

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ІНСТИТУТ МОДЕРНІЗАЦІЇ ЗМІСТУ ОСВІТИ
АСОЦІАЦІЯ НАВЧАЛЬНИХ ЗАКЛАДІВ УКРАЇНИ
ПРИВАТНОЇ ФОРМИ ВЛАСНОСТІ
АКАДЕМІЯ WSB У ДОМБРОВІ ГУРНІЧІЙ (ПОЛЬЩА)
УНІВЕРСИТЕТ TURİVA (ЛАТВІЯ)
НАЦІОНАЛЬНА ІНЖЕНЕРНА АКАДЕМІЯ
РЕСПУБЛІКИ КАЗАХСТАН
АСОЦІАЦІЯ СПЕЦІАЛІСТІВ КІБЕРБЕЗПЕКИ
ЄВРОПЕЙСЬКИЙ УНІВЕРСИТЕТ**

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА КІБЕРБЕЗПЕКА В ЗАБЕЗПЕЧЕННІ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

ТОМ II

Матеріали

*XXIX Міжнародної науково-практичної конференції
«Цифрова трансформація в економіці, менеджменті і бізнесі.
Проблеми науки, практики та освіти»
30 листопада 2023 р.*

до 32-річчя Європейського університету



Київ-2024

Видавництво Європейського університету

УДК: 004(063)

Редакційна колегія:

Тимошенко О.І. – ректор, доктор філософських наук, професор;

Гудзь Ю.Ф. – доктор економічних наук, доцент;

Єнікєєв О.Ф. – доктор технічних наук, доцент;

Склярєнко О.В. – кандидат фізико-математичних наук, доцент

Відповідальні секретарі:

Склярєнко О.В. – к.ф.-м.н., доцент.;

Яровий Р.О. – к.т.н.

Цифрова трансформація в економіці, менеджменті та бізнесі. Проблеми науки, практики і освіти. Том 2. Інформаційні технології та кібербезпека в забезпеченні цифрової трансформації: Матеріали XXIX Міжнарод. наук.-практ. конф., Київ, 30 листопада 2023 р. / Редкол.: О. І. Тимошенко та ін. – К.: Вид-во Європейського університету, 2024. – 78 с.

Збірник містить матеріали XXIX Міжнародної науково-практичної конференції «Цифрова трансформація в економіці, менеджменті і бізнесі. Проблеми науки, практики та освіти».

Матеріали друкуються за редакцією авторів

ЗМІСТ

Базиліук К.Ф., Піддубна Я.І.

Система моніторингу та класифікації хмарності..... 5

Білоусько Т.М.

Напрями використання інформаційних технологій в цифровій трансформації..... 6

Бондар М.С., Ніколаєвський О.Ю.

Дослідження засобів та механізмів забезпечення кібербезпеки в органах державної влади..... 9

Волошин Р.А., Скляренко О.В.

Методи і алгоритми інтелектуального аналізу електрокардіограм 11

Головченко Б.М.

Управління безпекою підприємств під впливом цифровізації..... 12

Гончаренко Д.Ю.

Політичні інституції у вирішенні конфліктів та кіберзагроз сучасного суспільства..... 14

Гуцуляк А.В., Кот М.В.

Використання методів штучного інтелекту для розпізнавання мовлення 16

Гущак О.М., Веремій А.А.

Мобільний застосунок для оптимізації алгоритмів побудови маршрутів 19

Єнікєєв О.Ф.

Система керування подачею палива на основі опрацювання даних непрямих вимірювань.... 20

Карповець М.Ю., Яровий Р.О.

Моделювання однорідних та ізотропних випадкових полів на сфері 23

Квятківська А.

Динаміка цифрової трансформації в Україні 25

Ковальов Л.І., Данильчук Г.Б.

Історія розвитку мережі інтернету речей (IoT)..... 28

Козак Я.П., Костецький М.Р.

Методи аналізу та розпізнавання рукописних текстів 29

Копилов М.С., Левченко С.В.

Трансформація методологій програмування: розвиток soft skills..... 31

Корельчук О.І.

Дослідження метрологічних характеристик аналого-цифрового перетворювача..... 32

Костецький А.Б., Пашорін В.І.

Використання криптографії в криптовалютах 34

Коцун В.І., Веремій А.А.

Мобільний додаток для ідентифікації користувача на основі даних акселерометра та гіроскопа 36

Кравченко М.О., Хайдуров В.В.

Аналіз сучасних методів передачі голосової інформації..... 38

Ляшенко А.В.

Реалізація проекту “Dependency Injection” за допомогою програмного середовища JAVA.... 41

Маркін Д.О., Островська К.Ю.	
Дослідження процесів оцифрування шахових друкованих видань та розпізнавання шахових діаграм	44
Морохович В.С.	
Інформаційні технології – основа цифрової трансформації	47
Недобосєв М.М.	
Безпека комп'ютерних мереж та інтернет	48
Осташко К.К., Литвиненко Л.О.	
Розробка програмного забезпечення для перетворення неструктурованої інформації в системах аналізу даних	51
Паньова І., Гримаська М.М.	
Управління інцидентами кібербезпеки в сучасному світі	51
Покидько Д.Ю.	
Розробка комп'ютерної гри для адаптивного онлайн навчання	53
Пойченко А.В., Доровська І.О.	
Майбутні напрямки досліджень реалізацій забезпечення відмовостійкості у мікросервісній архітектурі	54
Роман П.І., Невзоров А.В.	
Дослідження роевих алгоритмів комбінаторної оптимізації	56
Садло А.М., Ткаченко А.О.	
Використання статистичного моделювання для розв'язування стохастичних диференціальних рівнянь	58
Святобог О.С.	
Онлайн безпека. Спуфінг та фішінг	60
Сенишин Р.В.	
Веб-застосування для генерування матриці шифрування з використання дискретних методів	62
Собченко Р.	
Тенденції та перспективи розвитку технологій штучного інтелекту	63
Сушинський О.Є., Анісимов Н.В.	
Система прогнозування та аналіз впливу змін клімату за допомогою Python та машинного навчання	65
Танько О.О., Демідов В.В.	
Аналіз і проектування системи моделювання предметної області	68
Хорт В.С., Костецький М.Р.	
Застосування генетичних алгоритмів в задачах транспортної логістики	70
Чубенко В.В.	
Питання цифровізації як виклик та одночасно майбутнє України	72
Шевчук Л.М., Яромка В.М.	
Методи і алгоритми сентиментального аналізу	73
Yurchenko D., Parfenenko Yu.	
Resilience and security: technologies in mitigating cyber threats in smart home systems in Ukraine	75

СИСТЕМА МОНІТОРИНГУ ТА КЛАСИФІКАЦІЇ ХМАРНОСТІ

К.Ф. Базилюк¹

Я.І. Піддубна²

¹к. т. н., доц., доцент кафедри математики та комп'ютерних дисциплін

²магістрантка, Львівська філія ПВНЗ «Європейський університет»

Швидкий розвиток методів супутникового вимірювання та можливість стрімкого отримання оновлених супутникових карт, а також сучасне бачення перспектив подальшого їх використання в синоптична метеорології змінюються настільки швидко, що потрібно регулярно та періодично осмислювати цю проблему для більш ефективного практичного використання їх, що робить проблему моніторингу та класифікації хмарності доволі актуальною.

Аналіз за допомогою датчиків, встановлених на метеорологічних супутниках, широко використовується при моніторингу погоди. [1] Інтерпретація супутникових карт хмарності є доволі важливою для розуміння погодних умов та їх змін [2]. Проведення аналізу хмарності надає можливість визначити локацію фронтів, туманів, грозових осередків, ураганів та хмарності.

У знімках з супутника існування хмар має великий вплив на якість зображення і подальшу обробку зображень, оскільки зображення, покриті хмарами, містять мало корисної інформації. Тому виявлення і розпізнавання хмар є однією з основних проблем при використанні знімків з супутника.

Основним підходом до опрацювання супутникових карт хмарності є розпізнавання фону земної поверхні на зображеннях, відокремлення хмарності та об'єктів схожих на хмарність. Такий аналіз проводиться інфрачервоному та видимому ділянках спектру. З використанням різних частин спектру можливо отримати велику кількість різноманітних атрибутів, що дає можливість дати повну оцінку об'єктів на зображеннях на супутникових картах.

У цій роботі досліджуються алгоритми кластеризації інтенсивності хмарності такі як кластеризація методом к-середніх[3] та просте розбиття за рівнем інтенсивності сірого кольору. Це дозволяє доволі точно та об'ємно оцінити хмарність.

Розбиття за рівнями інтенсивності сірого кольору відбувається доволі просто. Усі пікселі вхідного зображення зводяться до значення інтенсивності сірого кольору (обирається максимальне значення RGB). Якщо інтенсивність пікселя знаходиться в певних межах, то цей піксел потрапляє у відповідний відрізок (кількість відрізків залежить від n).

Недоліком цього методу є його неточність, проте швидкість роботи залежить лише від розміру масиву пікселів. Що дозволяє виконувати аналіз на досить складних зображеннях.

З усіх методів кластеризації метод кластеризації к-середніх – найширше використований та найкраще досліджений. Він може мінімізувати спотворення, поширюючи дані між неперекритими регіонами та ідентифікуючи їх за їх центрами. Основними перевагами методу к-середніх є його простота та швидкість виконання. Метод к-середніх більш практичний для групування великої кількості спостережень.

Завдяки специфіці цих методів можливо також провести аналіз хмарності за певними ознаками. Наприклад, градація сірого вказує на масу хмарності.

Передбачається використання числових даних результату кластеризації для аналізу зображень у часі.

Список використаних джерел

1. *Understanding K-means Clustering in Machine Learning* [Електронний ресурс] – Режим доступу: <https://towardsdatascience.com/understanding-k-means-clustering-in-machine-learning-6a6e67336aa1>
2. *Cloud cover* [Електронний ресурс] – Режим доступу: https://en.wikipedia.org/wiki/Cloud_cover
3. *Understanding K-means Clustering in Machine Learning* [Електронний ресурс] – Режим доступу: <https://towardsdatascience.com/understanding-k-means-clustering-in-machine-learning-6a6e67336aa1>

НАПРЯМИ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ЦИФРОВІЙ ТРАНСФОРМАЦІЇ

Т. М. Білоусько

кандидат економічних наук, доцент, доцент кафедри комп'ютерних та інформаційних технологій і систем, Національний університет «Полтавська політехніка імені Юрія Кондратюка»

В сучасних умовах зростання вимог до інформаційних потреб у будь-якій галузі людської діяльності вимагають приділяти значної уваги інформаційним технологіям (ІТ), котрі відіграють ключову роль у цифровій трансформації. Дана трансформація відбувається у використанні цифрових технологій для змін та вдосконалення бізнес-процесів, культури та моделей взаємодії. Впровадження цифровізації на всіх рівнях підприємства дає змогу фахівцям контролювати процес виконання операцій, вносити необхідні корективи в разі непередбачуваних ситуацій та приймати управлінські рішення на основі актуальної інформації [2].

Відповідно до визначення, яке подано в Розпорядженні Кабінету Міністрів України «Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018 – 2020 роки та затвердження плану заходів щодо її реалізації» від 17.01.2018 № 67-р зазначається: «Цифровізація – насичення фізичного світу електронно-цифровими пристроями, засобами, системами та налагодження електронно-комунікаційного обміну між ними, що фактично уможливорює інтегральну взаємодію віртуального та фізичного, тобто створює кіберфізичний простір. Основна мета цифровізації полягає у досягненні цифрової трансформації існуючих та створенні нових галузей економіки, а також трансформації сфер життєдіяльності у нові більш ефективні та сучасні. Такий приріст є можливим лише тоді, коли ідеї, дії, ініціативи та програми, які стосуються цифровізації, будуть інтегровані, зокрема, в національні, регіональні, галузеві стратегії і програми розвитку. Цифровізація є визнаним механізмом економічного зростання завдяки здатності технологій позитивно впливати на

ефективність, результативність, вартість та якість економічної, громадської та особистої діяльності» [3].

Цифрова трансформація використовує інформаційні технології для перетворення традиційних бізнес-процесів та підходів у сучасні та ефективні. Нижче наведено деякі з основних напрямків використання інформаційних технологій у цьому процесі:

Автоматизація бізнес-процесів: ІТ може допомогти автоматизувати та оптимізувати різні бізнес-процеси, що сприяє підвищенню ефективності та зниженню витрат.

Збір та аналіз даних: Цифрова трансформація вимагає інтенсивного використання даних. ІТ може допомогти в зборі, обробці та аналізі великих обсягів даних для отримання цінного сайту.

Хмарні технології: Використання хмарних рішень дозволяє організації легко масштабувати свою інфраструктуру та підтримувати доступ до потужних обчислювальних та зберігальних можливостей.

Інтернет речей (IoT): IoT дозволяє підключати фізичні об'єкти до Інтернету, які у своєму часі дозволяють створювати дані та взаємодіяти з навколишнім середовищем.

Штучний інтелект та машинне навчання: ІТ-технології, такі як штучний інтелект і машинне навчання, можуть забезпечити автоматизацію проектів рішень, прогнозування та оптимізацію робочих процесів.

Мобільні технології: Мобільні застосунки та пристрої надають користувачам можливість отримувати доступ до інформації та взаємодіяти з нею з будь-якого місця.

Кібербезпека: Забезпечення безпеки інформації та відновлення даних стає важливою частиною цифрової трансформації, і ІТ відіграє важливу роль у забезпеченні кібербезпеки.

Електронна комунікація та співпраця: ІТ-інструменти для електронної пошти, спільної роботи та комунікації підвищують продуктивність та покращують комунікацію між співробітниками.

Результати цифрової трансформації бізнесу говорять самі за себе. За даними дослідження індексу цифрової трансформації Dell Technologies, цифрова трансформація сприяє прогнозуванню, управлінню ресурсами, відстеженню поставок і використанню блокчейну. Під час проведеного аналізу, було зроблено відповідні висновки, що 77% опитаних топ-менеджерів вважають, що в найближчі п'ять років вони будуть використовувати нові технології для прогнозування споживчого запиту; 68% планують використовувати передові технології для покращення прозорості ланцюга постачання, його відстеження та ефективності; 47% вважають, що будуть проводитися операції з використанням блокчейну [1].

Ці технології (хмарні технології, технології кібербезпеки, штучний інтелект; бездротові мережі 5G, Інтернет речей, віртуальна та доповнена реальність; чат боти; технології блокчейн; NFT; Web3; децентралізовані фінанси (DeFi)) разом сприяють створенню гнучких, інноваційних та конкурентоздатних бізнес-середовищ, що є основною метою цифрової трансформації.

Розвиток ІТ-сфери у той чи інший спосіб розглядається у світових технологічних форсайтах. Так, наприклад, у Звіті про передбачення до 2038 р., який був опублікований Європейською Комісією (ЄК), з визначених 100 радикальних проривів інновацій, які з високою ймовірністю впливатимуть на глобальну економіку, одним з ключових напрямків визначено розвиток штучного інтелекту та технології блокчейн, а також пов'язаних з цими напрямками технологій. Крім того, Національний інститут науки та технологічної політики (National Institute of Science and Technology Policy – NISTEP), що є одним з провідних експертів із передбачення в світі, визначаючи перспективні напрямки наукового та технологічного розвитку, значну увагу приділяють розвитку ІТ, зокрема, інформаційно-комунікаційним технологіям нового покоління, хмарним технологіям, робототехніці, технологіям штучного інтелекту, технологіям поширення знань та ін. Національною радою розвідки (США) також визначено у якості глобальних тенденцій до 2030 р. науковий розвиток у галузі інформаційних технологій, в тому числі: використанні великих даних, роботизації, використанні штучного інтелекту та ін. Міністерством науки та ІКТ і Корейським Інститутом оцінки та планування S&T (KISTEP) визначено серед напрямів наукового розвитку до 2040 р. найбільш ключовими технологіями: занурювальну віртуальну, розширену реальність; інтерфейс мозку та комп'ютера; індивідуальне медичне обслуговування на основі використання великих даних та ШІ; розумного робота з використанням ШІ; квантові обчислення; розумні ферми, заводи та фабрики; технології кібербезпеки; інші технології з використанням ШІ. [4]

Таким чином, аналіз досліджень вітчизняних та світових науковців надає можливість стверджувати, що сучасні напрямки використання інформаційних технологій забезпечують стратегію цифрової трансформації економіки та суспільства країни, а також, можливість визначити перспективні напрямки розвитку ІТ, а саме, новітнє покоління інформаційно-комунікаційних технологій, штучний інтелект, хмарні технології та робототехніка.

Список використаних джерел

1. Лебідь, О. (2023). Цифрові та інформаційні технології в управлінні підприємством: реальність та погляд у майбутнє. Економіка та суспільство, (55). <https://doi.org/10.32782/2524-0072/2023-55-19>
2. Обиденнова, Т., & Васильєв, В. (2023). Цифрові технології в управлінні підприємством: теоретичний аспект. Адаптивне управління: теорія і практика. Серія Економіка, 15(30). [https://doi.org/10.33296/2707-0654-15\(30\)-12](https://doi.org/10.33296/2707-0654-15(30)-12)
3. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки розпорядження Кабінету Міністрів України від 17 січня 2018 р. № 67-р. URL: <https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80> (дата звернення: 28.11.2023)
4. Хаустова В. Є., Решетняк О. І., Хаустов М. М. Перспективні напрямки розвитку ІТ-сфери у світі. Проблеми економіки. 2022. № 1. С. 3–19.

ДОСЛІДЖЕННЯ ЗАСОБІВ ТА МЕХАНІЗМІВ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В ОРГАНАХ ДЕРЖАВНОЇ ВЛАДИ

*М.С. Бондар,
здобувач другого (магістерського) рівня вищої освіти,
О.Ю. Ніколаєвський,
к.т.н., доцент кафедри кібербезпеки та захисту інформації
ПВНЗ «Європейський університет»*

Один з головних напрямів розвитку України є інформаційна грамотність суспільства. Заходи передбачають впровадження комунікаційних технологій та кібернетичного простору. Величезна кількість, яка зростає в напрямлення кіберзагроз, включаючи фішинг, хакерські атаки, дані, які вкрадені та вже створюють небезпеку приватності, конфіденційності інформації, що передається через мережі інтернет. На сьогоднішній день вже є витoki конфіденційних даних, які можуть мати серйозні наслідки для осіб та організацій, включаючи фінансові втрати, шкоду репутації, юридичні санкції, а також загрози національній безпеці. Щоб запобігти таким інцидентам, використовуються різні методи та засоби захисту інформації, а саме «шифрування даних», де є сучасні алгоритми шифрування, які забезпечують захист даних під час передачі та зберігання, роблячи їх незрозумілими без відповідного ключа, та «Багаторівневої аутентифікації».

Досвід зарубіжних країн передбачає переведення частини суспільних відносин у кібернетичний простір, яка в свою чергу має переваги та сприяє ефективності взаємодії між собою з представниками громадськості та міжнародною спільнотою. Одночасно також це швидкий розвиток засобів, технологічних систем та мереж, яка характеризується негативними моментами, такою як процвітання злочинності, яка обумовлена фактором технологій, які в свою чергу випереджають розвиток законодавства, котра регулює відносини в цій сфері, що створює в свою чергу процвітання злочинності та складність доведення його вини. Україна не є виключенням в цьому питанні.

Що ж таке кібербезпека для урядів? Урядові та військові державні адміністрації є головними цілями кібератак. Відповідно до звіту Check Point про кібербезпеку за 2023 рік, у 2022 році державні організації потерпали від кібератак у середньому 1661 атаки щотижня, що на 46% більше, ніж у попередньому році. Рішення з кібербезпеки для урядів зосереджені на усуненні цих загроз кібербезпеці. Впроваджуючи засоби захисту від провідних векторів кібератак, державні установи — як федеральні, так і місцеві — можуть зменшити ризик витоку даних та інших руйнівних і шкідливих кібератак.

Суспільне усвідомлення про приватність та конфіденційність даних зростає. Користувачі інформації вже стали більш обізнаними щодо ризиків, які пов'язані зі збереженням та передачею особистих даних в інтернет-мережі.

За останні роки існує значне збільшення кількості цифрових даних, завдяки новим технологіям як інтернет, соціальні мережі, хмарні обчислення, електронна комерція та інші цифрові технології, які справді стали невід'ємною частиною нашого повсякденного життя, перетворюючи спосіб яким ми купуємо

товари, спілкуємося, працюємо та розважаємося. Зі зростанням цифрової економіки зростає і обсяг даних, які ми генеруємо та зберігаємо онлайн, що у свою чергу, збільшує ризики пов'язані з їхньою безпекою.

В останні роки мала місце думка щодо потреби зміцнення національної кібербезпеки, але вже як результат – відсутність необхідного досвіду та нездатність протидіяти даним загрозам. Це є актуальністю комплексного вивчення правових засад забезпечення саме в Україні, де існує багато конкретних проблем у даному механізмі та баченні принципів і перспектив безпосереднього розвитку реалій та розвитку реалій і принципів конфлікту. На сьогодні актуальним питання залишається питання посилення кібербезпеки, де необхідною умовою є саме кібербезпека держави. Світовий досвід демонструє потребу з підвищення ефективності боротьби з кіберзлочинністю у захищеному форматі, і це питання вже непокоїть не тільки державу, а й кожного її громадянина. В сьогоденні дані про конфіденційність серйозно контролюються законодавчими актами, де встановлюються правила та регламент про захист даних, щоб регулювати збір, зберігання, обробку та передачу особистих даних, де різного рівня компаніям та органам влади потрібно дотримуватися вимог, тому що порушення призводить до результату, такого як штрафні санкції та найголовніше втрата репутації.

Дуже швидко зростає розвиток інформаційних технологій, який поступово змінює світ. Відкритий та вільний кіберпростір розширює можливість суспільства, яке в свою чергу створює новий ринок ідей та досліджень інновацій, забезпечує публічність та прозорість влади яка сприяє запобіганню корупції.

Отже, коли наша країна активно переходить на електронний документообіг і так звану діджиталізацію, під час якої в обіг електронної мережі потрапляє велика кількість персональних даних наших громадян, беззаперечно необхідно розвивати та продовжувати досліджувати дану тематику. Але беззаперечним фактом залишається одне, що скільки б ми не досліджували проблематику та шляхи покращення кібербезпеки, нам необхідні величезні кошти для того, щоб реалізовувати дані положення не тільки на папері, але і в реальних діях.

Список використаних джерел

1. Бухарєв В. В. Зарубіжний досвід забезпечення кібербезпеки та можливості його використання в Україні. Науковий вісник Ужгородського національного університету. Серія «Право». 2017. Вип. 43. Т. 3. С. 128–133.
2. Корченко О. Г., Бурячок В. Л., Гнатюк С. О. Кібернетична безпека держави: характерні ознаки та проблемні аспекти. Ukrainian Scientific Journal of Information Security. 2013. № 19. С. 40–44.

МЕТОДИ І АЛГОРИТМИ ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ ЕЛЕКТРОКАРДІОГРАМ

Р.А. Волошин,

магістрант,

О.В. Склярєнко,

к.ф.-м.н., доцент,

завідувач кафедри математичних дисциплін

та інноваційного проектування

ПВНЗ «Європейський університет»

Інтелектуальний аналіз даних поєднує широкий спектр математичних інструментів від класичного статистичного аналізу до новітніх кібернетичних методів, а також останні досягнення в галузі інформаційних технологій [1]. Технології інтелектуального аналізу гармонійно об'єднують строго формалізовані методи з методами неформального аналізу, які включають якісний та кількісний аналіз даних. Математичні методи обробки інформації та аналізу даних широко застосовуються для дослідження різноманітних систем і процесів [2-4].

З урахуванням того, що серцево-судинні захворювання посідають перше місце в світі, зокрема, в Україні серед причин смерті населення, виникла необхідність використання інтелектуальних методів обробки та аналізу даних електрокардіограм (ЕКГ), які дозволяють покращити точність діагностики, спростити аналіз даних і забезпечити швидку обробку інформації для діагностики та моніторингу захворювань.

Авторами проведено дослідження можливостей застосування інтелектуальних методів та алгоритмів для обробки та аналізу даних ЕКГ.

Були виконані наступні методи обробки ЕКГ:

- проведено попередню обробку даних та їх візуалізація;
- здійснено однофакторний та двофакторний дисперсійний аналіз;
- виконано пряме та обернене перетворення Фур'є;
- здійснено кореляційний аналіз та факторний аналіз;
- виконано кластеризацію даних за допомогою методу k-середніх.

На основі проведених досліджень можна зробити наступні висновки:

- 1) Інтелектуальні методи та алгоритми для обробки та аналізу даних електрокардіограм демонструють свою ефективність у виявленні та аналізі потенційних патологічних змін у серцевій діяльності.
- 2) Результати проведеного дослідження підтверджують високу релевантність та перспективи використання інтелектуальних методів обробки та аналізу даних у медичній практиці для діагностики та прогнозування серцево-судинних захворювань.
- 3) Використання інтелектуальних методів та алгоритмів може сприяти розробці нових апаратних та програмних засобів для покращення діагностики та моніторингу серцево-судинної системи.

- 4) Продовження досліджень у даній тематиці є доцільним з метою вдосконалення методів обробки та аналізу електрокардіограм та розробки нових підходів для покращення діагностики та лікування серцевих захворювань.

Список використаних джерел

1. Колодчак О. М. Інтелектуальний аналіз даних / О. М. Колодчак. // Вісник Національного університету "Львівська політехніка". – 2013. – №773. – С. 49-58.
2. Бахрушин В.Є. Методи аналізу даних : навчальний посібник для студентів / В.Є. Бахрушин. – Запоріжжя : КПУ, 2011. – 268 с.
3. Тютюник В. В. Методологічні основи планування експерименту / В. В. Тютюник. – Харків, 2015. – 422 с.
4. Яременко Л. І. Кількосні методи в поведінкових науках / Л. І. Яременко, І. В. Лупан. – Кропивницький, 2019. – 224 с.

УПРАВЛІННЯ БЕЗПЕКОЮ ПІДПРИЄМСТВ ПІД ВПЛИВОМ ЦИФРОВІЗАЦІЇ

Б.М. Головченко

*аспірант кафедри менеджменту та інноваційного провайдингу
ПВНЗ «Європейський університет»*

На сучасному етапі розвитку суспільства особливого значення в темпах економічного розвитку набули процеси формування цифрової економіки.

У сучасних умовах «цифрова економіка» стає драйвером розвитку суспільства, тому так важливо оцінити її вплив на економічну безпеку країни, а також її підприємств як чинника конкурентоспроможності та сталого соціального розвитку. економічний розвиток. Слід зазначити, що започатковані процеси цифрової трансформації сучасних економічних систем у суспільстві дозволяють знизити рівень впливу зовнішніх та внутрішніх загроз на діяльність суб'єктів господарювання підприємств, що робить їх більш стабільними та ефективними. У процесі активного розвитку цифрової економіки можлива заміна традиційних соціокультурних та економічних цінностей на інстинктивні, що зумовлює актуальність розгляду впливу цифрової економіки на економічну безпеку на всіх рівнях господарювання.

Розуміння сутності безпеки полягає у з'ясуванні стану захищеності від внутрішніх і зовнішніх загроз, що базується на виявленні, послабленні або усуненні загроз, здатних завдати шкоди та збитків.

Економічна безпека є більш вузьким поняттям, оскільки в її основі лежить здатність системи протистояти загрозам, руйнуванню, завданню шкоди підприємству.

Загрози економічній безпеці включають низку дестабілізуючих факторів, пов'язаних із недобросовісною конкуренцією та порушенням норм, принципів і законів, які лежать в основі ринкової економічної системи. Усі загрози можна розділити за рядом ознак:

- за місцем виникнення загрози можна поділити на внутрішні та зовнішні;
- за причинами можна назвати політичні, конкурентні, соціальні та правові;

- за наявністю – існуючі, приховані та потенційні;
- за наслідками дії – незначні, значні, критичні та катастрофічні;

Важливо також відзначити існування правопорядку в рамках ринкової економічної системи, що забезпечує реалізацію законодавчих актів держави та правових механізмів виробничих адміністрацій та органів місцевого самоврядування. Зрештою, стабільна правова база виробничих відносин призведе до нормалізації демографічної ситуації та стабілізації трудових відносин на ринку праці з максимальною зайнятістю населення та зниженням безробіття [1, 2].

Останнім часом міграція населення в пошуках роботи стала загрозою не тільки для підприємств, а й для держави в цілому. Особливо критичним є відтік спеціалістів з високим рівнем освіти та втрата фахівців у критичній для ринкової економіки інформаційній сфері. ІТ-спеціалістів запрошують за кордон міжнародні компанії, пропонуючи високу оплату праці, що спонукає спеціалістів залишати країну [3, 4].

Усунення цих загроз передбачає застосування комплексу методів і засобів безпечного використання інформації у виробничо-економічних системах. Найважливішими є такі заходи:

1. Управління доступом до важливої інформації та протидія можливим методам несанкціонованого доступу до інформації. Такі заходи передбачають ідентифікацію користувачів та персоналу органів управління підприємств шляхом прикріплення персонального ідентифікатора до кожного об'єкта.

2. Перевірка повноважень та визнання автентичності об'єкта-ідентифікатора за пред'явленим кодом або шифром, що дозволить їм отримати доступ до відповідної інформації.

3. Створення умов доступу та роботи з інформацією із встановленням регламенту роботи та обсягів доступу до відповідної інформації.

4. Обов'язкова реєстрація осіб і структур і термінів їх доступу до відповідної конфіденційної інформації, встановлення обсягів отриманої та обробленої ними інформації з подальшим її використанням у соціально-економічних і виробничо-технологічних відносинах.

5. Фіксація спроб несанкціонованого доступу і навіть спроб несанкціонованого доступу до інформації з ідентифікацією підозрюваних осіб або структур.

6. Розвиток спеціальних механізмів шифрування доступу до критичної інформації, які зростають у зв'язку з розвитком телекомунікаційних систем і розширенням систем зв'язку, особливо створення розгалуженої системи Інтернет з її необмеженим доступом до різноманітних баз даних і ресурсів.

7. Системна протидія вірусному зараженню баз даних, джерел інформації у відкритому доступі та локалізації та знищенню ресурсів або їх навмисного пошкодження та виходу з ладу комп'ютерних систем і пристроїв, які є досить дорогими та рідкісними [5, 6].

Процес цифровізації стрімко розвивається і оновлення виробничих економічних систем неможливе без залучення сучасних механізмів захисту інформації та подолання спроб її несанкціонованого використання.

Список використаних джерел:

1. Бойчук І. В. Інтернет в маркетингу: підручник / І. В. Бойчук, О. М. Музика. - К.: ЦУЛ, 2010.
2. Зубенко, І.Р. Психологічні детермінанти довіри до електронної комерції [Електронний ресурс].
3. Baigaryn, T. (2021). Approaches to changing business models by using digital technologies. *Central Asian Economic*, 22, 162-169.
4. Kolodinskyi, S.B., Dubnitskyi, V.I., & Kramskyi, S.O. (2021). Infrastructural support of regional innovation processes. Odesa: OSACA. "Ecology".
5. Дернова, І.А. (2022). Цифровізація економіки України в умовах пандемії: тренди та напрямки розвитку. *Економіка: реалії часу*. Науковий журнал, 1 (59), 22-29.
6. Andros, S.V., & Chang Si Tso (2019). Information technologies as the basis of innovative development of enterprises. *Economics: realities of the time*, 5, 16-25.

ПОЛІТИЧНІ ІНСТИТУЦІЇ У ВИРІШЕННІ КОНФЛІКТІВ ТА КІБЕРЗАГРОЗ СУЧАСНОГО СУСПІЛЬСТВА

Д.Ю. Гончаренко

аспірант, ПВНЗ «Європейський університет»

Сучасний світ стикається з безліччю гуманітарних викликів, включаючи масштабні міграції, конфлікти та гуманітарні кризи. У цьому контексті роль політичних інститутів стає надзвичайно важливою для вирішення цих проблем та створення стабільного глобального середовища.

Однією з ключових сучасних проблем є міграція, яка визначається як складний інтернаціональний процес. Політичні інституції відіграють рішучу роль у встановленні стратегій, які сприяють інтеграції мігрантів та забезпеченні їхніх прав та безпеки. Важливою також є співпраця на міжнародному рівні для розробки ефективних механізмів управління міграцією та подолання зумовлених нею викликів.

Конфлікти і війни є іншими серйозними викликами, що вимагають від політичних інститутів активної ролі у миротворчих процесах, примиренні та відновленні після конфліктів. Глобальна співпраця і взаємодія політичних інститутів на міжнародному рівні можуть сприяти уникненню конфліктів, або ж ефективному їх розв'язанню шляхом дипломатії та перемовин.

Конфлікти, будучи важливою частиною світової реальності, створюють не лише гострі геополітичні ситуації, але й серйозно впливають на життя мільйонів людей. У цьому контексті політичні інститути мають велику відповідальність у забезпеченні стабільності, миротворчих процесах та підтримці регіонів, які постраждали від конфліктів.

Глобальна співпраця політичних інститутів в розв'язанні конфліктів може включати різноманітні заходи, такі як дипломатичні переговори, миротворчі місії та ефективні механізми роззброєння. Важливо враховувати національні інтереси, але також шукати спільні рішення для побудови довготривалого миру. Політичні інститути повинні звертати увагу на корені конфліктів, аналізувати їхні причини та сприяти формуванню механізмів, спрямованих на вирішення основних суперечностей.

Міжнародні відносини та співпраця також грають важливу роль у вирішенні конфліктів. Спільні зусилля міжнародних організацій, таких як Організація Об'єднаних Націй (ООН), Європейський союз та інші регіональні блоки, можуть забезпечити ефективність та легітимність управління конфліктами. Зокрема, розгляд імплементації миротворчих операцій та підтримка демократичних інститутів у країнах-учасниць можуть допомогти стабілізувати ситуацію та запобігти подальшим вибухам насильства.

У світлі сучасних викликів, таких як тероризм і кіберзагрози, важливо, щоб політичні інститути пристосовували свої стратегії та реагували на нові виміри конфліктів. Ефективна боротьба з цими загрозами вимагає співпраці національних та міжнародних структур для розробки та впровадження стратегій, які забезпечать безпеку та захист прав людини.

В сучасному світі, де цифрові технології стають невід'ємною частиною нашого повсякденного життя, кіберзагрози зростають за змістом і складністю, ставши важливим елементом глобальної безпеки та політичних процесів. Політичні інститути повинні адаптувати свої стратегії, щоб ефективно впоратися з цими новими викликами.

Кіберзагрози включають в себе не лише традиційні атаки на комп'ютерні системи, а й маніпулювання інформацією, вплив на громадську думку та електоральні процеси. Політичні інститути повинні розробляти та впроваджувати заходи кібербезпеки, щоб захистити не лише свої внутрішні системи, але й дотримуватися демократичних принципів, таких як прозорість та недопущення маніпуляцій у виборчих процесах.

Одним з ключових аспектів в управлінні кіберзагрозами є співпраця міжнародних політичних структур і правозахисних організацій. Поширеність кібератак та їхній потенціал впливу на суспільство роблять неможливим обмеження боротьби з цим явищем на рівні окремих країн. Колективні зусилля для створення міжнародних стандартів кібербезпеки та обміну інформацією можуть допомогти створити більш ефективні механізми виявлення, запобігання та відновлення після кібератак.

Політичні лідери також повинні розуміти соціокультурний вимір кіберзагроз та їхній потенціал викликати дезінформацію та дестабілізацію суспільства. Забезпечення грамотності населення у цифровому середовищі, розвиток медіаграмотності та створення механізмів перевірки достовірності інформації може бути ефективним кроком у зменшенні впливу кіберманіпуляцій.

Також важливою є активна роль держав у розробці міжнародних договорів та правових рамок, що стосуються кібербезпеки. Визначення відповідальності за кібератаки та створення механізмів судового переслідування може стати стримувальним фактором для потенційних агресорів.

Узагальнюючи, кіберзагрози вимагають від політичних інститутів не лише реакції на події, а й системного підходу до забезпечення кібербезпеки на всіх рівнях, від національних до міжнародних. Співпраця, технологічні інновації та освіта – ключові елементи ефективної стратегії боротьби з кіберзагрозами в сучасному політичному ландшафті.

Гуманітарні кризи, пов'язані, наприклад, з природними катастрофами або епідеміями, вимагають негайної реакції та координації зусиль національних та

міжнародних політичних організацій. Політичні інститути мають забезпечити ефективний розгортання гуманітарної допомоги та реагування на надзвичайні ситуації, зближуючи світове співтовариство в обличчі спільного виклику.

Усі ці аспекти говорять про те, що співпраця між політичними інститутами на міжнародному рівні стає дедалі важливішою. Вона вимагає від політиків гнучкості, відкритості до новаторських підходів та готовності до спільних зусиль для створення стійкого, гуманітарного світу.

Список використаних джерел:

1. Clarke, R. A. (2010). "Cyber War: The Next Threat to National Security and What to Do About It." HarperCollins.
2. Libicki, M. C. (2014). "Cyberdeterrence and Cyberwar." Rand Corporation.
3. Rid, T. (2013). "Cyber War Will Not Take Place." *Journal of Strategic Studies*, 35(1), 5-32.
4. Nye, J. S. (2011). "The Future of Power." Public Affairs.
5. Schneier, B. (2015). "Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World." W. W. Norton & Company.
6. Goodman, S. E. (Ed.). (2019). "Routledge Handbook of Cybersecurity." Routledge.
7. Carr, J. (2016). "The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations." Oxford University Press.
8. Brenner, J. (2007). "America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare." Penguin.
9. Stiennon, R. (2015). "There Will Be Cyberwar: How the Move to Network-Centric Warfighting Has Set the Stage for Cyberwar." IT-Harvest Press.
10. Arquilla, J., & Ronfeldt, D. (1997). "Cyberwar is Coming!" *Comparative Strategy*, 16(2-3), 141-165.

ВИКОРИСТАННЯ МЕТОДІВ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ РОЗПІЗНАВАННЯ МОВЛЕННЯ

***А.В. Гуцуляк,
М.В. Кот***

ПВНЗ «Європейський університет»

У сучасному світі людина прагне автоматизувати всі аспекти свого життя, щоб полегшити його перебіг, сприяючи тим самим швидкому розвитку технологій. Серед численних інструментів оптимізації, що використовуються в цьому контексті, особливе місце займають штучні нейронні мережі.

Хоча цей вид технології з'явився нещодавно, він вже успішно використовується для вирішення різноманітних завдань, таких як системи розпізнавання та класифікації об'єктів на зображеннях, створення контекстної реклами, розпізнавання рукописних текстів та інших. Дане дослідження присвячене розробці простої моделі глибокого навчання, яка спроможна виявляти мовні команди в аудіо. У цьому контексті вона детально розглядає принципи обробки інформації та приводить до висновку щодо створення згорткової нейронної мережі як результату цього дослідження.

Згорткова нейронна мережа (ЗНМ) базується на математичній операції згортки, що представляє собою впорядковану процедуру змішування інформації з двох джерел. Для наочного уявлення, можна уявити ситуацію із двома мішками

із зерном, де зерно виступає як інформація. Зерна з обох мішків зсипаються в один великий контейнер і після цього піддаються перемішуванню згідно з певним способом. Кожен мішок із зерном має своє власне правило, яке визначає, як зерно з одного мішка комбінується з зерном з іншого.

У контексті ЗНМ, фільтр представляє собою колекцію ядер, де для кожного окремого вхідного каналу в даному шарі існує власне ядро, і кожне ядро унікальне. Результат для будь-якої кількості фільтрів ідентичний: кожен фільтр обробляє вхід із своїм унікальним набором ядер і здійснює скалярне зміщення, створюючи таким чином один вихідний канал.

Такий підхід дозволяє ЗНМ ефективно виявляти та аналізувати просторові особливості вхідних даних, роблячи його потужним інструментом для обробки зображень та інших видів даних, що мають просторову структуру.

Робота з вихідними даними у контексті навчання згорткової нейронної мережі.

1. Підготовка Даних

За основу для нашого дослідження було взято базу даних мовних команд від Google [1], яка містить приблизно 71 000 звукових доріжок, індексованих та розподілених за папками. Спочатку до тренувального набору не включали довгі файли з фононим шумом, вони додаються на окремому етапі. Для навчання нейромережі використовувались аудіофайли, серед яких були мовні команди, такі як "yes", "no", "up", "down", "left", "right", "on", "off", "stop", "go", а також 8193 невідомих ("unknown") шумових варіацій.

2. Обчислення мовних спектрограм та візуалізація даних

Для підготовки даних для ефективного навчання згорткової нейронної мережі, мовні сигнали були перетворені на log-mel спектрограми з визначеними параметрами, такими як тривалість кожного мовного кліпу, тривалість кожного кадру, крок за часом між кожним стовпцем та кількість log-mel-фільтрів.

Відбулася перевірка на файлах з сховища, підтверджуючи, що весь процес працює. Нормалізація та плавний розподіл даних були забезпечені, що є ключовим елементом ефективного тренування нейронних мереж.

3. Фоновий Шум

Розроблена мережа не лише здатна розпізнавати вимовлені слова, але й визначати, чи містить вхід тишу чи фоновий шум. Для цього створено зразки 4000 кліпів фонового шуму, що варіюються за тривалістю від однієї секунди та масштабуються у діапазоні від 10^{-4} до 1. Отримані спектрограми охоплюють від тиші до гучного шуму.

Спектрограми фонового шуму були розділені між навчальними, перевірочними та тестовими наборами, забезпечуючи велику кореляцію між фоновими вибірками в різних наборах даних. На цьому етапі також було збільшено ефективний розмір учбових даних, спрямований на запобігання надмірному навантаженню мережі

Робота з нейромережею у контексті розробки та тренування

1. Визначення архітектури нейронної мережі

Під час роботи була розроблена проста мережева архітектура у вигляді масиву шарів нейромережі. Використано згорткові та пакетні шари нормалізації, а також зменшення вибірки карт об'єктів за часом та частотою. Максимальне

об'єднання рівнів використовується для отримання інваріантності перетворення часу у вхідних спектрограмах. Розмірність мережі обмежена - п'ять згорткових шарів з кількома фільтрами та користувальницьким шаром для обчислення перехресної ентропійної втрати.

2. Навчання та тренування нейромережі

Для навчання мережі використовувався оптимізатор Adam, який є методом адаптивної швидкості навчання. Величина мініпакету становила 128. Тренувальний цикл складався з 25 повних проходів через весь набір тренувань, зі зменшенням швидкості навчання у 10 разів після 20 проходу.

3. Оцінка навченої мережі

Помилка мережі на тренувальному наборі становить 1.3806%, а на перевірконому – 4.2999%, що вказує на точність нейромережі на рівні 95.70%. Важливо відзначити, що розподіли даних тренування, перевірки та тестування схожі, але не обов'язково відображають реальне середовище.

Матриця плутанини свідчить про велику плутанину між невідомими словами та командами, такими як "up" та "down", "down" та "no", "go" та "no".

Розмірність мережі складає 255.709 Кб, а швидкість прогнозування при використанні процесора становить 3.944 мс. Мережа має можливість класифікації кількох зображень одночасно, що призводить до скорочення часу прогнозування для кожного зображення.

Висновки

У результаті проведеної роботи була успішно розроблена нейромережа, спроектована для розрізнення вимовлених слів. Оцінки, отримані алгоритмом, вражають своєю ефективністю, що підтверджується практично безперешкодною роботою системи навіть у складних умовах.

Зазначимо, що алгоритм виявляє стабільність при збільшенні розмірності вектора оцінюваних параметрів та розширенні кількості класів (слів, що розпізнаються). Точність розпізнавання розробленої системи сягає вражаючих 95.7%.

Зауважимо, що є можливість подальшого вдосконалення системи для розпізнавання більшого словникового запасу. Рекомендацією є збільшення кількості аудіофайлів для тренування, що, в свою чергу, сприятиме підвищенню точності розпізнавання.

Список використаних джерел

1. Haffner P., Waibel A. Multi-State Time Delay Neural Networks for Continuous Speech Recognition // Advances in Neural Information Processing Systems. San Mateo: Morgan Kaufmann Publ., 1992. Vol. 4. P. 579-588.
2. M. Gales and S. Young The Application of Hidden Markov Models in Speech Recognition. Foundations and Trends in Signal Processing, 2007, vol. 1, No. 3, pp. 195- 304.
3. Abougair A.J. Design and implementation of smart voice assistant and recognizing academic words // International Journal of Robotics and Automation. 2022.
4. Khurana D., Koli A., Khatter k., Singh S. Natural language processing: state of the art, current trends and challenges // Multimedia Tools and Applications. 2022.

МОБІЛЬНИЙ ЗАСТОСУНОК ДЛЯ ОПТИМІЗАЦІЇ АЛГОРИТМІВ ПОБУДОВИ МАРШРУТІВ

*О.М. Гущак¹
А.А. Веремій²*

¹к. т. н., доцент кафедри математики та комп'ютерних дисциплін

²магістрант,

Львівська філія ПВНЗ «Європейський університет»

Охорона довкілля, а також раціональне використання природних ресурсів є важливою частиною процесу суспільного розвитку України як держави, адже природні ресурси є базою життєдіяльності населення та економіки країни, і саме тому забезпечення їх збереження, відтворення та невиснажливого використання є однією з основних передумов постійного соціально-економічного розвитку країни. Саме тому дана робота спрямована на оптимізацію алгоритмів побудови маршрутів між пунктами приймання вторсировини та користувачем, що, в свою чергу, приведе до зменшення так званого екологічного сліду людини – стандартизованого показника, який відображає попит людей на природний капітал, що в найгірших випадках може перевищувати екологічну спроможність планети до регенерації вищевказаного капіталу.

В роботі представлений мобільний застосунок для оптимізації побудови маршрутів між користувачем та пунктами приймання вторсировини. Система побудована на ідеї відповідального споживання та утилізації продуктів щоденного вжитку. Процес взаємодії з додатком починається з пошуку на мапі найлояльнішого до екологічно чистих продуктів широкого вжитку магазину чи супермаркету, далі користувачеві пропонується відсканувати склад продукту і обрати екологічно найчистіший товар. Після використання обраного продукту система дозволяє обрати пункти приймання конкретних типів вторсировини та прокладає найефективніший маршрут від користувача до них. Саме так зменшується екологічний слід, який залишає за собою людина.

Для реалізації програмного продукту використано мобільну платформу Android, реляційну систему керування базами даних SQLite та мову програмування Java.

Розроблений мобільний застосунок представляє собою односторінковий додаток, на єдиній сторінці якого розташований весь функціонал сервісу, що робить його простим у використанні.

Функціонал мобільного додатку передбачає:

- перегляд карти місцевості;
- можливість побудувати маршрут між двома точками з урахуванням критеріїв;
- можливість вибору критеріїв для побудови маршруту;
- встановлення максимально допустимого відхилення від найкоротшого маршруту;
- відображення маршруту на карті.

Список використаних джерел

1. Екологія. Освіта.UA : веб-сайт. URL: <http://osvita.ua/vnz/reports/ecology/18852> (дата звернення: 16.11.2019)
2. Environmental Pollution article : веб-сайт. URL: <https://en.wikipedia.org/wiki/Pollution> (дата звернення: 16.11.2019)
3. Документація Android SDK : веб-сайт. URL: [https:// developer.android.com](https://developer.android.com) (дата звернення: 28.10.2019)
4. Scott Oaks, Java Performance: The Definitive Guide: навч. посібник. – Лондон, 2014. - 500с.
5. Bill Phillips - Android Programming: The Big Nerd Ranch Guide: навч. посібник. - 2013 — 602с.
6. Дорогунцов С.І., Коценко К.Ф., Хвесик М.А. Екологія, : довідник - 2005 – 371с.
7. Erik Hellman - Android Programming: Pushing the Limits навч. Посібник, 2013 – 432с.

СИСТЕМА КЕРУВАННЯ ПОДАЧЕЮ ПАЛИВА НА ОСНОВІ ОПРАЦЮВАННЯ ДАНИХ НЕПРЯМИХ ВИМІРЮВАНЬ

О.Ф. Єнікєєв

*д.т.н., доцент, завідувач кафедри комп'ютерних наук
та програмної інженерії
ПВНЗ «Європейський університет»*

Техніко-економічні показники двигунів залежать від фаз подачі палива у циліндри. Прямий метод моніторингу циліндрових потужностей передбачає вимірювання тиску циліндрів за допомогою блоку E14-140 фірми L-Card, первинного перетворювача 8QP505CS фірми AVL та прикладного програмного забезпечення «Power Graph». У результаті вимірювань отримуємо індикаторні діаграми циліндрів, подальше порівняння яких дозволяє встановити їхню ідентичність. Якщо є у тому потреба, виконується зміна налаштувань фаз подачі палива. Необхідність дороблення двигуна з метою встановлення давача тиску, використання ручної праці, наявність певної кількості циліндрів і з великі апаратні витрати суттєво обмежують застосування цього методу.

Відомий непрямий метод оцінювання ідентичності циліндрових потужностей в якості джерела вхідної інформації використовує ЧМ-сигнал швидкості обертання колінчастого валу. Його алгоритмічне забезпечення орієнтовано на отримання сигналу флуктуацій та подальше його опрацювання з метою оцінювання ідентичності циліндрових потужностей. Задавання кутів подачі палива у циліндри дасть економію палива на рівні 5% й скоротить витрати на профілактику, обслуговування та ремонт.

Пропонується ідея керування подачею палива у циліндри двигуна на основі опрацювання сигналу миттєвої швидкості обертання колінчастого валу. Синхронізацію роботи апаратних засобів із фазою обертання колінчастого валу забезпечує сигнал верхньої мертвої точки першого циліндру. У якості виконуючих механізмів для задавання подачі палива використано форсунки із п'єзоелектричним керуванням. Архітектуру апаратних засобів складають такі блоки: давач миттєвої швидкості обертання колінчастого валу, давач верхньої мертвої точки першого циліндру, вимірювальний перетворювач, обчислювальний пристрій (мікроЕОМ) та три виконавчі механізми.

У результаті аналізування крутної схеми двигуна пропонується: для отримання вхідної інформації використати впускний колінчастий вал, що суттєво обмежує кількість мас механічної моделі; ПП встановити біля першого циліндру; за умови врахування тертя та коливань між масами крутильну схему подати у вигляді механічної системи, яка має чотири ступені волі. Динаміка обертання циліндрових мас моделі описано системою диференціальних рівнянь. Для узагальнення результатів досліджень приведено систему диференціальних рівнянь до безрозмірного вигляду за допомогою теорем теорії подібності.

В якості математичного апарату аналізу механічної моделі крутної схеми використано перетворення Лапласу за нульових початкових умов. За допомогою методу визначників та програмного середовища Mathcad встановлено передавальні функції, які встановлюють інформаційні зв'язки між крутними моментами циліндрів та сигналом вимірювальної інформації. Дослідження передавальних функцій проведено за допомогою програмного середовища Matlab. Проведено спрощення отриманих виразів передавальних функцій за рахунок погашення коренів чисельника та знаменника, а також відкидання нестійких та коренів другого порядку малості.

В результаті аналізування отриманої інформації робимо такі висновки. ЛАФЧХ має нахил -20 Дб на декаду, що відповідає наявності ланцюга інтегрування у структурі каналів передавання крутних моментів, у смузі частот 1050 – 1400 с⁻¹ мають місце переколювання.

Також встановлено інформаційні зв'язки між крутними моментами та сигналом флуктуацій швидкості обертання першої маси за допомогою методів теорії сигнальних графів. У результаті аналізування структури алгебраїчних рівнянь й організації системи побудовано сигнальний граф. На основі цього графу за допомогою формули Мезона встановлено визначники. При аналізуванні отриманих даних встановлено збіг із попередніми розрахунками.

Використано індикаторну та діаграму стиснення першого циліндру для апроксимації крутних моментів. Його вираз подано обмеженим рядом Фур'є. Фазове запізнення циліндрів відносно першого кратно 120^0 й розраховується із урахуванням такої послідовності їхньої роботи: 1-2-3. Запропоновано подати коливання циліндрових потужностей у вигляді вагових коефіцієнтів циліндрів. Алгоритмічне забезпечення моніторингу циліндрових потужностей двигуна побудовано на встановленні величин вагових коефіцієнтів циліндрів. Для цього розв'язується система алгебраїчних рівнянь. Її ліву частину складають: матриця, коефіцієнти якої визначаються як добуток передавальних функцій та крутних моментів циліндрів в залежності від обраного методу розрахунку; та вектор-стовпець амплітудних коефіцієнтів. Її праву частину утворює вектор-стовпець різниці між частотним поданням сигналу вимірювальної інформації та сигналом флуктуацій за відсутності подачі палива у циліндри. Останній сигнал отримано заздалегідь на підставі частотного подання крутних моментів за відсутності подачі палива у циліндри та отриманих передавальних функцій.

Схему комп'ютерного моделювання рухів першої маси двигуна складено із урахуванням можливостей програмного середовища Matlab із розширенням Simulink на основі виразів отриманих передавальних функцій та частотного подання крутних моментів. Вихідним сигналом схеми комп'ютерного

моделювання є сигнал флуктуацій швидкості обертання першої маси колінчастого валу. Математичні моделі крутних моментів другого та третього циліндрів (Model M2 and Model M3) аналогічні першому із урахуванням відповідного фазового запізнення. Також моделі крутних моментів враховують нормування за амплітудою шляхом множення на базисний момент. При складанні схеми комп'ютерного моделювання також враховано можливість регулювання внесків окремих циліндрів у сигнал флуктуацій першої маси за допомогою вагових коефіцієнтів. Чисельні значення цих коефіцієнтів встановлюємо при ідентифікації параметрів математичної моделі механічної системи із чотирма ступенями волі. Для виконання цієї процедури застосовано метод моделі, яка навчається, та дослідні дані миттєвої швидкості обертання першої маси.

Найбільш перспективним методом побудови ВП параметрів ЧМ-сигналів є дискретизація за часом періодів проходження імпульсних послідовностей, які сформовано ПП. При дослідженнях метрологічних характеристик ВП параметрів ЧМ-сигналів використано методи теорії ймовірності, математичної статистики та теорії вимірювань, зокрема, інформаційний підхід.

Для побудови архітектури ВП параметрів ЧМ-сигналу запропоновано метод організації багатоканальних вимірювань проміжків часу, які формуються певною ризикою ПП і відповідають одному повному оберту валу. При такому методі вимірювань періодів ЧМ-сигналу швидкості обертання колінчастого валу кінематична невизначеність ПП призводить до зміщення в часі точок дискретизації. Зсув за часом точок дискретизації аналогового сигналу флуктуацій обумовлює динамічну невизначеність ПП. Її проаналізовано та на основі опрацювання ряду вимірювань із багаторазовими спостереженнями встановлено, що використання методу багатоканальних вимірювань зменшує невизначеність до 14%.

Кількість каналів для вимірювань періодів ЧМ-сигналу дорівнює кількості прорізів диска ПП. Блок ВП вимірює інтервали часу, тривалість яких дорівнює часу проходження поблизу чутливого елемента ДЧ обраної прорізі. У цьому випадку кінематична невизначеність диска не впливає на тривалість проміжків часу, які сформовано ПП. Отримані проміжки часу надходять на входи багатоканального пристрою для вимірювань тривалості, який реалізує метод дискретизації за часом. Частоту вихідного сигналу генератора стабілізовано кварцовим резонатором. Вихідні сигнали окремих каналів пристрою для вимірювань тривалості накладаються один на одного. Для усунення можливих накладень при формуванні сигналу вимірювальної інформації вирізається більша частина вимірюваного проміжку часу за допомогою лічильників імпульсів. Раціональний підбір обсягів лічильників та частоти сигналу генератора повністю усувають взаємні накладання вихідних сигналів пристроїв для вимірювань тривалості. Оскільки коефіцієнт перерахунку лічильника постійний, то тривалість проміжку часу, який вирізається, визначається стабільністю сигналу генератора. Отже, кінець проміжку часу, який вирізається, жорстко прив'язаний до його початку. Решта проміжку часу є інформаційними сигналами та підсумовуються в сигнал вимірювальної інформації за допомогою схеми АБО. Таким чином, на виході логічного елемента АБО виходить сигнал вимірювальної

інформації, в якому компенсовано кінематичну невизначеність ПП. Величина ентропійного інтервалу невизначеності ВП із пристроєм компенсації кінематичної невизначеності ПП складає $\Delta S=0.0075$, що доводить про доцільність використання пристрою.

МОДЕЛЮВАННЯ ОДНОРІДНИХ ТА ІЗОТРОПНИХ ВИПАДКОВИХ ПОЛІВ НА СФЕРІ

М.Ю. Карповець,

магістрант

Р.О. Яровий

к.т.н.доцент

ПВНЗ «Європейський університет»

В інженерній практиці для описання процесів та систем різної фізичної природи використовують, як правило, детерміністичні моделі розрахунку. При цьому їх властивості розглядаються як цілком визначені. Застосування детерміністичних моделей є обґрунтованим. Разом із тим, очевидно, не існує жодної величини, яка враховується у розрахунках, що не була б випадковою. Як немає жодного розрахунку, який за своїм змістом не був би ймовірнісним. Вплив випадкової зміни величин та факторів, що характеризують механічні системи, може відігравати суттєву, а іноді й визначну роль, тому нехтувати цим в інженерних розрахунках є неприпустимим.

Виразений випадковий характер мають аеродинамічні навантаження, що діють на елементи літальних апаратів у процесі лету, реакції дорожнього покриття на підвіску транспортних засобів, що рухаються, гідродинамічні навантаження, що виникають у турбулентних потоках та ін. Для адекватного описання такого роду навантажень та механічних систем, що перебувають під їх впливом, необхідно використовувати теорію випадкових процесів та полів.

Випадковим полем називається випадкова функція у загальному випадку декількох просторових або просторово-часових детерміністичних аргументів. Випадкові поля можуть бути скалярними (одновимірними) та векторними (n – вимірними).

Опис випадкових полів є тотожним опису випадкових величин та випадкових процесів: за допомогою характеристик розподілу, за допомогою моментних функцій та, як зручний апарат аналізу на основі цих способів, – за допомогою спектральних розкладів.

Випадкове просторове поле $W(\vec{r})$ – називається однорідним, якщо його ймовірнісні характеристики не залежать від паралельного перенесення системи координат, тобто вони залежать тільки від різниці просторових векторів точок аналізу.

Властивість однорідності просторового випадкового поля за просторовими координатами еквівалентна властивості стаціонарного випадкового процесу за часовим аргументом.

Однорідні й однорідні ізотропні поля частіше всього використовуються для нескінченних областей. У більшості практичних застосувань виявляється можливим використання скінченних реалізацій однорідних ізотропних полів (за аналогією з властивістю ергодичності стаціонарних випадкових процесів). Наприклад, турбулентні пульсації тиску на пластину скінченних розмірів можна апроксимувати у вигляді реалізації однорідного поля розподіленого навантаження, віднесеного до серединної поверхні пластини.

Однорідні ізотропні випадкові поля являють собою більш вузький клас порівняно з однорідними випадковими полями. Разом із тим ізотропні польові характеристики використовуються при описанні механічних властивостей матеріалів твердих тіл, що деформуються.

За визначенням, ізотропним називається таке випадкове поле, ймовірнісні характеристики якого є інваріантними відносно поворотів та дзеркальних віддзеркалень системи координат. Імовірнісні властивості такого поля є однаковими у будь-якому напрямку у будь-якій точці визначення. Властивість ізотропії може бути локальною та загальною. Прикладом локальної ізотропії є, наприклад, поле напружень у шарі, коли ймовірнісні характеристики поля залежать тільки від довжини вектора, що проведений із центра шару, і не залежать від напрямку цього вектора.

Для однорідного ізотропного поля кореляційна функція залежить від модуля різниці точок аналізу $|\vec{s}| = |\vec{r}' - \vec{r}| = s$

$$K_W(\vec{r}, \vec{r}') = K_W(|\vec{s}|) = K_W(s),$$

оскільки модуль вектора $|\vec{s}| = s$ є інваріантним відносно обертання системи координат.

Нехай $\xi = \{\xi(x), x \in S_d\}$ – дійсне субгауссове неперервне в середньому квадратичному випадкове поле на сфері S_d в d – вимірному просторі, ізотропне в широкому розумінні. Випадкове поле $\xi(x)$ зображується у вигляді

$$\xi(x) = \sum_{m=0}^{\infty} \sum_{l=1}^{h(m,d)} \xi_m^l S_m^l(x),$$

де ξ_m^l — послідовність незалежних субгауссових випадкових величин таких, що $E\xi_m^l = 0$, $E\xi_m^l \xi_r^s = \sigma_m \delta_m^r \delta_l^s$, $m = 0, 1, \dots$, $l = 1, \dots, h(m, d)$, $\sigma_m > 0$, δ_m^r —

символ Кронекера, $S_m^l(x) = S_m^l(\theta_1, \dots, \theta_{d-2}, \varphi)$ — ортонормовані сферичні

гармоніки ступеня m , $h(m, d) = (2m + d - 2) \frac{(m + d - 3)!}{(d - 2)! m!}$ — число таких гармонік,

$$\sum_{m=0}^{\infty} \sigma_m h(m, d) < \infty.$$

і має місце

На основі отриманих результатів будуються алгоритми побудови моделей гауссівських та субгауссівських випадкових полів, що зображуються у вигляді рядів.

Досліджено оцінки точності та надійності моделювання таких процесів в різних функціональних просторах та для різних зображень випадкових процесів, Нехай випадковий процес X та всі X_M , $M = 1, 2, \dots$ належать деякому функціональному банаховому простору $A(T)$ з нормою $\|\cdot\|$. Нехай задано два числа α та δ ($0 < \alpha < 1$, $\delta > 0$). Говоритимемо, що модель X_M наближає X з надійністю $1 - \alpha$ та точністю δ у нормі простору $A(T)$, якщо для цієї моделі має місце нерівність

$$P\{\|X(t) - X_M(t)\| > \delta\} \leq \alpha. \quad (1)$$

Отже, для побудови моделі потрібно знайти такі M , для яких при заданих δ та α виконується нерівність (1).

Список використаних джерел

1. Цибенко С. О. Ймовірнісні методи в механіці. / С. О. Цибенко, Ю. Я. Тарасевич. – Суми : Сумський державний університет, 2013. – 240 с.
2. Ю.В. Козаченко, А.О. Пашко. Точність моделювання випадкових процесів в рівномірній метриці.
3. G.S. Fishman (1999), Monte Carlo. Concepts, algorithms and applications, Springer-Verlag, New York-Berlin-Amsterdam.

ДИНАМІКА ЦИФРОВОЇ ТРАНСФОРМАЦІЇ В УКРАЇНІ

А. Квятківська

*здобувач освітнього ступеня «бакалавр»
спеціальності 051 Економіка ОП «Цифрова економіка»
факультету інформаційних технологій 3 курсу 1 групи
Державний торговельно-економічний університет
м. Київ, Україна*

В епоху четвертої промислової революції активно впроваджуються технології штучного інтелекту, цифровізації. Зокрема, діджиталізація впливає на всі сфери людини, допомагає оптимізувати всі процеси діяльності, ефективно використовувати ресурси. Досягнення четвертої промислової революції дозволяють повністю перейти на використання цифрових технологій, поєднавши їх із промисловими, що повністю змінює способи організації та ведення бізнесу. Багато економістів наголошують, що уряди країн, що розвиваються, мають активно цифровізувати всю державну систему.

Україна бере активну участь в цифровізації усіх систем. Україна має великий потенціал у сфері розвитку технологій та інновацій, проте на сьогодні ми маємо набагато нижчі показники, ніж передові країни. Це пов'язано з тим, що

в основному українське виробництво було зайнято у первинному та вторинному секторі економіки. Збільшення експорту ІТ-послуг почалося приблизно з 2019 року. Особливої уваги, варто виділити тим технологіям, які Україна виробляє самостійно, адже це важлива складова майбутньої відбудови та Євроінтеграції. Ці розробки дозволять країні створити високу концентрацію високотехнологічних компаній у регіонах України. Дані багатьох досліджень показують, що ІТ сфера від 24 лютого стала чи не є єдиною сферою, яка постраждала в меншій мірі. Частка послуг в експорті склала 48% (дані станом на серпень 2022 року). [1] Також великим здобутком у сфері цифровізації став застосунок Дія, що став предметом експорту. У Мінцифрі деталізували для DOU про зацікавленість в українських проектах, зокрема «Дії», на міжнародному ринку. Першим кроком до міжнародного розповсюдження продукту тут вважають те, що держави на кордоні з Україною почали приймати цифрові документи у Дії. Естонія запускає власний застосунок для державних послуг на базі Дії. Пілот застосунок хочуть розробити та запустити до кінця року.[2]

Ще однією перспективою є вихід України на цифровий ринок країн Європи. Європейський Союз планує запустити єдиний «гаманець» із цифровими документами, і Україна хоче взяти участь у цьому проєкті, адже це посилить нашу цифрову інтеграцію з ЄС. За словами представників Мінцифри, головне їх завдання в контексті зближення з ЄС – це отримання режиму внутрішнього ринку в секторі електронних комунікацій та поступова інтеграція до Єдиного цифрового європейського ринку.[2]

Для того, щоб детальніше проаналізувати перспективи та проблеми цифровізації України та світу, варто розглянути статистичні показники.

Одним з таких є індекс глобальної та цифрової конкурентоспроможності. Оскільки, надійність та безпеку даних в 2022 було складно отримати, варто проаналізувати дані 2021 року (табл. 1).

Країна	Рейтинг за GCI, 2020 р.	Рейтинг за GCI, 2021 р	Зміна рейтингу	Цифровий рейтинг за WDCI, 2020 р	Цифровий рейтинг за WDCI, 2021 р	Зміна рейтингу
Швейцарія	3	1	+2	6	6	0
Швеція	6	2	+4	4	3	+1
Данія	2	3	-1	3	4	-1
Нідерланди	4	4	0	7	7	0
Сінгапур	1	5	-4	2	5	-3
Норвегія	7	6	+1	9	9	0
Гонконг	5	7	-2	5	2	+3
Тайвань, Китай	11	8	+3	11	8	+3
ОАЕ	9	9	0	14	10	+4
США	10	20	0	1	1	0

Україна	55	54	+1	58	54	+4
---------	----	----	----	----	----	----

Табл. 1: Індекси глобальної та цифрової конкурентоспроможності за показниками 2020 та 2021 років. [3]

Як бачимо, Україна має позитивний приріст по двох показниках, враховуючи останні новини щодо цифровізації низки сфер, можна припустити, що темпи зростання будуть надалі підвищуватися.

Цифровізація є також важливим показником для вступу до ЄС. Зокрема, Європейська Комісія у щорічному звіті 2023 року щодо перспектив вступу України в союз, зазначає важливість цифровізації та зазначає, що Україна має значні успіхи в діджиталізації державної системи. Підтриманий Європейським Союзом проект «Цифрова трансформація для України» (DT4UA) продовжує покращувати ефективність і безпеку надання державних послуг та їх доступ громадянам і підприємствам в Україні, забезпечує швидке реагування на потреби, викликані війною, і розширює можливості щоденного управління. Естонська академія електронного урядування керує впровадженням із загальним бюджетом 17,4 мільйона євро. З 2016 року ЄС підтримує цифрову трансформацію України загальним бюджетом понад 51 мільйон євро. «Україна демонструє один із найдинамічніших процесів цифрової трансформації у світі – і це незважаючи на повномасштабну війну Росії. Наш обов'язок – допомогти Україні забезпечити постійний розвиток її цифрових послуг». — зазначив Посол Матті Маасікас, Голова Представництва Європейського Союзу в Україні. Загальний бюджет складає €17 400 000.[4]

Загальна тенденція розвитку технологій в Україні може бути позитивною, за підтримки продовження національних програм та підприємств, що активно цифровізують свою діяльність, мотивацією студентів інформаційних навчальних програм.

Список використаних джерел:

1. *Експорт ІТ-послуг [Електронний ресурс] – Режим доступу до ресурсу: <https://suspilne.media/289910-eksport-it-poslug-zris-na-16-za-8-misaciv-opendatbot/>*
2. *Які технології Україна експортуватиме після війни [Електронний ресурс] – Режим доступу до ресурсу: <https://dou.ua/lenta/news/fedorov-about-export-in-it/>*
3. *Раєвнева О.В., Аксьонова І.В., Бровко О.І., Порівняльний рейтинговий аналіз стану та тенденцій діджиталізації українського суспільства та економіки. (2021). [Електронний ресурс] –Режим доступу до ресурсу: https://www.problecon.com/export_pdf/problems-of-economy-2021-4_0-pages-56_66.pdf*
4. *Press and information team of the Delegation to UKRAINE. EU starts the largest support-project of Ukraine's digital transformation with a total budget of €17,4 million. [Електронний ресурс] – Режим доступу до ресурсу: https://www.eeas.europa.eu/delegations/ukraine/eu-starts-largest-support-project-ukraine%E2%80%99s-digital-transformation-total-budget_en?s=232*

ІСТОРІЯ РОЗВИТКУ МЕРЕЖІ ІНТЕРНЕТУ РЕЧЕЙ (ІОТ)

Л.І. Ковальов

магістрант

кафедри комп'ютерних наук та програмної інженерії

ПВНЗ "Європейський університет"

Г.Б. Данильчук

доцент кафедри економіки, фінансів, обліку, математичних та інформаційних дисциплін

Черкаської філії ПВНЗ "Європейський університет"

Концепція "інтернету речей" зародилася завдяки Кевіну Ештону, який у 1997 році впровадив технологію радіочастотної ідентифікації (RFID) для управління ланцюгами поставок. Ештонові інновації привели його до Массачусетського технологічного інституту, де він разом з колегами створив дослідницьку групу Auto-ID Center. З того часу, інтернет речей розвивався від базових радіо-міток до складної екосистеми.

Історія IoT починається з 1982 року, коли у Карнегі-Меллон університеті підключили до інтернету автомат з газованою водою. Згодом, у 1991 році HP представила перший мережевий принтер, а у 1993 році в Кембриджському університеті з'явилася перша інтернет-камера. Ключовим моментом для IoT став 1998 рік, коли було створено Bluetooth SIG, що знизило енергоспоживання та сприяло розвитку автономних пристроїв. У 2000 році HP запропонувала концепцію всепроникної комп'ютеризації "Cooltown", що поєднала обчислювальні та комунікаційні технології для створення інтернет-підключень. У 2005 році міжнародний союз електрозв'язку вперше оприлюднив прогнози щодо розвитку IoT. Після успішної розробки напівпровідникових світлодіодних ламп у 2008 році, почалося формування концепцій "розумного" освітлення та "розумного" дому.

Передбачається, що протягом наступних 5-7 років Інтернет речей проникне у всі сфери життя, включаючи промисловість, бізнес, охорону здоров'я та споживчий сектор. Сучасний світ цифрових технологій неможливо уявити без інтернету речей (IoT). З розвитком IoT з'являється потреба у вдосконаленні систем моніторингу та управління для забезпечення ефективної інтеграції та оптимізації роботи різних пристроїв.

Система моніторингу та управління може бути використана в "розумних" будинках для управління освітленням, температурою, та іншими побутовими функціями. В промисловості система може контролювати датчики та машини, забезпечуючи автоматизацію та підвищення ефективності виробничих процесів.

Список використаних джерел:

1. Building Real-time Mobile Solutions with MQTT and IBM MessageSight, IBM Redbooks 2014
2. IBM Podcast: Piper, Diaz, Nipper – MQTT.

МЕТОДИ АНАЛІЗУ ТА РОЗПІЗНАВАННЯ РУКОПИСНИХ ТЕКСТІВ

Я.П. Козак

магістрант,

М.Р. Костецький

к.е.н. доцент кафедри економіки

ПВНЗ «Європейський університет»

Тенденції в галузі технологій зростають в геометричній прогресії, і задачі розпізнавання текстів (як друкованих так і рукописних) стали актуальними, як тільки з'явилася можливість оцифровувати вміст як окремих документів так і цілих архівів та зберігати їх на невеликих носіях даних.

Сучасне суспільство дедалі більше схильне передавати інформацію в електронному вигляді. Згадайте: як давно ви ходили до бібліотеки, щоб знайти потрібні наукові матеріали? А коли останній раз використовували до цього ж Google? Отож бо. Звичайно, поціновувачі художньої літератури можуть годинами доводити, що в читанні «справжніх» книг є особливий шарм (і будуть абсолютно праві), та в зручності й компактності паперові книги очевидно програють своїм електронним версіям.

Та потреба в оцифруванні не обмежується лише науковою та історико-літературною сферою: загалом очікується, що до 2025 року розмір ринку оптичного розпізнавання символів становитиме 13,38 мільярдів доларів США, приріст на 13,7% у річному обчисленні. Це зростання зумовлене швидкою оцифровкою усіх можливих бізнес процесів у компаніях з використанням технологій розпізнавання, з метою зменшення витрат та збільшення ефективності та продуктивності роботи.

Задача розпізнавання тексту стала актуальною як тільки з'явилася потреба в диджиталізації паперових документів, книг, чеків, тощо. Припустимо, перед вами постала проблема оцифрувати статтю з якогось наукового журналу. Можна звичайно спробувати переписати її вручну та витратити на цю справу цілий день свого дорогоцінного життя. Та що робити, якщо стаття, яку необхідно перевести в текстовий формат, і не стаття зовсім, а товстений підручник? А що, якщо ви наприклад вчитель, і виникла потреба перевірити сотню-другу контрольних робіт, виконаних у тестовому форматі. Витрачати на подібні задачі час і зусилля не хочеться, та й насправді немає потреби, адже ці і ще тисячі і тисячі подібних задач можна виконати за лічені хвилини, перевіривши потрібні папери в цифровий формат за допомогою камери чи сканера і використавши програмне забезпечення для оптичного розпізнавання символів (Optical Character Recognition software).

Практично всі статистичні методи, що використовуються для етапу класифікації рукописних текстів, крім того, що мають сильний математичний фундамент, зазвичай потребують наявності таких припущень:

Кожен клас шаблонів має достатню кількість статистичних даних.

Набори ознак мають гаусівський або в крайньому випадку рівномірний розподіл.

Тестовий набір даних дозволяє виділити набір ознак, що однозначно представляють кожен клас шаблонів [1-2].

Розглянемо детальніше статистичні підходи, що використовуються у системах оптичного розпізнавання рукописних символів.

Байєсівський класифікатор. Байєсівська теорія (Bayesian Decision Theory) – це система, що призначена для мінімізації помилки при класифікації.

Ця класична методика ґрунтується на кількісному визначенні оптимальних компромісів між різними рішеннями, на основі ймовірностей, та втрат, що слідує за цими рішеннями.

Кластерний аналіз. Кластерний аналіз – це метод статистичної обробки даних, що базується на утворенні кластерів (груп) подібних даних. Метою кластерного аналізу можна вважати утворення таких груп подібних об'єктів, де «подібність» є глобальною мірою для усього вектора ознак [3].

Приховані марківські моделі. Приховане Марківське Моделювання (далі НММ) набуло популярності в розпізнаванні зашумлених, неточних сигналів, зокрема запису мовлення чи рукописних текстів, через його ймовірнісну природу та наявність ефективних методів для покращення параметрів моделей. В основу даного підходу покладено взаємодію двох механізмів: скінченних ланцюгів Маркова та випадкових функцій, що зв'язані з кожним станом [4].

Алгоритм Баума-Велша. Доволі добре на тренування НММ впливає метод Баума-Велша, який являє собою ітеративний процес, позволяючий оцінити її параметри. Так як цей алгоритм ітеративний, він починає роботу з початкової моделі, і оцінює переходи та викиди вираховуючи очікування за допомогою алгоритму прямого-зворотнього руху. Алгоритм підсумовує всі шляхи, що містять дану подію, поки не буде досягнуто збіжності[4]. Також з того, що цей метод ітеративний, впливає залежність кінцевої НММ та швидкості її отримання від початкового стану.

Список використаних джерел:

1. *Handwritten Character Recognition Using Bayesian Decision Theory* [Електронний ресурс] – Режим доступу до ресурсу: <http://www.ijcset.excelingtech.co.uk/Vol1Issue2/27-vol1-isse2.pdf>.
2. *An overview of character recognition focused on off-line handwriting* [Електронний ресурс] – Режим доступу до ресурсу: https://www.researchgate.net/publication/3421397_An_overview_of_character_recognition_focused_on_off-line_handwriting.
3. *Hierarchical clustering Agglomerative and Divisive clustering* [Електронний ресурс] – Режим доступу до ресурсу: <https://www.geeksforgeeks.org/ml-hierarchical-clustering-agglomerative-and-divisive-clustering/>.
4. *Fabian Alenius. Handwriting Recognition/Artificial Intelligence Using Statistical Methods / Fabian Alenius, Kjell Winblad and Chongyang Sun.*

ТРАНСФОРМАЦІЯ МЕТОДОЛОГІЙ ПРОГРАМУВАННЯ: РОЗВИТОК SOFT SKILLS

М.С. Копилов

*магістрант факультету
інформаційних систем і технологій,*

С.В. Левченко

*старший викладач кафедри комп'ютерних наук та програмної інженерії
ПВНЗ «Європейський університет»*

В умовах невідомо рухливого світу, ІТ-сфера зазнає принципових змін в своїй роботі та функціональності. Сучасний світ пропонує безліч викликів як до ІТ-компаній так і для працівників що в них працюють. Починаючи з пандемії Covid-19, методології сучасного програмування пережили великі зміни. Традиційні методи роботи відійшли на другий план, а дистанційна комунікація поставила принципові виклики перед усіма працівниками що залучені в менеджмент та роботу команд.

Для нас – українців ці зміни особливо відчутні в умовах повномасштабного вторгнення російських загарбників – працівники ІТ-сфери в Україні, показуючи неймовірні адаптаційні здібності та витривалість, повинні працювати над проектом в умовах що змінюються щогодини. Від блэкаутів в холодну пору року до вже звичайних повітряних тривог робота над проектом або частиною функціонального завдання не повинна зупинятись. Такі реалії спонукають CEO, product та project-менеджерів впроваджувати нові рішення. Саме в таких рішеннях стають на зараді сучасні методології програмування з урахуванням підвищення коефіцієнту гнучких навичок.

Методології Agile та Scrum стали невід'ємною частиною сучасного програмування та замінили в більшості випадків використання Waterfall в українському ІТ-ринку, забезпечуючи необхідний рівень гнучкості та адаптації. Короткі ітерації, які є стандартом у Scrum, дозволяють змінювати пріоритети та виправляти шлях проекту швидше та ефективніше. Agile, в свою чергу, стимулює постійну взаємодію з замовником та командною співпрацю, надаючи здатність пристосовуватися до нових вимог та обставин та часто – не залежати від всіх членів команди. Ці методології вимагають від всіх розробників та менеджменту більший рівень гнучкості та адаптації, тут кожному допоможуть прокачані Soft-skills.

В продовженні сфера DevOps виступає як ключовий компонент та новий вузол для розширення області відповідальності розробників, адміністраторів та тестувальників. Таке об'єднання дозволяє змінювати проект швидше та впроваджувати зміни безпечніше. За таким підходом, зміни в реальному часі стають меншим викликом. Спільна відповідальність, автоматизація багатьох процесів та інші компоненти принципово впливають на гнучкість команди та її реакцію на зміни середовища або умов проекту.

Також важливо зазначити імплементацію методологій дизайну мислення (Design Thinking) – зосередження на користувачеві стає елементом яким користуються розробники який підтягує за собою необхідність в емпатії зі

сторони розробника. Здатність до спільної роботи та виявлення інноваційних рішень допомагає швидше адаптуватися до змін в умовах повної нестабільності.

У висновку можна сказати що перед українськими розробниками, менеджерами та всіма працівниками ІТ-сфери стоїть нелегка задача – продовжувати свою роботу в постійно змінних умовах. Розвиток методологій потребує підвищення в першу чергу soft skills, котри в свою чергу допомагають таким елементам як Agile, Scrum, DevOps та Design Thinking переходити на глибші рівня розуміння проекту. Розвиток гнучких навичок виступає не лише як потреба, але і як стратегічний крок для подальшого успіху в умовах невизначеності та стрімких змін.

ДОСЛІДЖЕННЯ МЕТРОЛОГІЧНИХ ХАРАКТЕРИСТИК АНАЛОГО-ЦИФРОВОГО ПЕРЕТВОРЮВАЧА

О.І. Корельчук

*студент факультету інформаційних систем та технологій
ПВНЗ “Європейський університет”*

Аналого-цифровий перетворювач (АЦП) – периферійний пристрій мікроконтролера, що забезпечує перетворення величини вхідної напруги пропорційний їй код. Наприклад: у структурі мікроконтролера LPC2138 розміщено два 10-розрядні АЦП послідовного наближення з часом перетворення понад 2.44 мкс; частота квантування перетворювача налаштовується вбудованим подільником і не повинна перевищувати 4.5МГц; максимальна частота вибірок - 410 вибірок за секунду. Дуже цікаве може бути питання дослідити метрологічні характеристики цих пристроїв. Для цього використаємо опрацювання ряду вимірювань з багато разовими спостереженнями. Відповідно, невизначеність яку ми встановлюємо буде належати категорії А.

Методологія опрацювання дослідних даних використовує інформаційний підхід теорії вимірювань. Використаємо лабораторне джерело живлення для тестування АЦП. Інформація бази даних комп’ютерної системи являє собою ряд періодичних вимірів із багаторазовими спостереженнями значень напруги джерела живлення. Відповідно, невизначеність знаходить свій кількісний прояв у розсіюванні вимірів. Інформаційна технологія опрацювання дослідних даних з метою встановлення статистичних характеристик розподілу випадкового ряду вимірів із багаторазовими спостереженнями значень напруги та складає такі обчислювальні дії:

- вимірювальна інформація являє собою такий ряд $x_1, x_2, x_3, \dots, x_n$;
- встановлюємо математичне очікування $\underline{X} = \frac{1}{n} \sum_{i=1}^n x_i$;
- обчислюємо дисперсію ряду вимірювань $D = \frac{1}{n} \sum_{i=1}^n (\underline{X} - x_i)^2$;
- розраховуємо середнє квадратичне відхилення $\sigma = \sqrt{D}$;
- визначаємо третій момент розподілу $M_3 = \frac{1}{n} \sum_{i=1}^n (\underline{X} - x_i)^3$;
- обчислюємо асиметрію розподілу $A = \frac{M_3}{\sigma^3}$;

- розраховуємо четвертий момент розподілу $M_4 = \frac{1}{n} \sum_{i=1}^n (\underline{X} - x_i)^4$;
- за умови нормування відносно нормального розподілу дослідних даних встановлюємо ексцес ряду вимірів із багаторазовими спостереженнями напруги джерела живлення таким чином $\varepsilon = \frac{M_4}{\sigma^4} - 3$.

Математичне очікування, середнє квадратичне відхилення, асиметрія та ексцес утворюють статистичні характеристики розподілу випадкової величини напруги джерела живлення. Використано метод Монте-Карло для побудови гістограми розсіювання дослідних даних вимірювань напруги лабораторного джерела живлення:

- знаходимо максимальне та мінімальне значення ряду вимірювань напруги x_{max}, x_{min} ;
- встановлюємо інтервал зміни випадкових величин вимірювальної напруги $\Delta = x_{max} - x_{min}$;
- відрізок $[x_{max} - x_{min}]$ накриває усі вибірккові значення випадкової функції. Розбиваємо його на декілька рівних інтервалів $r = 6, 8, 10, \dots$ та при обиранні величини Δ_1 округлення виконуємо до найближчого більшого рівня;
- встановлюємо кількість вибірккових значень вимірів періодів проходження сигналу генератора, які попали у кожний інтервал $\pm \Delta_1, \pm \Delta_2, \dots, \pm \Delta_{0.5r}$;
- будуємо гістограму розсіювання дослідних даних.

Гістограма розсіювання дослідних даних напруги являє собою ступінчасту лінію. На основі гістограми підбираємо закон розподілу випадкової функції $F(x)$ дослідних даних за наступної умови

$$\int_{x_{min}}^{x_{max}} F(x) dx = \frac{1}{N} \sum_{i=1}^N p(x_i) \Delta_i.$$

Інформаційна технологія опрацювання ряду вимірів із багаторазовими спостереженнями складає наступні дії:

- рівняння згладженої кривої розсіювання вихідного коду має вигляд

$$f(x) = \frac{1}{2\sigma} e^{-\frac{|x|}{\sigma}} \text{ при } X \in (x_{max}, x_{min}).$$

- звідси ентропія невизначеності набуває такого вигляду

$$H\left(\frac{x}{x_n}\right) = \ln(2\sigma e^{\mu_1 \sigma^{-1}}).$$

- ентропійний інтервал невизначеності вихідного коду має вигляд

$$\Delta = \sigma e^{\mu_1 \sigma^{-1}}.$$

При застосуванні інформаційного підходу до опрацювання невизначеності результатів вимірювань з багаторазовими спостереженнями напруги джерела живлення оперують із половиною ентропійного інтервалу. Отже, ентропійний інтервал невизначеності напруги джерела живлення становив $\Delta=0.016$. Така невизначеність вимірювань свідчить про доцільність використання пристрою.

ВИКОРИСТАННЯ КРИПТОГРАФІЇ В КРИПТОВАЛЮТАХ

А.Б. Костецький,

магістрант,

В.І. Паширін

к.т.н. професор

ПВНЗ «Європейський університет»

У сучасному світі криптовалюти здобувають все більшу популярність як альтернативна форма електронних платежів та зберігання активів. Криптовалюта є цифровим активом, що використовує криптографічні методи для забезпечення безпеки та контролю над транзакціями. Одним з ключових елементів криптовалют є цифровий підпис, який використовується для підтвердження автентичності та цілісності транзакцій. Цифрові підписи відіграють важливу роль у забезпеченні автентичності, цілісності та конфіденційності транзакцій, що робить їх дослідження та вдосконалення важливим завданням для розвитку безпечного та інструменту.

Криптовалюта – це форма цифрових або віртуальних валют, що використовує методи криптографії для забезпечення безпеки та контролю над створенням нових одиниць, а також для підтвердження та регулювання транзакцій. Вона базується на принципах криптографії, де математичні алгоритми забезпечують захист фінансових операцій та переведення власності[1].

Криптовалюти використовують децентралізовані системи, такі як блокчейн, для збереження інформації про власників та транзакції.

Блокчейн – це публічний розподілений реєстр, який містить всю історію транзакцій у мережі. Він дозволяє учасникам мережі перевіряти та підтверджувати транзакції без необхідності довіряти централізованому органу. Це робить криптовалюти більш прозорими, незалежними від урядових органів та банків, і дає можливість користувачам здійснювати безпечні та анонімні транзакції.

У світі криптовалют існує безліч різних валют, таких як Bitcoin, Ethereum, Ripple та багато інших. Кожна з цих валют має свої особливості, протоколи та функціональні можливості. Принципи криптовалют можуть варіюватися в залежності від конкретної валюти, але загальні принципи безпеки, децентралізації та анонімності залишаються основними складовими будь-якої криптовалюти.

Криптографія є невід'ємною складовою криптовалют і блокчейн технології. Вона використовується для забезпечення безпеки та

конфіденційності транзакцій, аутентифікації користувачів і захисту від несанкціонованого доступу. Криптографічні алгоритми, такі як еліптична крива криптографія та хеш-функції, дозволяють генерувати приватні та публічні ключі, підписувати та перевіряти транзакції, а також забезпечувати безпечне зберігання активів.

Bitcoin використовує еліптичну криптографію (ECC) та алгоритм безпечного хешування SHA-256 для генерації публічних ключів з відповідних приватних ключів.

Публічний ключ використовується для створення адреси криптогаманця для отримання вхідних транзакцій, тоді як приватний ключ необхідний для підпису транзакцій та підтвердження власності коштів.

Приватний ключ – це важлива частина ключової пари та зберігається в криптогаманці. Технічно, криптогаманець зберігає доступ особи до їх криптовалюти, а не саму криптовалюту. Самі кошти є лише записами даних, збереженими в блокчейні, і можуть бути ідентифіковані та розблоковані за допомогою ключів, збережених у вашому гаманці.

Еліптична криптографія – це використання особливої математичної кривої, яка має горизонтальну симетрію. Якщо провести будь-яку лінію через цю криву, вона перетне криву максимум тричі. Еліптичні криві є важливою частиною криптовалюти і дозволяє користувачам генерувати публічний ключ.

Для генерації ключової пари Bitcoin спочатку потрібно створити приватний ключ.

Приватний ключ Bitcoin – це випадково згенероване 256-бітне число. Це число зазвичай генерується в момент створення криптогаманця.[4]

Публічний ключ потім генерується з цього числа за допомогою множення на еліптичну криву. Це включає в себе вибір початкової точки на еліптичній кривій (відомої як точка генератора) та множення її на випадкове число приватного ключа для отримання нової точки на кривій.

Ця нова точка стає публічним ключем зі специфічними координатами x та y . Знаходження приватного ключа за відомим публічним ключем майже неможливе через складність задачі дискретного логарифмування.

Теоретично, для знаходження цього числа протягом одного дня потрібен квантовий комп'ютер з більш ніж 13,000,000 фізичних кубітів. На сьогоднішній день один з найбільш сучасних квантових комп'ютерів у світі, процесор IBM Osprey, має лише 433 кубітів.

Криптографічна хеш-функція ("cryptographic hash function") – це алгоритм хешування (відображення довільного двійкового рядка в бінарний рядок фіксованого розміру n -бітів).[5]

У підсумку можна зазначити, що аналіз архітектури криптовалют та особливостей використання цифрового підпису в криптовалютах дозволяє глибше зрозуміти принципи функціонування таких систем та оптимізувати їх захист.

Список використаних джерел:

1. Кравченко П. Блокчейн і децентралізовані системи / П. Кравченко, Б. Скрябін, О. Дубініна. – Харків, 2019. – 474 с.

2. Bitcoin and cryptocurrency technologies: a comprehensive introduction. / [A. Narayanan, J. Bonneau, E. Felten та ін.]. – Princeton, New Jersey: Princeton University Press., 2016. – 336 с. – (Princeton University Press).
3. SETH S. What Is a Cryptocurrency Public Ledger, How It Works, Risks [Електронний ресурс] / SHOBHIT SETH. – 2021. – Режим доступу до ресурсу: <https://www.investopedia.com/tech/what-cryptocurrency-public-ledger/>.
4. Private key [Електронний ресурс] – Режим доступу до ресурсу: https://en.bitcoin.it/wiki/Private_key.
5. Menezes A. Handbook of Applied Cryptography / A. Menezes, P. van Oorschot, S. Vanstone., 1996.

МОБІЛЬНИЙ ДОДАТОК ДЛЯ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧА НА ОСНОВІ ДАНИХ АКСЕЛЕРОМЕТРА ТА ГІРОСКОПА

В.І. Коцун¹
А.А. Веремій²

¹к. т. н., доц., завідувач кафедри математики та комп'ютерних дисциплін

²магістрант,

Львівська філія ПВНЗ «Європейський університет»

За даними за 2021 рік близько 5 мільярдів людей у світі володіють смартфонами. Кількість продажів смартфонів наразі перевищує кількість продажів як ноутбуків, так і персональних комп'ютерів. Це свідчить не тільки про хороші рекламні кампанії, організовані виробниками смартфонів, але і про те, що люди сьогодні довіряють все більше і більше обов'язків своєму смартфону. Смартфон застосовують для бізнес комунікацій, збереження персональної інформації, інтернет банкінгу та організації власного часу.

Разом з тим, багато користувачів висловлюють занепокоєння безпекою їхніх даних. Серед найпоширеніших механізмів засобів, впроваджених у більшості сучасних пристроїв, є паролі, пін-коди та графічні паролі. Хоча ці методи і є точними та надійними, безпека при їх використанні залежить від запам'ятовування користувачем ключової фрази чи патерну. Сучасні методи ідентифікації користувача, такі як сканери відбитків пальців та розпізнавання обличчя, хоч і вирішують цю проблему, та все ж потребують безпосередньої участі користувача у процесі ідентифікації, що може викликати фрустрацію, особливо у ситуаціях, коли користувач кудись поспішає чи використовує смартфон «на ходу».

Одним із запропонованих методів вирішення цих проблем є «постійна ідентифікація». Сучасні смартфони обладнані сенсорами, що постійно збирають інформацію про навколишнє середовище та поведінку користувача. Серед такої інформації можна назвати голос, пульс користувача, форму його вуха, жести, патерни дотиків до екрану при виконанні базових операцій.

Одним із методів постійної ідентифікації є розпізнавання рухових активностей людини. Мобільність смартфонів призводить до того, що часто вони використовуються під час руху. Час, коли смартфон лежить у кишені, у сумці чи на поясі користувача, можна використати для ідентифікації користувача. У такому випадку немає затримки коли користувач бере смартфон у руки, адже він

уже ідентифікований, а отже уже немає потреби запитувати у користувача пароль чи пін-код. При достатній деталізації вхідних даних таку ідентифікацію важко обманути, оскільки характеристики ходьби кожної людини є унікальними. Впровадження такого методу ідентифікації користувача не потребує додаткових апаратних засобів. Для виконання цього завдання достатньо даних, отриманих із вбудованих сенсорів смартфона – акселерометра та гіроскопа.

З іншого боку, при такій ідентифікації виникатимуть певні труднощі і проблеми, які треба вирішити. На ходьбу людини може вплинути одяг, взуття, людина може бути втомленою чи нести важкі об'єкти. Не всі люди тримають смартфони у одній позиції, різні виробники смартфонів встановлюють на свої пристрої різні сенсори і т. д.

Враховуючи зазначені вище проблеми, рекомендується застосовувати ідентифікацію на основі розпізнавання активностей людини як частину багатосарової системи захисту, що включає в себе більш традиційні методи ідентифікації, такі як пароль, розпізнавання обличчя чи сканер відбитків пальців.

Метою роботи є розроблення мобільного додатку для ідентифікації користувача смартфону за даними акселерометра і гіроскопа.

У результаті виконання роботи буде здійснено порівняння алгоритмів класифікації в умовах розпізнавання активностей людини, при потребі розроблено модифікований алгоритм, який підвищить ефективність розрізнення активностей окремих людей та розроблено мобільний додаток для розпізнавання активностей людини у фоновому режимі з метою ідентифікації.

Теоретичною основою виконання роботи є теорія розпізнавання образів (pattern recognition), а саме один з її підрозділів – класифікація. Основна ідея класифікації – поділити всі вхідні дані на множину «підписаних» груп, використовуючи навчальні набори даних для тренування системи. Проаналізувавши існуючі наукові статті та вивчивши стан ринку програмного забезпечення зроблено висновок, що додаток для розпізнавання активностей людини може стати актуальним та конкурентноспроможним, а результати наукових досліджень корисними для подальших робіт у цій області.

Список використаних джерел

1. Siirtola, Pekka, 2015. "Recognizing human activities based on wearable inertial measurements. Methods and applications", University of Oulu, Finland.
2. AppLock Face/Voice Recognition [Електронний ресурс] // Sensory Inc – 2019 – Режим доступу до ресурсу: <https://www.sensory.com/products/applications/applock/>
3. Фітнес: відстеження стану здоров'я й активності [Електронний ресурс] // Google – 2019 – Режим доступу до ресурсу: <https://www.google.com/fit/>
4. Tundo, M.D., Lemaire, E.D., & Baddour, N., 2013. "Correcting Smartphone orientation for accelerometer-based analysis". 2013 IEEE International Symposium on Medical Measurements and Applications (MeMeA).
5. Ortiz Laguna J., Olaya A.G., Borrajo D., 2011. "A Dynamic Sliding Window Approach for Activity Recognition". In: Konstan J.A., Conejo R., Marzo J.L., Oliver N. (eds) User Modeling, Adaption and Personalization. UMAP 2011. Lecture Notes in Computer Science, vol 6787. Springer, Berlin, Heidelberg.
6. T. Huynh and B. Schiele, 2005. "Analyzing features for activity recognition. In Proceedings of the 2005 joint conference on Smart objects and ambient intelligence: innovative context-aware services: usages and technologies", ACM, 2005

7. Cemil Altın & Orhan Er, 2016. "Comparison of Different Time and Frequency Domain Feature Extraction Methods on Elbow Gesture's EMG," European Journal of Interdisciplinary Studies Articles, European Center for Science Education and Research, vol. 5, May-August.

АНАЛІЗ СУЧАСНИХ МЕТОДІВ ПЕРЕДАЧІ ГОЛОСОВОЇ ІНФОРМАЦІЇ

М.О. Кравченко

магістрант

кафедри комп'ютерних наук та програмної інженерії

ПВНЗ "Європейський університет"

В.В. Хайдуров

доцент кафедри економіки, фінансів, обліку, математичних та

інформаційних дисциплін

Черкаської філії ПВНЗ "Європейський університет"

Сучасні системи передачі залишаються вкрай актуальними і відіграють ключову роль сучасному суспільстві [1–3]. Системи передачі інформації забезпечують глобальний зв'язок, дозволяючи людям та компаніям обмінюватись даними та комунікувати в режимі реального часу незалежно від фізичної відстані [3–5]. Інтернет та мобільні мережі стали невід'ємною частиною повсякденного життя, забезпечуючи доступ до інформації, комунікації та розваги у будь-якій точці світу.

Нині існують кілька сучасних методів передачі голосової інформації, включаючи традиційні та мережеві технології. Деякі з них описані нижче.

Ø Традиційні телефонні мережі – це класичний спосіб передачі голосу, який використовує дротові мережі. Традиційні телефонні мережі, також відомі як громадські телефонні мережі, що комутуються, являють собою структуру, засновану на фіксованих лініях передачі і комутації сигналів. Ось деякі з переваг традиційних телефонних мереж: Такі мережі часто вважаються надійнішими порівняно з деякими мережевими технологіями, такими як VoIP. Оскільки вони працюють на фізичних лініях, вони менш схильні до збоїв, викликаних інтернет-проблемами або електроживленням. Ці мережі забезпечують стабільну та високоякісну аналогову якість звуку. Це особливо важливо у випадках, коли якість зв'язку має вирішальне значення, наприклад, у бізнес-комунікаціях або за термінових ситуацій. Телефони традиційних мереж зазвичай простіші у використанні для кінцевих користувачів. Вони не вимагають складного налаштування і часто можуть бути використані "з коробки". Мережі такого типу широко поширені та доступні у більшості областей навіть у віддалених районах, де може бути недоступний широкопasmовий інтернет. Традиційні телефонні мережі надають інформацію про місцезнаходження викликаного при дзвінку до служби екстреної допомоги (наприклад, 911 у США), що важливо для оперативного реагування у разі нещасних випадків. Тим не менш, слід зазначити, що традиційні телефонні мережі також мають недоліки, такі як більш високі операційні витрати, обмежені можливості передачі даних, і їх адаптація до нових технологій може бути більш складною. З розвитком технологій та поширенням

більш сучасних методів зв'язку, переваги можуть зрушуватися у бік мережевих та цифрових рішень.

Ø Мобільний зв'язок – стільникові мережі забезпечують передачу голосу бездротовими каналами. Стандарти, такі як GSM, CDMA, 3G, 4G LTE та 5G, забезпечують мобільний голосовий зв'язок. Користувачі можуть спілкуватись у будь-якому місці, вкритому мережею, забезпечуючи високий рівень мобільності. Стільникові мережі надають широке географічне покриття, що робить мобільний зв'язок доступним у більшості областей. Будівництво стільникових мереж відбувається швидше, ніж проведення традиційних провідних інфраструктур, що полегшує доступ до зв'язку. Крім голосового зв'язку, мобільні пристрої підтримують передачу даних, доступ до Інтернету, текстові повідомлення, мультимедійні повідомлення та програми. Стільникові оператори швидко впроваджують нові технології, такі як 4G та 5G, забезпечуючи вищі швидкості передачі даних. Стільникові мережі мають обмежену пропускну спроможність, і в періоди високої завантаженості можуть виникнути проблеми з якістю обслуговування. Мобільні мережі можуть бути вразливими для кібератак та перехоплення даних, хоча сучасні технології намагаються забезпечити високий рівень безпеки. Використання мобільних пристроїв та зв'язку може надати користувачам ризик щодо порушення приватності, особливо в разі стеження за місцем розташування. Постійне використання мобільних пристроїв вимагає підзарядки акумуляторів, що може бути незручним без доступу до джерела живлення. Загалом, мобільний зв'язок надає значні переваги в галузі мобільності та доступності, але також пов'язаний з деякими обмеженнями та ризиками.

Ø VoIP (Voice over Internet Protocol): Це технологія, яка дозволяє передавати голосову інформацію за допомогою Інтернет-підключення. Популярні програми, такі як Skype, WhatsApp і Zoom, використовують технологію VoIP. VoIP-дзвінки зазвичай коштують дешевше, ніж традиційні телефонні дзвінки, особливо в міжнародному та довгостроковому плані, оскільки дані передаються через інтернет. VoIP забезпечує можливість передачі голосу, відео та даних у межах однієї мережі, що покращує інтеграцію з іншими програмами та сервісами. VoIP-системи можуть бути використані з будь-якого місця, де є доступ до інтернету, що забезпечує гнучкість та мобільність. VoIP-системи часто надають широкий спектр додаткових функцій, таких як переадресація дзвінків, голосова пошта, конференц-дзвінки та інші. Якість VoIP-дзвінків може залежати від якості інтернет-підключення. Недостатня пропускну здатність або нестабільне з'єднання можуть спричинити проблеми з якістю звуку. У разі відсутності електроживлення або збою інтернет-з'єднання VoIP-пристрою можуть бути тимчасово недоступні.

Ø WebRTC (Web Real-Time Communication) – це технологія, яка призначена для забезпечення голосового зв'язку та відеозв'язку у веб-браузерах без необхідності додаткових плагінів. WebRTC забезпечує простоту впровадження і його використання не потребує встановлення додаткового програмного забезпечення або плагінів. Оскільки WebRTC інтегрована в багато сучасних веб-браузерів, користувачі можуть використовувати голосовий та відеозв'язок прямо у веб-додатках, міняючи необхідність встановлювати

сторонні програми. WebRTC є відкритим стандартом, що означає, що він доступний для розробників без ліцензійних обмежень, що сприяє його поширенню та покращенню. WebRTC забезпечує високу якість передачі звуку та відео, особливо при стабільному інтернет-з'єднанні. Технологія підтримує взаємодію між різними пристроями, такими як комп'ютери, смартфони та планшети. WebRTC включає вбудоване шифрування, забезпечуючи безпеку передачі даних. У хоча більшість сучасних браузерів підтримують WebRTC, деякі старі версії або браузери можуть не забезпечувати повну сумісність. Як і у випадку з іншими технологіями передачі даних у реальному часі, якість зв'язку в WebRTC залежить від стабільності інтернет-з'єднання. У ряді випадків WebRTC може споживати значні ресурси, особливо під час роботи з великим обсягом даних. Загалом WebRTC надає потужний інструмент для веб-комунікацій, але розробники та користувачі повинні враховувати як його переваги, так і недоліки при виборі та використанні цієї технології.

Ø Багато месенджерів, таких як Telegram, WhatsApp і Viber, надають можливість надсилання голосових повідомлень. Голосові повідомлення можуть передавати емоції та інтонації природніше, ніж текстові повідомлення, що особливо важливо у спілкуванні. Голосові повідомлення можуть бути ефективнішими, ніж набір тексту, особливо коли потрібно передати великий обсяг інформації. Надсилання голосових повідомлень може бути зручним під час руху або в ситуаціях, коли складно використовувати клавіатуру. Голосові повідомлення можуть прискорити процес спілкування, оскільки вимагають часу на набір тексту. Завдяки інтонаціям та емоціям, голосові повідомлення можуть допомогти уникнути непорозуміння, які іноді виникають у текстовому листуванні. Вибір між голосовими та текстовими повідомленнями в месенджерах залежить від ситуації, особистих уподобань та цілей комунікації. Зазвичай використання обох форматів в залежності від контексту може бути найкращим підходом.

Системи передачі інформації, такі як електронна пошта та месенджери, дозволяють людям спілкуватися та передавати інформацію миттєво, покращуючи ефективність комунікацій. Сучасні системи забезпечують можливість онлайн-колаборації та віддаленої роботи, що стає все більш важливим в умовах зміни робочих практик та тенденції до глобалізації ринку праці. Хмарні технології дозволяють зберігати, обробляти та передавати дані на віддалених серверах, забезпечуючи гнучкість та доступність у галузі зберігання та обробки інформації. Розвиток систем передачі інформації підтримує зростання Інтернету речей, дозволяючи пристроям обмінюватися даними та робити наше повсякденне життя більш "розумним" та пов'язаним. Системи передачі інформації є ключовим елементом цифрової трансформації бізнесу, забезпечуючи швидку та ефективну передачу даних для ухвалення бізнес-рішень. Розвиток бездротових технологій, таких як 5G, забезпечує вищу швидкість передачі даних, що підтримує нові можливості та програми, такі як розширена реальність (AR) та віртуальна реальність (VR). Сучасні системи передачі інформації продовжують відігравати ключову роль у нашому житті, забезпечуючи зв'язність та можливості в різних галузях, від бізнесу до освіти та повсякденного спілкування.

Список використаних джерел

1. Junyi Gong, Yunpu Zhu, Chengqiao Song. (2019) Design of embedded wireless audio acquisition system. J. Foreign Electronic Measurement Technology., 38: 74-78.
2. Hui Tang, Feiyang Chen, Lingyun Zheng, Hu Huang. (2016) Design of a wireless voice transmission system. J. Audio Engineering., 40: 53-57.
3. Feng Wang. (2019) Analysis of speech codec algorithm based on ARM platform and its design and implementation in the wireless transmission system. D. Xidian University.
4. Deshui Yu. (2021) Simulation and analysis of the multipath effect on wireless signal transmission .J. Information Recording Materials., 22: 241-243.
5. Yuan Wang, Kaikai Wang, Yuhan Shang, Hongyan Zhan. (2019) Audio Sampling and Wireless Transmission System Based on Compressed Sensing Theory.J. Microcontrollers & Embedded Systems., 19: 18-21.

РЕАЛІЗАЦІЯ ПРОЕКТУ “DEPENDENCY INJECTION” ЗА ДОПОМОГОЮ ПРОГРАМНОГО СЕРЕДОВИЩА JAVA

А.В. Ляшенко

*студент факультету інформаційних систем та технологій
ПВНЗ “Європейський університет”*

Dependency Injection це техніка розроблення програмного забезпечення, яка спрощує керування залежностями компонента^[1]. Dependency Injection вирішує наступні проблеми:

- бере на себе відповідальність за доставку залежності (типу dependency) до компоненту;
- спрощує написання коду;
- спрощує керуванням залежностями компонентів.

Програмне забезпечення Dependency Injection є окремою формою [Inversion of control](#). Розглянемо деякі приклади застосування даної техніки. Приклад №1. Припустимо, ми маємо клас сервісів типу ServiceImpl (рис. 1), який виконує бізнес логіку, та клас Controller (рис. 2). Сервіс типу ServiceImpl використовує клас Controller. Відповідно він є клієнтом тому *залежним* компонентом.

```
public class ServiceImpl {  
    1 usage  
    public void processData(String data) {  
        System.out.println("processing data ...");  
    }  
}
```

Рисунок 1 – сервіс типу ServiceImpl

```

public class Controller {

    1 usage
    private final ServiceImpl service = new ServiceImpl();

    public void doSomething() {
        String data = "data";
        service.processData(data);
    }
}

```

Рисунок 2 - клас Controller

В загальному випадку, щоб використати залежність типу ServiceImpl в класі Controller, треба зробити його ініціалізацію наступним чином (рис. 3).

```

private final ServiceImpl service = new ServiceImpl();

```

Рисунок 3 – Ініціалізація сервісу ServiceImpl

Без використання програми Dependency Injection доведеться ініціалізовувати всі залежності явно через оператор **new**, що не є гарною практикою для випадку коли проект достатньо великий та складний. Яким чином це можливо зробити розглянемо на прикладі 2. Тепер переробимо попередній приклад з використанням Dependency Injection^[2]:

```

@Component
public class ServiceImpl {

    1 usage  👤 Andrii Liashenko
    public void processData(String data) {
        System.out.println("processing data ...");
    }
}

```

Рисунок 4 – Використання Dependency Injection

Як бачимо на рис. 4 клас **ServiceImpl** має анотацію **@Component** що сигналізує DI контейнеру що він є компонентом контексту. Тобто він може бути як залежністю будь-якого іншого компонента так і мати свою залежність яку DI контейнер сам буде шукати у контексті і сам впровадить у компонент.

На рис. 5 ми бачимо що в компоненті **Controller** залежність має анотацію **@Inject**, котра вказує DI контейнеру, що він має впровадити сюди компонент з контексту, тобто об'єкт типу **ServiceImpl**. Принцип роботи такий:

- DI контейнер (як зрозуміло з назви) є контейнером компонентів;
- він використовує рефлексію (Reflection API) щоб рекурсивно шукати компоненти у вказаному пакеті та додати їх у контекст^[3] тобто у DI контейнері.

Коли всі компоненти було додано, відповідно DI контейнер проходить по всім компонентам шукаючи поля, які анотовано **@Inject**, після того як він знайде таке поле, він буде шукати компонент з таким типом даних який вказаний у даному полі. Якщо такий компонент не знайдено то буде кинуте виключення типу **org.openCDI.exceptions.ComponentNotFoundException**.

Якщо у контексті будуть декілька компонентів з одним типом то можна вказати кожному ім'я **@Inject(«ім'я компоненту»)** для того щоб їх розрізнити. В такому випадку DI контейнер буде шукати не по типу даних а по імені компоненту.

```
@Component
public class Controller {

    1 usage
    @Inject
    public ServiceImpl service;

    1 usage  👤 Andrii Liashenko
    public void goSomething() {
        String data = "data";
        service.processData(data);
    }
}
```

Рисунок 5 – Компонент Controller

Висновок:

- використовуючи техніку Dependency Injection спрощуємо написання програми, її масштабування;
- замість того щоб явно ініціалізовувати залежності в сервісах ми віддаємо цю задачу DI контейнеру. Цим ми добиваємось такого функціоналу для якого провівши ініціалізацію об'єкту даного класу ми маємо доступ по ньому з будь якої частини нашої програми;
- розглянуто малу частку того що може дати дана техніка, для більш детального огляду рекомендую перейти на такі сторінки https://en.wikipedia.org/wiki/Dependency_injection, <https://docs.spring.io/spring-framework/reference/core/beans/dependencies/factory-collaborators.html>;
- дана техніка використовується всюди, де проект вийшов за межі всім відомого HelloWorld. Якщо на проекті використовується Spring Framework то з вірогідністю в 100% там використовується DI контейнер (від самого Spring).

Список використаних джерел

1. В контексті java часто вживається як **bean** (компонент) через вплив технології [Enterprise JavaBeans](https://en.wikipedia.org/wiki/Enterprise_JavaBeans)
2. Для цього прикладу буде використовуватись своя базова реалізація Dependency Injection контейнера код дивіться на GitHub <https://github.com/LiashenkoAndrey/OpenCDI>
3. У англомовних ресурсах часто можна зустріти як Application Context

ДОСЛІДЖЕННЯ ПРОЦЕСІВ ОЦИФРУВАННЯ ШАХОВИХ ДРУКОВАНИХ ВИДАНЬ ТА РОЗПІЗНАВАННЯ ШАХОВИХ ДІАГРАМ

Д.О. Маркін
магістрант,

спеціальність «Комп'ютерні науки»

К.Ю. Островська

к.т.н. доцент

Український державний університет
науки і технологій (м. Дніпро, Україна),

Постановка проблеми. Тема «Шахи» є однією з найпоширеніших тем у світовій спортивній літературі та періодиці. Багата історична, теоретична та культурна спадщина по цій тематиці накопичувалась з часів середніх віків і до сьогодення, особливо численними були друковані видання за попередні 100 років. Завдяки постійному інтересу до шахів попит на шахову літературу знаходиться на дуже високому рівні, а можливість ознайомлення як зі старими, та і з новими виданнями завдяки розвитку технологій та поширенню електронних форматів видань робить шахову тематику ще більш актуальною.

За підрахунками Української спілки любителів шахової літератури, тільки за роки незалежності в нашій державі та за її межами вийшло приблизно 700-800 брошур та книжок авторства українських шахістів та перекладних видань, не враховуючи періодичні та спеціалізовані разові видання, присвячені окремим

шаховим подіям. Тому важливим є питання оцифрування старих видань, термін дії авторських прав на які вже припинився, або тих, на оцифрування яких отримано належний дозвіл. Особливою метою оцифрування також є збереження та відокремлення української шахової спадщини ХХ сторіччя від загальнорадянської та необхідність та зацікавленість українських та європейських любителів шахів у вивченні теоретично та історично значущих робіт українських провідних шахістів. При цьому досвід з оцифрування може бути розповсюджений на оцифрування та виготовлення якісних цифрових копій видань будь-яких авторів, написаних на будь-якій мові. [1]

Мета та виконання дослідження. В роботі досліджено та систематизовано особливості обробки сканів видань (книжки, спеціалізовані та загальні періодичні видання) за темою «Шахи». Запропоновано чітку та оптимальну, з точки зору витрат часу та отримання високої якості, методику обробки та оцифрування шахових діаграм в процесі обробки сканів видань за темою «Шахи». Методику складено з урахуванням сучасного стану відповідного програмного забезпечення та поставленого автором обмеження – відмови від використання програмних продуктів російського походження. Це має дозволити знизити економічні та соціальні зв'язки та ризики кібератак зі сторони представників країни-агресора. Розглянуто основні формати та вимоги до оцінки якості отримуваних цифрових версій друкованих видань, актуальні проблемні питання виготовлення цифрових видань. [2, 3] Досліджено сучасні програмні засоби для застосування їх в процесі обробки сканів за темою «Шахи» та відзначено особливості роботи з ними, окремо відзначено рекомендовані та nereкомендовані (в т.ч. російського походження) до застосування програмні засоби; серед останніх особливо виділяється програмне забезпечення компаній АBBYY та Yandex, а також багато різноманітних мережевих сервісів та вільно розповсюдженого програмного забезпечення (ScanKromsator, WinDjVu та ін.). Розглянуто альтернативне програмне забезпечення, яке пропонується використовувати в процесі обробки сканів друкованих видань. [3, 4]

Дослідження засобів розпізнавання шахових діаграм. За допомогою емпіричних методів виконано оцінку складності та доцільності розробки інтегрованого програмного рішення для автоматичної обробки сканів від етапу отримання початкових сканів до етапу оформлення електронного видання, розглянуто методи та програмні засоби для генерації шахових діаграм для заміни діаграм в наявних сканах в процесі обробки або використанні їх в репринтних виданнях. Розробка подібного програмного рішення визнана економічно не доцільною, але при цьому визначено способи оптимізації процесів обробки.

При проведенні дослідження виявлено кращі програмні засоби для розпізнавання та генерації зображень шахових діаграм. Для інтеграції в загальний процес виготовлення електронної версії видань найзручнішим визнано сервіс Chess OCR, але за якістю розпізнавання зображень з тестової вибірки складних зображень він поступився мобільному застосунку Chessify. Обидві програми виявили особливості використання при розпізнаванні конкретних проблемних позицій. Програмний комплекс ChessVisionAI, який має в своєму складі мобільний застосунок для розпізнавання шахових діаграм, наразі не продемонстрував конкурентоспроможні результати.

Виявлено основні помилки, які зустрічаються при розпізнаванні зображень шахових діаграм, а саме: невірна ідентифікація типу фігури; невірна ідентифікація кольору фігури; хибне виявлення фігури на клітинці; хибне виявлення фігури на клітинці; похибка, пов'язана зі злиттям фону темних клітинок та зображення фігур (здебільшого чорних). [5, 6, 7]

Запропонований алгоритм розпізнавання. На основі аналізу отриманих результатів сформульовано алгоритм розпізнавання шахових діаграм в загальному вигляді з урахуванням виявлених особливостей та найчастіших помилок розпізнавання зображень шахових діаграм сучасними програмними засобами.

В роботі відзначено, що розпізнавання шахових діаграм є завданням, яке потребує високої точності та є гарною задачею для розв'язання за допомогою штучного інтелекту, нейронних мереж, а також регулярного навчання на великому обсязі даних.

Додатково розглянуто актуальні програмні засоби для генерації діаграм на основі розпізнаних раніше зображень з використанням різних типів шахових шрифтів, детально проаналізовано приклад обробки шахового видання за допомогою розглянутих програмних засобів.

Висновки. Наявна робота є систематизацією багаторічного досвіду та рекомендацій колективу українських фахівців з обробки шахових видань, в ній детально розглянуто специфіку процесу обробки сканів і отримання електронних копій шахових видань за допомогою сучасного програмного забезпечення.

Результати роботи та висновки з неї можуть бути поширені на процеси оцифрування видань, присвячених будь-яким іншим інтелектуальним іграм, які проводяться на графічному полі (шашки, го, рендзю та ін.), та можуть стати базою для досліджень в цих напрямках.

Список використаних джерел

1. Майстренко А. А. Оцифровування архівних документів у зарубіжних країнах: інформаційно-аналітичний огляд / А. А. Майстренко, Р. В. Романовський // Архіви України. - 2018. - № 1. - С. 64-87. - Режим доступу: http://nbuv.gov.ua/UJRN/ay_2018_1_5.
2. ISO 19005-1:2005. Document management – Electronic document file format for long-term preservation – Part 1: Use of PDF 1.4 (PDF/A-1)
3. Навчально-методичний посібник «Стандартизація електронних видань» / укл. Дуболазов О.В., Солтис І.В.- Чернівці: Чернівецький нац. унт, 2022. – 51 с.
4. Мультимедійні технології відновлення друкованих видань в електронному виді [Текст] : навч. посіб. / О. П. Коханівський. - К.: НТУУ «КПІ», 2015. - 154 с.
5. Web сервіс ChessOCR [Електронний ресурс] // Режим доступу: <https://helpman.komtera.lt/chessocr/>.
6. Web сервіс Chessify [Електронний ресурс] // Режим доступу: <https://chessify.me/mobile>.
7. Web сервіс ChessVisionAI [Електронний ресурс] // Режим доступу: <https://play.google.com/store/apps/details?id=ai.chessvision.scanner>.

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ – ОСНОВА ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

В.С. Морохович

*кандидат фізико-математичних наук, доцент,
доцент кафедри інформатики та фізико-математичних дисциплін,
ДВНЗ «Ужгородський національний університет»*

Інформаційні технології розвиваються стрімкими темпами, проникаючи у всі сфери людської діяльності. Використання цифрових технологій здатне підняти на якісно новий рівень економіку держави та, відповідно, суттєво вплинути на рівень життя її населення. Що стосується реального сектору економіки, то найближчими десятиліттями всі бізнес-процеси, взаємодія підприємств зі стейкхолдерами, а також ринки всіх ресурсів зазнають значних трансформацій, підлаштовуючись під вимоги цифрових технологій і систем.

Технології великих даних, машинного навчання, розподілених реєстрів, роботизації, розумних речей, віртуальної та доповненої реальності, бездротового зв'язку та багато інших, у тому числі й ті, про які поки що міркують, засновані на безумовному та масштабному застосуванні цифрових наборів даних, визначають наше найближче та віддалене майбутнє вже сьогодні.

Цифрова трансформація змусила змінити спосіб роботи підприємств до такої міри, що стала фундаментальною частиною корпоративної стратегії. Вплив цифрової трансформації призводить до змін у поведінці споживачів, оцінці послуг і продуктів, а також очікуваннях. Щоб впоратися зі змінами в поведінці ринку, багато підприємств усвідомлюють необхідність трансформації бізнес-моделей, щоб отримати стійку конкурентну перевагу та йти в ногу з цифровою еволюцією своїх галузей [1].

Діджиталізація, відмінна від цифрової трансформації, розглядається як процес, що забезпечує перетворення доступного продукту або послуги в цифровий варіант, який пропонує більше переваг, ніж матеріальний продукт. Цифровізація не просто означає застосування цифрових інструментів у бізнесі, а й слугує засобом впровадження інноваційних бізнес-моделей та довгострокових корпоративних стратегій. Вона описує, як цифрові технології можуть перетворити наявні бізнес-процеси. Ця зміна вимагає впровадження цифрових технологій для формування нової організаційної технологічної структури, що було б неможливо без своєчасного впливу цифрових інструментів. Інформаційні технології можуть полегшити управління взаємозв'язками бізнес-процесів і добре підходять для організації, стаючи ключовими складовими операцій управління людськими ресурсами [2].

Цифрова трансформація характеризується ключовим організаційним зрушенням, що забезпечується, створюється або підтримується цифровими технологіями, які змінюють підхід до бізнес-операцій. Вона застосовує цифрові стратегії для досягнення важливих реформ в управлінні бізнесом, що призводить до значних змін в організації чи галузі загалом. Цифрова трансформація перетворює спосіб роботи всієї організації, особливо бізнес-процеси та завдання. Крім того, вона сприяє покращенню взаємодії організації з клієнтами завдяки

інноваційним технологіям. Таким чином, цифрові інструменти можуть підтримати підприємства у використанні наявних компетенцій або розвитку нових для отримання конкурентних переваг. Цифрова трансформація тісно пов'язана зі стратегічними змінами в бізнес-моделях завдяки впровадженню цифрових технологій.

Діджиталізація, цифрова трансформація і цифрові інновації тісно переплітаються і взаємодіють між собою. По-перше, ці поняття базуються на використанні цифрових технологій. Діджиталізація може стати результатом цифрових інновацій через впровадження цифрових змін у процесі їх поширення. Також, цифровізація та цифрові інновації можуть викликати значні трансформації в способах ведення бізнесу.

Список використаних джерел

1. Мандич О., Бабко Н., Лишенко М., Харчевнікова Л. Цифрова трансформація та новітні комунікації як платформа для стійкого розвитку бізнесу. [Modeling the development of the economic systems](#). 2022. №4. С.15-19.
2. Zhang J., Chen Z. Exploring human resource management digital transformation in the digital age. Journal of the knowledge economy. 2023. <https://doi.org/10.1007/s13132-023-01214-y>

БЕЗПЕКА КОМП'ЮТЕРНИХ МЕРЕЖ ТА ІНТЕРНЕТ

М.М. Недобосєв

магістрант,

Львівська філія ПВНЗ «Європейський університет»

Безпека мережі (Network security) – заходи, які захищають інформаційну мережу від несанкціонованого доступу, випадкового або навмисного втручання в роботу мережі або спроб руйнування її компонентів. Безпека інформаційної мережі включає захист обладнання, програмного забезпечення, даних і персоналу.

Мережева безпека охоплює різноманітні комп'ютерні мережі, включаючи як державні, так і приватні, які використовуються в повсякденних робочих умовах для здійснення угод і спілкування між підприємствами, державними установами та приватними особами. Ці мережі можуть бути приватними, як, наприклад, внутрішні мережі компаній, або публічними, доступними для загального використання. Мережева безпека відіграє важливу роль в організаціях, підприємствах та інших установах. Один із найпоширеніших і простих методів захисту ресурсів мережі полягає в присвоєнні їм унікальних імен і використанні відповідних паролів.

Сама концепція мережевої безпеки починається з базових речей як аутентифікації, що включає в себе пароль та ім'я користувача. При однофакторній автентифікації необхідно вказати лише один вид авторизаційних даних, наприклад ім'я та пароль. Такий спосіб менш надійний у порівнянні з двофакторною автентифікацією, що вимагає введення додаткових відомостей або виконання підтверджуючих дій на інших пристроях. Двох факторна автентифікація(2FA) – це метод захисту для керування ідентичностями та

доступом. Він вимагає дві форми ідентифікації для доступу до ресурсів і даних. Двох факторна автентифікація дає компаніям змогу відстежувати й захищати найуразливіші дані та мережі.

Недостатньо використання сильних та складних паролів у теперішньому світі, необхідно дотримуватися багатьох інших практик що можуть забезпечити безпеку комп'ютерних мереж, а саме:

- навчання персоналу;
- шифрування даних;
- заборона доступу до мережі;
- моніторинг та журналювання;
- регулярний аудит безпеки;
- захист від DDoS-атак;
- оновлення програмного забезпечення

Забезпечення безпеки комп'ютерних мереж та Інтернет – це постійний процес, оскільки загрози постійно змінюються. Тому важливо слідкувати за останніми трендами в цій галузі і підтримувати своє обладнання та програмне забезпечення в актуальному стані.

Список використаних джерел

1. *Захист інформації в комп'ютерних система та мережах - 2014*
URL:

http://www.dgma.donetsk.ua/docs/kafedry/avp/metod/_%D0%91%D0%9A%D0%9C%20%D0%9F%D0%BE%D1%81_%D0%B1%D0%BD%D0%B8%D0%BA.pdf

2. *Безпека мережі* URL: https://en.wikipedia.org/wiki/Network_security

РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ПЕРЕТВОРЕННЯ НЕСТРУКТУРОВАНОЇ ІНФОРМАЦІЇ В СИСТЕМАХ АНАЛІЗУ ДАНИХ

К.К. Осташко,
магістрант

Л.О. Литвиненко,
к.т.н., доцент

ПВНЗ «Європейський університет»

Виклики, пов'язані з перетворенням великої кількості неструктурованої інформації, стають все більш актуальними у світі, що стрімко цифровізується. Ця робота презентує розробку програмного забезпечення, яке використовує ігрові механізми для ефективного аналізу та систематизації неструктурованих даних, сприяючи підвищенню рівня залучення користувачів та їх розуміння оброблюваних даних.

Основні етапи роботи включають аналіз існуючих методологій, проектування програмної архітектури, розробку інтерактивного ігрового інтерфейсу, та інтеграцію з банківськими системами для реального застосування у фінансовому секторі. Результати демонструють важливість глибокого

розуміння неструктурованих даних та можливості їх перетворення в цінні інсайти для бізнесу та освіти.

Програмне забезпечення, розроблене в рамках цієї роботи, є інноваційним рішенням для перетворення неструктурованої інформації, яка включає текст, зображення та інші форми даних у структуровані формати, оптимізовані для аналізу даних. Використання гейміфікації в процесі роботи з даними не тільки покращує взаємодію з користувачами, але й сприяє глибшому зануренню у матеріал, що дозволяє користувачам виявляти важливі тенденції та зразки в інформації. Розробка програмного забезпечення включає детальне вивчення існуючих підходів до обробки даних, розробку алгоритмів для їх перетворення та створення користувацького інтерфейсу, який дозволяє ефективно взаємодіяти з системою.

В ході розробки програмного забезпечення були застосовані мови програмування Python та JavaScript, які дозволили створити гнучку та інтерактивну платформу для роботи з даними. Зокрема, Python використовувався для написання бекенд-логіки та обробки даних, тоді як JavaScript забезпечив реактивний фронтенд інтерфейс. Результатом стала система, яка дозволяє користувачам візуально маніпулювати неструктурованими даними, перетворюючи їх у структуровані формати для подальшого аналізу. Система також інтегрувала ігрові елементи для підвищення залученості та ефективності навчання користувачів.

Завершальна фаза проекту демонструє, що застосування сучасних мов програмування та гейміфікаційних технік може значно підвищити ефективність обробки неструктурованих даних. Розроблена система не лише відповідає технічним вимогам сучасного аналізу даних, але й втілює інноваційний підхід до взаємодії користувачів з інформацією, перетворюючи складний процес аналізу на захоплюючу діяльність. Висока залученість користувачів та позитивні відгуки стейкхолдерів підтверджують важливість та ефективність реалізованого проекту.

Список використаних джерел

1. Бабенко, Т. П. "Методи обробки текстових даних в програмному забезпеченні для аналізу даних."
2. Гончаренко, Л. М. "Гейміфікація в бізнес-аналітиці: використання інтерактивних ігор для покращення аналітичних процесів."
3. Гордієнко, В. М. "Аналіз неструктурованих даних у програмному забезпеченні для аналізу даних."
4. Коваленко, П. В. "Гейміфікація в програмному забезпеченні для аналізу текстових даних: теорія та практика."
5. Ковальчук, Ю. М. "Гейміфікація в програмному забезпеченні для аналізу даних: теорія та практика."
6. Лавриненко, С. О. "Методи обробки текстових даних у програмному забезпеченні для аналізу даних."
7. Литвиненко, О. П. "Використання гейміфікації в програмному забезпеченні для обробки неструктурованої інформації у системах аналізу даних."
8. Максименко, О. С. "Архітектурні рішення у програмному забезпеченні для аналізу неструктурованих даних."
9. Петров, Д. С. "Методи аналізу текстових даних у програмному забезпеченні для бізнес-інтелекту."

10. Савченко, О. В. "Архітектура програмного забезпечення для аналізу текстових даних в сучасних системах обробки інформації."
11. Чернишов, О. І. "Використання гейміфікації в програмах аналізу даних: практичний досвід."
12. Іваненко, В. О. "Обробка текстових даних в сучасних системах аналізу даних."

УПРАВЛІННЯ ІНЦИДЕНТАМИ КІБЕРБЕЗПЕКИ В СУЧАСНОМУ СВІТІ

І. Паньова

студентка факультету інформаційних систем та технологій,

М.М. Гримальська,

викладач

ПВНЗ «Європейський університет»

Інциденти інформаційної безпеки є окремим підкласом кризових і надзвичайних ситуацій, що можуть відбутися в інформаційній, соціальній, технічній інфраструктурі держави, організації, як окремий випадок, – в організаційно-технічних системах та інформаційно-комунікаційних мережах, впливаючи на стан державних інформаційних ресурсів і національної безпеки. Дослідженню процесів реагування, обробки, розслідування, керування інцидентами кібербезпеки присвячено багато публікацій, зокрема науковотеоретичного, науково-прикладного та виробничо-практичного змісту. Існує стандартизована міжнародна нормативно-методологічна база. Але на сьогодні все ще існує цілий ряд наукових, технічних, організаційних і нормативно-правових завдань, які є недостатньо вирішеними. Як в Україні, так і в світовій практиці завдання підтримки прийняття рішень й автоматизації керування інцидентами кібербезпеки потребує подальшого дослідження. В жодному міжнародному чи вітчизняному нормативно-технічному документі, які частково торкаються або повністю.

Інциденти у сфері високих технологій: характерні ознаки та проблемні аспекти. Процедура обрання раціонального варіанта реагування на кібернетичні втручання і загрози Із розвитком ІКТ, ІТС та глобальної мережі Інтернет світове співтовариство, отримавши небачені досі можливості в плані обміну інформацією, стало надзвичайно вразливим щодо стороннього кібернетичного впливу [1,2], а саме щодо фактично неприхованих спроб впливу протиборчих сторін на інформаційний і кіберпростори один одного за рахунок використання засобів сучасної обчислювальної і/або спеціальної техніки й відповідного програмного забезпечення – кібервтручань, а також інших проявів їхнього дестабілізуючого впливу на той чи інший об'єкт, здійснюваного за рахунок технологічних можливостей інформаційного і кіберпростору, зі створенням небезпеки – так званих кіберзагроз, як для цього простору, так і для свідомості кожної людини. Нині з метою уникнення багатозначності тлумачень відповідних термінів інструктивні матеріали Інтерполу поділяють їх на групи, що охоплюють:

- власне комп'ютерні інциденти, які полягають, наприклад, у втручанні в роботу обчислювальних систем, порушенні авторських прав на програмне забезпечення, а також у розкраданні даних і комп'ютерного часу;

- інциденти, пов'язані з комп'ютерами, що супроводжують здебільшого протиправні дії з фінансового шахрайства;

- мережні інциденти, що призводять до укладання незаконних угод. Під інцидентами у сфері високих технологій розумітимемо події, що полягатимуть в реалізації певної загрози та порушенні встановленого рівня безпеки інформаційно-комунікаційних систем.

Процесом управління інцидентами називатимемо процес реєстрації інформації про стан безпеки та рівноваги ІКС, передавання інформації в пункти її нагромадження, переробки й аналізу, з ухваленням прийняття рішення та формуванням певного керуючого впливу на об'єкт управління. Інша класифікація таких дій визначає сім основних їх груп, які характеризують передусім способи, що їх використовують зловмисники для здійснення нападу, а саме: перехоплення паролів інших користувачів; «соціальна інженерія»; використання помилок ПЗ і програмних закладок, а також помилок механізмів ідентифікації користувачів і недосконалості протоколів передавання даних; одержання інформації про користувачів стандартними засобами операційних систем; блокування сервісних функцій системи, що зазнає атаки. Зауважимо, що інтерес у плані класифікації кібернетичних втручань і загроз становить схема, запропонована Конвенцією Ради Європи 2001 року й спрямована на боротьбу з кіберзлочинністю [4].

У ній йдеться про чотири можливі групи таких дій.

1. Інциденти, що мають на меті завдати шкоди конфіденційності, цілісності й доступності комп'ютерних даних та систем і реалізуються через:

- несанкціонований доступ в інформаційне середовище (протиправний навмисний доступ до комп'ютерної системи або її частини, а також до ІР протиправної сторони, здійснений в обхід систем безпеки);

- втручання в дані (протиправна зміна, ушкодження, вилучення, перекручування або блокування комп'ютерних даних і керуючих команд за допомогою кібератак на інформаційні системи, ресурси та мережі державного і військового управління);

- втручання в роботу системи (протиправне порушення або створення перешкод функціонуванню комп'ютерної системи через розробку та поширення вірусного ПЗ, застосування апаратних закладок, радіоелектронного та інших видів впливу на технічні засоби й системи телекомунікацій і зв'язку, на обробку та передавання інформації, на системи захисту ІР, систем і мереж, програмно-математичне забезпечення, протоколи передавання даних, алгоритми адресації та маршрутизації);

- незаконне перехоплення (протиправне навмисне аудіовізуальне і/або електромагнітне перехоплення не призначених для загального доступу комп'ютерних даних, переданих СІТС в обхід заходів безпеки);

- незаконне використання комп'ютерного й телекомунікаційного обладнання або його повне вилучення.

2. Шахрайство та підробка, пов'язані з використанням комп'ютерів, а саме [3]:

- підробка документів із застосуванням комп'ютерних засобів (протиправне навмисне внесення, змінювання, вилучення або блокування комп'ютерних даних, що призводить до зниження вірогідності документів);
- шахрайство із застосуванням комп'ютерних засобів (втручання у функціонування комп'ютерної системи з метою навмисного протиправного одержання економічної вигоди).

Отже, на сьогодні актуальність проблеми кібербезпеки не викликає жодних сумнівів: щодня кожен громадянин України стикається з необхідністю користування інформаційними технологіями: від соціальних мереж і розміщення інформації, що містить персональні дані в мережі Інтернет, до користування банкоматами, банківськими рахунками тощо. У зв'язку із цим питання керування інцидентами кібербезпеки вимагає ефективних механізмів.

Список використаних джерел:

1. Дубов Д. В. Кібербезпека : світові тенденції та виклики для України / Д. В. Дубов, М. А. Ожеван. – К. : НІСД, 2011. – 30 с. Negnevitsky M. Artificial intelligence: a guide to intelligent systems. Addison-Wesley, 2002.
2. СБУ: Головні проблеми для України – тероризм і кіберзлочинність // Українська Правда [Електронний ресурс]. – Режим доступу: <http://www.pravda.com.ua/news/2012/03/23/6961285>.
3. Управління боротьби з кіберзлочинністю // Міністерство внутрішніх справ України [Електронний ресурс]. – Режим доступу: <http://mvs.gov.ua/mvs/control/main/uk/publish/article/544754>.
4. Securing Cyberspace for the 44th Presidency / James A. Lewis // Center for Strategic and International Studies [Електронний ресурс]. – Режим доступу: http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf.

РОЗРОБКА КОМП'ЮТЕРНОЇ ГРИ ДЛЯ АДАПТАТИВНОГО ОНЛАЙН НАВЧАННЯ

Д.Ю. Покидько
аспірант,

ПВНЗ «Європейський університет»

Нині цифрові технології та кліпова культура є частиною нашого життя. Тому впровадження ігрових технологій відповідає запитам сучасного студента і дозволяє враховувати його індивідуальні особливості, дозволяє розвивати як аналітичні навички, так і креативність.

Значні подорожі навчальних комп'ютерних ігор дозволяють зробити висновок, що дорослі також витрачають багато часу в ігровому світі, а потім розпочинають активну бізнес-діяльність в реальному світі. Сьогодні існує великий вибір навчальних ігор в інформаційно-освітньому просторі. Особливо ці ігри поширені в онлайн світі. Наприклад, Duolingo – гейміфікована платформа для вивчення іноземних мов; LIFESAVER: Crisis Simulator – додаток, що вчить здійснювати серцево-легеневу реанімацію; Medieval Swansea – інтерактивна історична гра.

В роботі запропоновано розробку комп'ютерної гри з інтерактивного навчання географії. Програма написана на мові C# та рушію Unity. Розроблена програма Map Of World Quiz дозволяє в ігровому форматі вивчати країни, їх географічні умови та культуру. Особливості гейміфікації Map Of World Quiz:

- сценарії, що гуртуються на цікавих задачах та квестах;
- інтерактивні карти;
- гравець сам керує тим, що хоче вивчити, може повторно обрати завдання, робити паузи, слідкувати за своїм прогресом.

Запропоновану навчальну гру можна використати не тільки для навчання школярів та студентів, а і для залучення клієнтів туристичних компаній. Від існуючих прототипів, таких як WorldMapQuiz, GeaCron запропонована розробка відрізняється функціональністю, інтуїтивним інтерфейсом користувача методами візуальної подачі та комунікації між гравцями.

Таким чином, комп'ютерні ігри в освіті дуже важливі для адаптації до цифрової епохи. Навчатись за допомогою ігрових механік – ефективний спосіб отримання нових знань та навичок. Запропонований програмний засіб є однією із сходинок адаптації та створення нових підходів до навчання.

Список використаних джерел:

1. Buckley P., Doyle E. Individualising gamification: An investigation of the impact of learning styles and personality traits on the efficacy of gamification using a prediction market // Computers and Education. Volume 106, 1 March 2017, Pages 43-55.

МАЙБУТНІ НАПРЯМКИ ДОСЛІДЖЕНЬ РЕАЛІЗАЦІЙ ЗАБЕЗПЕЧЕННЯ ВІДМОВСТІЙКОСТІ У МІКРОСЕРВІСНІЙ АРХІТЕКТУРІ

А.В. Пойченко,

здобувач другого (магістерського) рівня вищої освіти,

І.О. Доровська

к.т.н., доц.

ПВНЗ «Європейський університет»

Мікросервісна архітектура полягає у розбитті програмного додатка на систему менших сервісів, які взаємодіють один з одним [1]. Це сприяє можливості незалежно замінювати одні сервіси іншими, спрощуючи тим самим процес модифікації та оновлення різних частин системи. Важливо відзначити, що мікросервісна архітектура дуже схожа на сервісно-орієнтовану архітектуру, де також присутня система взаємодіючих додатків; проте, в мікросервісній архітектурі наголошується на розбитті цілісного продукту на менші компоненти.

Зменшення розміру сервісів спрощує їхню розробку та підтримку, а також прискорює впровадження нових мікросервісів. Це робить систему більш гнучкою до змін у навантаженні. Проте, перехід від монолітної системи, де всі компоненти об'єднані в одному додатку, до мікросервісної архітектури призводить до нового типу проблем. У монолітній системі всі залежності розташовані в межах одного сервера, тоді як у мікросервісній архітектурі можуть

виникнути залежності на тимчасово недоступних серверах. Непередбачений такий сценарій під час проектування системи може призвести до виходу з ладу послідовно розташованих залежних сервісів, що в свою чергу може спричинити каскадний збій значної частини системи. Запобігання таким ситуаціям може бути здійснене за допомогою різних підходів, серед яких одним з ефективних є використання шаблону проектування під назвою "circuit breaker" [2].

Аналогічно до автоматичного вимикача, концепція шаблону "circuit breaker" полягає в обмеженні відправки запитів до недосяжного сервісу від інших сервісів при досягненні певної максимальної кількості невдалих спроб. Після цього періоду, недосяжному сервісу відводиться певний час на відновлення, після чого до нього відправляється пробний запит. У разі успішного виконання запиту система продовжує взаємодію з цим сервісом, як раніше. У випадку невдачі система повторює цикл, відводячи час до наступної спроби відновлення.

В той час, опис шаблону не накладає додаткових обмежень на його реалізацію, залишаючи багато питань для подальших досліджень. Наприклад, щодо оптимального підходу до визначення максимальної кількості спроб або того, як довго та в якій прогресії слід виділяти час перед кожною наступною спробою, залишається багато невизначених питань.

Іншою категорією невирішених питань може бути розташування цього функціоналу у системі. Хоча широко використовується практика використання бібліотек, таких як Hystrix Netflix чи Rybbreaker на стороні клієнта [3], при цьому додається цей функціонал до кожного клієнта окремо. Ще одним підходом може бути включення реалізації circuit breaker на стороні сервера, але це зазвичай неможливо у випадку із сторонніми системами. Як альтернатива обом цим підходам може бути інтеграція логіки circuit breaker у окремий мікросервіс, оптимальне поєднання якого з усіма іншими компонентами системи може стати ще одним напрямком для подальших досліджень.

Висновки. Слід відзначити, що забезпечення відмовостійкості є ключовим аспектом при розробці мікросервісної архітектури. Один із методів досягнення цієї відмінності полягає у використанні шаблону проектування "circuit breaker", реалізація якого може приймати різноманітні форми. Таким чином, визначено два потенційних напрямки для майбутніх досліджень у цьому контексті. Перше напрямком включає вивчення внутрішньої логіки "circuit breaker" з погляду оптимальної кількості спроб та часу очікування. Другий напрямок орієнтується на високорівневе питання щодо оптимального розташування функціоналу "circuit breaker" у системі мікросервісів.

Список використаних джерел

1. Jamshidi, P (2018). Microservices: The journey so far and challenges ahead./ Jamshidi, P., Pahl, C., Mendonça, N. C., Lewis, J., & Tilkov, S.// IEEE Software, 2018 – 35(3) - pp. 24-35.
2. Surendro, Kridanto. Circuit Breaker in Microservices: State of the Art and Future Prospects./ . Surendro, Kridanto, Wikan Danar Sunindyoo// IOP Conference Series: Materials Science and Engineering. 2021, - Vol. 1077. –No. 1.
3. Montesi, Fabrizio. Circuit breakers, discovery, and API gateways in microservices./ Montesi, Fabrizio, Janine Weber// 2016.

ДОСЛІДЖЕННЯ РОЄВИХ АЛГОРИТМІВ КОМБІНАТОРНОЇ ОПТИМІЗАЦІЇ

П.І. Роман
магістрант,
А.В. Невзоров
к.т.н. доцент

ПВНЗ “Європейський університет”

Ідеї деяких сучасних алгоритмів оптимізації нав'язані природою. Серед них виділяються такі, які відносять до ройового інтелекту (swarm intelligence) – алгоритмів, що мають справу з природними та штучними системами, які складаються з багатьох індивідів (елементів, агентів, частинок), координація та узгодження дій між якими здійснюється шляхом децентралізованого управління та самоорганізації. Зокрема, ройовий інтелект зосереджується на колективній поведінці, що є результатом локальних взаємодій окремих особин між собою та з навколишнім середовищем. Прикладами таких систем є колонії мурах і термітів, косяки риб, зграї птахів, стада наземних тварин.

Серед відомих алгоритмів ройового інтелекту в комбінаторній оптимізації найбільший інтерес становлять алгоритми оптимізації мурашиною колонією (ОМК; ant colony optimization – ACO), оптимізації роєм частинок (ОРЧ), бджолині алгоритми [1-4].

Найбільшого поширення при розв'язанні задач комбінаторної оптимізації набули запропоновані Марком Доріго (1992) мурашині алгоритми [2].

Мурашині алгоритми – це багатоагентні системи, де поведінка кожного агента, який називається штучною мурахою, заснована на поведінці справжніх мурашок. Вони застосовуються для розв'язання багатьох типів оптимізаційних задач, починаючи з класичної задачі комівояжера.

Ройовий інтелект – це група алгоритмів, яка має справу з природними та штучними системами, що складаються з багатьох агентів (елементів, індивідів, частинок), координація та узгодження дій між якими також здійснюється шляхом децентралізованого контролю та самоорганізації [3-4].

Прикладами таких систем є знову таки колонії мурах і термітів, косяки риб, зграї птахів, стада наземних тварин. Деякі розробки людини також належать до сфери ройового інтелекту, зокрема окремі мультироботні системи чи деякі комп'ютерні програми, що написані для розв'язання задач оптимізації та аналізу даних.

Ідея методу оптимізації роєм частинок, нав'язана схемою соціальної взаємодії та спілкування, властивою окремим видам птахів і риб. Варто зазначити, що метод ОРЧ – це інструмент не тільки оптимізації, але й подання соціального пізнання (пізнавальної здатності) людини та штучних агентів, яке базується на принципах соціальної психології.

Окремі науковці вважають, що знання оптимізується соціальною взаємодією, а мислення є не тільки особистісним процесом, але й міжособистісним.

Оптимізація роєм частинок як оптимізаційний інструмент є популяційною пошуковою процедурою, де агенти, які називаються частинками, взаємодіючи між собою, змінюють свої позиції (положення, стани) з часом з метою досягнення поставлених цілей.

У схемі оптимізації роєм частинок частинки рухаються в багатовимірному просторі пошуку задачі, що розв'язується. Під час руху кожна частинка коригує своє положення (варіант розв'язку) з урахуванням свого досвіду та досвіду сусідньої(их) частинки(ок), використовуючи при цьому найкраще з положень, знайдених нею, і найкращі положення, знайдені її сусідами. Таким чином, метод оптимізації роєм частинок комбінує локальний пошук із глобальним пошуковим методом, намагаючись збалансувати стратегії інтенсифікації та диверсифікації пошуку.

оптимізації роєм частинок спочатку було запропоновано як засіб неперервної оптимізації, але пізніше його було модифіковано для застосування до розв'язання задач комбінаторної оптимізації.

Базові принципи оптимізації роєм частинок описуються доволі просто. Множина частинок (варіантів розв'язків), що можуть рухатися, "закидається" у простір пошуку. Кожна частинка володіє такими властивостями:

- позицією та швидкістю;
- знає своє поточне положення та значення цільової функції свого поточного положення;
- пам'ятає своє найкраще попереднє положення;
- знає своїх сусідів, їхнє найкраще попереднє (або поточне) положення та відповідні значення цільової функції.

На кожному кроці поведінка певної частинки є компромісом між:

- продовженням свого руху;
- рухом до свого найкращого (у розумінні цільової функції) положення;
- рухом до найкращої частинки з околу або до найкращого попереднього положення сусідніх частинок.

Серед біологічно навіяних алгоритмів комбінаторної оптимізації важливе місце займають бджолині, які базуються на результатах спостереження за бджолиними роями при пошуку ними нектару [3]. Особливості поведінки бджолиних колоній можуть бути використані для моделювання інтелектуальної та колективної поведінки.

Основними поняттями у бджолиних алгоритмах є:

- джерела нектару;
- фуражири (робочі бджоли);
- бджоли-розвідники.

Незважаючи на накопичений досвід, розробка й впровадження алгоритмів комбінаторної оптимізації вимагає як наявності базових знань, так і творчого підходу: складність поєднання цих аспектів якраз визначає і успішність фахівців, і велике задоволення від процесу розв'язування задач та отриманих результатів.

Список використаних джерел

1. Гуляницький Л. Ф. Прикладні методи комбінаторної оптимізації / Л. Ф. Гуляницький, О. Ю. Мулеса. – К. : Видавничо-поліграфічний центр "Київський університет", 2016. – 133 с.
2. Dorigo M. Ant colony optimization theory: A survey / M. Dorigo, C. Blum // Theoretical Computer Science. – 2005. – 344.
3. Глибовець М. М. Еволюційні алгоритми / М. М. Глибовець, Н. М. Гуляєва. – К. : НаУКМА, 2013.
4. Субботін С. О. Неітеративні, еволюційні та мультиагентні методи синтезу нечіткологічних і нейромережних моделей / С. О. Субботін, А. О. Олійник, О. О. Олійник. – Запоріжжя : ЗНТУ, 2009.

ВИКОРИСТАННЯ СТАТИСТИЧНОГО МОДЕЛЮВАННЯ ДЛЯ РОЗВ'ЯЗУВАННЯ СТОХАСТИЧНИХ ДИФЕРЕНЦІАЛЬНИХ РІВНЯНЬ

А.М. Садло

магістрант,

А.О. Ткаченко

к.т.н., доцент кафедри комп'ютерних наук

та програмної інженерії

ПВНЗ "Європейський університет"

Насьогодні випадкові процеси відіграють важливу роль в економіці, фінансах, теорії керування, теорії зв'язку та багатьох інших областях науки та життєдіяльності.

За допомогою диференціальних рівнянь вже не одне десятиліття математики намагаються описати процеси і явища, які нас оточують.

На відміну від загальних диференціальних рівнянь, розв'язком яких є функція, розв'язком стохастичних диференціальних рівнянь є змінна в часі випадкова величина (випадковий процес). Тому надзвичайно важливою та цікавою є задача знаходження асимптотичних властивостей та збіжностей траєкторій розв'язків саме стохастичних диференціальних рівнянь.

Фізичним інтерпретуванням таких властивостей може бути, наприклад, те як поведе себе капітал кампанії (тобто до якої детермінованої функції будуть збігатися траєкторії) за достатньо великий проміжок часу.

Нехай $X(t) \in R^n$, $a(t, x) \in R^{n \times m}$, $\sigma(t, x) \in R^{n \times m}$ – матрична функція розмірності $n \times m$, $W(t) \in R^m$ - вінерівський процес, $v \in R^n$ - початкова умова.

Означення. Випадкова функція $X(t)$ є розв'язком стохастичного диференціального рівняння

$$dX(t) = a(t, X(t))dt + \sigma(t, X(t))dW(t) \quad (1)$$

на проміжку $T = [0; T]$ з початковою умовою $X(0) = v$, якщо її можна представити у вигляді

$$X(t) = v + \int_0^t a(\tau, X(\tau)) d\tau + \int_0^t \sigma(\tau, X(\tau)) dW(\tau)$$

Це в загальному випадку, нехай $n=m=1$.

Для побудови розв'язків стохастичних диференціальних рівнянь скористаємось методом статистичного моделювання.

Рівняння (1) можна подати у вигляді різницевого рівняння

$$X(t + \Delta t) - X(t) = a(t, X(t)) + \sigma(t, X(t))(W(t + \Delta t) - W(t))$$

Або

$$X(t + \Delta t) = X(t) + \Delta t[a(t, X(t)) + \sigma(t, X(t))(W(t + \Delta t) - W(t))]$$

Різницю $(W(t + \Delta t) - W(t))$ будемо будувати методом статистичного моделювання. Розіб'ємо інтервал $[0, T]$ на N підінтервалів. Прирости вінерівського процесу є незалежними гауссівськими випадковими величинами $\{\xi_k\}, k=1, 2, \dots, N$, що мають нульве середнє $E\xi_k = 0, k=1, 2, \dots, N$ і дисперсією $D\xi_k = \Delta t = \frac{T}{N}, k=1, 2, \dots, N$

Нехай початкова умова $X(0)=v$ має деякий розподіл, наприклад, рівномірний на інтервалі $[0, 1]$. Нехай $a(t, x) = \sigma(t, x) = 1$.

На рис. 1 зображена реалізація гауссівських випадкових величин, як приростів вінерівського процесу, на рис. 2 зображені реалізації розв'язків стохастичного диференціального рівняння (1).

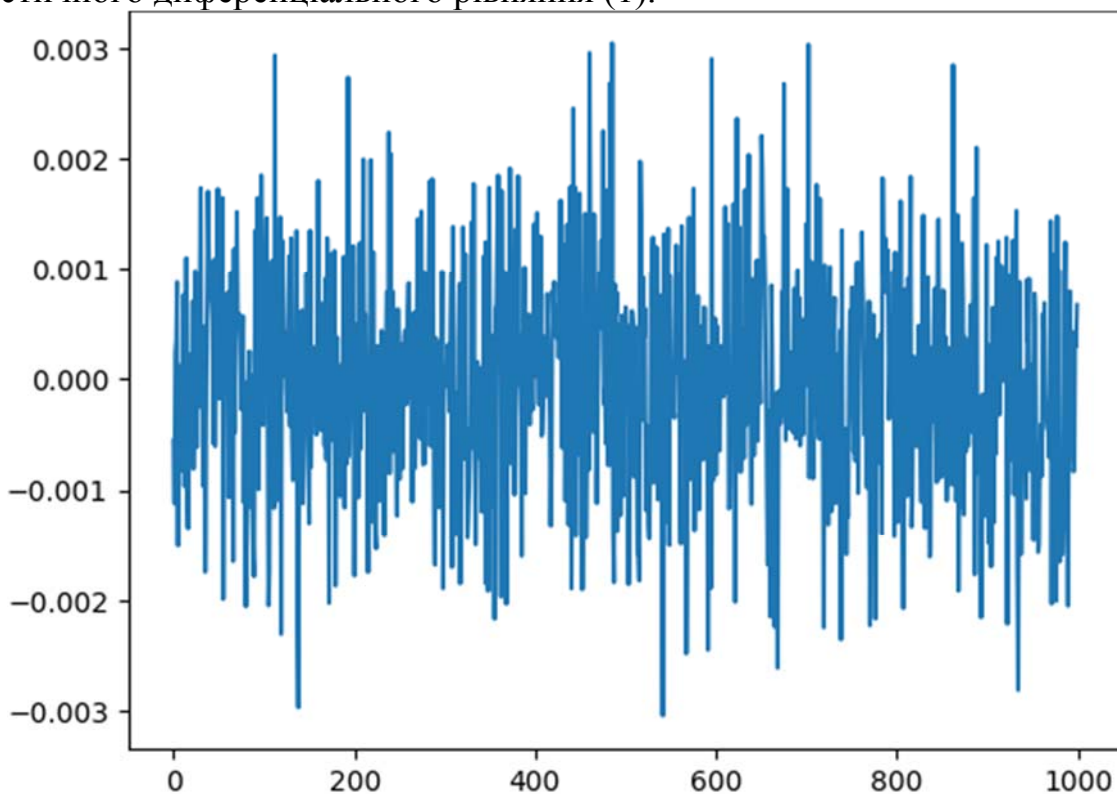


Рис. 1. Реалізація приростів вінерівського процесу

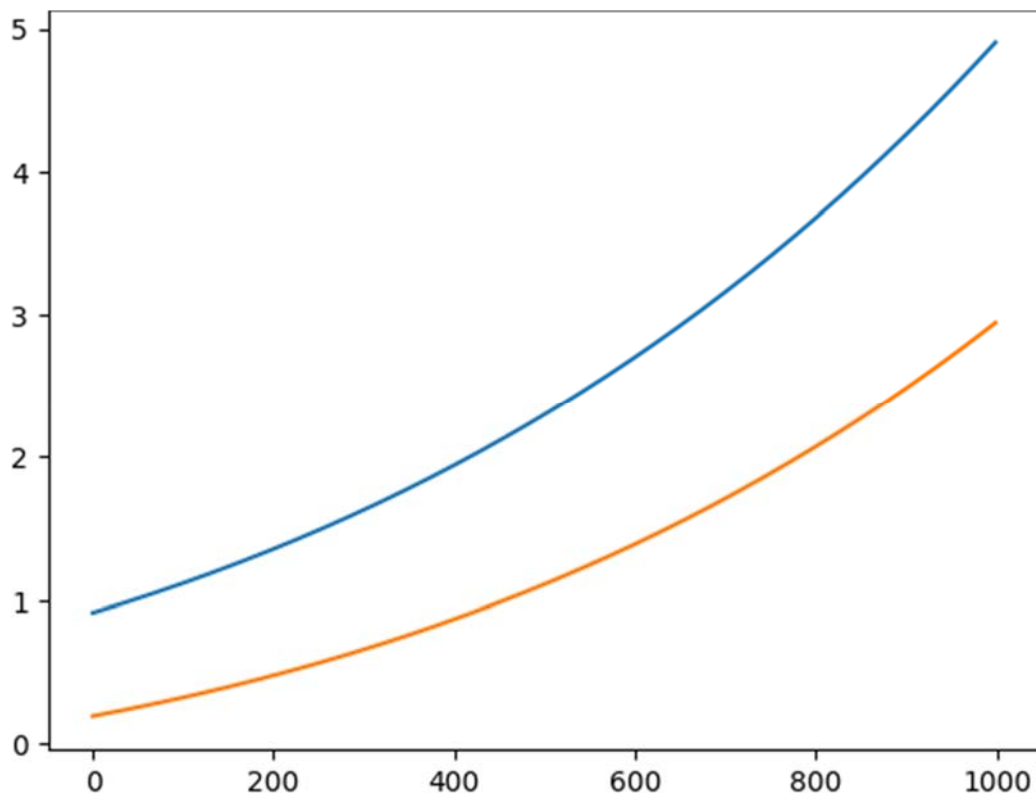


Рис. 2. Реалізації розв'язку стохастичного диференціального рівняння

У роботі було показано, що методи статистичного моделювання для розв'язування стохастичних диференціальних рівнянь є потужним інструментом як для доповнення аналітичних результатів, так і для самостійного аналізу та розв'язування задач.

Список використаних джерел

1. Allen, E. J., Allen, L., Arciniega, A., Greenwood, P.: *Construction of Equivalent Stochastic Differential Equation Models*. <http://www.sherrytowers.com/equivalentsdes.pdf>
2. V. V. Buldygin and O. A. Tymoshenko, *On the exact order of growth of solutions of stochastic differential equations with time-dependent coefficients*, *Theor Stoch. Process.*, 16 (2010), 12–22.
3. G. Keller, G. Kersting, U. Rösler *On the asymptotic behaviour of solutions of stochastic differential equations* <https://link.springer.com/content/pdf/10.1007/BF00531776.pdf>

ОНЛАЙН БЕЗПЕКА. СПУФІНГ ТА ФІШІНГ

О.С. Святобог

*аспірант кафедри менеджменту та маркетингу
Європейського університету*

Кожен день приносить нам нові повідомлення про викрадення даних, злив інформації, блокування роботи сайтів і т.ін. Загрози нас чекають всюди, злочинці не дрімають і кожен день видумують нові ходи, нові варіанти кібератак. Адже тепер вони також можуть використовувати штучний інтелект для цього. Їх ціллю

стають не лише великі чи малі компанії та державні установи, потерпають також і приватні особи. Причини цих атак можуть бути різними і не завжди вони націлені на отримання грошей.

Давайте розглянемо деякі види із атак і те як на них треба реагувати, щоб залишатися захищеними та в безпеці.

Підробка листів (Spoofing and Phishing)

Лист направлений на вашу електронну адресу, можливо особисту, від вашого колеги чи керівника. Він може бути направлений з адреси, яка схожа на ваші робочі адреси, але не є такою насправді. Як же перевірити справжність відправника? Перш за все необхідно уважно глянути на ім'я відправника та e-mail – чи вони сходяться? Якщо ви використовуєте корпоративний Microsoft Outlook ви можете побачити статус людини – онлайн, на зустрічі і т. ін. Якщо ж система позначила користувача, як зовнішнього – це уже повинно насторожити вас. Якщо лист від вашого колеги надійшов вам на особисту пошту, це також незвично, також слід звернути увагу на час відправки листа – надісланий в робочий час? Зверніть увагу чи відправник просить вас про щось таємно, чи терміново? Запропонуйте йому поспілкуватися з приводу цього листа у телефонному дзвінку, в зумі, чи іншим месенджером. А наступною вашою дією має бути обов'язкове звернення до ІТ служби вашої компанії, чи організації. У жодному разі не потрібно приховувати це чи ігнорувати.

Зловмисники можуть використовувати сайти схожі за назвою на назви відомих компаній чи брендів. Наприклад буква І (Ай) схожа на малу літеру «l» і от уже сайт olx стає oIx. Після чого вони використовуючи відоме ім'я звертаються до вас, як представника компанії з проханням переказати кошти на нові реквізити через їх зміну. Уникнути цього допоможе лише система контролю за платежами у вашій компанії, та уважна перевірка вами таких листів та підтвердження зміни реквізитів у вашого контрагента.

Хто стоїть за такими листами – хакери, конкуренти, різного роду «активісти», колишні співробітники. Цілі які вони переслідують використовуючи ці методи : отримання доступу до конфіденційної інформації, заволодіння вашими коштами, чи коштами вашої компанії, створення перешкод для діяльності вашої компанії чи ваших контрагентів.

Джерела звідки зловмисники беруть інформацію – соціальні мережі, ваші веб-сайти, новини з відкритих джерел, а також з необережного спілкування ваших співробітників в кафе офісного центру куди можуть потрапити також і люди з вулиці.

Список використаних джерел:

1. Стаття. Scams – Spam, Phishing, Spoofing and Pharming.
<https://www.ttu.edu/cybersecurity/lubbock/digital-life/digital-identity/scams-spam-phishing-spoofing-pharming.php>
2. Стаття Cybersecurity Awareness Month 2023 Blog Series | Recognizing and Reporting Phishing
<https://www.nist.gov/blogs/cybersecurity-insights/cybersecurity-awareness-month-2023-blog-series-recognizing-and>
3. Стаття Protect Your Business from Today's Biggest Cyber Threats
https://www.proofpoint.com/us/resources/threat-reports/state-of-phish?utm_source=google&utm_medium=cpc&gad=1&gclid=EAIaIQobChMI8KGVuqubgQMVBCzAB08fgYgEAAAYAiAAEgKZU_D BwE&gclsrc=aw.ds

ВЕБ-ЗАСТОСУВАННЯ ДЛЯ ГЕНЕРУВАННЯ МАТРИЦІ ШИФРУВАННЯ З ВИКОРИСТАННЯ ДИСКРЕТНИХ МЕТОДІВ

Р.В. Сенишин
магістрант,
Львівська філія ПВНЗ
«Європейський університет»

Сфера застосування криптографії за останній період значно розширилася і означає не лише забезпечення таємної передачі повідомлень між двома отримувачами, але і методи перевірки цілісності повідомлень, визначення відправника/одержувача (автентифікація), цифрові підписи, інтерактивні підтвердження доступу та безпечні технології комунікації, тощо. Тобто можна стверджувати, що криптографія необхідна для тієї інформації, котра потребує захисту. Зазвичай така інформація має містити таємницю, чи має бути захищеною від зловмисника, секретною, конфіденційною [1, 2]. Тому, в більшості випадків, такі напрями як генерування даних та освоєння класичних методів захисту інформації є першими кроками у вивченні криптографії, на що і зроблено нахил в цій роботі.

На сьогодні існує велика кількість криптографічних алгоритмів, варіативність яких базується як на певних наборах загальних характеристик, так і на певних принципах і механізмах їх роботи. Надійність цих алгоритмів також не є однаково визначеною: існують такі алгоритми, які здатні пройти усі умови захисту, та такі, що не гарантують та не можуть забезпечити жодного захисту в реальних умовах. Поясненням такого факту є питання складності проектування дійсно надійного криптографічного алгоритму. Крім того, очевидно, показник надійності є залежним від часу та доволі відносним – велика кількість алгоритмів, які розроблялися давніше та які підтвердили надійність є зараз або ненадійними, або забезпечують невідповідну до реалій надійність. Саме з цих причин важливим є врахування тенденцій розвитку інформаційних технологій, факторів ринку, актуальних стандартів, а також інші фактори, що потенційно можуть знизити стійкість та надійність криптографічного алгоритму в майбутньому.

Мета даної роботи полягає в представленні на кон-кретних прикладах особливостей ре-алізації криптографічних методів захисту тек-стової інформації з використанням матриць шифрування, а також розробити відповідну автоматизовану систему генерування матриць шифрування дискретними методами з використанням сучасних програмних засобів.

Предметом дослідження є методи і засоби розроблення програмного забезпечення, яке дасть змогу генерувати матриці (де)ши-фру-вання даних з відповідною криптографічною стійкістю алгоритму.

Список використаних джерел

1. Коваль-чук А. Підвищення стійкості системи RSA при шифруванні зображень // Технічні вісті. – 2009. – № 1-2. – С. 70-71.
2. Красиленко В.Г. Матричні Афінні шифри для створення цифрових підписів на тек-стографічні документи / В.Г. Красиленко, С.К. Грабовляк // Системи оброблення інформації: зб. на-ук. пр. – Х.: ХУПС, 2011. – Вип. 7 (97). – С. 60-63.

ТЕНДЕНЦІЇ ТА ПЕРСПЕКТИВИ РОЗВИТКУ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ

Р. Собченко

студент,

Європейського університету,

Миколаївська філія

Штучний інтелект (ШІ) швидко розвивається та справляє значний вплив на життя людей, бізнес і політичні процеси в усьому світі. Незважаючи на те, що галузь штучного інтелекту виникла понад півстоліття тому, вона все ще відносно нова, особливо щодо її застосування в рамках міжнародного розвитку. Будучи рушійною силою Четвертої промислової революції, вона вносить глибокі та далекосяжні зміни в те, як люди живуть, працюють і розважаються. У той самий час, коли досягнення в галузі штучного інтелекту дають позитивні результати в масштабах різних секторів і регіонів, важливо розглянути питання про те, як забезпечити відповідальне розгортання штучного інтелекту.

Широке використання та політична активність навколо штучного інтелекту з'явилися лише в останні кілька років. Першою країною у світі, яка оголосила про національну стратегію штучного інтелекту в березні 2017 року, стала Канада. Але сьгоднішні досягнення ґрунтуються на майже 70-річних дослідженнях і розробках [3]. Якщо глибше розібратися в теоретичних основах галузі, то історію штучного інтелекту можна простежити набагато далі, аж до його ранніх витоків у математиці та механіці в 1300-х роках.

З тих пір, як термін «штучний інтелект» вперше з'явився в дослідницькій пропозиції Дартмутського коледжу 1956 року (де описано «гіпотезу про те, що кожен аспект навчання або будь-яка інша особливість інтелекту в принципі може бути описана настільки точно, що машину можна симулювати»), визначення штучного інтелекту продовжують з'являтися, наголошуючи на різноманітних аспектах галузі.

Штучний інтелект використовує комп'ютери для автоматизованого прийняття рішень, які мають імітувати людський інтелект. Автоматизовані рішення можуть бути безпосередньо впроваджені (наприклад, у робототехніці) або запропоновані людині, яка приймає рішення (наприклад, рекомендації продукту в онлайн-магазинах); найважливіше для нашої мети полягає в тому, що деякі процеси прийняття рішень автоматизовані. ШІ часто включає машинне навчання (під час використання прогнозів на основі даних для прийняття кращих рішень), але це не обов'язково [4]. Машинне навчання — це набір методів, за допомогою яких комп'ютери розпізнають шаблони в даних і використовують ці

шаблони для прогнозування майбутнього. Для скорочення можна подумати про машинне навчання як про «прогнози на основі даних».

Корисно зрозуміти, наскільки далеко людство просунулося в розумінні та розробці ШІ з точки зору складності речей, які він нині здатний досягти. Для цього корисно підходити до штучного інтелекту з точки зору його трьох основних елементів: входи, процеси та результати. Кожен із цих елементів може мати різний рівень складності. Наприклад, на одному кінці спектра алгоритм може застосовувати суворі правила та вагові коефіцієнти до невеликих структурованих наборів даних, щоб виробити окреме рішення чи дію. З іншого боку, може бути побудований алгоритм для обробки та повторної обробки необмеженої кількості неструктурованих даних, що призводить до складних рішень та/або дій.

Зі зростанням складності (а в деяких випадках і непрозорості) рішень штучного інтелекту розуміння їхнього впливу на сферу розробки так само вимагатиме нових/досконаліших методів моніторингу та оцінки. Слід звернути увагу на ширші, вторинні наслідки впровадження рішень ШІ в системи, які можуть включати вплив на зайнятість, права людини, інклюзивне зростання та багато інших сфер. Розробка підходів до моніторингу та оцінки, які відповідають складності систем штучного інтелекту, може передбачати:

- структури для оцінки якості та потенційних упереджень, властивих наборам даних, що використовуються системами штучного інтелекту, ефективності моделей штучного інтелекту та рівня впевненості в результатах, які вони генерують;
- надійні підходи до інтерпретації даних/аналізу, створених ШІ, і способів їх використання для прийняття рішень, включаючи розуміння потенційної вартості помилок;
- використання змішаних методів, включаючи якісні підходи за участю, для підтвердження/скасування висновків.

Крім можливостей і переваг, які привносять технології ШІ, залежність від них у майбутньому також посилить потенційні загрози для обороноздатності країни світу. Серед потенційних загроз розвитку ШІ можуть бути визначені такі [1]:

- системи ШІ особливо вразливі до кібератак, коли навмисне вороже втручання в їх дію може призвести до помилкових рекомендацій або неоптимальних дій;
- досягнення в технологіях обробки та синтезу мовлення дають можливість створення реалістичних дипфейків (Deep Fake). У поєднанні з твіттер-ботами та іншими хакерами соціальних мереж удосконалений ШІ (наприклад, генеративні змагальні мережі (GAN)) значно підвищить масштаби й ефективність гібридних атак;
- непередбачувана поведінка в системах ШІ є як сильною стороною (наприклад, створення абсолютно нових стратегій [5]), так і водночас підвищує відповідальність за аберантні рішення;
- системи навчання на базі ШІ дозволяють створювати нові покоління саморобних вибухових пристроїв, менш сприйнятливих до традиційних контрзаходів.

Серед проблем, з якими можуть зіткнутися системи забезпечення обороноздатності країн світу, також є сумісність ІІІ із системами оперативного прийняття рішень, що пов'язано з необхідністю використання різних стандартів верифікації, підтвердження та акредитації (VV&A) [2]; різних правил управління даними, таксономії та побудови навчальних наборів даних; концепцій об'єднання людини та машини, їх симбіозу тощо.

Список використаних джерел:

1. Cheney, C (2018) *The promise and pitfalls of artificial intelligence for global development* <https://www.devex.com/news/the-promise-and-pitfalls-of-artificial-intelligence-for-global-development-91881>
2. Anyoha, R (2017) *The History of Artificial Intelligence* <http://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/>
3. Marr, B (2018) *The Key Definitions Of Artificial Intelligence (AI) That Explain Its Importance* <https://www.forbes.com/sites/bernardmarr/2018/02/14/the-key-definitions-of-artificial-intelligence-ai-that-explain-itsimportance/#6a9af0fa4f5d>
4. Хаустова В. Є., Решетняк О. І. Дослідження стану та тенденцій розвитку науки в країнах світу та Україні. Проблеми економіки. 2019. № 3. С. 11–22. DOI: <https://doi.org/10.32983/2222-0712-2019-3-11-22>
5. Kyzym M., Reshetnyak O., Bielousov D. *Forecasting scientific support for the advancement of the digital economy. Studies of Applied Economics*. 2020. Vol. 38. No. 4.

СИСТЕМА ПРОГНОЗУВАННЯ ТА АНАЛІЗ ВПЛИВУ ЗМІН КЛІМАТУ ЗА ДОПОМОГОЮ RYTHON ТА МАШИННОГО НАВЧАННЯ

О.Є. Сушинський¹

Н.В. Анісимов²

¹д. т. н., професор кафедри математики
та комп'ютерних дисциплін

²магістрант,

Львівська філія ПВНЗ «Європейський університет»

Зміна клімату є одним із найактуальніших викликів нашого часу, який має далекосяжні наслідки для різних аспектів нашого довкілля та суспільства. Розуміння та прогнозування цих впливів є вирішальними для ефективного планування та стратегій пом'якшення. В останні роки досягнення в галузі науки про дані та алгоритми машинного навчання надали нові можливості для аналізу та прогнозування моделей зміни клімату.

Зміна клімату відноситься до довготривалих явищ, що спричиняє зміни у середніх погодних умовах, що часто призводить до підвищення температури, екстремальних погодних явищ і підвищення рівня моря. Причини зміни клімату багатогранні, вони впливають із поєднання природних процесів і діяльності людини.

Однією з ключових природних причин зміни клімату є сонячна радіація. Земля поглинає енергію сонячного випромінювання, а потім випромінює її назад в атмосферу. Зміни в інтенсивності сонячного світла або відстані Землі від сонця

можуть призвести до зміни кількості поглиненої енергії, що впливає на глобальну температуру.

Іншим природним фактором, що сприяє зміні клімату, є вулканічна активність. В результаті виверження вулканів в атмосферу викидається велика кількість газів, у тому числі вуглекислого газу (CO_2). CO_2 – це парниковий газ, який утримує тепло в атмосфері Землі, тим самим підвищуючи температуру.

Зміна клімату, спричинена діяльністю людини, головним чином спричинена викидом парникових газів, що є результатом різноманітної діяльності. Спалювання викопного палива, зокрема вугілля, нафти та природного газу, викидає в атмосферу значну кількість CO_2 . Ці викиди неухильно збільшувалися з часів промислової революції, оскільки зросли потреби в енергії. Крім того, вирубка лісів сприяє зміні клімату. Деревина поглинають CO_2 , тож коли їх вирубують, цей CO_2 вивільняється, прискорюючи глобальне потепління.

Зміна клімату є однією з найактуальніших проблем нашого часу, що вимагає комплексного збору даних, щоб краще зрозуміти її причини, наслідки та потенційні стратегії пом'якшення. Збір даних є невід'ємною частиною розуміння моделей зміни клімату, визначення тенденцій і прийняття обґрунтованих рішень. Точні й надійні дані стають основою для розробки ефективних політик, стратегій і рішень.

Дані про зміну клімату охоплюють різні категорії, такі як температура, опади, підвищення рівня моря, викиди парникових газів і втрата біорізноманіття. Методи збору даних включають дистанційне зондування, наземні спостереження, палеокліматичні дослідження, супутникові технології, кліматичні моделі та громадські наукові ініціативи. Декілька проблем заважають точному збору даних про зміну клімату. До них належать прогалини в даних у віддалених районах, неузгодженість методів вимірювання, історичні упередження, обмежене просторове та часове охоплення та доступ до надійного фінансування та ресурсів.

Оцінка та аналіз невизначеностей у прогнозах зміни клімату є складним завданням через численні змінні та складні системи. Сучасні статистичні методи можуть допомогти зрозуміти розподіл можливих результатів та їхню ймовірність. Зазвичай використовуються такі методи, як моделювання Монте-Карло, розрахунок байєсівської функції та ймовірнісне прогнозування. Моделі кліматичної економіки можна використовувати для оцінки політичних наслідків невизначеностей, таких як розрахунок оптимальної ставки контролю або податку на викиди вуглецю на основі оцінок шкоди клімату в результаті потепління. Ці моделі зазвичай об'єднують економічні фактори з кліматичними моделями, щоб оцінити потенційний вплив різних політичних рішень.

Прогнозування зміни клімату є гострою глобальною проблемою, і вона потребує комплексних методів, які можуть отримати інформацію з величезних обсягів даних. Моделі машинного навчання, які є аналітичними алгоритмами, призначеними для навчання та прийняття прогнозів або рішень на основі даних, пропонують багатообіцяючий підхід до вирішення цієї складної проблеми.

Щоб прогнозувати зміни клімату, дослідники використовують різні методи машинного навчання. Одним із широко використовуваних підходів є

регресія, коли моделі навчені встановлювати кореляції між вхідними змінними та вихідними кліматичними результатами.

Іншим часто використовуваним методом є класифікація, яка включає класифікацію кліматичних моделей на окремі класи. Наприклад, моделі машинного навчання можуть класифікувати моделі атмосферного тиску як ознаки екстремальних погодних явищ або ні. Цей класифікаційний метод може допомогти в оцінці ризику, пов'язаного з певними кліматичними явищами, таким чином інформуючи політиків і зацікавлених сторін про потенційні наслідки та стратегії пом'якшення.

Одним із викликів у прогнозуванні клімату за допомогою моделей машинного навчання є робота з невизначеністю та упередженнями, пов'язаними з кліматичними даними. Наприклад, недосконалі або неповні спостереження можуть створювати шум і впливати на продуктивність моделі.

Використання моделі лінійної регресії є поширеним підходом для прогнозування та аналізу зміни клімату. Для реалізації процесу прогнозування пропонується використати бібліотеку Pandas, яка є потужним засобом аналізу та обробки даних із відкритим кодом для Python. Вона створена на основі двох основних бібліотек Python – Matplotlib для візуалізації даних і NumPy для математичних операцій. Pandas надає гнучкі та ефективні структури даних, які спрощують маніпулювання та аналіз складних даних. Для реалізації обробки кліматичних даних вибираємо відповідні функції та цільову змінну. У нашому випадку: функції («Рік» і «Рівні CO₂») і цільову змінну («Температура»).

Візуалізація фактичних і прогнозованих значень цільової змінної є важливим кроком у розумінні того, наскільки добре модель прогнозування фіксує закономірності в даних. У контексті прогнозування та аналізу зміни клімату ця візуалізація допомагає оцінити точність прогнозів і визначити області, де модель може потребувати вдосконалення.

Висновки. Тенденції розвитку сучасних технологій збереження та обробки даних дозволяє запропонувати їх функціонал для реалізації прогнозування та аналізу впливу змін клімату. Використання відповідних бібліотек Python та алгоритмів машинного навчання дозволило проаналізувати великі набори даних і візуалізувати дані для прийняття відповідних прогнозних рішень з метою впливу на покращення кліматичної ситуації на планеті.

Список використаних джерел

1. Climate Change - An Overview. (2022). Climate Change - An Overview. 17(2). <https://doi.org/10.51220/jmr.v17i2.23>.
2. Gutterman, A. S.. (2022). Causes and Impacts of Climate Change. <https://doi.org/10.2139/ssrn.4307025>.
3. Wheeling, K.. (2020). Machine Learning Improves Weather and Climate Models. 101. <https://doi.org/10.1029/2020EO142422>.
4. Sabancı, D., Yurekli, K., Comert, M. M., Kiliçarslan, S., & Erdoğan, M.. (2023). Predicting reference evapotranspiration based on hydro-climatic variables: comparison of different machine learning models. 68(7). <https://doi.org/10.1080/02626667.2023.2203824>.
5. Yao, W., & Li, L.. (2014). A New Regression Model: Modal Linear Regression. 41(3). <https://doi.org/10.1111/SJOS.12054>.

АНАЛІЗ І ПРОЕКТУВАННЯ СИСТЕМИ МОДЕЛЮВАННЯ ПРЕДМЕТНОЇ ОБЛАСТІ

О.О. Танько

магістрант

кафедри комп'ютерних наук та програмної інженерії

ПВНЗ "Європейський університет"

В.В. Демідов

старший викладач кафедри економіки, фінансів, обліку, математичних

та інформаційних дисциплін

Черкаської філії ПВНЗ "Європейський університет"

Важливим етапом підготовки до розробки інформаційної системи є аналіз та формулювання вимог до моделі, структури, реалізації та програмного продукту. Опис функціональних можливостей та обмежень, накладених на функціонування інформаційної системи, допоможе виявити конфлікти, проблеми, потреби та небажані моменти.

Вибір технології проектування варіюється між структурно-орієнтованою та об'єктно-орієнтованою технологіями проектування ІС.

Первинні вимоги допомагають зрозуміти команді що саме хоче і вимагає замовник, відобразити первинні вимоги можна за допомогою діаграми прецедентів.

Перед побудовою всіх діаграм вони повинні бути описані без використання сленгу та жаргонізмів для того щоб вся інформація була легка для розуміння замовником.

Детальні вимоги документують вимоги спеціально структурованої мови, використовуючи діаграми діяльності та схеми взаємодії. Вони деталізують основні вимоги [2].

На сьогодні існує два підходи до розробки ПЗ інформаційних систем, відмінність між ними зумовлена різними методами декомпозиції систем. Так структурний підхід який базується на принципі функціонального розкладання, в якому структура системи описується з точки зору підпорядкування функцій системи та того як передається інформація між функціональними елементами. Об'єктно-орієнтований підхід з використанням декомпозиції об'єктів описує структуру ІС з точки зору об'єктів та взаємозв'язків між ними, а також поведінки системи з точки зору обміну повідомленнями між об'єктами.

Суть структурного підходу розробки ПЗ інформаційних систем в тому, що вся розробка розкладається на автоматизовані окремі функції: тобто вся система спочатку розбивається на функціональні підсистеми, після чого ті поділяються на підфункції, вони поділяються на завдання і так далі до конкретних процедур. Також, ІС підтримує цілісність презентації, в цей момент всі компоненти взаємопов'язані, але вже при розробці, цілісність втрачається, адже при описі інформаційної взаємодії окремих компонентів з'являються проблеми.

Виділення двох основних принципів не означає, що інші принципи є другорядними, оскільки ігнорування будь-якого з них може призвести до непередбачуваних наслідків.

Структурний аналіз використовує в основному дві групи інструментів, щоб проілюструвати функції, що виконуються системою, і взаємозв'язок між даними.

Кожній групі засобів відповідають свої індивідуальні діаграми, найпоширенішими є наступні:

- SADT (Structured Analysis and Design Technique) моделі і відповідні функціональні діаграми;
- DFD (Data Flow Diagrams) діаграми потоків даних;
- ERD (Entity–Relationship Diagrams) діаграми «сутність-зв'язок».

Перелічені моделі разом, дадуть замовнику та всій команді опис інформаційної системи, будь вона вже реалізована і розроблена чи нещодавно розроблена.

Об'єктно-орієнтоване проектування програмного забезпечення зводиться насамперед до розробки моделі реальної системи, для вирішення завдання якої вона створюється.

Метод об'єктно-орієнтованого проектування засновано на наступних принципах:

- моделі побудови системи, як сукупності об'єктів абстрактного типу даних;
- модульній структурі програм;
- спадному проектуванні, використовуваному при виділенні об'єктів [1].

Об'єктно-орієнтований підхід до проектування використовує об'єкти, які містять власні коди та дані як будівельні блоки. На відміну від структурного проектування, де структура програм представляється деревом ієрархій, структура програм у об'єктно-орієнтованому підході представляється графом взаємодії об'єктів.

Основними переваги об'єктно-орієнтованого проектування є:

- активне використання абстракції предметної області;
- підвищення стабільності в представленні змін;
- існування різнопланових модельних поглядів;
- на базі модельних поглядів покращуються можливості для повторного використання;
- з'являється можливість управління масштабованістю.

На основі перелічених вище фактів для проектування розробленої системи була обрана технологія об'єктно-орієнтованого проектування. Це спростить і покращить розробку ІС.

Для моделювання домену використовуються різні технології візуалізації інформаційних потоків та їх обробники. Однією з таких технологій є діаграми

UML. Діаграма класів UML дозволить вам приблизно зрозуміти, як повинна працювати майбутня система.

Список використаних джерел:

1. T. DeMarco. (1997) The Deadline: A Novel About Project Management. Dorset House Publishing Co., New York.
2. A Guide to the Project Management Body of Knowledge (PMBOK Guide) – Third Edition USA, Project Management Institute – 2004. – 411 p.

ЗАСТОСУВАННЯ ГЕНЕТИЧНИХ АЛГОРИТМІВ В ЗАДАЧАХ ТРАНСПОРТНОЇ ЛОГІСТИКИ

В.С. Хорт

магістрант

М.Р. Костецький

*к.е.н. доцент кафедри економіки
ПВНЗ «Європейський університет»*

Генетичні алгоритми – це потужний інструмент для розв'язання складних проблем оптимізації і пошуку, що використовують принципи еволюції і натурального відбору. Ці методи отримали широке застосування в різних областях, включаючи машинне навчання, обробку сигналів, комп'ютерний дизайн і багато іншого.

Еволюційні процеси, які підтримують життя через адаптацію і розвиток, є основною концепцією, на яку спираються генетичні алгоритми як методи оптимізації. Центральними елементами еволюції є принципи випадкової мутації та генетичної рекомбінації, що стають фундаментальними основами для роботи генетичних алгоритмів.

Процес створення та використання генетичних алгоритмів (ГА) містить декілька ключових етапів:

1. **Ініціалізація:** На цьому етапі створюється початкова популяція можливих рішень (індивідів). Кожне рішення часто представляється у вигляді хромосоми - набору генів, які кодують деталі рішення.

2. **Оцінка:** Кожен індивід в популяції оцінюється за допомогою функції пристосованості, яка визначає, наскільки добре рішення вирішує поставлену задачу.

3. **Селекція:** На цьому етапі індивіди вибираються для участі у генетичних операціях на основі їх пристосованості. Часто використовуються тактики, які більш ймовірно вибирають індивідів з вищою пристосованістю.

4. **Кросовер (схрещування):** Вибрані індивіди комбінуються для створення нового покоління індивідів. Цей процес може бути дуже різним і залежить від конкретного ГА, але зазвичай він включає обмін генами між двома батьківськими хромосомами.

5. **Мутація:** Після кросоверу нові хромосоми можуть піддаватися мутації, яка випадковим чином змінює деякі з їх генів. Це допомагає зберегти різноманітність в популяції та запобігає застрягненню в локальних мінімумах.

6. **Ітерація:** Процес повторюється з новим поколінням індивідів, починаючи з оцінки.

Ці етапи продовжуються до тих пір, поки не буде досягнуто критерії зупинки, такі як вичерпання максимального числа поколінь або досягнення достатнього рівня пристосованості.

Однією з важливих областей застосування ГА є задачі оптимізації та планування в задачах транспортної логістики.

Транспортна логістика є важливою складовою сучасного економічного простору, що включає планування, координацію та контроль переміщення товарів та послуг від початку до кінця. Вона включає різні аспекти, включаючи управління запасами, складування, транспортування, а також координацію між різними учасниками ланцюга поставок.

Генетичні алгоритми (ГА) можуть виявитися корисними у цій сфері, особливо при вирішенні складних проблем оптимізації, таких як планування маршрутів доставки, оптимізація використання складського простору, розкладу, і так далі.

В роботі досліджено використання генетичних алгоритмів в транспортній логістиці. Розглянуто теоретичні аспекти ГА, їхні параметри та механізми, а також розроблено та впроваджено ГА для розв'язання конкретних задач в транспортній логістиці.

Транспортна логістика може бути представлена у вигляді послідовності етапів. Деякі з них можуть включати:

1. **Планування:** Цей етап включає в себе визначення стратегії логістики, вибір найефективніших маршрутів доставки, розробку графіків і термінів, та інше. За допомогою ГА можна оптимізувати цей процес, знаходячи найкращі маршрути та графіки.

2. **Складування:** Задачі, пов'язані із складуванням, можуть включати оптимальне розміщення товарів на складі, управління запасами, оптимізацію розміщення для швидкого доступу до популярних товарів, та інше. ГА можуть допомогти в розв'язанні цих задач, знаходячи оптимальні стратегії розміщення та управління запасами.

3. **Транспортування:** Тут ГА можуть бути використані для розробки оптимальних маршрутів доставки, що мінімізують витрати на паливо, час доставки, або інші критерії. Вони також можуть допомогти в плануванні розвантаження та завантаження транспортних засобів.

4. **Моніторинг і контроль:** На цьому етапі важливо відслідковувати виконання плану, виявляти та реагувати на відхилення. ГА можуть допомогти в розробці систем, які динамічно адаптуються до змін умов.

5. **Аналіз та вдосконалення:** Після виконання логістичних операцій необхідно проаналізувати результати, виявити можливості для вдосконалення та застосувати ці вдосконалення для покращення майбутніх операцій. ГА можуть допомогти в цьому процесі, використовуючи історичні дані для покращення стратегій планування та виконання.

Розглянуті генетичні алгоритми можуть бути застосовані на кожному з цих етапів для покращення загальної ефективності та продуктивності транспортної логістики.

Список використаних джерел

1. Frolovsky V., Pushkaryova G. Metal cutting motion optimization for NC-programs design, using genetic algorithms // Proc. of the 6th International Conference 3IA'2003 in Computer Graphics and Artificial Intelligence (May 2003). — Limoges (France), 2003. — P. 143–152.
2. Pashko, A., Oleshko, T., Biesiedina, S. Stochastic Algorithms for Optimization of the Path of Robotic Systems. Lecture Notes in Networks and Systems [this link is disabled](#), 2022, 463 LNNS, стр. 227–236.
3. Глибовець М.М. Основи комп'ютерних алгоритмів / М.М. Глибовець — К.: Вид.дім «КМ Академія», 2003. — 452 с.

ПИТАННЯ ЦИФРОВІЗАЦІЇ ЯК ВИКЛИК ТА ОДНОЧАСНО МАЙБУТНЄ УКРАЇНИ

В.В. Чубенко

магістрант

***факультету інформаційних систем та технологій,
ПВНЗ «Європейський університет»***

Незважаючи на хвилю реформ після Революції Гідності 2013-2014 років за прозорість, боротьбу з корупцією та покращення державних послуг насправді державне управління в Україні продовжує страждати через структурні недоліки належного управління, які також безпосередньо впливають на боротьбу з корупцією та доброчесністю. Цікавим фактом є те, що у 2022 році Україна посіла 116 місце із 180 у міжнародному рейтингу «Індекс сприйняття корупції» [1].

З часів незалежної України її державне управління демонструє дуже посередні показники із сильним дефіцитом якісно наданих державних послуг, відповідно сьогодні питання сприяння цифровізації на державному рівні у сучасному розвитку України все більше набирає своєї актуальності та нагальної потреби запроваджувати системні зміни. Адже відсутня якісна ІТ-інфраструктура, брак наявних людських ресурсів та фінансових коштів вимагають потужних та швидких змін в сучасному контексті задля відповідного реагування та потреби та зміни України в питаннях відбудови під час війни.

Питання цифровізації підіймається на різних майданчиках (таких як: н-д форум «Україна 30. Цифровізація» (2021 р.), форум «Цифрової трансформації» (2023 р.), форум «Цифрових громад» (2023 р.), тощо) задля привернення уваги української спільноти, органів місцевого самоврядування та українського уряду до проблем та викликів, які водночас є вектором для України на шляху її розвитку, адже питання розробки та використання нових відповідних цифрових рішень є основоположним для більшої прозорості дій українського уряду в управлінні задля задоволення потреб або ж досягнення значного прогресу щодо перехресних сфер боротьби з корупцією в рамках адміністративної реформи та децентралізації як частини впровадження Угоди про асоціацію з ЄС [2,3].

На сьогоднішній день багато міжнародних партнерів підтримують вже обраний курс України в питаннях сприяння цифровізації та надають потужну підтримку в рамках різних навчальних заходів, робочих консультацій, фахового обміну для інноваційних розробок різноманітних цифрових рішень, що мають на меті покращити або посилити спроможності урядових інституцій задля

досягнення високого рівня прозорості і довіри українського уряду та громадянського суспільства, представників приватного бізнесу, а також різних інвесторів та міжнародних партнерів із розвитку. З допомогою міжнародних партнерів сьогодні створюються нові послуги та рішення, все більше з'являється відкритий доступ до різноманітних джерел інформації для представників громадянського суспільства, бізнесу та міжнародних партнерів.

Яскравим прикладом є реалізація проєкту «Сервіс-портал «Дія», що реалізується Міністерством цифрової трансформації України, що має на меті до 2024 року досягти 100% послуг, які надаватиме держава онлайн. Даний портал як надавач державних онлайн-послуг демонструє постійний активний розвиток власних сервісів для кожного пересічного громадянина України, адже усі потрібні документи знаходяться в одному місці, в одному смартфоні. І цікавим фактом є те, що на розробку даного сервіс-порталу «Дія» державні кошти не витрачаються, адже даний портал створено у співпраці Міністерства цифрової трансформації за підтримки низки партнерів з розвитку як Проєкт USAID/UK aid «Прозорість та підзвітність у державному управлінні та послугах TAPAS», Програма EGAP, що фінансується Швейцарською агенцією з розвитку та співробітництва та реалізується Фондом Східна Європа та Innovabridge, Проєкт EU4DigitalUA, що є частиною підтримки України Європейським Союзом, та реалізується Академією електронного врядування (eGA, Естонія) і Міжнародним та іbero-американським фондом державного управління та політики (FIIAPP F.S.P., Іспанія), Проєкт DT4UA, що є частиною підтримки України Європейським Союзом, Проєкту USAID «ВзаємоДія!» (SACCI) [4].

Також Міністерство цифрової трансформації України крім успішного проєкту «Дія» активно реалізовує низку інших проєктів як «Дія. Бізнес», «Дія.City», «Е-резидентство», «Дія. Освіта» та інше.

Таким чином, можна стверджувати, що попри постійні виклики та постійні запити громадянського суспільства на покращення надання якісних адміністративних послуг український уряд продовжує активно впроваджувати процеси цифровізації та демонструвати якісні результати міжнародного рівня.

Список використаних джерел:

1. Індекс сприйняття корупції – 2022, <https://cpi.ti-ukraine.org/>
2. CDTO Annual Forum: підсумки та плани щодо цифровізації в Україні, <https://diia.gov.ua/>
3. Форум цифрових громад 2023, <https://eef.org.ua/forum-tsyfrovyh-gromad-2023/>
4. Сайт Міністерства цифрової трансформації України, <https://thedigital.gov.ua/>

МЕТОДИ І АЛГОРИТМИ СЕНТИМЕНТАЛЬНОГО АНАЛІЗУ

Л.М. Шевчук

магістрант ПВНЗ Європейський університет

В.М. Ярмолка

к.е.н. Європейський університет директор Рівненської філії

Обробка природної мови на сьогоднішній день включає багато складних задач таких як машинний переклад, класифікація текстів, виділення знань з

тексту тощо. Аналіз емоційного забарвлення тексту є одним з ключових прогресивних напрямків в сфері обробки мови.

Напрямок набирає свою популярність у комерційних сферах, засобах масової інформації; в соціальних мережах.

З появою форумів та різних типів соціальних мереж, споживачі мають у своєму розпорядженні великий майданчик для висловлення своїх думок, позитивного чи негативного ставлення щодо будь-яких новин, ідей, продуктів і сервісів, що надають компанії.

Методи, призначені для виявлення людських емоцій і думок по відношенню до об'єктів в тексті відносяться до *сентимент-аналізу (СА)* або іншими словами *аналізу тональності тексту* [1]. СА є одним із ключових напрямків в області NLP. Перші згадки по темі СА можна знайти у дослідженнях ШІ 70-80х років минулого століття, але набагато більший ажіотаж навколо цієї теми спостерігається протягом останніх років.

На сучасному ринку можна знайти різноманітну кількість практичних застосунків СА в залежності від методів і підходів до вилучення фактів, сутностей, сентименту; набору додаткового функціоналу, що полегшує аналіз; області застосування.

Одним із перспективних напрямків практичного застосування виділення тональності є аналіз споживацьких відгуків у віртуальному просторі, адже такі дані допомагають брендам покращуватися і оцінювати свій вплив на аудиторію. Отримання негативного ставлення може говорити про необхідність оновлення продукту або необхідність покращити обслуговування, змінити маркетингову стратегію.

Перелік емоційно забарвлених слів та фраз називається *тональним словником*. Більшість словників містять синоніми та антоніми для кожного слова, що полегшує пошук сентименту документу.

Але, звичайно цей метод також має певні вади. Перше це те що для його використання треба мати дані без помилок в словах, але наша предметна область це відгуки написані звичайними людьми, які не часто дотримуються правил, використовують сленгові вирази та скорочення.

В роботі досліджується підхід, що базується на новій архітектурі «Трансформер». Google опублікувала статтю [2] в якій розглядається ефективність механізмів «уваги» в нейронних мережах та була представлена нова архітектура «Трансформер».

В основі архітектури трансформерів лежать наступні ключові ідеї [2]:

1. Внутрішня увага – це механізм, який трансформери використовують для представлення окремих лексем документу та вивчення зв'язків між ними.

2. *Multihead attention*. Трансформери делегують завдання внутрішньої уваги декільком головам, тобто реалізована спільна обробка інформації з різних позицій. Це дозволяє їм ефективно працювати на великих наборах даних, використовуючи навчання без учителя.

3. Трансферне навчання: використання знань, отриманих з попереднього тренування та застосуванням їх до інших задач. Це досягається двоступеневим процесом: попередній пошук і подальше корегування.

Трансформер виконує лише невелику кількість кроків, що робить його більш привабливим інструментом у порівнянні з RNN та CNN,.

Таким чином, у роботі вирішуються поставлені задачі на основі моделей трансформерів.

Список використаних джерел:

1. Bo Pang and Lillian Lee (2008), "Opinion Mining and Sentiment Analysis", Foundations and Trends® in Information Retrieval: Vol. 2: No. 1–2, pp 1-135.
2. Attention Is All You Need / Ashish Vaswani, Noam Shazeer, Niki Parmar та ін.], 2017. – 15 с. Amazon Stats and Facts - Company Growth, User Trends, and More [Електронний ресурс] // I. Mitic, Fortunly– 2022. – Режим доступу до ресурсу: <https://fortunly.com/statistics/amazon-statistics/#gref>.
3. Text analytics [Електронний ресурс] //Azure Microsoft – 2022. – Режим доступу до ресурсу: <https://azure.microsoft.com/en-us/services/cognitive-services/text-analytics/#features>

RESILIENCE AND SECURITY: TECHNOLOGIES IN MITIGATING CYBER THREATS IN SMART HOME SYSTEMS IN UKRAINE

Yurchenko D.,

Parfenenko Yu.

*PhD Student, Associate Professor,
Sumy State University*

The development of smart home systems has transformed modern living, offering convenience and efficiency. However, the integration of these systems has also opened up new avenues for cyber threats. A comprehensive approach to cybersecurity in these systems must address a range of threats while being tailored to local conditions [1].

One of the primary cyber threats to smart home systems is data breaches. These systems often collect extensive personal information to optimize user experience, making them a lucrative target for cybercriminals. Implementing advanced encryption protocols is crucial in safeguarding this sensitive data. Encryption not only protects data during transmission but also secures it at rest, reducing the risk of unauthorized access.

Power outages in Ukraine add a layer of complexity to cybersecurity. These outages can lead to system vulnerabilities, particularly when the system reboots, making it susceptible to cyber-attacks. Integrating resilient power backup systems and surge protection technologies ensures that smart home systems remain operational and secure, even during outages. Another aspect of enhancing cybersecurity in smart home systems is the use of real-time monitoring. This involves constantly tracking system activity to detect any unusual behavior or data traffic, which could indicate a security breach. Early detection is key in preventing or minimizing the damage from cyber-attacks.

The application of machine learning algorithms and IoT technologies in smart home systems offers dual benefits [2]. Firstly, it enables the system to adapt and respond to the user's changing behavior, improving personalization and efficiency. More importantly, from a cybersecurity perspective, machine learning algorithms can

identify deviations from normal usage patterns, signaling potential security threats. This capability is particularly valuable in detecting sophisticated cyber-attacks that might not be immediately apparent.

In conclusion, securing smart home systems in challenging environments like Ukraine requires a multifaceted approach. By addressing these key areas, smart home systems can be fortified against a range of cyber threats, ensuring both their functionality and the security of user data.

References

1. Sauanova, K. et al. (2019). Development of a Model of Cyber Security Management for Automated Systems. *International Journal of Civil Engineering and Technology*, 10(03), 2019, pp. 454-463, Available at SSRN: <https://ssrn.com/abstract=3455849>
2. Alam Majumder, A.J., Veilleux, C.B., & Miller, J.D. (2020). A Cyber-Physical System to Detect IoT Security Threats of a Smart Home Heterogeneous Wireless Sensor Node. *IEEE Access*, 8, 205989-206002.

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА КІБЕРБЕЗПЕКА В ЗАБЕЗПЕЧЕННІ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

ТОМ II

Матеріали

*XXIX Міжнародної науково-практичної конференції
«Цифрова трансформація в економіці, менеджменті і бізнесі.
Проблеми науки, практики та освіти»
30 листопада 2023 р.*

до 32-річчя Європейського університету

Підписано до друку 05.03.2024. Формат 60x84¹/₁₆.
Папір офсетний. Гарнітура Times New Roman.
Ум. друк. арк. 4,65. Зам. № 7.

Друк: поліграфкомбінат Європейського університету.
03115, Україна, Київ-115, вул. Депутатська, 15/17.
Тел.: (+38044) 503-33-96

Реєстраційне свідоцтво ДК №3833 від 14.07.2010 р.