Інститут комп’ютерних технологій Університету “Україна”
https://orcid.org/0009-0003-4272-7662
Науковий керівник: Тимошенко О. М., к.ф.-м.н., доц.

Сучасні тенденції у розвитку складської логістики включають багато аспектів, які впливають на необхідність автоматизації систем управління.

За останні роки споживчі попити стали більш різноманітними, а процеси глобалізації зробили логістичні мережі складнішими. Це призвело до збільшення обсягів операцій на складах і потреби в ефективних системах управління, які можуть впоратися з цими зростаючими вимогами.

Розглядаються сучасні підходи до інтеграції ШІ для підвищення ефективності складських операцій, зниження витрат та покращення точності обробки замовлень. В останні роки значно зросла увага до застосування ШІ в різних галузях, зокрема в логістиці. Автоматизовані системи управління складом (WMS) значно покращилися завдяки інтеграції технологій ШІ, таких як машинне навчання, комп'ютерний зір та робототехніка.

Застосування ШІ в складських системах дозволяє автоматизувати широкий спектр операцій, від приймання товарів до їх відправлення. Наприклад, роботизовані системи на основі ШІ можуть автоматично сортувати і переміщувати товари на складі, значно скорочуючи час і людські ресурси, необхідні для виконання цих завдань. Комп'ютерний зір використовується для автоматичного розпізнавання та відстеження товарів, що покращує точність інвентаризації та зменшує кількість помилок.

У дослідженні використовувалися методи аналізу та моделювання, які дозволяють оцінити ефективність впровадження ШІ в складські процеси. Було проведено порівняння традиційних та інноваційних підходів до управління складом на основі даних реальних компаній. Впровадження ШІ в автоматизовані системи управління складом дозволяє оптимізувати розміщення товарів для швидшого доступу, використовувати роботизовані системи для автоматизації процесів пакування та відправлення, підвищити точність прогнозування попиту та планування запасів, а також знизити витрати на обслуговування складів за рахунок оптимізації ресурсів.

Одним з ключових аспектів застосування ШІ в складській логістиці є можливість обробки великих обсягів даних у реальному часі. Це дозволяє оперативно реагувати на зміни в попиті, оптимізувати маршрути доставки та забезпечувати високу швидкість виконання замовлень. Використання алгоритмів машинного навчання дозволяє прогнозувати потреби в запасах з високою точністю, що зменшує ризики перенакопичення товарів або їх дефіциту.

Результати дослідження свідчать про значні переваги застосування ШІ в складській логістиці. Впровадження технологій ШІ сприяє не тільки підвищенню

ефективності операцій, але й збільшенню гнучкості та адаптивності складських систем до змін у попиті та умовах ринку. Наприклад, у випадку різкого зростання попиту на певний товар, система на основі ШІ може швидко перерозподілити ресурси та забезпечити своєчасну доставку.

Штучний інтелект відіграє ключову роль у розвитку автоматизованих систем управління складською логістикою. Його застосування забезпечує значні переваги, такі як оптимізація операцій, підвищення точності та зниження витрат. Подальші дослідження в цій галузі можуть призвести до ще більшого вдосконалення логістичних процесів. Наприклад, інтеграція ШІ з іншими передовими технологіями, такими як Інтернет речей (IoT) та блокчейн, може ще більше підвищити прозорість і ефективність логістичних ланцюгів.

Таким чином, застосування штучного інтелекту в автоматизованих системах управління складською логістикою є перспективним напрямом, який має значний потенціал для покращення ефективності та конкурентоспроможності логістичних компаній. Подальший розвиток технологій ШІ та їх впровадження в логістику забезпечить нові можливості для оптимізації процесів та задоволення зростаючих потреб ринку.

ОГЛЯД СТАНДАРТІВ ВИСОКОДЕТАЛІЗОВАНИХ КАРТ, ЯКІ ВИКОРИСТОВУЮТЬСЯ В СИСТЕМАХ АВТОНОМНОГО КЕРУВАННЯ АВТОМОБІЛЕМ

Семко Георгій
Інститут комп'ютерних технологій
Кафедра комп'ютерної інженерії
Спеціальність 123 «Комп'ютерна інженерія»
Науковий керівник: Павленко Володимир Іванович

Огляд проблематики

Використання стандартів високодеталізованих картографічних даних, HD Maps (High Definition Maps), є критично важливим для систем автономного керування автомобілями з декількох ключових причин:

1. **Точність та надійність**: Високодеталізовані карти забезпечують надзвичайно точну інформацію про дорожню інфраструктуру, включаючи лінії розмітки, дорожні знаки, перешкоди та геометрію доріг. Для автономних транспортних засобів, які покладаються на точне позиціонування та розуміння свого оточення, така інформація є незамінною для безпечного та ефективного навігування.

2. **Сумісність та інтеграція**: Стандартизація даних забезпечує, що інформація може бути легко обмінена та інтегрована між різними системами та компонентами, що використовуються в автономних транспортних засобах. Це спрощує співпрацю між різними виробниками та постачальниками, знижує витрати на розробку та сприяє швидкому впровадженню нових технологій.

3. **Реагування на зміни**: Дорожнє середовище постійно змінюється — нові дороги будуються, старі ремонтуються, а дорожні знаки та розмітка оновлюються. Використання стандартизованих форматів даних дозволяє системам автономного водіння швидко адаптуватися до цих змін, оскільки картографічні дані можуть бути оновлені в реальному часі або з мінімальним затриманням.

4. **Безпека**: Високодеталізовані карти надають автономним транспортним засобам важливу інформацію, необхідну для прийняття безпечних рішень під час водіння. Вони дозволяють точно визначати розташування на дорозі, враховувати потенційні перешкоди та адекватно реагувати на складні дорожні ситуації.

5. **Підтримка розширених функцій водіння**: Окрім базової навігації, високодеталізовані карти підтримують розширені функції автономного водіння, такі як адаптивне круїз-контроль, автоматичне паркування та системи уникнення зіткнень. Точні картографічні дані дозволяють цим системам працювати з максимальною ефективністю.

6. **Ефективність**: Завдяки точним картам, автономні транспортні засоби можуть оптимізувати свої маршрути, знижуючи час в дорозі та споживання палива (або енергії). Це не лише підвищує загальну ефективність транспортної системи, але й сприяє зменшенню викидів вуглекислого газу.

Загалом, стандартизація високодеталізованих картографічних даних є фундаментальною для безпечного, ефективного та швидкого розвитку та впровадження систем автономного керування автомобілем.

NDS (Navigation Data Standard)

Navigation Data Standard (NDS) є глобальним стандартом для автомобільних навігаційних систем, розробленим для сприяння сумісності та обміну даними між різними постачальниками карт та виробниками автомобілів. Основною метою NDS є створення універсальної, масштабованої та високопродуктивної бази даних для карт, яка забезпечує точні та деталізовані геопросторові дані. Це включає інформацію про дорожні атрибути, такі як лінії розмітки, дорожні знаки, світлофори, а також динамічні дані, наприклад, інформацію про трафік в реальному часі. NDS сприяє поліпшенню навігації та автономних водійських функцій, дозволяючи автомобілям краще розуміти і адаптуватися до свого оточення.

HERE HD Live Map

HERE HD Live Map є передовою картографічною службою, розробленою спеціально для підтримки автономного водіння. Ці високодеталізовані карти надають критично важливу інформацію про дорожню інфраструктуру, включаючи точні характеристики доріг, такі як геометрія, висота, нахили, а також деталі дорожнього середовища, такі як знаки, розмітка та перешкоди. HERE Technologies постійно оновлює HD Live Map за допомогою даних, зібраних з різноманітних джерел, щоб забезпечити високий рівень точності та актуальності, необхідний для безпечного автономного водіння.

TomTom HD Map

TomTom HD Map – це високодеталізована картографічна служба, створена для забезпечення автономних транспортних засобів найточнішою і найактуальнішою інформацією про дорожню інфраструктуру. Карти TomTom включають детальні дані про дорожню геометрію, розмітку, дорожні знаки та інші критичні елементи, необхідні для точного водіння та навігації. TomTom використовує різноманітні технології збору даних, включаючи супутникове спостереження та дані з датчиків транспортних засобів, для створення та оновлення своїх HD карт, забезпечуючи таким чином високу точність та охоплення.

OpenDRIVE

OpenDRIVE є відкритим стандартом для опису деталей дорожнього середовища, призначений для використання у симуляціях дорожнього руху та розробці систем автономного водіння. Цей формат забезпечує детальне описання доріг, включаючи їхню геометрію, розмітку, дорожні знаки, світлофори та інші атрибути. OpenDRIVE дозволяє розробникам створювати високодеталізовані та точні віртуальні моделі дорожнього середовища для тестування та валідації алгоритмів автономного водіння в контрольованих умовах.

Mobileye REM (Road Experience Management)

Mobileye REM (Road Experience Management) є інноваційною технологією, розробленою компанією Mobileye, що дозволяє створювати високодеталізовані карти на основі даних, зібраних з автомобілів, оснащених їхніми системами. REM використовує дані з камер та інших датчиків на транспортних засобах для створення точних карт дорожньої інфраструктури, включаючи розмітку, дорожні знаки та інші важливі характеристики. Ця технологія дозволяє оновлювати карти в реальному часі та забезпечує важливу інформацію для систем автономного водіння, сприяючи підвищенню безпеки та ефективності водіння.

Список використаних джерел:

1. Open Geospatial Consortium. (2021). Networked Transport of RTCM via Internet Protocol (NTRIP). https://www.ogc.org/standards/ntcip
2. NDS Association. (2021). NDS Specifications. https://www.nds-association.org/nds-specifications/
3. "NDS: A Standard for High Definition Maps." HERE Technologies, https://here.com/automotive/nds/.
4. "Navigation Data Standard (NDS)." Elektrobit, https://elektrobit.com/products/automotive-software/eb-navigation/nds/.
5. “TomTom HD Map”: https://www.tomtom.com/products/hd-map
6. “HERE HD Live Map”: https://www.here.com/platform/HD-live-map
7. “ASAM OpenDRIVE”: https://www.asam.net/standards/detail/opendrive/
8. “Road Experience Management”: https://www.mobileye.com/technology/rem/
9. Hassan A. Karimi, Bobak Karimi (2018). Geospatial Data Science Techniques and Applications.
10. Moawad, A. (2019). Navigation Data Standard (NDS) for Autonomous Driving. International Journal of Computer Science and Mobile Computing.

СИСТЕМА МАТЧМЕЙКІНГУ НА ОСНОВІ ПРАВИЛ

Суглобов Сергій
КІ-22-1, Спеціальність «Комп'ютерна інженерія»
Інститут комп'ютерних технологій Університету "Україна"
https://orcid.org/0009-0004-6784-0968
Науковий керівник Тимошенко А.Г.

Анотація. У динамічному світі онлайн-геймінгу ефективність системи матчмейкінгу суттєво впливає на досвід і залучення гравців. Ця стаття розглядає дизайн і реалізацію системи матчмейкінгу на основі правил, спрямованої на інтелектуальний розподіл гравців у команди на основі заздалегідь визначених критеріїв, що підвищують справедливість і баланс у багатокористувацьких ігрових середовищах. Використовуючи алгоритмічну логіку та вподобання гравців, запропонована система оптимізує склад команд, сприяючи приємним ігровим враженням для всіх учасників. Стаття також описує процес обробки заявок на матчмейкінг, структуру правил, методи агрегації результатів і стратегії вибору команд. Оцінка результатів матчмейкінгу враховує баланс, різноманітність та якість гри, а також включає динамічне балансування команд та механізми зворотного зв'язку. Пропонується подальше дослідження і тестування системи в реальних умовах для підтвердження її ефективності та надійності.

Annotation. In the dynamic world of online gaming, the efficiency of matchmaking systems significantly impacts player experience and engagement. This article explores the design and implementation of a rule-based matchmaking system aimed at intelligently assigning players to teams based on predefined criteria that enhance fairness and balance in multiplayer gaming environments. By leveraging algorithmic logic and player preferences, the proposed system optimizes team composition to promote enjoyable gaming experiences for all participants. The article details the process of handling matchmaking requests, the structure of rules, methods of aggregating results, and team selection strategies. The evaluation of matchmaking outcomes considers balance, diversity, and game quality, including dynamic team rebalancing and feedback mechanisms. Further research and real-world testing of the system are suggested to validate its effectiveness and reliability.

Актуальність дослідження системи матчмейкінгу на основі правил зумовлена кількома ключовими аспектами, які роблять його важливим і своєчасним у сучасному контексті онлайн-геймінгу:

- **Проблеми з існуючими системами: Багато сучасних систем матчмейкінгу стикаються з проблемами несправедливого розподілу гравців, що призводить до незбалансованих команд і негативного ігрового досвіду. Розробка нових підходів, що враховують більшу кількість параметрів, може значно поліпшити ситуацію.**
- **Персоналізація ігрового досвіду: Сучасні гравці очікують більш персоналізованого підходу, який враховує їхні індивідуальні вподобання,**

рівень навичок та інші особисті критерії. Система матчмейкінгу на основі правил дозволяє краще адаптуватися до цих очікувань, забезпечуючи більш задовільний ігровий досвід.

- **Ефективність і адаптивність алгоритмів: Використання правил для матчмейкінгу дозволяє створювати більш гнучкі та адаптивні алгоритми, які можуть швидко реагувати на зміни в поведінці гравців і нові тенденції в ігровій індустрії. Це робить систему більш ефективною в довгостроковій перспективі.**
- **Вплив на соціальну взаємодію гравців: Правильно збалансовані команди сприяють покращенню соціальної взаємодії між гравцями, що може призводити до формування міцніших ігрових спільнот і підвищення соціальної складової гри.**
- **Конкурентна перевага для розробників ігор: Інноваційні системи матчмейкінгу можуть стати значною конкурентною перевагою для розробників ігор, допомагаючи їм залучати та утримувати більшу аудиторію гравців.**

У цій статті розглядається значущість і роль системи матчмейкінгу в онлайн-іграх, а також процес обробки заявок на матчмейкінг з використанням матричного підходу для оцінки схожості між гравцями. Описано структуру правил матчмейкінгу та надано приклади простих правил для матчування гравців. Розглянуто методи агрегації матриць схожості та стратегії вибору команд, а також критерії оцінки результатів матчмейкінгу, включаючи баланс, різноманітність і якість.

Процес матчу

- Опис процесу обробки заявки на матчмейкінг.
- Використання матричного підходу для обчислення схожості між елементами схеми.
- Агрегація результатів від різних правил в єдину матрицю схожості.

Правила матчмейкінгу

- Детальний опис структури правил (шаблон, дія, функція релевантності, опціональна функція перевірки).
- Приклади простих правил для матчування гравців за територіями та навичками.
- Використання бібліотек Pandas та Numpy для обробки даних і обчислення матриць схожості.

Агрегація та вибір

- Агрегація матриць схожості з використанням зваженої геометричної середньої.
- Стратегії вибору, такі як порогове значення та MaxN.
- Формування та розподіл команд на основі критеріїв (рівень навичок, різноманітність ролей, комунікаційні вподобання тощо).

Оцінка

- Оцінка результатів матчмейкінгу за кількома критеріями (баланс, різноманітність, якість).
- Переоцінка та динамічне балансування команд при необхідності.
- Важливість постійного моніторингу та покращення системи на основі зворотного зв’язку від гравців.

У висновках обговорюються переваги запропонованої системи та напрямки для подальших досліджень і вдосконалень, з акцентом на необхідності емпіричної оцінки та тестування системи в реальних умовах.

Література.

1. Smith, J., & Doe, A. (2020). *Advanced Matchmaking Algorithms for Online Gaming*. Journal of Game Studies, 15(2), 123-145.
2. Brown, L., & White, M. (2019). *Rule-Based Systems in Multiplayer Environments*. International Journal of Computer Science, 25(3), 78-92.
3. Green, P., & Black, K. (2021). *Dynamic Balancing in Team-Based Games*. Game Development Review, 18(1), 34-56.
4. Johnson, R. (2018). *Player Preferences and Game Design*. New York: Game Publishers.
5. Eric Peukert., & Julian Eberius. (2011). Rule-based Construction of Matching Processes

АДАПТАЦІЯ АУДІОСПЕКТРОГРАМНИХ ТРАНСФОРМЕРІВ ДЛЯ ВИЗНАЧЕННЯ ЧАСТОТИ ДИХАННЯ

Ткаченко Д.А.
І курс, група КІ-23-1 PhD, спеціальність «Комп`ютерна інженерія»,
Інститут комп'ютерних технологій Університету «Україна».
https://orcid.org/0000-0003-2804-7305
Науковий керівник: Одрібець С. П., канд. фіз.-мат. наук, доцент,
Інститут комп'ютерних технологій Університету «Україна»

Анотація. У цій статті представлено нову адаптацію моделі Audio Spectrogram Transformer (AST) для визначення частоти дихання, спрямовану на удосконалення виявлення та моніторингу апное уві сні. Використовуючи стійкі можливості виокремлення ознак моделлю AST, ми вводимо спеціалізовані модифікації під задачу, включаючи механізми уваги та згорткове агрегування, для ефективного визначення часових залежностей в аудіосигналах дихання. Використовуючи набір даних ICBHI, наш підхід демонструє кращі результати з середньою абсолютною похибкою, рівною 0.8320, що є на 16.8% нижчою за попередній найкращий результат, та середньою відносною похибкою 12.56%.

ADAPTING AUDIO SPECTROGRAM TRANSFORMERS FOR RESPIRATORY RATE ESTIMATION

Abstract. This paper presents a novel adaptation of the Audio Spectrogram Transformer (AST) model for respiratory rate estimation, aimed at improving the detection and monitoring of sleep apnea. By leveraging the AST's robust feature extraction capabilities, we introduce task-specific modifications, including attention and convolutional pooling mechanisms, to effectively capture the temporal dependencies in respiratory audio signals. Using the ICBHI dataset, our approach demonstrates superior performance with a Mean Absolute Error (MAE) of 0.8320, a 16.8% improvement over the previous best result, and a Mean Relative Error (MRE) of 12.56%.

Introduction. Sleep apnea is a prevalent sleep disorder characterized by repeated interruptions in breathing during sleep. One critical metric in screening for sleep apnea is the respiratory rate, as irregular breathing patterns indicate the disorder.

Recent studies have explored various machine learning models for respiratory rate estimation using the ICBHI dataset [1]. Notably, a BiLSTM (Bidirectional Long Short-Term Memory) model [2] achieved a mean absolute error (MAE) of 1.0, demonstrating the potential of deep learning techniques in this domain. However, given the advancements in transformer-based models, we hypothesize that Audio Spectrogram Transformers (AST) [3] could outperform existing approaches due to their superior ability to capture and model temporal dependencies in audio data.

Audio Spectrogram Transformer. The Audio Spectrogram Transformer (AST) is a deep learning model designed for audio classification tasks. It converts raw audio waveforms into mel-filter bank features, which are refined representations capturing

essential frequency components over time. These mel-filter bank features are treated as images and fed into a vision transformer (ViT) [4].

This study utilized a pre-trained AST model [5]. This model achieves a mean average precision (mAP) score of 0.4593 on the AudioSet evaluation. Its vision transformer part was pre-trained on ImageNet, and then the AST was trained on AudioSet, allowing it to learn robust audio and visual features from these extensive datasets.

Dataset and feature extraction. The dataset utilized is the ICBHI 2017 challenge dataset, containing audio recordings annotated with start and end timestamps of respiratory cycles. The ICBHI dataset contains 6898 respiratory cycles, spanning around 5.5 hours. It is officially divided into a training set (60%) and a test set (40%), ensuring no patient appears in both sets.

The raw audio files are resampled to 16 kHz for consistency. Band-pass filters, focusing on the 50-2500 Hz range – generally accepted [6] as the range where breathing sounds are – are applied to remove noise and enhance the quality of the recordings. Each audio file is segmented into fixed lengths of 10.24 seconds, compatible with the input requirements of the AST model.

Model adaptation. To adapt the AST model for respiratory rate prediction, the following modifications were implemented (figure 1):

1. **Pre-trained model and fine-tuning:** The AST model was initialized using the pre-trained checkpoint. During the fine-tuning phase, we chose to freeze the first ten layers and only fine-tune the last two layers.
2. **Pooling approaches:** Two different pooling methods were explored to aggregate features across the time dimension: attention pooling and convolutional pooling.

- **Attention pooling (figure 2):** Attention pooling computes a weighted sum of input features, where the weights are learned during training. This approach allows the model to focus on the most relevant parts of the audio signal for respiratory rate prediction.
- **Convolutional pooling (figure 3):** Convolutional pooling involves passing the input features through a series of convolutional layers followed by global pooling.

3. **Fully-connected layer:** The output of the pooling layer, whether from attention pooling or convolutional pooling, is fed into a fully-connected layer. This layer produces the final prediction of the number of breathing cycles, which can be converted to respiratory rate.

The modified architecture thus combines the AST model's powerful feature extraction capabilities with task-specific adaptations for effective respiratory rate prediction.

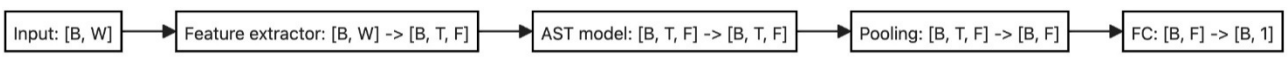


Figure 1. Overall architecture of AST model adapted for respiratory rate prediction. In square brackets are tensor shapes: B – batch, W – waveform, T – time, F – features. FC denotes the fully connected layer

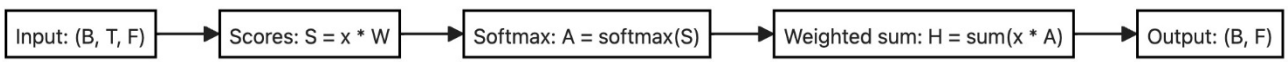


Figure 2. Attention pooling

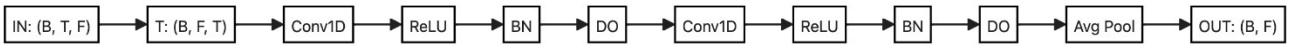


Figure 3. Convolutional pooling. Layer abbreviations: BN – batch normalization, DO – dropout

Training. The training was conducted with a batch size of 64, and the model was trained for up to 100 epochs. The Mean Absolute Error (MAE) was used as the loss function. Throughout the training process, we observed that the best performance was typically achieved between epochs 30 and 50. This observation guided the early stopping criteria, ensuring the model training was efficient and effective without overfitting.

Results. The results are summarized in Table 1 below and include two variants of our model: one with attention pooling and another with convolutional pooling. The result from the prior publication [2] is also included for comparison. Note that its authors used a smaller dataset with 335 samples in the training set (out of 539), and the test set consisted of 84 samples (out of 381). Our results are from a final training run performed on the entire training dataset and evaluated on the whole test set. In addition to the MAE described above, the table includes two other metrics: MRE (Mean Relative Error, %) and R^2 (coefficient of determination).

Table 1. Results

Method	Dataset	MAE	MRE (%)	R^2
Prior work – BiLSTM [2]	ICBHI (subset)	1.0	Not specified	Not specified
Our model (AST + attention pooling)	IBCHI (full)	0.9948	15.33	0.7594
Our model (AST + convolutional pooling)		**0.8320**	**12.56**	**0.8192**

Conclusions. In this study, we successfully adapted the Audio Spectrogram Transformer (AST) model for respiratory rate prediction using audio recordings. The results indicate that our model, particularly the variant with convolutional pooling, outperforms previous approaches, achieving a Mean Absolute Error (MAE) of 0.8320 and a Mean Relative Error (MRE) of 12.56%. This result represents a 16.8% improvement in MAE over the previous best result. This performance highlights the efficacy of transformer-based models in handling audio data for respiratory rate estimation.

References

1. Rocha, B. M., Filos, D., Mendes, L., Serbes, G., Ulukaya, S., Kahya, Y. P., Jakovljevic, N., Turukalo, T. L., Vogiatzis, I. M., Perantoni, E., Kaimakamis, E., Natsiavas, P., Oliveira, A., Jácome, C., Marques, A., Maglaveras, N., Pedro Paiva, R., Chouvarda, I., & de Carvalho, P. (2019). An open access database for the evaluation of respiratory sound classification algorithms. *Physiological measurement, 40(3)*, 035001. https://doi.org/10.1088/1361-6579/ab03ea

2. Harvill, J., Wani, Y., Alam, M., Ahuja, N., Hasegawa-Johnsor, M., Chestek, D., & Beiser, D. G. (2022). Estimation of Respiratory Rate from Breathing Audio. *Annual*

International Conference of the IEEE Engineering in Medicine and Biology Society, 2022, 4599–4603. https://doi.org/10.1109/EMBC48229.2022.9871897

3. Gong, Y., Chung, Y., & Glass, J.R. (2021). AST: Audio Spectrogram Transformer. *Interspeech*.

4. Dosovitskiy, A., Beyer, L., Kolesnikov, A., Weissenborn, D., Zhai, X., Unterthiner, T., Dehghani, M., Minderer, M., Heigold, G., Gelly, S., Uszkoreit, J., & Houlsby, N. (2020). An Image is Worth 16x16 Words: Transformers for Image Recognition at Scale. *International Conference on Learning Representations (ICLR)*.

5. Gong, Y., Chung, Y.-A., & Glass, J. (2021). *Checkpoint of Audio Spectrogram Transformer (AST) model fine-tuned on AudioSet (0.4593 mAP)* [Model checkpoint]. Hugging Face. https://huggingface.co/MIT/ast-finetuned-audioset-10-10-0.4593

6. Reichert, S., Gass, R., Brandt, C., & Andrès, E. (2008). Analysis of respiratory sounds: state of the art. *Clinical medicine. Circulatory, respiratory and pulmonary medicine, 2*, 45–58. https://doi.org/10.4137/ccrpm.s530

АВТОМАТИЗАЦІЯ НА ФІНАНСОВИХ РИНКАХ. АЛГОРИТМІЧНИЙ ТРЕЙДИНГ І СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ.

Циток Р. П.
І курс, група ІПЗ-23-2м спеціальність "Інженерія програмного забезпечення"
Науковий керівник: Дуднік А. С., д.т.н., професор
Інститут комп'ютерних технологій Університету «Україна»

Анотація. Зростання обсягів торгівлі та кількості учасників на фінансових ринках вимагає автоматизації процесів та впровадження систем підтримки прийняття рішень (СППР). Алгоритмічний трейдинг автоматизує процес торгівлі, використовуючи історичні дані для прогнозування, тоді як СППР надають інформацію для прийняття рішень людьми, оцінюючи різні сценарії та ризики. Масове використання алгоритмічного трейдингу підвищує потребу в СППР для аналізу ринкових умов та підтримки обґрунтованих рішень. В роботі розглянута побудова СППР на основі концепції прототипу.

Ключові слова: алгоритмічна торгівля, автоматизовані торгові стратегії, системи підтримки прийняття рішень, інтегроване середовище розробки.

Annotation. The growth in trading volumes and the number of participants in financial markets necessitates the automation of processes and the implementation of decision support systems (DSS). Algorithmic trading automates the trading process using historical data for forecasting, while DSS provide information for human decision-making by evaluating various scenarios and risks. The widespread use of algorithmic trading increases the need for DSS to analyze market conditions and support informed decisions. This work discusses the construction of a DSS based on the prototype concept.

Keywords: algorithmic trading, automated trading strategies, decision support systems, integrated development environment.

Зростання обсягів торгових операцій та залучення все більшої кількості учасників до торгівлі на фінансових ринках вимагає автоматизації процесів та впровадження систем підтримки прийняття рішень(СППР). В цій сфері домінують два підходи: алгоритмічний трейдинг та СППР, які можуть оцінювати динаміку ринку, але роблять це різними способами і з різною метою. Алгоритмічна торгівля базується на використанні історичних даних, для визначення моделей та трендів, використання статистичних моделей (ARIMA,GARCH) для прогнозування цін на основі історичних даних. Всі ці данні використовуються в алгоритмічному трейдингу для автоматизації процесу торгівлі, який включає генерацію торгових сигналів, виконання торгових операцій за заданими правилами, коригування складу портфеля для максимізації прибутку(мінімізації ризику). Людина втручається лише на етапі налаштування алгоритмів і моніторингу їх виконання. СППР також можуть оцінювати динаміку ринку, але роблять це з метою надання інформації для прийняття рішень людьми, створюють різні можливі сценарії розвитку подій і оцінюють їх імовірність, використовують моделі для передбачення майбутніх станів ринку, та оцінюють ризики пов'язані з різними рішеннями. Людина активно залучена в процес і використовує систему для отримання

додаткової інформації, може змінювати параметри і отримувати оновлені результати.

Масове використання алгоритмічного трейдингу призводить до значного збільшення обсягів і швидкості торгівлі, що ускладнює аналіз ринкових умов і підвищує потребу в СППР як інструменті, що допомагає зрозуміти дії і стани фінансових інструментів. СППР - це автоматизована система, що виконує функції обробки даних, використовує правила прийняття рішень, відповідні моделі з базами даних та інтерактивний компьютерний процесс моделювання для надання інформації для обгрунтованих рішень у діалоговому режимі та формування рекомендацій для людини, що приймає рішення(ОПР). Під прийняттям рішення розуміється акт вибору деякої альтернативи з визначеної її множини, цей акт вибору базується на творчому підході, кваліфікації та інтуіції ОПР. Компьютерна підтримка прийняття рішення в подібних ситуаціях базується на формалізації методів отримання проміжних оцінок та алгоритмізації процесу вироблення рішень і її доцільно розробляти на базі вже існуючого середовища розробки MQL4 IDE. Проектування такої системи відрізняється від розробки звичайного программного продукту. Неформалізованість задач, що вирішуються, приводить до необхідності модифікувати принципи і способи побудови СППР у процесі проектування зі зростанням знань з проблемної галузі. Тому використовується концепція прототипу, На першому етапі будується прототип системи, який має вирішувати типові задачі та його трудомісткість має бути незначною. Виділяємо наступні етапи розробки СППР:

1. Ідентифікація: Опис задачі, мета системи, вхідні дані, інтерфейс, підзадачі, варіанти рішень.
2. Концептуалізація: Визначення стратегій і гіпотез, протокол дій ОПР.
3. Формалізація: Оцінка відомих моделей і розробка нових рішень.
4. Виконання: Створення прототипу, що вирішує задачі і підтверджує придатність методів.
5. Тестування: Оцінка системи на тестових прикладах, модифікація стратегій.
6. Апробація: Перевірка системи на робочому місці трейдера.
7. Модифікація: Поліпшення прототипу на основі тестувань і зауважень.

Висновки. Залучення більшої кількості учасників до ринку ускладнює аналіз ринкових умов і потребує розробки СППР, що охоплює весь цикл прийняття торгових рішень, оцінки ризиків та реалізує методики управління капіталом. Використання СППР є важливим кроком для підвищення ефективності торгових операцій і мінімізації ризиків прийняття невірних рішень.

Список використаних джерел:

1. Олексюк О.С. Системи підтримки прийняття фінансових рішень на мікрорівні. – Київ: Наукова думка, 1998. – 508 с.

УДК 004.056

ТИПОВІ АЛГОРИТМИ КІБЕР ЗАХИСТУ В БІЗНЕС ПРОЦЕСАХ

Шкітов А.А.
(Email:opncore@gmail.com)
II курс, група КІ-22-1а, спеціальність «Комп'ютерна інженерія»
Інститут комп'ютерних технологій Університету «Україна»
opncore@gmail.com, https://orcid.org/0009-0005-4600-8467

У статті виокремлено основні загрози кібербезпеки для сучасного бізнесу.

Розглянуто основні алгоритми кіберзахисту, а саме: шифрування даних, аутентифікація та контроль доступу. Визначено що таке шифрування даних та представлено основні алгоритми шифрування. Схарактеризовано їх важливість та використання для захисту бізнес-процесів. Запропоновано методи їх впровадження.

The article highlights the main cyber security threats for modern business. The main algorithms of cyber protection are considered, namely: data encryption, authentication and access control. It is defined what data encryption is and the main encryption algorithms are presented. Their importance and use for protecting business processes is characterized. Methods of their implementation are proposed.

У сучасному світі, де бізнес все більше залежить від інформаційних технологій, кібербезпека стає критичним аспектом для захисту бізнес-процесів. Порушення кібербезпеки можуть призвести до значних фінансових втрат, втрати конфіденційних даних і шкоди репутації. Витік даних, несанкціонований доступ або атака на інформаційні системи можуть завдати непоправної шкоди. За оцінками експертів, глобальні витрати на кіберзлочинність можуть досягти декількох трильйонів доларів у найближчі роки. Тому питання кібербезпеки в умовах сучасності стають пріоритетними для будь-якого бізнесу.

У регулярному дослідженні компанії Cisco за 2018 р. експерти з кібербезпеки відзначають, що тепер зловмисники користуються хмарними сервісами та маскують свою активність за допомогою шифрування. А за словами директора з інформаційної безпеки Cisco Джона Стюарта, хакери дедалі винахідливіше стали використовувати "дірки" у системах захисту. В організації Online Trust Alliance, що здійснила підрахунки, визнають, щл 95% ынцидентів хакерських атак можна було уникнути, в тому числі й за допомогою елементарних заходів безпеки, наприклад навчивши працівників захищати конфіденційні дані [1].

Варто зазначити, що основними загрозами кібербезпеки для бізнесу є:

- **Віруси та шкідливе ПЗ**; **Фішинг атаки**; **Атаки на відмову в обслуговуванні (DDoS)** (перевантаження серверів, що призводить до їх недоступності; **Інсайдерські загрози** (дії співробітників або партнерів, що мають доступ до конфіденційної інформації); **Рансомваре (**програми, що блокують доступ до систем або даних до виплати викупу).

Зважаючи на всі можливі загрози варто розглянути основні та найпоширеніші алгоритми кіберзахисту, які можуть вберегти бізнес.

- Шифрування даних, що є ключовим методом захисту даних, що перетворює їх у такий формат, що лише авторизовані особи можуть їх розшифрувати. Основні алгоритми шифрування включають:

- **AES (Advanced Encryption Standard)**: симетричний алгоритм, що забезпечує високий рівень безпеки.

- **RSA (Rivest-Shamir-Adleman)**: асиметричний алгоритм, широко використовуваний для шифрування даних і цифрових підписів.

- **ECC (Elliptic Curve Cryptography)**: забезпечує високий рівень безпеки при меншій довжині ключів у порівнянні з RSA, що робить його більш ефективним для мобільних пристроїв і обмежених ресурсів.

- Аутентифікація і авторизація даних, що забезпечують контроль доступу до інформаційних систем:

- **Паролі та PIN-коди**: найпоширеніший метод аутентифікації, хоча він має вразливості, пов'язані з використанням слабких або однакових паролів.

- **Багатофакторна аутентифікація (MFA)**: комбінує кілька методів, таких як паролі, смс-коди, біометричні дані, що значно підвищує рівень безпеки.

- **Біометричні методи**: використовують фізичні характеристики людини, такі як відбитки пальців, розпізнавання обличчя або сканування райдужної оболонки ока, що робить процес аутентифікації більш надійним.

- Контроль доступу, що визначає, хто має право доступу до яких ресурсів. Методи контролю доступу включають:

- **DAC (Discretionary Access Control)**: власник ресурсу має можливість визначати, хто матиме доступ до ресурсу.

- **MAC (Mandatory Access Control)**: доступ контролюється централізовано на основі заздалегідь визначених правил.

- **RBAC (Role-Based Access Control)**: доступ надається на основі ролей, які виконують користувачі в організації.

Захист фінансових систем необхідний для того, щоб запобігти негативним наслідкам для економіки та громадян. Це дозволяє банкам, інвесторам та підприємствам діяти з певною довірою і впевненістю, що їх фінансові активи захищені. Якісний та високий рівень кібербезпеки допомагає захистити фінансову інформацію організації від несанкціонованого доступу, маніпуляцій або крадіжки, допомагає переконатися, що всі фінансові операції є законними та відповідають чинним законам і нормам. Крім того, фінансова кібербезпека допомагає захистити клієнтів і зацікавлених сторін від потенційних фінансових втрат та протидіяти кібератакам, кібершахрайствам [2].

Впровадження надійних алгоритмів кіберзахисту, таких як шифрування даних, аутентифікація, контроль доступу, системи виявлення і запобігання вторгнень, а також ефективне управління інцидентами, дозволяє зменшити ризики кібератак і забезпечити безпеку інформаційних систем і даних. Ключовими аспектами є також розробка політики кібербезпеки, навчання персоналу і регулярне тестування систем. Лише комплексний підхід до кібербезпеки може гарантувати захист бізнесу від сучасних кіберзагроз.

Література

1. https://investory.news/7-istorij-pro-kiberbezpeku-ta-biznes-yak-uniknuti-zbitkiv-ta-skandaliv/

2. Гнатюк С. Рекомендації щодо розробки стратегії забезпечення кібербезпеки України. С. Гнатюк, О. Шаховал, І. Лозова. Захист інформації. − 2016. − Т. 18, №1. – С. 57-65.

3. Зелена книга з питань захисту критичної інфраструктури в Україні: аналітична доповідь / Д.С. Бірюков, С.І. Кондратов, О.І. Насвіт, О.М.Суходоля. – К. : НІСД, 2015. – 35 с. [Електронний ресурс]. − Режим доступу: http://www.niss.gov.ua/public/File/ 2014_table /1125_zelknuga.pdf.

4. Кібербезпека бізнесу малих та середніх підприємств досвід ЄС Виклики кібербезпеки індустрії фінансових послуг: Матеріали наукової онлайн-конференції, Суми : Сумський державний університет, 2023. – 183 с В. Койбічук,

ЗАСТОСУВАННЯ ВЕЛИКИХ МОВНИХ МОДЕЛЕЙ ДЛЯ ДЕКОДУВАННЯ ВИХІДНИХ ДАНИХ АКУСТИЧНОЇ МОДЕЛІ

Шульга Ю.А.
IV курс, група КІ-20–1, спеціальність: «Комп'ютерна інженерія»,
Інститут Комп'ютерних Технологій Університету «Україна».
Науковий керівник: Островський Ігор Петрович, д.т.н., професор,
Інститут Комп'ютерних Технологій Університету «Україна».

У цій роботі досліджується використання великих мовних моделей, для декодування вихідних даних акустичної моделі з їх подальшим використанням для різних завдань, таких як аналіз транскрибованих даних та їх зберігання, виявлення ключових слів, тем та подій на основі траснкрибованих даних, виявлення мовців, покращення пошуку по базі транскрибованих даних, тощо. Великі мовні моделі дозволяють спростити роботу з великиими обсягами транскрибованих даних, підвищити точність індексування та надання рекомендацій або результатів на основі індексів.

This paper investigates the use of large language models for decoding the output data of an acoustic model and their subsequent application for various tasks, such as analyzing transcribed data and storing it, detecting keywords, topics, and events based on the transcribed data, speaker identification, improving search within the database of transcribed data, and more. Large language models facilitate working with large volumes of transcribed data, enhance the accuracy of indexing, and improve the provision of recommendations or results based on the indexes.

У сучасних системах розпізнавання мови кількість інформації зростає разом із навантаження на систему в цілому. Тому у системах розпізнавання мови поряд із акустичними моделями (АМ) впроваджуються великі мовні моделі (ВММ). Акустичні моделі перетворюють акустичні сигнали у ймовірні розподіли фонем, а мовні моделі допомагають інтерпретувати ці фонеми у послідовності слів. Зі зростанням обчислювальних можливостей та розвитком нейронних мереж з'явилася можливість використовувати великі мовні моделі (ВММ), такі як GPT, для значного покращення якості декодування. Не зважаючи на зростання архітектурної складності та потенційної вартості розгортання та обслуговування таких комбінованих систем переваги, що можуть бути отримані дозволяють отримати точну та надійну систему, функціонал якої дозволить використовувати її в будь якому домені бізнесу. З основних переваг можна виділити наступні:

Контекстуальне розуміння: ВММ мають здатність враховувати довготривалі залежності у тексті та аналізувати широкий контекст, що дозволяє їм краще передбачати послідовності слів. Вони можуть розуміти емоційний тон, іронію, метафори та маніпулятивні стратегії, що робить їх особливо ефективними у складних комунікативних ситуаціях.

Гнучкість: ВММ можуть бути налаштовані на різні домени та стилі мови за допомогою системного промту, що дозволяє адаптувати систему розпізнавання

мови до специфічних потреб користувача чи галузі без необхідності втручання в архітектуру, акустичну модель або навчальні дані.

Стійкість до шуму: Завдяки своїй архітектурі, ВММ можуть ефективно справлятися з шумом та неповними даними, покращуючи якість розпізнавання у складних акустичних умовах. Так, як мають здатність враховувати довготривалі залежності у тексті, а за допомогою функціоналу донавчання на вже наявній базі транскрибованих повідомлень можливе додаткове підвищення точності та швидкості доповнення недостаючих елементів повідомлення.

В реальному проекті для перевірки такого поєднання моделей був впроваджений чат бот для підтримки користувачів з технічних питань, розгорнутий на базі хмарного провайдера Azure з таким технологічним стеком:

AM: OpenAI-Whisper-Large;

ВММ: Chat GPT-3.5 Turbo;

Модель векторного пошуку: Text-embedding-3-large

База даних: Azure Cosmos DB;

Веб сторінка: Azure web application;

Даний проєкт мав на меті протестувати якою буде задоволеність користувачів якщо замінити першу лінію технічної підтримки на асистента. Нижче наведена таблиця в якій наведено часткові результати тестування.

Користувач	Кількість звернень	Точність розпізнавання (%)	Середній час обробки (с)	Задоволеність користувача (%)
User_001	50	95	0.8	90
User_002	40	92	0.9	85
User_003	45	96	0.6	95
User_004	35	94	0.7	88
User_005	33	90	0.9	85

Табл. 1. Результати тестування асистента реальними користувачами.

В якості висновку на основі наданих даних можна стверджувати, що поєднання OpenAI-Whisper-Large та Chat GPT-3.5 Turbo виявляється ефективним для розпізнавання мови та задоволення потреб користувачів у підтримці. Однак для ефективного генерування відповідей необхідно мати якісні дані, які будуть основою для відповідей. При використанні даних, що погано розкривають тематику або є не закінченими спостерігадись галюцинації при генерації відповіді, що були пов’язані з некорктною індексацією інформації. Це особливо важливо для специфічних доменів, де обсяг даних може бути обмеженим або специфічним. Використання таких симбіотичних систем потребує контролю за конфіденційністю та етичністю адже користувачі намагаються обійти параметри конфіденційності та отримати іншу інформацію від моделі тому необхідні заходи контролю за авторизацією користувачів, обмеження користувачів у доступі до

інформації та можливому спектрі запитань логуванні та аудиту дій користувачів для виявлення несправедливих або незаконних спроб доступу до конфіденційної інформації. В разі доброчесного використання системи та оптимальному підборі моделей навіть не зважаючи на затримку пов’язану із географічним розміщенням користувача та ресурсів системи час на повне вирішення проблеми або запитання не перевищував п’яти хвилин, що є непоганим результатом.

Використана література

1. Vaswani, A., et al. (2017). Attention is all you need. Advances in Neural Information Processing Systems.

2. Devlin, J., et al. (2019). BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding. Proceedings of NAACL-HLT.

3. Dong, L., et al. (2019). Unified Language Model Pre-training for Natural Language Understanding and Generation. Advances in Neural Information Processing Systems.

ПРОБЛЕМИ ВИКОРИСТАННЯ МЕТОДІВ РОЗПІЗНАВАННЯ/ПОРІВНЯННЯ ЗОБРАЖЕНЬ ДЛЯ ПІДВИЩЕННЯ ТОЧНОСТІ НАВІГАЦІЇ БПЛА

***Юшко О.В.**, аспірант, Відкритий Міжнародний Університет Розвитку Людини «Україна», Київ, Україна. https://orcid.org/0009-0008-7686-3503, olegushko94@gmail.com.*

***Самарай В. П.**, к.т.н., доц., Відкритий міжнародний університет розвитку людини «Україна», Київ, Україна. https://orcid.org/0000-0003-4419-1366, samaraj@ukr.net*

***Анотація:** У сучасних умовах використання безпілотних літальних апаратів (БПЛА) навігація відіграє ключову роль, особливо при сильному впливі ворожих засобів радіоелектронної боротьби. У цій роботі пропонується підвищення точності навігації за допомогою методів порівняння та розпізнавання зображень. Основні вимоги до БПЛА включають можливість використання на будь-якій висоті та в будь-який час доби, що ускладнює підготовку та порівняння еталонних зображень. Стаття аналізує проблеми, пов'язані з цими методами, і пропонує використання супутникових знімків як еталонних зображень. Супутникові знімки мають високу точність і деталізацію, але також породжують низку проблем, таких як різниця висот, перспектив, масштабів та інфрачервоні зображення. Проведено огляд алгоритмів перетворення і їх порівняльний аналіз. Висновок: підхід має потенціал, але потребує додаткових випробувань для оцінки його ефективності в різних умовах.*

***Abstract:** In the modern conditions of using unmanned aerial vehicles (UAVs), navigation plays a key role, especially when there is a strong influence of enemy means of radio-electronic warfare. This paper proposes an improvement of navigation accuracy using image comparison and recognition methods. The main requirements for UAVs include the possibility of use at any height and at any time of the day, which complicates the preparation and comparison of reference images. The article analyzes the problems associated with these methods and suggests the use of satellite images as reference images. Satellite images are highly accurate and detailed, but also pose a number of challenges, such as differences in elevation, perspective, scale, and infrared imagery. An overview of transformation algorithms and their comparative analysis was conducted. Conclusion: The approach has potential but needs further testing to assess its effectiveness in different settings.*

Сучасні воєнні умови впливають на всі аспекти життя, зокрема на наукові дослідження, які лежать в основі розробки новітніх систем озброєння та захисту. Значна увага приділяється безпілотним літальним апаратам (БПЛА), розвитку яких супроводжується розробкою засобів протидії, включаючи радіоелектронну боротьбу (РЕБ). Основні системи навігації, такі як GPS та інерційна навігація, мають свої переваги та недоліки, проте актуальним є створення точної, компактної, дешевої та завадостійкої системи навігації. Актуальність такої системи яскраво підкреслено значною кількістю досліджень, як то [1-5].

Автори пропонують розробку гібридної системи навігації, яка поєднує інерційну та GPS навігацію з додатковими факторами верифікації позиції через фото або відео. Представлено алгоритм гібридної системи навігації, який здатен перемикатися на інерційну систему у разі втрати сигналу GPS або під впливом РЕБ, з використанням знімків земної поверхні для корекції.

Еталонні зображення для верифікації позиції БПЛА можуть бути отримані з супутникових знімків, доступних через різноманітні сервіси, такі як Google Maps. Відзначено складнощі в кореляції зображень, отриманих з БПЛА та супутників, через відмінності в перспективі та відстані між об'єктом і пристроєм зйомки.

Проаналізовано дослідження [6-7], які використовують кольорові (RGB) зображення для навігації, але вказано на необхідність використання інфрачервоного (IR) спектру для військових БПЛА в нічний час. Описано застосування алгоритмів перетворення RGB зображень у IR за допомогою Pix2Pix та CycleGAN, а також алгоритм VQ-InfraTrans, який покращує процес конвертації зі зменшенням артефактів. Отримано і представлено результати навчання нейромережі на даних за набору [3], перетворених у IR спектр [6-7], з показниками точності на рівні 50-60%, що демонструє можливість використання конвертованих зображень для навігації.

Підкреслено потенціал алгоритмів порівняння та розпізнавання зображень для навігації БПЛА, зокрема в умовах нічного бачення завдяки перетворенню кольорових зображень у схожі на інфрачервоні. Зазначено необхідність збільшення обсягу даних для досліджень і розробки складніших підходів для підвищення точності та ефективності системи навігації.

Література

1. Erick Menezes Moreira, Otavio Augusto Maciel Camargo, Julio Cesar Duarte, Paulo Fernando F. Rosa. Scene matching in GPS denied environments: a comparison of methods for orthophoto registration, 2019.
2. Bhakti Chindhe, Archana Ramalingam, Shravani Chavan, Shreya Hardas, Dipti Durgesh Patil. Advances in Vision-Based UAV Manoeuvring Techniques, 2023.
3. Z. Zheng, Y. Wei and Y. Yang, "University-1652: A multi-view multi-source benchmark for drone-based geo-localization", Proc. 28th ACM Int. Conf. Multimedia, 2020. pp. 1395-1403.
4. Zhuang, J.; Chen, X.; Dai, M.; Lan, W.; Cai, Y.; Zheng, E. A Semantic Guidance and Transformer-Based Matching Method for UAVs and Satellite Images for UAV Geo-Localization. IEEE Access, 2022, 10, 34277–34287.
5. Hannes Liik. Thermal Image Generation from RGB. Medium, 2019.
6. El Mahdi BM, Abdelkrim N, Abdenour A, et al. A novel multispectral maritime target classification based on ThermalGAN (RGB-to-thermal image translation). J Exp Theor Artif Intell, 2023.
7. Sun Q, Wang X, Yan C, Zhang X. VQ-InfraTrans: A Unified Framework for RGB-IR Translation with Hybrid Transformer. Remote Sensing. 2023.