

Київський столичний університет імені Бориса Грінченка
Факультет інформаційних технологій та математики
Кафедра комп'ютерних наук

Затверджено на засіданні кафедри
комп'ютерних наук
протокол №10 від 06.11.2024

Студентський науковий пошук - 2024

**Збірник тез
студентської наукової конференції**

7 листопада 2024
м. Київ

Київ – 2024

ЗАХИСТ АЛГОРИТМУ ДІФФІ-ГЕЛЬМАНА ВІД АТАКИ ПО БОКОВОМУ КАНАЛУ

Абрамов Сергій Вадимович

*аспірант групи ІБДдф-21-4.0д, спеціальності 125 "Кібербезпека",
Київського столичного університету імені Бориса Грінченка,
науковий керівник – к.т.н., доц.Соколов В.Ю.*

Асиметричний алгоритм шифрування Діффі-Гельмана створений у 1976 році [1] для согласування ключів використовуючи відкрити канали зв'язку. Після появи повідомлень про створення незабаром квантових комп'ютерів, які легко зламують деякі шифри, виникла постквантова криптографія (PQC), що вивчає квантово-стійкі криптографічні алгоритми. Найбільш перспективним напрямом PQC є використання алгоритму CSIDH (Commutative Supersingular isogeny Diffie-Hellman key exchange) на ізогеніях еліптичних кривих [2, 3]. Пізніше було запропоновано використовувати в алгоритмах CSIDH еліптичні криві у формі Едвардса [2].

Одним з недоліків алгоритмів CSIDH є схильність до атаки по стороннім каналам [3]. Атака сторонніми каналами використовує непряму інформацію про фізичні процеси в пристроях. З параметрів процесів використовують час виконання операції на ґрунті спостереження за споживаною потужністю, електромагнітним випромінюванням тощо. В оригінальному алгоритмі усі ізогенії обчислюються по черзі. Атака ґрунтується на припущенні, що різні операції виконуються у пристрої за різний час, залежно від поданих вхідних даних. Таким чином, вимірюючи час обчислень та проводячи статистичний аналіз даних, можна отримати повну інформацію про секретний ключ. Особливо схильні до атак за часом алгоритми, що використовують множення, розподіл, зведення в ступінь і бітові операції над довільним числом біт [4].

Суть даної атаки полягає в тому, що крипто аналітик з високою точністю вимірює параметри (наприклад, енергоспоживання) пристрою і таким чином отримує інформацію про виконувані у пристрої операції. Під час аналізу цієї інформації визначаються секретні дані.

Щоб криптоаналітик не зміг провести атаку за часом виконання, всі етапи шифрування в пристрої повинні виконуватися за однаковий час. Наприклад, використовується метод вирівнювання часу виконання операцій. У зв'язку з цим у більшості статей з цієї теми [5] розглядаються різні варіанти «constant time CSIDH», в яких секретна кількість кроків по ізогенії нарощуються до верхньої межі фіктивними ланцюжками ізогеній. Такий захист досягається значною надмірністю та уповільненням алгоритму в середньому вдвічі.

У [6] пропонується альтернативний метод захисту від атаки бокового каналу. Для алгоритмів на нециклічних парах скручених кривих Едвардса пропонується метод рандомізації шляху по ізогенним ланцюжкам класів нециклічних кривих Едвардса. В оригінальному алгоритмі CSIDH на еліптичних кривих кроки по ізогеніям виконуються по черзі у межах кожної ізогенії. Пропонується метод, у якому кроки виконуються не по черзі, а у

випадковому порядку, а вибір класу кривої теж здійснюється випадково. Враховується, що кроки по ізогеніях є комутативними і їх можна виконувати у будь-якому порядку.

При цьому криптоаналітик не може чітко визначити по якій ізогенії здійснюється крок. У роботі [3] рекомендується для надійності використовувати кількість ізогеній 74, тоді ймовірність успішної роботи криптоаналітика дорівнює 2^{-74}

Необхідно враховувати що, в алгоритмі CSIDH вже закладений природний захист від подібної атаки тим, що аналітик може вимірювати довжину кроку, але не може знати напрямок, тобто криву по якій здійснюється рух. В результаті при рекомендованій в [3] кількості ізогеній 74 і кількості кроків по кожній з них 3, маємо середню довжину шляху по графу $3 \cdot 74 = 222$. Тоді загальна ймовірність успіху аналітика навіть в умовах безпомилково знайдених ізогеній дорівнює p^{-222} де p – ймовірність безпомилкового визначення ступеня ізогенії аналітиком на одному кроці протоколу. Тоді, навіть при ймовірності визначення кожного кроку $p = 1/2$ ймовірність успіху при визначенні секретних даних буде $p = 2^{-222}$.

Враховуючи природний захист і рандомізацію маємо ймовірність успіху криптоаналітика 2^{-296} . Що значно нижче за рівень безпеки 2^{-128}

ДЖЕРЕЛА

1. W. Diffie and M.E. Hellman, "New Directions in Cryptography," IEEE Transactions on Information Theory, IT-22, n. 6, Nov 1976, pp. 644-654.
2. Bernstein D.J., Lange T. Faster Addition and Doubling on Elliptic Curves // Advances in Cryptology—ASIACRYPT'2007 (Proc. 13th Int. Conf. On the Theory and Application of Cryptology and Information Security. Kuching, Malaysia. December 2–6, 2007). Lect. Notes Comp. Sci. V. 4833. Berlin: Springer, 2007. PP. 29–50.
3. Castryck, W., Lange, T., Martindale, C., Panny, L., Renes, J.: CSIDH: An efficient post-quantum commutative group action. In: Peyrin, T., Galbraith, S. (eds.) Advances in Cryptology { ASIACRYPT 2018. pp. 395–427. Springer International Publishing, Cham (2018).
4. Брюс Шнайер. Прикладна криптографія. Протоколи, алгоритми, ісходні тексти на языке Си Applied Cryptography. Protocols, Algorithms, and Source Code in C.—М.: Триумф, 2002.— 816 с.—3000 экз.—ISBN 5-89392-055-
5. H.Onuki, Y.Aikawa, T.Yamazaki, T.Takagi. A Faster Constant-time Algorithm of CSIDH keeping Two Points. ASIACRYPT, 2020.
6. Bessalov, A. ., Kovalchuk, L., Abramov, S. (2022). Рандомізація алгоритму CSIDH на квадратичних та скручених кривих Едвардса. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(17), 128–144. <https://doi.org/10.28925/2663-4023.2022.17.128144>

ВЕБ-БРАУЗЕРНІ РОЗШИРЕННЯ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ WEBASSEMBLY: ПОТЕНЦІАЛ ТА ВИКЛИКИ

Андрієвич Дмитро Юрійович
студент групи ІАСм -1-23-І.4д,

*Київського столичного університету імені Бориса Грінченка,
науковий керівник – д.т.н., проф. Бушма О.В.*

У сучасному світі веб-технологій спостерігається стрімкий розвиток, що відкриває нові можливості для створення потужних та ефективних веб-застосунків. Особливу увагу привертає технологія WebAssembly (WASM), яка дозволяє виконувати код у браузері зі швидкістю близькою до нативної [1]. Це відкриває нові горизонти для розробки веб-браузерних розширень, які можуть значно розширити функціональний потенціал браузерів та практичні можливості користувачів.

Мета роботи – визначити можливості та виклики, пов'язані з використанням WebAssembly для розробки веб-розширень. В ході розвідки не лише теоретично обґрунтовуються переваги цієї технології, але й практично визначається доцільність її застосування на прикладі розробки реального веб-розширення.

WebAssembly є бінарним форматом інструкцій, розроблених для ефективного виконання коду у веб-середовищі [1]. Для дослідження проблем та викликів, пов'язаних з використанням WebAssembly, проведено практичне дослідження, у ході якого розроблено застосунок у вигляді веб-розширення, що дозволяє планувати задачі. При цьому використовувався Rust та фреймворк Leptos для створення користувацького інтерфейсу, а також WebAssembly для компіляції та виконання коду в браузері. З функціональної точки зору розширення включає базовий набір функцій для управління задачами, зокрема, створення, редагування, видалення та сортування задач. Особливу увагу було приділено безпеці, а саме: було впроваджено систему автентифікації та шифрування даних для забезпечення конфіденційності користувацької інформації.

Дослідження показало, що використання WASM має ряд суттєвих переваг над розробкою з використанням лише JavaScript:

1. **Висока продуктивність** – WASM-код виконується значно швидше, ніж JavaScript, що особливо важливо для розширень, які містять складні обчислення або обробку даних.
2. **Безпека** – виконання коду в ізольованому середовищі [2] підвищує загальний рівень безпеки розширень, що є критичним фактором для користувачів.
3. **Оптимізація ресурсів** – WASM-модулі зазвичай мають менший розмір порівняно з еквівалентним JavaScript-кодом, що сприяє більш швидкому завантаженню та покращеному досвіду користувачів.

Незважаючи на значний потенціал, було виявлено ряд викликів, пов'язаних з використанням WebAssembly для розробки веб-розширень:

1. **Обмежений доступ до API браузера** – WASM-модулі мають обмежений прямий доступ до функцій браузера, що вимагає додаткової інтеграції з JavaScript. Це, в свою чергу, вимагає більшої залученості з боку розробників та збільшує витрати часу на розробку.

2. **Труднощі з налагодженням** – інструменти для налагодження WASM-коду все ще перебувають на ранніх стадіях розвитку, що може ускладнювати процес розробки.

3. **Складність розробки** – розробка з використанням WebAssembly вимагає від розробників додаткових зусиль та навчання, особливо якщо вони раніше працювали лише з JavaScript.

Важливим наступним етапом дослідження є порівняльний аналіз швидкодії розробленого WASM-розширення з аналогічними розширеннями, створеними з використанням JavaScript. Це дозволить оцінити реальні переваги використання WebAssembly, особливо при створенні високопродуктивних веб-розширень [3].

Було визначено, що WebAssembly має значний потенціал для розробки високопродуктивних веб-розширень. Проте важливо звернути увагу на певні проблеми, які було виявлено на етапі розробки: недостатня кількість документації та відсутність базового функціоналу, наявного у відповідних JavaScript фреймворках. Ці проблеми потребують додаткового дослідження та покращення відповідних інструментів для полегшення процесу створення WASM-розширень з використанням Rust.

Подальші дослідження технології WebAssembly дозволять розширити її можливості, полегшити розробку веб-розширень та вирішити наразі існуючі проблеми. Поява зручних інструментів для розробників неминуче прискорить загальну інтеграцію WebAssembly в множину технологій створення потужних веб-застосунків.

ДЖЕРЕЛА

1. WebAssembly Concepts. URL: <https://developer.mozilla.org/en-US/docs/WebAssembly/Concepts> - 2024.
2. D. Lehmann, J. Kinder, M. Pradel. Everything old is new again: Binary security of WebAssembly. – USENIX Association, 2020.
3. A. Jangda, B. Powers, E. D. Berger, A. Guha. Not So Fast: Analyzing the Performance of WebAssembly vs. Native Code. – USENIX Association, 2019.

ІГРОВІ МЕХАНІКИ У БАГАТОКОРИСТУВАЦЬКИХ ОНЛАЙН-ІГРАХ

Бойко Максим Олександрович
студент групи ІАСм -1-23-1.4д,

*Київського столичного університету імені Бориса Грінченка,
науковий керівник – д.т.н., проф. Бушма О.В.*

На сьогодні багатокористувацькі онлайн-ігри (БОІ) є одним з найбільш популярних видів цифрових розваг, охоплюючи мільйони гравців у всьому світі. З огляду на зростаючу важливість цифрових технологій, роль ігор не обмежується лише сферою розваг. Вони також мають значний вплив на соціальну взаємодію, комунікацію та навіть навчання. Ігрові механіки, що використовуються в БОІ, сприяють не лише підвищенню залученості гравців, а й впливають на структуру соціальної взаємодії в грі. Ці механіки спрямовані на підтримку інтересу до гри, формування та зміцнення спільнот, а також створення конкурентних чи кооперативних відносин між гравцями.

Проте, багато аспектів впливу ігрових механік на гравців, особливо в контексті БОІ, залишаються недостатньо вивченими. Існуючі дослідження часто зосереджені на окремих аспектах, таких як психологічний вплив гри або рольовий розподіл у команді, але комплексний аналіз, що охоплює як соціальні, так і технічні аспекти, є рідкістю. Відсутність таких напрацювань утруднює формування стратегії розвитку ігрових механік, що могли б сприяти як довготривалому зацікавленню гравців, так і їх позитивній взаємодії у грі. Дослідження ігрових механік у багатокористувацьких онлайн-іграх є актуальним, оскільки воно дозволить виявити нові можливості для оптимізації гравців і створення сприятливого середовища для спільного проведення часу.

Метою дослідження є визначити та обґрунтувати використання ігрових механік, що сприяють підвищенню залученості гравців і підтримують стабільну позитивну соціальну взаємодію в багатокористувацьких онлайн-іграх.

Об'єкт дослідження – багатокористувацькі онлайн-ігри як явище цифрових технологій та соціальної взаємодії.

Предмет дослідження – ігрові механіки, що використовуються в багатокористувацьких онлайн-іграх для підтримання залученості гравців та сприяння соціальній взаємодії.

Для досягнення поставленої мети необхідно вирішити такі завдання:

1. Визначити основні ігрові механіки у багатокористувацьких онлайн-іграх на прикладі Counter-Strike, Path of Exile, World of Warcraft, PUBG: BATTLEGROUNDS, Stardew Valley та Minecraft.
2. Сформулювати порівняльний аналіз впливу ігрових механік цих ігор на залучення та утримання гравців.
3. Дослідити соціальні аспекти взаємодії гравців у зазначених іграх та визначити роль різних ігрових механік у формуванні спільнот.
4. Визначити економічні моделі цих ігор та визначити механіки, які стимулюють внутрішньоігрову економіку та обмін ресурсами між гравцями.

5. Провести детальний розбір ігрових механік Path of Exile, включно з аналізом її впливу на поведінку гравців, розвиток спільноти та внутрішньої ігрової економіки.

6. На основі проведеного аналізу сформулювати рекомендації щодо розробки ігрових механік, які сприяють залученню, утриманню та активній взаємодії гравців у багатокористувацьких онлайн-іграх.

Основний акцент зроблено на детальному розборі ігрових механік багатокористувацької онлайн-гри Path of Exile (PoE), яка є однією з найскладніших та найглибших за структурою БОІ. Вибір цієї гри для аналізу обґрунтовано унікальністю механік, які залучають гравців та утримують їхню зацікавленість завдяки широким можливостям для персоналізації, стратегічного мислення та колективної взаємодії. У PoE наявні такі унікальні аспекти, як дерево пасивних навичок, система дорогоцінних каменів для навичок, механіка ліг (сезонних подій) і торговельна система.

У ході дослідження здійснено комплексний аналіз ігрових механік у багатокористувацьких онлайн-іграх та визначено найефективніші з них для підтримки інтересу до гри й позитивної соціальної взаємодії. Отримані результати дозволять обґрунтувати рекомендації для розробників ігор щодо вибору та вдосконалення ігрових механік, які допоможуть створювати більш захопливі та соціально значущі онлайн-ігри.

ДЖЕРЕЛА

1. Dive into the world of MSC (music and sound creation) games at tellmyplay.com – unleash your musical talents and create melodies that resonate. *Dive into the World of MSC (Music and Sound Creation) Games at TellMyPlay.com – Unleash Your Musical Talents and Create Melodies that Resonate.* URL: <https://www.tellmyplay.com/> (date of access: 30.10.2024).

2. Ducheneaut N. The social side of gaming: a study of interaction patterns in a massively multiplayer online game. *researchgate*. URL: https://www.researchgate.net/publication/220878888_The_Social_Side_of_Gaming_A_Study_of_Interaction_Patterns_in_a_Massively_Multiplayer_Online_Game (date of access: 30.10.2024).

3. Frontiers | massively multiplayer online games and well-being: a systematic literature review. *Frontiers*. URL: <https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2021.698799/full> (date of access: 30.10.2024).

4. Game studies - defining game mechanics. *Game Studies - Issue 2403, 2024*. URL: <https://gamestudies.org/0802/articles/sicart> (date of access: 30.10.2024).

5. Mind studios. *Custom Software Development Company - Mind Studios - Mind Studios*. URL: <https://themindstudios.com/> (date of access: 30.10.2024).

6. Polydin studio | game art studio. *Polydin*. URL: <https://polydin.com/> (date of access: 30.10.2024).

7. The complete guide to video game design. *Video Game Design and Development*. URL: <https://www.gamedesigning.org/> (date of access: 30.10.2024).

ТЕХНОЛОГІЇ МОНІТОРИНГУ ЯКОСТІ СНУ

Великодний Артем Русланович

студент групи ІАСм -1-23-І.4д,

Київського столичного університету імені Бориса Грінченка,

науковий керівник – д.т.н., проф. Бушма О.В.

В умовах сучасного суспільства якість сну є важливим фактором загального здоров'я та продуктивності людини. Дослідження показують, що порушення сну можуть призводити до серйозних проблем, зокрема, збільшення ризику серцево-судинних та ендокринних захворювань. У зв'язку з цим зростає інтерес до інноваційних методів контролю та моніторингу якості сну за допомогою мобільних додатків та смарт-пристроїв.

Метою роботи є визначення технологій моніторингу якості сну для мобільних додатків, які мають найкращих комплекс функціональних параметрів.

Основою наукового підходу до вимірювання якості сну є полісомнографія (ПСГ) – золотий стандарт для оцінки сну. Однак проведення ПСГ у лабораторних умовах є дорогим, складним та незручним для щоденного застосування. Альтернативні технології, такі як акселерометри, фотооптичні сенсори, а також сучасні біорадарні системи, роблять контроль сну доступнішим. Біорадар, наприклад, може виявляти життєво важливі показники людини, передаючи електромагнітні хвилі крізь неметалеві перешкоди, що дозволяє здійснювати моніторинг без фізичного контакту [1].

Основні параметри, які досліджуються при аналізі якості сну, включають тривалість сну, стадії сну (глибокий, REM, легкий), рухову активність під час сну, частоту серцевих скорочень та рівень кисню в крові. Багато додатків також відстежують зовнішні фактори, такі як температура повітря, рівень шуму та навіть цикли дихання. Сучасні мобільні додатки для моніторингу сну інтегруються із системами розумного дому. Наприклад, деякі додатки можуть синхронізуватися з автоматичними жалюзі, які відкриваються вранці, щоб природним світлом допомогти користувачеві прокинутися, або регулюють температуру у спальні залежно від стадії сну користувача [2].

Сьогодні існує широкий спектр мобільних додатків для моніторингу сну, таких як *Sleep Cycle*, *Pillow*, *Headspace* та *Calm*. Ці програми використовують акселерометри смартфонів або фітнес-трекери для збору даних про рухи тіла під час сну. Вони можуть синхронізуватися з розумними годинниками або іншими пристроями для більш точного вимірювання, забезпечуючи інтеграцію з календарями та системами штучного інтелекту для аналізу великих обсягів даних. Наприклад, деякі системи вивчають тривалість та якість сну протягом кількох тижнів, формуючи індивідуальні рекомендації щодо покращення гігієни сну. Це може включати поради щодо встановлення регулярного часу відходу до сну або зниження рівня стресу перед сном.

Розробка таких додатків включає використання сучасних фреймворків, таких як *React Native*, що дозволяє створювати додатки одночасно для iOS та Android. Для збору та аналізу даних застосовуються машинне навчання та

алгоритми обробки сигналів. Інтерфейси оптимізуються для зручного користування, оскільки простота використання є ключовою для залучення користувачів [3]. Окрім того, мобільні додатки активно інтегрують біологічний зворотний зв'язок (biofeedback), що дозволяє користувачам самостійно регулювати свої фізіологічні параметри, наприклад, через дихальні вправи або медитацію, що сприяє розслабленню перед сном.

Мобільні додатки для моніторингу сну вже зараз значно впливають на медицину, надаючи як пацієнтам, так і лікарям нові можливості для покращення якості життя та персоналізації лікування. Завдяки цим технологіям можливий безперервний контроль та аналіз сну, що сприяє профілактиці серйозних захворювань та знижує навантаження на медичні установи.

Індустрія мобільних додатків для моніторингу сну постійно розвивається, і в майбутньому очікується впровадження нових технологій, які покращать точність та розширять функціональні можливості таких додатків. Серед перспектив — використання штучного інтелекту для передбачення порушень сну та розробка алгоритмів, які будуть здатні аналізувати величезні обсяги даних, щоб надавати більш індивідуальні рекомендації. Також планується інтеграція з іншими медичними пристроями та системами охорони здоров'я для створення повноцінних екосистем моніторингу здоров'я. Окремо варто згадати потенціал у сфері профілактики розладів сну: технології машинного навчання зможуть передбачати ризики розвитку безсоння чи обструктивного апное сну, допомагаючи запобігати цим станам заздалегідь.

Додатки також можуть інтегруватися з іншими розумними системами для поліпшення умов сну, такими як автоматичне налаштування температури, освітлення або навіть створення індивідуальних звукових середовищ для релаксації. Такі можливості відкривають нові горизонти для індустрії цифрової медицини, роблячи моніторинг сну все більш персоналізованим та ефективним.

ДЖЕРЕЛА

1. Іванова Я. О., Федорін І. В., Вдовиченко О. В. Огляд сучасних технологій для діагностики якості сну // Біомедична інженерія і технологія. 2021. № 6. С. 1–10. URL: <https://ela.kpi.ua/server/api/core/bitstreams/5ffa0377-5888-44e9-a624-b0cc5b18d67f/content>
2. Як мобільні додатки трансформують галузь охорони здоров'я? Stfalcon. URL: <https://stfalcon.com/uk/blog/post/How-Mobile-Apps-Are-Transforming-the-Healthcare-Industry>
3. Інновації в електроніці та медицині: мобільні програми для моніторингу стану здоров'я. Mobilniki.by. URL: <https://mobilniki.by/innovatsii-v-elektronitsi-ta-meditsini-mobilni-programi-dlya-monitoringu-stanu-zdorov-ya.html>

ПОРІВНЯННЯ МОЖЛИВОСТЕЙ ЗАСТОСУВАННЯ CODEGPT ТА GITHUB COPILOT

Горбачевський Максим Геннадійович

студент групи ІАСм -1-23-1.4д,

*Київського столичного університету імені Бориса Грінченка,
науковий керівник – к.т.н. Яскевич В.О.*

Сучасні інструменти автоматизації написання коду, такі як CodeGPT [1] та GitHub Copilot [2], спрямовані на спрощення процесу розробки програмного забезпечення, але кожен з них має унікальні особливості та різні сфери застосування. Обидва рішення розроблені на базі моделей штучного інтелекту, але мають свої сильні сторони й обмеження, які впливають на їх ефективність у різних завданнях.

CodeGPT, створений на основі моделей GPT від OpenAI, інтегрується в середовища розробки, такі як Visual Studio Code, IDE від JetBrains тощо і пропонує широкі можливості. Його функціонал охоплює не тільки автоматичне заповнення коду, але й рефакторинг, надання відповідей на запитання з програмування, а також генерацію документації. CodeGPT здатний допомагати з більш комплексними завданнями, оскільки окрім генерації коду надає текстові пояснення й пропонує приклади, що можуть бути корисними для розробників, які бажають розібратися в алгоритмах або функціональності певного фрагмента коду.

GitHub Copilot, натомість, створений GitHub у співпраці з OpenAI та базується на моделі Codex, спеціально оптимізованій для програмування. Цей інструмент має вузьку спеціалізацію: його основне завдання – швидке автозаповнення коду на основі наданого контексту, що дозволяє значно прискорити написання шаблонного коду й базових функцій. Він прогнозує наступний рядок, аналізуючи написане, і зручний для стандартних завдань, коли потрібна швидкість та постійний робочий потік без глибоких пояснень. Інтеграція з платформою GitHub додає Copilot значної переваги в середовищах командної роботи, де необхідно злагоджено координувати дії розробників.

При порівнянні обох інструментів можна відзначити, що CodeGPT надає ширші можливості щодо відповідей на запити. Він здатен генерувати докладні текстові пояснення до коду, підтримує більшу гнучкість у розв'язанні нестандартних завдань, а також забезпечує користувачеві більший рівень взаємодії. GitHub Copilot, хоча й може передбачати певний контекст, більше підходить для виконання швидких, передбачуваних завдань з генерацією коду. Завдяки спеціалізації на автодоповненні він забезпечує плавний і швидкий робочий процес, але його функціональність обмежується відсутністю детальних пояснень.

Основною відмінністю між ними є рівень контекстності: Copilot більш орієнтований на швидке автозаповнення і тому надає рекомендації на основі лише наявного контексту коду, тоді як CodeGPT підходить для більш загальних запитів, глибокого аналізу та детальних пояснень. CodeGPT може вирішувати

складніші завдання з програмування, надаючи інструкції та допомагаючи розробникам зрозуміти концепцію, у той час як Copilot призначений для швидкої генерації шаблонного коду, що значно економить час у простіших проєктах.

Використання кожного з інструментів залежить від поставлених завдань. CodeGPT краще підходить для глибоких досліджень, отримання пояснень до коду, а також написання документації. Розробникам, яким потрібно вирішувати складніші задачі з програмування та отримувати структуровані відповіді або пояснення до коду, варто використовувати саме CodeGPT. З іншого боку, GitHub Copilot буде ідеальним вибором для розробників, які потребують швидкого написання коду та підтримки постійного потоку в проєктах, що вимагають швидких ітерацій.

ДЖЕРЕЛА

1. CodeGPT [Електронний ресурс] – Режим доступу до ресурсу: <https://codegpt.co/>
2. GitHub Copilot [Електронний ресурс] – Режим доступу до ресурсу: <https://github.com/features/copilot>

СТВОРЕННЯ ТА ВИКОРИСТАННЯ МОБІЛЬНОГО WEB-ДОДАТКУ ДЛЯ МОНІТОРИНГУ ОСНОВНИХ ПАРАМЕТРІВ ФУНКЦІОНУВАННЯ МАГАЗИНУ СПОРТТОВАРІВ

Грабовський Єгор Романович
студент групи ІАСм -1-23-1.4д,

*Київського столичного університету імені Бориса Грінченка,
науковий керівник – к.т.н., доц. Абрамов В.О.*

Актуальність дослідження полягає в необхідності забезпечення ефективного управління магазином спортивних товарів через оперативний моніторинг ключових показників його функціонування. Мобільний web-додаток, розроблений для цих цілей, забезпечує доступ до актуальної інформації, що дозволяє приймати обґрунтовані управлінські рішення в реальному часі. Метою дослідження є створення додатку, який дозволить моніторити продажі, залишки товарів, відвідуваність магазину та ефективність маркетингових акцій, сприяючи покращенню процесу прийняття управлінських рішень. Для досягнення цієї мети були поставлені наступні завдання: аналіз вимог до системи моніторингу, розробка архітектури мобільного web-додатку, реалізація функціоналу, тестування додатку в реальних умовах експлуатації та надання рекомендацій щодо його впровадження і подальшого розвитку.

Об'єктом дослідження є бізнес-процеси управління магазином спортивних товарів, а предметом — інформаційні технології для моніторингу основних параметрів функціонування магазину. Методологія дослідження включає системний аналіз, об'єктно-орієнтоване проектування, моделювання

бізнес-процесів, тестування програмного забезпечення та аналіз результатів. Наукова новизна роботи полягає у розробці унікального мобільного web-додатку, що дозволяє в режимі реального часу отримувати доступ до ключових даних магазину. Практичне значення роботи полягає в можливості використання додатку не лише для спортивних магазинів, але й для інших рітейлових мереж, які прагнуть підвищити ефективність управління.

У ході дослідження було створено мобільний web-додаток, що успішно протестовано в умовах реальної експлуатації. Результати показали, що додаток має високу зручність використання та ефективність у відстеженні ключових показників. Використання такого додатку сприяє підвищенню ефективності управлінських рішень та оптимізації бізнес-процесів магазину. Таким чином, розробка та впровадження мобільного web-додатку є важливим кроком для автоматизації управлінських процесів і покращення функціонування магазинів спортивних товарів [5].

Проект присвячений розробці та впровадженню мобільного web-додатку, що дозволяє відстежувати ключові параметри функціонування магазину спорттоварів у режимі реального часу. Основною метою є оптимізація управління бізнес-процесами шляхом впровадження цифрових рішень, які забезпечать швидкий доступ до інформації та зручність користування. В умовах зростаючої конкуренції у роздрібній торгівлі, особливо у сфері продажу спортивних товарів, важливо забезпечити ефективний контроль за діяльністю магазину та своєчасно реагувати на зміну попиту та ринкових тенденцій [1].

Додаток має забезпечити можливість для менеджменту переглядати інформацію про обсяги продажів, рівень залишків товарів на складі, поточні знижки та акції, а також інші критично важливі показники для ефективної роботи магазину. Функціонал передбачає інтеграцію з існуючими базами даних та автоматизованими системами управління, що дозволить об'єднати всю інформацію у єдину інформаційну панель для зручності користувача. Крім того, передбачена можливість налаштування персональних повідомлень та сповіщень щодо змін ключових показників, таких як недостатня кількість товару або досягнення цільових обсягів продажу [2].

У розробці мобільного додатку було використано сучасні технології програмування та розробки web-інтерфейсів, зокрема, JavaScript, HTML, CSS, а також backend-технології для обробки даних у реальному часі. Особливу увагу було приділено інтерфейсу користувача, щоб забезпечити максимальну зручність і доступність для різних категорій працівників. Інтерфейс додатку є інтуїтивно зрозумілим, що дозволяє швидко навчитися його використовувати, навіть якщо користувач має мінімальний досвід у роботі з мобільними додатками [3].

Впровадження мобільного додатку сприятиме підвищенню продуктивності роботи магазину, зниженню операційних витрат, а також дозволить ефективніше управляти залишками товарів, що в свою чергу позитивно вплине на рівень задоволеності клієнтів [4].

ДЖЕРЕЛА

1. Козловський, О. М. "Розробка мобільних додатків: теорія та практика". Київ: Видавничий дім "Студія", 2019.
2. Лисенко, І. В. "Мобільні технології в сучасному бізнесі". Львів: Видавництво ЛНУ, 2020.
3. Петров, А. С., Шевченко, М. Г. "Основи програмування мобільних додатків". Харків: Фактор, 2021.
4. Кравчук, С. О. "Управління інформаційними системами в бізнесі". Чернівці: ЧНУ, 2018.
5. Ткаченко, П. В. "Технології веб-розробки та їх застосування у сфері рітейлу". Одеса: ОНУ, 2021.

ВИКОНАННЯ ПРОЄКТІВ ЯК ІНСТРУМЕНТ МАТЕМАТИЧНОГО МОДЕЛЮВАННЯ

Груздьева Катерина Ігорівна

студентка групи Мам-1-23-1.4д,

Київського столичного університету імені Бориса Грінченка,

науковий керівник – к..ф-м.н., доц. Астаф'єва М.М.

Через тривалі перерви у навчанні, спричинені пандемією, повномасштабним вторгненням та блекаутами, навчальні досягнення з математики здобувачів освіти помітно знизилися [2]. Тому є необхідним пошук ефективних підходів до навчання, здатних підвищити рівень математичної компетентності учнів. Одним із таких підходів є використання математичного моделювання як педагогічної технології. Проте математичне моделювання в шкільній практиці поки що відіграє другорядну роль. Незважаючи на те, що кількість задач шкільної математики, які потребують моделювання, за останні роки помітно зросла, вони, ці задачі, здебільшого розраховані на використання готових моделей, їх умови завчасно ідеалізовані, не потребують відбору суттєвих параметрів тощо. Через свою «нежиттєвість» вони не зацікавлюють учнів. На нашу думку цей недолік може бути частково подоланий через виконання учнями проєктів, спрямованих на розв'язання (з допомогою математичного моделювання) життєво важливих для них самих проблем.

Ми перевірили цю та інші гіпотези [1] у 8 класах Ліцею №129 Дніпровського району міста Києва та отримали позитивні результати.

Ідеться, зокрема, про участь восьмикласників у міждисциплінарному проєкті «Збережемо навколишнє середовище разом». «Математики» в цьому проєкті досліджували об'єми використання води вдома та шляхи оптимізації споживання. Метою даного проєкту було формування в здобувачів освіти математичної компетентності шляхом розв'язання реальної життєвої задачі, підвищення зацікавленості у вивченні математики, розвиток аналітичних та критичних навичок.

Реалізація проєкту здійснювалася в такі етапи.

Дослідницький (збір даних про споживання води кожним членом сім'ї чи побутовим приладом, ознайомлення з поняттями «витрати», «економія», «раціональне використання»; *мета* – розвиток навичок дослідження та збору інформації, формування екологічної свідомості).

Аналіз та систематизація отриманих результатів (структурування зібраної інформації; *мета* – формування аналітичної компетентності, здатності працювати з великою кількістю інформації, виявляти закономірності, розвиток критичного мислення).

Математичне моделювання (створення і аналіз математичної моделі для обчислення середньомісячного споживання води; *мета* – розвиток компетенції математичного моделювання, здатності застосовувати математичні знання на практиці, обчислювати, прогнозувати результати досліджень).

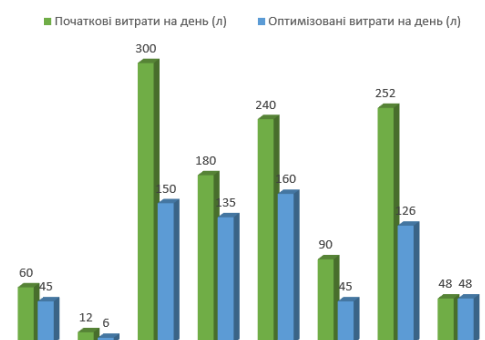
Оптимізація кількості водних витрат (розробка рекомендацій та плану дій щодо заощадження води; *мета* – стимулювання творчого підходу до вирішення проблем, здатності обирати оптимальне в даних умовах рішення із кількох можливих, формування екологічної компетентності, розвиток відповідального ставлення до природних ресурсів).

Презентація отриманих результатів (презентація та захист проєкту; *мета* – формування комунікативних навичок, розвиток здатності аргументувати).

Важливо зазначити, що учні на власному досвіді пересвідчилися в корисності командної роботи та «міждисциплінарності», які допомагали долати труднощі, що виникали в ході реалізації проєкту. Наприклад, із проблемою структурування і обробки (на папері!) значної кількості зібраних даних та наочної презентації результатів легко впоралися «інформатики» за допомогою програми для роботи з електронними таблицями excel (Рис. 1а, б).

осіб економії	Початкові витрати на день (л)	Оптимізовані витрати на день (л)	Економія води на день (л)	Економія на місяць (л)
Миття рук з аератором	60	45	15	450
Чищення зубів (вимикання води)	12	6	6	180
Прийняття душу (скорочення часу)	300	150	150	4500
Миття посуду (аератор)	180	135	45	1350
Прання (функція економії води)	240	160	80	2400
Промивання овочів/фруктів у мисці	90	45	45	1350
Злив унітазу (половина баку)	252	126	96	2880
Загальна питна вода	48	48	0	0

а



б

Рис. 1. Дослідження зміни витрат води

Виконання подібних проєктів підвищує мотивацію учнів до вивчення математики, допомагають їм побачити, як математика інтегрується з іншими науками, готує до вирішення складних комплексних завдань у майбутньому.

ДЖЕРЕЛА

1. Груздьева К. І. Математичне моделювання як педагогічна ехнологія навчання математики матеріали *Інформаційні технології –2024*: зб. тез XI

Всеукраїнської науково–практичної конференції молодих учених, 16 трав. 2024р., м. Київ / Київ. столичний ун-т ім. Б. Грінченка, 2024. С. 202—203.

2. Звіти/Дані. *Український центр оцінювання якості освіти*. URL: <https://testportal.gov.ua/zvity-dani-efi/> (дата звернення: 31.10.2024).

ЦИФРОВІ ТЕХНОЛОГІЇ В БОТАНІЧНИХ САДАХ: РОЗРОБКА МОБІЛЬНОГО ДОДАТКУ ДЛЯ ПОКРАЩЕННЯ ДОСВІДУ ВІДВІДУВАЧІВ

Дембицька Анна Ігорівна
студентка групи ІАСм -1-23-1.4д,
Київського столичного університету імені Бориса Грінченка,
науковий керівник – к.т.н., доц. Машкіна І.В.

Сучасні ботанічні сади мають не лише зберігати біорізноманіття, але й задовольняти потреби відвідувачів. Використання цифрових технологій, зокрема додатків, здатне підвищити інтерес відвідувачів і покращити їхній досвід, надаючи доступ до інформації про години роботи, локації рослин, екологічні ініціативи тощо.

Розробка мобільного додатку для ботанічного саду, що враховує особливості різних груп цільової аудиторії та включає ключові функції для забезпечення зручності планування візитів, навчання й відпочинку.

На даний момент проведено детальний аналіз існуючих веб-сайтів ботанічних садів, зокрема Royal Botanic Gardens, Kew, Montreal Botanical Garden та Desert Botanical Garden [1,2,3]. Ключові результати свідчать про важливість оптимізації навігаційної структури та контенту. Наприклад, у веб-сайті Kew Gardens спостерігається зручна навігація, яка дозволяє відвідувачам легко знаходити потрібну інформацію, тоді як сайт Montreal Botanical Garden має складну навігацію, що може заплутати користувачів.

Дослідження також виявило, що користувачі шукають не лише базову інформацію про години роботи та ціни, а й більше інтерактивного контенту, такого як віртуальні тури, інформаційні ресурси для дітей, а також можливість участі у заходах та освітніх програмах. Серед позитивних аспектів, які виділяються, є функціональність календаря подій на сайті Desert Botanical Garden, що дозволяє відвідувачам легко планувати візит. Це підкреслює необхідність інтеграції подібних функцій у мобільний додаток.

Аналіз цільових груп показав, що різні категорії користувачів мають свої специфічні потреби. Наприклад, любителі природи шукають детальну інформацію про рослини, тоді як сім'ї з дітьми потребують інтерактивних і освітніх ресурсів. Таким чином, важливо врахувати ці потреби при розробці функціоналу додатку. Попередні результати також підтверджують, що користувацький досвід може бути значно покращений за рахунок інтерактивних елементів, таких як можливість створення персоналізованих маршрутів, доступу до фотогалерей та інтерактивних навчальних матеріалів.

Крім того, було виявлено, що швидкість завантаження сторінок є критично важливим фактором для утримання користувачів. Сайти, які демонструють повільну швидкість, як у випадку з Montreal Botanical Garden, зазнають значних втрат у відвідуваності. Отже, розробка нового додатку повинна включати оптимізацію швидкості завантаження як один із пріоритетів.

Пропонований додаток для ботанічного саду повинен мати інтуїтивну структуру з інтерактивною картою, інформацією про екологічні заходи та можливістю персоналізації профілю. Розробка включатиме дослідження потреб цільових груп, що охоплює як студентів-біологів, так і сім'ї з дітьми та людей, які прагнуть релаксації.

Отже, розробка мобільного додатку для ботанічного саду є не лише актуальною, а й необхідною для підвищення залученості відвідувачів. Визначені потреби цільових груп вказують на важливість інтерактивних елементів і функціональності, які значно покращать користувацький досвід. Наявні проміжні результати свідчать про потенціал для вдосконалення функціоналу, що дозволить створити сучасний, зручний та інформативний ресурс, орієнтований на різні категорії відвідувачів ботанічного саду.

ДЖЕРЕЛА

1. Royal Botanic Gardens, Kew | Kew. URL: <https://www.kew.org/> (дата звернення: 10.10.2024).
2. Montreal Botanical Garden. URL: <https://espacepurlavie.ca/en/botanical-garden> (дата звернення: 10.10.2024).
3. Desert Botanical Garden in Phoenix, Arizona | DBG. Desert Botanical Garden. URL: <https://dbg.org/> (дата звернення: 10.10.2024).

ПРОВІДНІ ТЕНДЕНЦІЇ У ГАЛУЗІ РОЗРОБКИ МОБІЛЬНИХ ЗАСТОСУНКІВ

Здебська Антоніна Анатоліївна
студентка групи ІАСм -1-23-І.4д,
Київського столичного університету імені Бориса Грінченка,
науковий керівник – к.т.н., доц. Машикіна І.В.

Мобільні застосунки відіграють важливу роль у житті сучасної людини, а розвиток індустрії мобільних застосунків продовжується завдяки технологічному прогресу та підвищеним потребам користувачів. Очікується, що у 2025 році мобільні застосунки принесуть понад 613 мільярдів доларів доходу [1]. Прогрес у цій сфері створює нові можливості для бізнесу та споживачів, формуючи тенденції, які визначають майбутнє галузі.

Однією з провідних тенденцій розвитку мобільних застосунків є кросплатформна розробка, що дозволяє створювати застосунки для декількох платформ одночасно, використовуючи єдину кодову базу. Фреймворки, як-от React Native та Flutter, дозволяють писати код один раз та розгортати його на різних операційних системах, що знижує витрати та час розробки. Окрім цього,

кроссплатформні рішення зберігають послідовність користувацького досвіду, що позитивно впливає на популярність застосунків серед користувачів.

Кроссплатформна розробка має суттєві переваги. Економічна ефективність, яку забезпечує єдина кодова база, сприяє значному скороченню витрат. Додатковою перевагою є швидкий вихід на ринок, що дає можливість швидко реагувати на потреби аудиторії. З погляду користувацького досвіду, єдність дизайну і функціональності сприяє зручності в роботі з застосунком.

Проте кроссплатформна розробка має певні обмеження. Продуктивність таких застосунків іноді поступається нативним, особливо при виконанні складних графічних анімацій або обробці даних у реальному часі. Ще одним викликом є обмежений доступ до нативних функцій, таких як сенсори та специфічні API, що може вплинути на функціональність застосунків у певних бізнес-галузях.

Flutter та React Native — найпопулярніші фреймворки для кроссплатформної розробки. Flutter, розроблений Google, використовує мову Dart і забезпечує контроль над інтерфейсом користувача завдяки власному рушію рендерингу, який дозволяє досягати високої продуктивності та плавних анімацій. React Native, створений Meta, орієнтований на JavaScript та дозволяє створювати інтерфейси, які виглядають нативно на Android та iOS. Основною перевагою обох фреймворків є функція гарячого перезавантаження, що дозволяє швидко тестувати зміни без перезапуску програми.

У випадках, де потрібна глибока інтеграція з платформами або використання складних функцій, як-от доповнена реальність, нативна розробка може бути більш оптимальним рішенням. У порівнянні з Flutter, який демонструє високу продуктивність, React Native може мати проблеми з анімаціями та плавністю інтерфейсу, але перевагою є широка спільнота розробників і бібліотек.

Ще одна сучасна тенденція — підвищена увага до дизайну користувацького досвіду (UX), що є критичним фактором успіху мобільного застосунку. Інтуїтивно зрозумілі, адаптивні, доступні інтерфейси значно впливають на утримання користувачів та їх загальне задоволення застосунком. Для вдосконалення UX широко використовуються аналітичні інструменти, які дозволяють відстежувати поведінку користувачів, визначати причини відтоку, а також тестувати варіанти інтерфейсів через A/B тестування. Аналіз таких даних допомагає виявити проблемні зони, вдосконалюючи UX та забезпечуючи кращу взаємодію з застосунком.

Хмарні технології стали важливим компонентом для розвитку мобільних застосунків, особливо для бізнес-застосунків. Вони забезпечують безпеку даних, швидкий доступ до інформації та підвищену адаптивність. За прогнозами, цей ринок зростатиме на 25,28% щорічно до 2029 року [2]. Використання хмарних технологій сприяє не лише збереженню даних, але й можливості інтеграції з іншими бізнес-системами.

Розвиток мобільних застосунків та технологічні інновації, як-от кроссплатформна розробка, дизайн користувацького досвіду та хмарні рішення, формують новий ландшафт індустрії. Мобільні застосунки стали важливим

інструментом у повсякденному житті та бізнесі, надаючи користувачам можливість швидкого доступу до інформації, спрощеного використання і задоволення потреб у будь-який час.

ДЖЕРЕЛА

1. Number of mobile app downloads worldwide from 2016 to 2023. Statista. URL: <https://www.statista.com/statistics/271644/worldwide-free-and-paid-mobile-app-store-downloads/> (дата звернення: 29.10.2024).
2. Mobile cloud computing market size & share analysis - growth trends & forecasts (2024 - 2029). Mordor Intelligence. URL: <https://www.mordorintelligence.com/industry-reports/global-mobile-cloud-market-industry> (дата звернення: 29.10.2024).

TELEGRAM-БОТ ДЛЯ ПАРСИНГУ РОЗКЛАДУ ЗАНЯТЬ З САЙТУ УНІВЕРСИТЕТУ І ЙОГО ІНТЕГРАЦІЇ В TELEGRAM

Коновал Євгеній Юрійович, Пігіда Данило Сергійович

студенти групи ІНБІ-23-4.0д,

*Київського столичного університету імені Бориса Грінченка,
науковий керівник – к.т.н. Яскевич В.О.*

Сучасні інформаційні технології дозволяють створювати автоматизовані системи, що полегшують отримання актуальної інформації у повсякденному житті. Однією з таких систем є Telegram-бот, який автоматично виконує парсування розкладу занять із офіційного сайту університету та надає його у зручному форматі в месенджері Telegram. Це рішення є відповіддю на потребу швидкого доступу до актуальної інформації про розклад занять для студентів і викладачів, які часто стикаються з його змінами.

Метою реалізації проєкту є створення зручного та функціонального Telegram-бота для автоматизації процесу отримання розкладу занять з офіційного сайту Київського столичного університету імені Бориса Грінченка. Бот забезпечує можливість надання розкладу у форматі, доступному через Telegram, з мінімальними зусиллями з боку користувача.

Основні завдання:

1. Парсинг HTML-контенту з сайту Університету Грінченка.
2. Інтеграція з API Telegram[1] для надання розкладу через команди.
3. Забезпечення стабільної роботи навіть при змінах структури сайту.
4. Реалізація функцій для запиту розкладу на певний день або тиждень.

Опис реалізації:

Telegram-бот реалізований за допомогою мови програмування Python і використовує такі бібліотеки:

1. Aiogram для роботи з API Telegram.
2. BeautifulSoup [3] для парсингу HTML-сторінок.

3. Playwright [2] для автоматизації взаємодії з динамічним контентом, отримання сторінки розкладу.

4. Aiosqlite для зберігання даних про користувачів та розкладу пар.

Таблиця 1

Аналіз швидкодії парсингу

Опис	Значення(секунди)
Перший запит від початку програми	4
Другий запит	6.5
Третій запит	9

Незважаючи на асинхронність програми, в певній мірі запити йдуть один за одним, з приблизною різницею в 2 секунди, час виконаний на один запит ≈ 3 секунди на парсинг повністю 1 півріччя. Такі результати відповідно тільки при унікальному значенні даних, яких ще нема в локальній базі даних. З бази ≈ 0.4 секунд, не залежить від кількості даних.

Алгоритм роботи:

1. Користувач надсилає команду в Telegram, наприклад, /start.
2. Бот виконує запит до офіційного сайту Університету Грінченка, парсить відповідний HTML-код і знаходить необхідну інформацію.
3. Отримана інформація передається користувачу у вигляді повідомлення в Telegram.

Вимоги до системи серверу:

1. Python 3.10+
2. Telegram Bot API Token
3. Бібліотеки: aiogram, beautifulsoup4, playwright, aiosqlite, python-dotenv, python-dateutil.

Таким чином, Telegram-бот є ефективним рішенням для автоматизації процесу отримання розкладу навчальних занять, що полегшує студентам і викладачам доступ до актуальної інформації.

Висновки

Telegram-бот "Розклад КСУБГ" є ефективним рішенням для автоматизації процесу отримання розкладу навчальних занять. Завдяки простому інтерфейсу та швидкому доступу до розкладу через Telegram, бот значно полегшує студентам та викладачам отримання актуальної інформації. У подальшому можливе розширення функціоналу, включаючи персоналізацію запитів та інтеграцію з іншими сервісами.

ДЖЕРЕЛА

1. Telegram Bot API Documentation. URL: <https://core.telegram.org/bots/api>
2. Python Playwright Documentation. URL: <https://playwright.dev/python/>
3. BeautifulSoupDocumentation. URL: <https://www.crummy.com/software/BeautifulSoup/>

МАТЕМАТИЧНІ МЕТОДИ ДОСЛІДЖЕННЯ ТА МОДЕЛЮВАННЯ КРИПТОСИСТЕМ З ВІДКРИТИМ КЛЮЧЕМ

Кононенко Ігор Олегович

студент групи МАМм-1-23-1.4.д

*Київського столичного університету імені Бориса Грінченка,
науковий керівник – к..ф-м.н., доц.. Жданова Ю.Д.*

В епоху цифрової трансформації захист інформації є одним з найважливіших аспектів. Застосування криптосистем з відкритим ключем стало однією з фундаментальних основ сучасної інформаційної безпеки, що забезпечує захищений обмін даними у мережі.

Метою дослідження було поставлено глибоке дослідження математичних основ, на яких побудовані сучасні криптосистеми з відкритим ключем, аналіз їх сильних і слабких сторін. Виходячи з мети, основними завданнями стали:

- Огляд існуючих криптосистем з відкритим ключем, зокрема алгоритмів RSA, ElGamal та криптосистем на основі еліптичних кривих [1].
- Вивчення математичних апаратів, що лежать в основі криптографії з відкритим ключем.
- Розроблення математичні моделі для опису роботи криптосистеми з відкритим ключем.

Особливу увагу приділено порівнянню симетричних і асиметричних алгоритмів, що дає змогу зрозуміти унікальність криптосистем з відкритим ключем, де ключ для зашифрування є загальнодоступним, а ключ для розшифрування – закритим. Основними алгоритмами, що використовуються в таких криптосистемах, є RSA (алгоритм Рівеста-Шаміра-Адлемана), ElGamal, DSA (цифровий підпис) та ECC (криптографія на еліптичних кривих). Кожен з них має свої переваги і недоліки, пов'язані з ефективністю та безпекою. Наприклад, RSA заснована на задачі факторизації великих чисел, а ECC використовує властивості еліптичних кривих, що дозволяє знизити обчислювальні ресурси при збереженні рівня безпеки.

Для криптосистем з відкритим ключем важливими задачами є факторизація великих чисел (для RSA) та обчислення дискретного логарифма (для ECC). Стійкість цих криптосистем забезпечується складністю відповідних задач: їх розв'язок потребує значних обчислювальних ресурсів, що унеможливорює злам ключів традиційними методами.

Також досліджуються сучасні методи криптоаналізу, зокрема, алгоритм Шора, здатний розв'язувати завдання факторизації та дискретного логарифмування на квантових комп'ютерах, і алгоритм Полларда, який застосовується для знаходження дискретного логарифма. Наведено приклади оцінки стійкості криптосистем з відкритим ключем, які показують, що з розвитком квантових обчислень виникає необхідність удосконалення існуючих систем захисту [2].

Велику роль в побудові та опису роботи криптосистем з відкритим ключем відіграють математичні моделі, які дозволяють формально аналізувати властивості алгоритмів і проводити теоретичні дослідження.

Зокрема, розглянуто модель криптосистеми RSA та досліджено її ефективність при використанні різних довжин ключів. Також моделюється криптосистема на еліптичних кривих (ECC), яка демонструє високу ефективність при меншій розрядності ключів, порівняно з RSA. Наведено результати експериментів, які порівнюють швидкість шифрування, розшифрування та рівень безпеки, залежно від параметрів криптосистем.

Оцінка показала, що ECC має значні переваги над RSA в умовах обмежених ресурсів, що дозволяє широко використовувати її в мобільних і вбудованих системах. Однак для галузей з високими вимогами до безпеки криптосистема RSA все ще залишається популярною, оскільки забезпечує стабільність і можливість використання дуже великих ключів.

Дослідження показало, що криптосистеми з відкритим ключем є ефективними для захисту інформації, проте їхня стійкість залежить від складності відповідних математичних задач. Аналіз також показує, що розвиток квантових обчислень ставить під загрозу безпеку класичних криптографічних алгоритмів, зокрема RSA. У зв'язку з цим перспективним є впровадження алгоритмів на еліптичних кривих та дослідження нових постквантових методів шифрування.

Дослідження методів моделювання криптосистем з відкритим ключем є актуальним і перспективним напрямом для подальшого розвитку захищених комунікацій, зокрема в умовах наближення ери квантових обчислень.

ДЖЕРЕЛА

1. Yafei Xie. A comparative analysis of public key cryptographic algorithms: RSA, ELGamal, and elliptic curve encryption. *Proceedings of the 3rd International Conference on Computing Innovation and Applied Physics*, 2023.
2. Jiang, Y., et al. "Lightweight Public Key Encryption in the Post-Quantum Era." *IEEE Xplore*, 2023.

МОБІЛЬНИЙ ДОДАТОК ДЛЯ МОНІТОРИНГУ ХАРЧУВАННЯ ЛЮДИНИ

Кравець Денис Віталійович

студент групи ІАСм -1-23-1.4д,

Київського столичного університету імені Бориса Грінченка,

науковий керівник – д.т.н., проф. Бушма О.В.

В сучасному світі спостерігається стрімке зростання захворювань, пов'язаних з порушенням харчування. За даними ВООЗ, понад 1.9 мільярда дорослих мають надмірну вагу, а 650 мільйонів страждають від ожиріння. Існуючі мобільні додатки для контролю харчування мають суттєві обмеження: відсутність персоналізованих рекомендацій на основі особливостей

користувача, неточності в розрахунках нутрієнтів, складний інтерфейс введення даних, що призводить до низької прихильності користувачів. Відсутній комплексний підхід, який би поєднував точний облік харчування, персоналізовані рекомендації та зручний користувацький інтерфейс в одному мобільному рішенні.

Мета: Створення мобільного додатку з інтуїтивним інтерфейсом та системою персоналізованих рекомендацій для точного обліку та аналізу харчування користувачів.

Завдання:

1. Формування переліку критичних обмежень існуючих мобільних додатків для моніторингу харчування
2. Визначення ключових функціональних вимог до мобільного додатку на основі виявлених обмежень.
3. Створення прототипу користувацького інтерфейсу з мінімальною кількістю кроків для введення даних.
4. Розробка архітектури програмного забезпечення з урахуванням вимог до швидкодії та масштабованості.
5. Створення алгоритму персоналізованих рекомендацій на основі профілю користувача.
6. Формування структури бази даних для зберігання інформації про продукти та користувацькі дані.
7. Створення програмного коду мобільного додатку згідно розробленої архітектури.
8. Визначення показників ефективності роботи додатку через тестування на фокус-групі.
9. Формування рекомендацій щодо подальшого вдосконалення додатку на основі зібраних метрик.

Більшість доступних додатків орієнтовані на англomовну аудиторію та не враховують специфіку локального асортименту продуктів харчування. Їх бази даних містять переважно американські та європейські продукти, що створює значні незручності для користувачів з інших регіонів. Це призводить до того, що користувачі змушені вручну додавати інформацію про локальні продукти або шукати приблизні аналоги, що знижує точність обліку та збільшує часові витрати на ведення щоденника харчування.

Було розроблено мобільний додаток для відстеження харчування користувачів з використанням React Native[1] та Firebase[2]. Додаток дозволяє користувачам вести облік спожитих калорій, встановлювати цілі та відстежувати прогрес. Функціональні можливості React Native дозволяють створювати додатки з компонентною структурою, що сприяє модульності, продуктивності та можливості масштабування цифрового продукту.

Процес автентифікації починається з AuthScreen [3], де користувач може увійти через Google або створити обліковий запис. При створенні облікового запису дані (ім'я користувача) передаються у ProfileSetup. На екрані ProfileSetup користувач додає своє фото та базову інформацію (зріст, вага, вік, алергени). Ця інформація зберігається в додатку та доступна через props іншим компонентам.

Після автентифікації користувач потрапляє на MainScreen, який відображає UserHeader з інформацією про користувача (ім'я та фото). MainScreen керує відображенням CaloriesCard, що показує поточний прогрес споживання калорій відносно денної цілі, використовуючи ProgressBar для візуалізації.

MainScreen також містить MealsList, який відображає список прийомів їжі через компоненти MealItem. Для додавання нового прийому їжі користувач може використати AddMealModal, який пропонує два способи введення: ручне введення або сканування штрихкоду через BarcodeScanner. При скануванні штрихкоду, BarcodeScanner передає дані про продукт назад до AddMealModal, який потім додає цю інформацію до загального списку прийомів їжі та оновлює загальну кількість калорій в CaloriesCard.

Всі компоненти використовують єдиний стан додатку для зберігання та оновлення даних, що забезпечує однорідність відображення інформації між різними частинами додатку. Навігація між екранами здійснюється через React Navigation, а передача даних між компонентами відбувається через props та callback-функції.

В рамках виконання проєкту було розроблено мобільний додаток для відстеження харчування, що вирішує ряд критичних обмежень існуючих рішень: персоналізований підхід, спрощений процес введення даних. Ефективна архітектурна реалізація на базі React Native є перевагою пропонованого додатку.

Розроблений додаток створює підґрунтя для подальшого вдосконалення та розширення функціоналу на основі зворотного зв'язку від користувачів та аналізу метрик використання. Це дозволить постійно покращувати якість сервісу та його відповідність потребам цільової аудиторії.

ДЖЕРЕЛА

1. React Native Learn once, write anywhere. *React Native · Learn once, write anywhere*. URL: <https://reactnative.dev> (дата звернення: 01.11.2024).
2. Understand Firebase projects | Firebase Documentation. Firebase. URL: https://firebase.google.com/docs/projects/learn-more?hl=en&authuser=0&_gl=1*1bqxdvh*_ga*NzcxMTI1OTk5LjE3MzA0MjI0MDA.*_ga_CW55HF8NVT*MTczMDQyMjQwMC4xLjEuMTczMDQyMjQwNS41NS4wLjA. (дата звернення: 01.11.2024).
3. Firebase Authentication. Firebase. URL: <https://firebase.google.com/docs/auth> (дата звернення: 01.11.2024).
4. React Navigation | React Navigation. React Navigation | React Navigation. URL: <https://reactnavigation.org/> (дата звернення: 01.11.2024).
5. Компоненти і пропси – React. React – JavaScript-бібліотека для створення користувацьких інтерфейсів. URL: <https://uk.legacy.reactjs.org/docs/components-and-props.html> (дата звернення: 01.11.2024).
6. Communication between native and React Native React Native. React Native Learn once, write anywhere. URL:

<https://reactnative.dev/docs/0.74/communication-android> (дата звернення: 01.11.2024).

РОЗРОБКА МОБІЛЬНОГО ДОДАТКУ
ДЛЯ ПЕРЕВІРКИ ПРАВОПИСУ УКРАЇНСЬКОЇ МОВИ

Максимів Олексій Андрійович
студент групи ІАСм -1-23-І.4д,
Київського столичного університету імені Бориса Грінченка,
науковий керівник – к.т.н., доц. Носенко Т.І.

Сучасні ІТ-технології відіграють важливу роль у філології, полегшуючи доступ до ефективних інструментів для роботи з мовою.

Згідно з дослідженням [1], правильний правопис та граматика грають критичну роль у бізнес-комунікації, тому важливо надавати належну увагу правильному оформленню текстів.

Таблиця 1
Порівняльний аналіз функціоналу популярних мобільних додатків для перевірки правопису

Критерій	Grammarly	Ginger	Microsoft Word Mobile
Оцінка користувачів	4.7* на Google Play Store 4.8* на App Store	4.5* з 5 на Google Play Store, 4.7* на App Store	4.3* на Google Play Store, 4.6* на App Store.
Авто виправлення	Автоматичні корекції правопису, граматики та стилю під час введення	Автоматичні корекції правопису та граматики під час набору тексту	Автоматична корекція правопису та граматики
Інтерфейс користувача	Зрозумілий та зручний з легким доступом до всіх функцій.	Зручний, але може вимагати додаткового часу для звикання.	Простий та зручний з легким доступом до основних функцій.
Підтримка мов	Підтримує понад 20 мов	Підтримує до 40 мов	Підтримка англійської, французької, німецької мов, без спеціалізованих інструментів для інших мов.

Автори [2] аналізують різні системи перевірки та їх ефективність, а також прогнозують майбутні напрямки розвитку цієї технології. Дослідження показують, що автоматизовані системи перевірки правопису та граматики є дуже важливими для покращення якості письмової комунікації, та відкривають нові перспективи для забезпечення якісного тексту.

Аналіз доступних методів та програм для перевірки правопису [3], [4], [5] показує, що більшість з них мають свої обмеження або вимагають платну підписку.

Отже, розробка мобільного додатку для перевірки правопису є перспективною та важливою задачею, яка може сприяти поліпшенню якості письмової комунікації та зробити її більш доступною та ефективною для користувачів.

ДЖЕРЕЛА

1. Geoffrey K. Pullum. (2023). "The Importance of Spelling and Grammar in Business Communication." *Journal of English Linguistics*, 15(2), 45-62.

2. Lynne Truss. (2022). "Automated Spelling and Grammar Checking: Current Trends and Future Directions." *Linguistic Society of America Proceedings*, 10(1), 11-12.

3. Михайленко О. Використання онлайн-ресурсів і мобільних додатків для корекційної роботи щодо збагачення словникового запасу та підвищення розуміння значень слів учнями з комбінованими порушеннями слуху й інтелекту (на допомогу практикам) [Електронний ресурс] / Оксана Михайленко // *Exceptional Child: Teaching & Upbringing*, 2022, Vol 105, Issue 1, p43 – Режим доступу до ресурсу: <https://openurl.ebsco.com/EPDB%3Agcd%3A10%3A23276362/detailv2?sid=ebsco%3Aplink%3Ascholar&id=ebsco%3Agcd%3A173596085&crl=c>.

4. Зозуля І. Є. Використання онлайн-ресурсів та мобільних додатків у вивченні української мови як іноземної [Електронний ресурс] / І. Є. Зозуля, А. С. Стадній. – 2019. – Режим доступу до ресурсу: <http://ir.lib.vntu.edu.ua/handle/123456789/26271>.

5. Мусієнко О. Главная › Поради › 7 сервісів для перевірки правопису української мови 7 сервісів для перевірки правопису української мови [Електронний ресурс] / Олена Мусієнко. – 2022. – Режим доступу до ресурсу: <https://www.imena.ua/blog/services-for-ukrainian-spelling-check/>.

МЕТОДОЛОГІЧНІ ЗАСАДИ РОЗРОБКИ ГЕЙМДИЗАЙН ДОКУМЕНТАЦІЇ В КОНТЕКСТІ ОПТИМІЗАЦІЇ ІГРОВИХ ПРОЕКТІВ

Остапенко Дмитро Русланович

студент групи ІАСм -1-23-І.4д,

Київського столичного університету імені Бориса Грінченка,

науковий керівник – к.т.н., доц. Мельник І.Ю.

В умовах стрімкого розвитку індустрії комп'ютерних ігор особливої актуальності набуває питання стандартизації та оптимізації процесів розробки. Ключовим елементом успішної реалізації ігрового проекту є якісна геймдизайн документація, яка забезпечує чітке розуміння концепції гри всіма учасниками команди та слугує дорожньою картою розробки.

Мета роботи: розробити систематизований підхід до створення геймдизайн документації, який дозволить оптимізувати процес розробки ігрових проектів та підвищити їх якість.

Аналіз сучасного стану геймдизайн документації виявляє низку проблем:

- відсутність єдиних стандартів оформлення та структурування документації;
- неузгодженість термінології та методологічних підходів;
- складнощі в адаптації документації до змін у процесі розробки;
- недостатня увага до документування ігрової механіки та балансу.

Дослідження передбачає створення уніфікованої методології написання геймдизайн документації, розробку шаблонів документації для різних жанрів ігрових проектів, формування критеріїв оцінки якості геймдизайн документів та впровадження системи версіонування та оновлення документації.

Дослідження Game Developer Research Institute (2023) демонструє, що структурований підхід до створення геймдизайн документації суттєво впливає на ефективність розробки [1]. Впровадження стандартизованих шаблонів документації скорочує час розробки проекту на 20-30% завдяки зменшенню кількості ітерацій та переробок. Систематизація процесу документування знижує кількість критичних помилок на етапі реалізації на 40-50% через краще розуміння вимог командою. За даними опитування 200 провідних студій, 78% успішних проектів мали детально розроблену геймдизайн документацію на початковому етапі [2]. Ці висновки підтверджуються практичним досвідом таких компаній як Ubisoft та Electronic Arts, які впровадили структуровані системи документації та відзвітували про значне покращення показників розробки [3].

Очікувані результати дослідження включають створення комплексної методології розробки геймдизайн документації, розробку автоматизованих інструментів для генерації та валідації документів, формування рекомендацій щодо інтеграції документації в agile-процеси розробки та публікацію практичних посібників для розробників

Практичне впровадження методології полягало в розробці геймдизайн документації для ігрового проекту на основі сесійного командного top-down екшену, яка відображає механіку боїв на арені, а також детально описує архітектуру та візуальний стиль ігрового світу. У процесі реалізації було створено чітку структуру документації, яка охоплює всі етапи створення гри: від формування загальної концепції до розробки геймплейних елементів, таких як правила бою, системи здібностей персонажів, ігрові режими та інтеграцію різних ефектів на типи шкоди.

Документ містить опис усіх аспектів ігрового світу, таких як архітектура арени, яка умовно поділена на дві тематичні частини – Світло та Темряву. Це дозволило створити візуально виразне середовище, що підтримує сюжет ігрового процесу та підвищує рівень занурення гравців.

Підсумовуючи, у практичному розділі дослідження вдалося показати ефективність розробленої методології для створення чіткої і послідовної геймдизайн документації. Завдяки застосуванню стандартизованого підходу була досягнуто забезпечення якісного документування всіх ключових елементів гри, що є важливим аспектом у комерційному геймдизайні.

ДЖЕРЕЛА

1. Winget M. A., Sampson W. W. Game development documentation and institutional collection development policy. Proceeding of the 11th annual international ACM/IEEE joint conference, Ottawa, Ontario, Canada, 13–17 June 2011. New York, New York, USA, 2011. URL: <https://doi.org/10.1145/1998076.1998083>.
2. Maxwell K., Johnson P. "Best Practices in Game Design Documentation". Game Developer Magazine, 2023, Vol. 15, No. 4, pp. 45-52.
3. Electronic Arts. "Annual Game Development Productivity Report", 2023. URL: <https://ir.ea.com/press-releases/press-release-details/2024/Electronic-Arts-Reports-Q4-and-FY24-Results/default.aspx>

ВИКОРИСТАННЯ POWER BI ДЛЯ АНАЛІТИКИ РУХУ ТОВАРІВ ПРИ ВПРОВАДЖЕННІ СКЛАДСЬКОГО ОБЛІКУ КОМЕРЦІЙНОГО ПІДПРИЄМСТВА

Пінчук Андрій Григорович

студент групи ІАСм -1-23-1.4д,

Київського столичного університету імені Бориса Грінченка,

науковий керівник – к.т.н., доц. Машкіна І.В.

Автоматизація складських процесів комерційного підприємства здатна не тільки підвищити ефективне ведення бізнесу, але і підняти прибуток компаній. Основні завдання, які вирішують автоматизовані програми для ведення складського обліку:

- рух товару - скорочує час на оформлення товару, номенклатури;

- управління товарними залишками - дозволяє в режимі реального часу слідкувати за залишками товарів;
- оптимізація роботи складу - дозволяє оптимізувати роботу співробітника на пошук і збір товару, відвантаження;
- оптимізувати роботу складських підрозділів і операторів - актуальна інформація про залишки товарів на складах зменшує час на оформлення замовлень;
- інвентаризація - дозволяє порахувати залишки, не зупиняючи роботу складу;
- ефективне планування - звіти про рух товару формують фактичне уявлення про залишки та рух товарів яке передається керівнику в пару кліків миші, планування, прогнозування результатів буде максимально точним [1].

Одним із важливих принципів ведення бухгалтерського та складського обліку на комерційному підприємстві є "повне висвітлення", який показує, що фінансова звітність повинна містити всю інформацію про фактичні та потенційні наслідки господарських операцій та подій, здатних вплинути на рішення, що приймаються на її основі. Користувачам має надаватися доречна та достовірна інформація про фінансовий стан, облік товарів і результати діяльності підприємства [2].

Power BI є зручним набором програмних служб, додатків та з'єднань, які, працюючи разом, перетворюють непов'язані джерела даних на узгоджену, візуально зрозумілу статистику. Отримані дані можна представити в табличній формі, або колекцією хмарних і локальних гібридних сховищ даних. POWER BI дозволяє легко з'єднуватися з джерелами даних будь якого підприємства і представляти їх у зручній формі виявляти пріоритети, планувати і ділитися даними [3].

Power BI є потужним інструментом для бізнес-аналітики від Microsoft, який дозволяє користувачам консолідувати, візуалізувати та аналізувати дані з різних джерел у реальному часі. Основні можливості Power BI:

- Консолідація даних: Power BI дозволяє об'єднувати дані з різних джерел, таких як бази даних, Excel, веб-сервіси та інші системи наприклад BAS, SAP, ODOO, Microsoft та інші.
- Візуалізація даних: Інструмент пропонує широкий спектр візуалізацій, включаючи графіки, діаграми, карти та інші інтерактивні елементи.
- Інтерактивні панелі: Користувачі можуть створювати інтерактивні панелі (dashboards), які оновлюються в режимі реального часу.
- Мобільний доступ: Power BI має мобільні додатки для Windows, iOS та Android, що дозволяє переглядати звіти на ходу.
- Хмарні технології: Використання хмарних сервісів для зберігання та обміну звітами, що забезпечує доступність і зручність роботи.
- Інтеграція з іншими системами: Power BI підтримує інтеграцію з багатьма іншими системами та сервісами, що дозволяє автоматизувати процеси збору та аналізу даних.

Доречність та актуальність даних разом із зручною формою їх подачі для аналізу мають створити сприятливі умови для прийняття управлінських рішень. Тому застосування функціоналу Power BI є невід’ємною частиною при впровадженні складського обліку комерційного підприємства.

ДЖЕРЕЛА

1. Автоматизація складу. uit.kiev.ua. URL: <https://uit.kiev.ua/avtomatizacija-skkladu/> (дата звернення: 30.10.2024).
2. Основні принципи бухгалтерського обліку. StudFiles. URL: <https://studfile.net/preview/8836789/page:6/> (дата звернення: 30.10.2024).
3. What is Power BI? - Power BI. Microsoft Learn: Build skills that open doors in your career. URL: <https://learn.microsoft.com/en-us/power-bi/fundamentals/power-bi-overview> (дата звернення: 30.10.2024).

РОЗРОБКА СИСТЕМИ УПРАВЛІННЯ ЗАПАСАМИ ТОРГОВЕЛЬНОГО ПІДПРИЄМСТВА

Попов Євгеній Станіславович
студент групи ІАСм -1-23-І.4д,

Київського столичного університету імені Бориса Грінченка,
науковий керівник – к.т.н., доц. Абрамов В.О.

Управління запасами є критично важливою функцією для будь-якого торговельного підприємства. Це передбачає планування, організацію та контроль надходження товарів на підприємство, їхній внутрішній розподіл та постачання з підприємства. Ефективне управління запасами допомагає підвищити прибутковість, зменшити витрати та задовольнити попит клієнтів.

Традиційні методи управління запасами можуть бути трудомісткими, схильними до помилок і неефективними. Щоб вирішити ці проблеми були розроблені системи управління запасами. Системи спрямовані на автоматизацію різноманітних завдань управління запасами, покращення видимості запасів, оптимізацію рівня запасів і надання цінної інформації для прийняття рішень.

Впровадження системи управління запасами надає торговельному підприємству численні переваги. Вона може покращити видимість запасів, надаючи інформацію про розташування та рівні запасів, оптимізувати рівні запасів, запобігаючи дефіциту та надлишку запасів, та спростити обробку та доставлення для швидшого виконання замовлень. На основі цих даних керівництво матиме краще розуміння для прийняття обґрунтованих бізнес-рішень.

Однак процес реалізації може супроводжуватися певними викликами. Наприклад, перенесення наявних даних інвентаризації в нову систему та забезпечення сумісності з іншими корпоративними системами. Також потрібні початкові інвестиції та, врешті, подолання опору співробітників, які звикли до ручних процесів.

Метою даного дослідження є розробка системи управління запасами, яка орієнтована на мале торгівельне підприємство. Така система повинна забезпечувати автоматизований облік товарів, моніторинг їх руху, аналіз попиту та оптимізацію процесів закупівлі. На ринку представлені різні рішення для автоматизації управління запасами, починаючи від простих електронних таблиць, закінчуючи комплексними ERP-системами. Такі рішення як Odoo та Zoho Inventory надають інтуїтивно зрозумілий інтерфейс для моніторингу запасів та аналізу даних. Проте, більшість з цих систем можуть бути надто складними або дорогими для малого бізнесу, що потребує легшого та більш адаптованого рішення. Важливим аспектом розробки є створення вебпрограми, яка забезпечить зручний доступ до інформації про запаси для прийняття оперативних рішень [1; 2].

Розробка системи управління запасами є стратегічним вкладенням для будь-якого торгівельного підприємства. Автоматизуючи завдання з управління запасами, покращуючи видимість запасів і надаючи цінну інформацію, система може значно підвищити операційну ефективність, зменшити витрати та покращити загальну продуктивність бізнесу.

ДЖЕРЕЛА

1. Сучасна система інвентаризації | Odoo. Odoo. URL: https://www.odoo.com/uk_UA/app/inventory (дата звернення: 24.10.2024).
2. Online inventory management software | zoho inventory. Zoho | Cloud-Software-Suite für Unternehmen. URL: <https://www.zoho.com/inventory/> (дата звернення: 24.10.2024).

РОЗРОБКА ІНТЕРАКТИВНОГО МОДУЛЯ ДЛЯ ГРИ MINECRAFT З ПІДТРИМКОЮ ВЗАЄМОДІЇ ГРАВЦІВ ЧЕРЕЗ ЧАТ ПРЯМИХ ТРАНСЛЯЦІЙ

Посенко Данило Романович
студент групи ПДМ-62

*Державного університету інформаційно-комунікаційних технологій
науковий керівник - к.т.н. Яскевич В.О.*

В час високих технологій та великого обсягу відео-контенту все більше з'являється попит на стрімінгові сервіси, такі як YouTube Gaming [1]. Інтерактивність є ключем до залучення глядачів і сприяє росту популярності таких платформ. Взаємодія між стрімером і глядачем важлива для розвитку як окремих стрімерів, так і стрімінгових платформ загалом [2]. Однак поточні платформи обмежують користувачів у інтерактивності, дозволяючи взаємодіяти лише через текстовий чат [3]. Для підвищення інтерактивності постає завдання розробити модуль для гри Minecraft, який дозволить глядачам впливати на ігровий процес за допомогою команд у чаті та через донати. Це включає створення механізму обробки тексту і донатів у реальному часі, їх

перетворення в ігрові події та розробку стабільного базового модуля для самої гри [4].

Основною метою цього дослідження є розробка та тестування інтерактивного модуля для Minecraft, який дозволить глядачам змінювати події в грі в реальному часі. Це дослідження зосереджене на пошуку найкращих способів інтеграції гри Minecraft з YouTube та Twitch, кількісному оцінюванні можливості стрімерів взаємодіяти з чатом у такий спосіб та вивченні впливу інтерактивності на залученість глядачів і тривалість перегляду [5].

У результаті було створено інтерактивний модуль, який під'єднується до гри Minecraft та отримує доступ до чатів платформ YouTube і Twitch, а також до донатних платформ для обробки команд глядачів. За допомогою цього модуля глядачі можуть створювати різноманітні події в грі, наприклад, динамічну зміну погоди, утворення нових біомів, спавн мобів та генерацію предметів. Модуль протестовано на кількох тестових стрімах, що дозволило збільшити кількість глядачів на 70%, а також покращити статистику утримання глядачів на трансляціях. На основі результатів розроблено рекомендації для вдосконалення інтерактивних елементів і налаштувань модуля для забезпечення стабільної роботи в реальному часі, що також дає змогу масштабувати модуль для підтримки більшої кількості користувачів та додавання нових видів взаємодії.

ДЖЕРЕЛА

1. Smith, J. (2023). The Evolution of Streaming Platforms: A Deep Dive into YouTube Gaming and Twitch. *Journal of Digital Media*, 15(4), 237-256.
2. Wilson, R. (2022). Interactive Streaming and Viewer Engagement: Exploring the Trends. *Interactive Media Studies*, 21(2), 89-101.
3. Brown, M., & Lee, D. (2023). Limits of Interactivity on Streaming Platforms and Viewer Retention Strategies. *Media Engagement Review*, 8(3), 115-130.
4. Kumar, A., & White, S. (2024). Real-Time Interaction in Video Games: A Case Study of Minecraft and Streaming. *Gaming Technology Quarterly*, 11(1), 45-67.
5. Green, T., & Carter, E. (2023). Evaluating Viewer Engagement in Live Streaming Events. *Streaming Analytics Journal*, 12(4), 299-312.

РОЗРОБКА МЕТОДІВ ТА ЗАСОБІВ УПРАВЛІННЯ ІГРОВИМИ ПОДІЯМИ ЧЕРЕЗ ІНТЕГРАЦІЮ З ДОНАТ-СЕРВІСАМИ

Посенко Данило Романович
студент групи ПДМ-62

*Державного університету інформаційно-комунікаційних технологій,
науковий керівник - к.т.н. Яскевич В.О.*

В ході популяризації української мови та процесу відділення українського сегменту від загального зросійщеного медіа простору з'явилась

велика кількість україномовних стрімерів, як на платформі YouTube, Twitch, так і TikTok, що пов'язані безпосередньо з іграми[1]. Задача полягає в тому, щоб використати потенціал підтримки з боку спільноти глядачів створивши методи та засоби для управління ігровими подіями через донат-сервіси[2].

Метою дослідження є створення засобів, завдяки яким буде можлива організація взаємодії між глядачем та стрімером, що створить загальне ігрове середовище, де гравець зможе прямо впливати на події в грі, паралельно підтримуючи автора стріма та розвиваючи таким чином національний медіа простір.

Створення програмного забезпечення, що робить можливим організацію спільного ігрового середовища для глядача та стрімера. В глядача є змога впливати на внутрішньоігрові події в режимі реального часу через донат, завдяки чому трансляції стали більш інтерактивними та почали збирати більшу кількість глядачів, оскільки додається змінна «непередбачуваних обставин». Кожен глядач має змогу змінити ігровий процес. Зміна залежить від суми донату. Стрімер має змогу коригувати ігрові події, вмикати та редагувати функціонал, що розділений на категорії по рівням складності, а також змінювати вартість кожного івенту індивідуально. В той же час в глядача є змога надіслати повідомлення прямо в гру, дати стрімеру певні бонуси чи встановити на його шляху перешкоди. Завдяки API є можливість об'єднання різних методів та засобів в єдину систему, що включатиме можливість інтеграції з різними донат сервісами, такими як: Donatello, Diaka та банка MONO, залежно від вподобань стрімера [3]. Створення ядра даного засобу надає йому безмежний потенціал [4]. Кількість та різноманітність івентів в подальшому залежить виключно від фантазії та можливостей гри, на базі якої створено ядро. В даному випадку це Minecraft, оскільки спільнота глядачів даної гри є найбільшою.

ДЖЕРЕЛА

1. Detector.media. Режим доступу: <https://ms.detector.media/internet/post/33843/2023-12-27-obsyag-ukrainskomovnykh-translyatsiy-na-twitch-za-rik-zris-pryblyzno-na-200/>
2. Parasocial Interactions and Relationships with Media Characters - An Inventory of 60 Years of Research. Режим доступу: https://www.researchgate.net/publication/333748971_Parasocial_Interactions_and_Relationships_with_Media_Characters_-_An_Inventory_of_60_Years_of_Research
3. CurseForge Upload API. Режим доступу: <https://support.curseforge.com/en/support/solutions/articles/9000197321-curseforge-upload-api>
4. Java Documentation. Режим доступу: <https://docs.oracle.com/en/java/>

ДОСЛІДЖЕННЯ МЕТОДІВ ФАКТОРИЗАЦІЇ МНОГОЧЛЕНІВ ТА ЇХ ЗАСТОСУВАННЯ В КРИПТОГРАФІЇ

Самосєєв Євгеній Дмитрович

студент групи МАМм-1-23-1.4.д

*Київського столичного університету імені Бориса Грінченка,
науковий керівник – к.ф.-м.н., доц.. Жданова Ю.Д.*

Факторизація многочленів – одна з центральних задач в алгебрі та теорії чисел, яка має важливе значення як у чистій математиці, так і в прикладних дисциплінах, зокрема в криптографії. Можливість розкласти многочлен на незвідні множники дозволяє розширити теоретичні знання про структуру полів і кілець, забезпечити фундамент для алгоритмів у комп'ютерній алгебрі, а також знайти нові шляхи забезпечення захисту інформації в криптографії [1]. У даній роботі ми дослідили різні методи факторизації многочленів, визначили їх особливості та придатність до застосування в криптографічних протоколах, зокрема в умовах сучасних технологічних викликів.

Метою дослідження було поставлено огляд і порівняння різних методів факторизації многочленів та аналіз їх можливостей застосування в криптографії. Виходячи з мети, основними завданнями стали:

- Аналіз класичних і сучасних методів факторизації многочленів.
- Оцінка ефективності та складності різних алгоритмів для факторизації над раціональними числами та скінченними полями.
- Дослідження криптографічних застосувань факторизації, особливо для протоколів з відкритим ключем та квантово-стійких систем.

Многочлени можуть бути розкладені на множники за допомогою різних методів, які поділяються на детерміновані й ймовірнісні. Серед основних методів факторизації можна виділити:

1. Алгоритм Евкліда – використовується для знаходження найбільших спільних дільників многочленів і є основою для багатьох інших алгоритмів факторизації.
2. Алгоритм Берлекемпа – підхід для факторизації многочленів над скінченними полями, який спирається на розклад характеристичного многочлена.
3. Алгоритм Кантора-Цассенгауза – модифікація, яка підвищує швидкість факторизації, використовуючи властивості скінченних полів.
4. Алгоритм Ленстри-Ленстри-Ловаса (LLL) – метод, що дозволяє факторизувати многочлени з раціональними коефіцієнтами за допомогою редукції ґраток.
5. Алгоритм Шора – квантовий алгоритм, здатний факторизувати многочлени й цілі числа значно швидше, ніж класичні методи, що становить загрозу для сучасних криптосистем.

Дослідження цих методів показало, що кожен має свої переваги залежно від типу поля, у якому проводиться факторизація, а також від потреби у швидкості або стійкості до зломів.

Порівняння алгоритмів факторизації вказує на їхню ефективність і складність залежно від обраного підходу. Наприклад, алгоритм LLL є надзвичайно ефективним для многочленів з раціональними коефіцієнтами, а алгоритм Кантора-Цассенгауза більш придатний для факторизації в скінченних полях. Сучасні дослідження показують, що ефективні методи факторизації, такі як LLL та його модифікації, можуть використовуватися для факторизації над скінченними полями, що знижує потребу в квантових обчисленнях.

Факторизація многочленів є основою для багатьох криптографічних систем, включаючи:

1. RSA та криптографія з відкритим ключем. Основу криптографічної системи RSA становить факторизація великих чисел, яка може бути поширена на випадок многочленів. Зокрема, виявлення незвідних многочленів може сприяти розробці стійких схем шифрування.

2. Постквантова криптографія. Квантові обчислення, зокрема алгоритм Шора, дозволяють розв'язувати задачі факторизації многочленів значно швидше, що підриває стійкість сучасних криптографічних систем. Тому розглядаються нові алгоритми шифрування, стійкі до квантових атак, які можуть використовувати факторизацію над скінченними полями.

3. Криптографія на еліптичних кривих. Тут факторизація многочленів використовується для аналізу дискретного логарифму на еліптичних кривих, що є основою безпеки еліптичних криптосистем.

4. Схеми на основі ґраток. Ґраткові криптосистеми, що використовують факторизацію многочленів, розглядаються як перспективний напрям у постквантовій криптографії, оскільки факторизація у ґраткових структурах важко обчислювана навіть для квантових комп'ютерів.

Дослідження показало, що факторизація многочленів є важливою математичною задачею з широким спектром застосувань у криптографії. Методи факторизації багато в чому визначають ефективність і безпеку сучасних криптографічних систем. Удосконалення існуючих алгоритмів і розробка нових методів факторизації, зокрема тих, що використовуються в криптографії з відкритим ключем і постквантовій криптографії [2], дозволить захистити інформацію у швидко змінюваному цифровому світі.

ДЖЕРЕЛА

1. Fan, X., Xu, C., & Zhang, Y. (2020). Efficient Factorization of Polynomials over Finite Fields using Heuristic Approaches. *Journal of Symbolic Computation*, 99, 45-58.
2. Bernstein, D. J., Lange, T. (2017). Post-quantum cryptography. *Nature*, 549, 188-194.

ВИКОРИСТАННЯ ГЕОЛОКАЦІЙНИХ СЕРВІСІВ ДЛЯ ВІЗУАЛІЗАЦІЇ ЗАБРУДНЕНOSTІ ТЕРИТОРІЇ РАДІОАКТИВНИМИ НУКЛІДАМИ

Свищо Максим Іванович

студент групи ІАСм -1-23-І.4д,

*Київського столичного університету імені Бориса Грінченка,
науковий керівник – к.т.н., доц. Носенко Т.І.*

Забруднення радіоактивними нуклідами навколишнього середовища є проблемою, що важко помітити неозброєним оком. Саме тому, важливо своєчасно отримати інформацію, яку можна проаналізувати, узагальнити і опрацювати. Сучасні інформаційно-комунікаційні технології дозволяють швидко та якісно отримати та опрацювати необхідну інформацію з будь-якого куточку світу. Одним з прикладів може слугувати використання геолокаційних сервісів. Зображення забрудненості за допомогою мап дозволяє якісно і зрозуміло показати масштаби та величину забруднення.

Мета роботи полягає в дослідженні та аналізі можливостей використання геолокаційних сервісів для створення візуалізації карт забруднення радіоактивними нуклідами.

В Україні технологію віртуальних мап вже використовують як в приватних, так і державних Веб-застосунках. Наприклад, сервіси SaveEcoBot [1], Eco-City [2], Онлайн-мапа Українського гідрометеорологічного центру [3] та Екозагроза від Міндовкілля України [4]. В них, зазвичай, дані про забруднення позначено точково, позначаючи ситуацію навколо певних міст. Створення систем для аналізу радіоактивного забруднення мало місце у роботах Забулонова Ю. Л.[5]. Використання сучасних ГІС-технологій для відображення проблем екології наявна у роботах Каменевої І. П. [6] та Переметчика П.П [7].

У дослідженні було проаналізовано три найпопулярніші геолокаційні сервіси: Google Maps [8], Mapbox [9] і Carto [10]. Кожен сервіс має свої інструменти та можливості для реалізації мети. Порівняльний аналіз деяких критеріїв узагальнено в таблиці 1.

Виходячи з результатів аналізу, автори вибрали Google Maps. Завдяки своїй детальній документації, безкоштовному ліміті і широкій підтримці різних веб-фреймворків, його легко інтегрувати і почати експериментувати у своєму проекті. Його було використано для зображення даних про забруднення радіоактивними нуклідами. Дані було зібрано під час польоту дрону з допомогою спеціального зчитуючого пристрою. Кожна точка в даних містить довготу, широту та радіоактивність на відповідній точці. Приклад перетворення точок у теплову мапу зображено на рисунку 1.

Скупчення точок та підвищення активності є показником інтенсивності, що відповідає кольорам теплової мапи, де найменший показник - синій, найбільший - червоний.

Таблиця 1

Порівняння геолокаційних сервісів

Сервіс	Безкоштовне використання	Підтримка теплових мап	Повна стилізація мап	Вбудована обробка координат	Підтримка мобільної розробки	Сервіс як платформа
Google Maps	28500 запитів в місяць	+	+	+	-	-
Mapbox	50000 запитів в місяць	+	+	+	+	+
Carto	Лише студентам	+	-	-	-	+

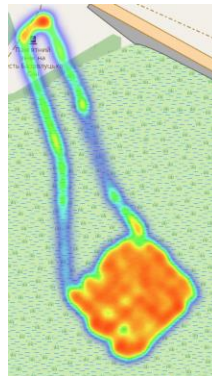


Рис. 1. Теплова мапа забруднення

Було виявлено, що теплові мапи у поєднанні з геолокаційним сервісом дають змогу швидко зрозуміти обсяги та інтенсивність забруднення, а також зручно перевірити стан навколишніх територій. Отже, використання подібних інструментів сприяє підвищенню екологічної безпеки та інформуванню громадськості.

ДЖЕРЕЛА

1. SaveEcoBot, URL: <https://www.saveecobot.com/radiation-maps>
2. Eco-City, URL: <https://eco-city.org.ua/>
3. Онлайн-мапа Українського гідрометеорологічного центру, URL: <https://www.meteo.gov.ua/#RADIO>
4. Екозагроза (Міндовкілля України), URL: <https://ecozagroza.gov.ua/map?layer=radiation>
5. Система автоматизованого оперативного контролю радіаційної обстановки швидкого реагування на базі літального апарату / Ю.Л. Забулонов, В.М. Буртняк, Л.А. Одукалець // Наука та інновації. — 2020. — Т. 16, № 3. — С. 39-46. — Бібліогр.: 4 назв. — укр.
6. Комплексний аналіз екологічної безпеки міста на основі сучасних ГІС-технологій / І.П. Каменева, А.В. Яцишин, Д.О. Полішко, О.О. Попов //

Екологія довкілля та безпека життєдіяльн. — 2008. — № 5. — С. 41-46. —
Бібліогр.: 7 назв. — укр.

7. Побудова карто-схем забруднення атмосфери для системи екологічного моніторингу м. Дніпропетровська / Переметчик М.М., Поліщук С.З. URL:

http://eco.com.ua/sites/eco.com.ua/files/lib1/konf/2vze/zb_m/0048_zb_m_2VZE.pdf

8. Google Maps Developer Docs, Google, URL: <https://developers.google.com/maps>

9. Mapbox Docs, Mapbox, URL: <https://docs.mapbox.com/>

10. Carto Docs, Carto, URL: <https://docs.carto.com/carto-user-manual/maps>

ВИДИ АПАРАТНО-ПРОГРАМНИХ КОМПЛЕКСІВ (АПК) МОНІТОРИНГУ ЯКОСТІ ПОВІТРЯ

Степанець Михайло Володимирович

студент групи ІАСм -1-24-І.4д,

Київського столичного університету імені Бориса Грінченка,

науковий керівник –к.т.н., доц. Мельник І.Ю

Моніторинг якості повітря став невід'ємною частиною екологічної політики багатьох країн. Забруднення повітря спричиняє серйозні наслідки для здоров'я та екосистем, і за даними Всесвітньої організації охорони здоров'я (ВООЗ), щороку близько 7 мільйонів людей помирають передчасно через забруднення повітря. Апаратно-програмні комплекси (АПК) для моніторингу якості повітря допомагають відслідковувати рівні забруднюючих речовин та сприяти прийняттю обґрунтованих рішень для покращення екологічної ситуації. Існує декілька типів АПК, які використовують різні підходи, технології та платформи для збору і передачі даних.

Стаціонарні комплекси – це великі установки, які розташовані на фіксованих локаціях. Їх використовують для довготривалого і безперервного спостереження за концентрацією забруднювачів на певній території, наприклад, у містах чи промислових зонах. Використовують високоточні датчики для вимірювання концентрації основних забруднювачів, таких як SO₂, NO₂, CO, PM_{2.5}, PM₁₀ тощо. Зазвичай підключені до центральної бази даних, де дані зберігаються і аналізуються в режимі реального часу.

Переносні пристрої забезпечують можливість мобільного моніторингу якості повітря. Ці пристрої корисні для короткотермінових досліджень, особистого використання та для відстеження забруднення на місцевому рівні. Мобільні, працюють на акумуляторі, що дозволяє проводити вимірювання у будь-якому місці. Оснащені сенсорами для визначення концентрацій основних забруднювачів.

ІоТ-системи для моніторингу якості повітря засновані на використанні недорогих сенсорів та бездротових технологій, які дозволяють створювати розподілені системи для збору даних на великих територіях. В основі часто

використовуються платформи, такі як Arduino, Raspberry Pi, ESP32, що дозволяє знизити вартість і спростити розробку. Дані передаються на хмарні сервери через Wi-Fi, LoRaWAN або GSM, що дозволяє проводити аналіз в режимі реального часу.

Персональні системи моніторингу якості повітря використовуються для індивідуального контролю навколишнього середовища і часто мають зручний інтерфейс для відображення даних на смартфоні. Компактні, мобільні пристрої з Bluetooth або Wi-Fi для передачі даних на мобільний додаток. Дають можливість в реальному часі отримувати інформацію про забрудненість повітря.

Для моніторингу якості повітря у важкодоступних місцях та на великих територіях використовуються комплекси, що встановлюються на транспортні засоби. Вони дозволяють створювати динамічну карту якості повітря. Працюють від акумулятора або електромережі транспортного засобу. Зазвичай обладнані GPS-модулем для відстеження локації та картування даних.

Моніторинг якості повітря є критично важливим завданням, яке вимагає використання різних типів АПК для забезпечення надійної інформації у реальному часі. Використання сучасних IoT технологій дозволяє створювати більш доступні та масштабовані системи, які можуть ефективно інтегруватися в структуру розумних міст, громадських місць або для персонального контролю.

В ході роботи було проведено детальне дослідження проблем, пов'язаних з вимірюванням індексу забруднення повітря, та розглянули різноманітні способи їх вирішення. На основі отриманих результатів буде розроблено систему моніторингу якості повітря, що базується на мікроконтролері ESP32. Ця система дозволить точно визначати концентрацію шкідливих речовин, таких як дрібні частинки пилу PM2.5 та PM10, діоксид азоту (NO₂) та чадний газ (CO), безпосередньо у помешканні або за його межами. Для зручності використання буде створено спеціальний мобільний додаток, який забезпечить постійний доступ до актуальних даних про стан повітря та дозволить відстежувати зміни в динаміці."

ДЖЕРЕЛА

1. Повітря під час війни. Чому важливо моніторити забруднення та розповідати про це. ua.boell.org. URL: <https://ua.boell.org/uk/2022/11/16/povitrya-pid-chas-viyny-chomu-vazhlyvo-monitoryty-zabrudnennya-ta-rozpovidaty-pro-tse>.
2. Що таке пост моніторингу якості повітря і для чого він потрібен місту? ecoclubrivne.org. URL: https://ecoclubrivne.org/air_quality_monitoring_post/.
3. Дослідження Глобального Альянсу зі здоров'я та забруднень (ГАНП), грудень 2019. – 56 с.
4. Концепція запровадження та обслуговування системи моніторингу якості атмосферного повітря у м. Києві як основа для створення екологічно безпечного міста. [Електронний ресурс]. – Режим доступу: https://darn.kyivcity.gov.ua/done_img/f/Konceptoin.pdf

ФОРМУВАННЯ РАХУНКІВ КІЛЬКОХ ВІДВІДУВАЧІВ РЕСТОРАНУ

Циба Володимир Олексійович
студент групи ІАСм -1-23-1.4д,

*Київського столичного університету імені Бориса Грінченка,
науковий керівник – д.т.н., проф. Бушма О.В.*

У сучасному суспільстві стрімкого розвитку цифрових технологій та посилення конкуренції в ресторанному бізнесі особливого значення набуває підвищення якості обслуговування клієнтів і оптимізація внутрішніх процесів закладів громадського харчування. Використання мобільних додатків для автоматизації роботи персоналу стає невід'ємною частиною сучасного сервісу, сприяючи ефективності та швидкості обслуговування [1].

Аналіз існуючих рішень показав, що популярні мобільні додатки для поділу рахунку, такі як Splitwise [2], Монобанк [3], Venmo [4], орієнтовані переважно на кінцевого споживача та не враховують специфіку роботи офіціантів. Вони не надають можливості швидкого та точного поділу рахунку з боку персоналу ресторану, що може призводити до затримок і помилок при обслуговуванні. Відсутність інтегрованих інструментів для офіціантів у відомих додатках створює потребу в розробці спеціалізованого рішення, яке б забезпечило автоматизацію процесу поділу рахунку безпосередньо на рівні обслуговуючого персоналу.

Метою роботи є створення мобільного додатку для офіціантів, який забезпечить зручний, швидкий та точний поділ загального рахунку між кількома відвідувачами ресторану, підвищуючи ефективність роботи персоналу та якість обслуговування.

Об'єкт дослідження – процес обслуговування відвідувачів ресторану з акцентом на поділ загального рахунку.

Предмет дослідження – методи та технології реалізації поділу загального рахунку між кількома відвідувачами в мобільному додатку офіціанта на платформі Android із використанням Kotlin та Firebase [5, 6, 7].

Для досягнення мети необхідно виконати наступні завдання:

- **Проаналізувати** існуючі методи поділу рахунку в ресторанных додатках та визначити їхні переваги та недоліки.
- **Дослідити** можливості інтерфейсу користувача для спрощення процесу поділу рахунку офіціантом.
- **Розробити** архітектуру мобільного додатку та структуру бази даних для зберігання та обробки інформації про замовлення та рахунки.
- **Реалізувати** функціонал додатку з використанням мови програмування Kotlin та платформи Firebase, забезпечивши інтеграцію з базою даних.
- **Провести** тестування додатку в реальних умовах експлуатації та **оцінити** його ефективність і зручність використання.

- **Розробити** рекомендації щодо впровадження додатку в ресторанний бізнес та можливості його подальшого вдосконалення.

На сьогоднішній день більшість існуючих рішень зосереджені на клієнтському боці процесу поділу рахунку, тоді як інструменти для офіціантів залишаються обмеженими. Це призводить до затримок у обслуговуванні, можливих помилок при розрахунках та зниження задоволеності клієнтів.

Розроблений мобільний додаток дозволяє офіціантам:

- Призначати окремі позиції меню кожному відвідувачу, що спростить індивідуальний розрахунок.
- Автоматично розподіляти загальний рахунок за різними схемами (рівномірно, пропорційно замовленням тощо).
- Швидко оновлювати інформацію про замовлення та рахунки завдяки інтеграції з базою даних.
- Зменшити ймовірність помилок при розрахунках та прискорити процес обслуговування.

Використання сучасних технологій та інструментів розробки, таких як Kotlin та Firebase, забезпечить надійність, швидкодію та масштабованість додатку. Впровадження цього рішення в ресторанний бізнес сприятиме підвищенню ефективності роботи персоналу, зменшенню часу обслуговування та підвищенню рівня задоволеності клієнтів, що є ключовими факторами успіху в сучасних умовах конкуренції.

ДЖЕРЕЛА

1. Онлайн-додаток для ресторану – чому це вам потрібно? [Електронний ресурс] // Remdim.info. – 2021. – Режим доступу: <https://remdim.info/5640-onlain-dodatok-dlia-restoranu-chomu-tse-vam-potribno.html>.
2. Splitwise [Електронний ресурс] // Splitwise. – 2024. – Режим доступу: <https://www.splitwise.com/>.
3. Монобанк запустив сервіс швидкого розрахунку в кафе та ресторанах [Електронний ресурс] // ІТС.ua. – 2021. – Режим доступу: <https://itc.ua/news/monobank-zapustiv-servis-shvidkogo-rozrahunku-v-kafe-ta-restoranah/>.
4. Venmo [Електронний ресурс] // Venmo. – 2024. – Режим доступу: <https://venmo.com/>.
5. Android Developers [Електронний ресурс] // Google Developers. – 2024. – Режим доступу: <https://developer.android.com/>.
6. Kotlin Programming Language [Електронний ресурс] // Kotlinlang.org. – 2024. – Режим доступу: <https://kotlinlang.org/>.
7. Firebase Documentation [Електронний ресурс] // Firebase. – 2024. – Режим доступу <https://firebase.google.com/docs>.

РОЗРОБКА ДОДАТКУ ДЛЯ ПЛАНУВАННЯ ОСОБИСТОГО БЮДЖЕТУ

Шебет Євгеній Ігорович
студент групи Інб -1-21-1.4д,

*Київського столичного університету імені Бориса Грінченка,
науковий керівник – к.т.н., доц. Носенко Т.І.*

Планування бюджету є невід'ємною частиною, так як завдяки цьому є можливість чітко розуміти своє фінансове положення, а також покращити фінансову грамотність [1]. Громадяни часто змушені економити на товарах та послугах першої необхідності, що є не доцільним і не раціональним підходом. Допомогти людині вирішити цю важливу проблему можуть мобільні додатки, призначені для ведення особистого бюджету та контролю витрат [2].

Метою роботи автори визначили розробку функціонального мобільного додатку для планування особистого бюджету для покращення фінансового положення користувача завдяки документуванню фінансових операцій та аналізу фінансової поведінки.

Предметом дослідження є процес розробки програмного забезпечення для планування особистого бюджету, який має інтуїтивний інтерфейс. Об'єктом дослідження є мобільний додаток для планування особистого бюджету.

Завдання дослідження:

1. Аналіз сучасних мобільних додатків для контролю над власними коштами для визначення їх функціональних можливостей, структури, сильних та слабких сторін.
2. Розробка моделі додатку, структури даних та взаємодії користувача і системи.
3. Розробка інтерфейсу додатку.
4. Реалізація основних функціональних модулів: введення даних про доходи та витрати та їх категоризація, генерація звітів, налаштування сповіщень тощо.
5. Тестування розробленого додатку для виявлення вразливих місць та усунення помилок, оцінка його ефективності та зручності використання [3].

Отже, мобільний додаток для планування особистого бюджету покращить контроль над власними фінансами та надасть аналітичні дані користувачу з метою контролю та планування їх використання фінансів.

ДЖЕРЕЛА

1. Економіка підприємства: пошук шляхів розвитку: Посібник / МАУП. – К.: МАУП, 2005 – 80 с.
2. Як вести особистий бюджет? Лайфхаки з планування та економії. [Електронний ресурс].— Режим доступу: <https://happymonday.ua/osobystyj-bjudzhet-sposoby-kontrolju>
3. Авраменко В.С., Авраменко А.С. Проектування інформаційних систем: навчальний посібник / В.С. Авраменко, А.С. Авраменко. – Черкаси: Черкаський національний університет ім. Б. Хмельницького, 2017. – 434 с.

TF-IDF ДЛЯ ОЧИЩЕННЯ ТЕКСТОВИХ ДАНИХ У КЛАСИФІКАЦІЙНИХ ЗАДАЧАХ З ВИКОРИСТАННЯМ NLP

Шидловський Тимофій Максимович

студент групи ІАСм1-23-1.4д,

*Київського столичного університету імені Бориса Грінченка,
науковий керівник – к.т.н. Яскевич В.О.*

Одна з проблем NLP (Natural Language Processing) – це очищення текстових даних перед навчанням та прогнозуванням. Стандартні методи очищення включають приведення тексту до нижнього регістру, видалення пунктуації та стоп-слів, токенизацію, а також стемінг або лематизацію. Ці підходи спрямовані на зменшення шуму та приведення даних до єдиного формату.

Проте, в задачах класифікації тексту можна додатково покращити очищення за допомогою алгоритму TF-IDF (Term Frequency-Inverse Document Frequency). Зазвичай TF-IDF використовують для оцінки важливості слів в документах, відносно всього тексту [1]. Іншими словами, він допомагає знайти та оцінити, які слова краще всього характеризують документ. Але, в задачах класифікації можна застосовувати TF-IDF для визначення значущості слів для кожного з класів.

Такий підхід дозволяє присвоїти різні ваги словам під час навчання моделі, підкреслюючи ті, що будуть найбільш релевантними до певного класу та зменшуючи вплив більш поширених слів. Також, можна перед навчанням прибирати слова, які не будуть мати достатньої ваги в жодному з класів. Таким чином, модель може зосередитися на найбільш значущих ознаках, що потенційно підвищить точність класифікації.

Однак, цей метод може і погіршити результати моделі, якщо вона використовує шари (layers), які враховують контекст попередніх слів, такі як LSTM (Long Short-Term Memory). Видаляючи слова за допомогою TF-IDF, ми ризикуємо втратити важливу контекстуальну інформацію, оскільки певні слова (які були поширені у корпусі) можуть суттєво змінювати контекст/сенси речення. Наприклад, слово «не» може мати малу вагу при використанні TF-IDF, але це слово *не* може повністю змінити сенс речення.

Тому при застосуванні TF-IDF для очищення даних необхідно балансувати між зменшенням шуму та збереженням контексту. Але при правильному використанні можна не тільки покращити результати нейромережі, а й ще зменшити її розмір та збільшити її швидкість.

ДЖЕРЕЛА

1. TF-IDF in NLP (Term Frequency Inverse Document Frequency) | by Abhishek Jain | Medium, 2024, URL: <https://medium.com/@abhishekjainindore24/tf-idf-in-nlp-term-frequency-inverse-document-frequency-e05b65932f1d>

*Зміст***ЗАХИСТ АЛГОРИТМУ ДІФФІ-ГЕЛЬМАНА ВІД АТАКИ ПО БОКОВОМУ КАНАЛУ**

Абрамов Сергій Вадимович..... 2

ВЕБ-БРАУЗЕРНІ РОЗШИРЕННЯ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ WEBASSEMBLY: ПОТЕНЦІАЛ ТА ВИКЛИКИ

Андрієвич Дмитро Юрійович..... 4

ІГРОВІ МЕХАНІКИ У БАГАТОКОРИСТУВАЦЬКИХ ОНЛАЙН-ІГРАХ

Бойко Максим Олександрович..... 6

ТЕХНОЛОГІЇ МОНІТОРИНГУ ЯКОСТІ СЛУ

Великодний Артем Русланович..... 8

ПОРІВНЯННЯ МОЖЛИВОСТЕЙ ЗАСТОСУВАННЯ CODEGPT ТА GITHUB COPILOT

Горбачевський Максим Геннадійович..... 10

СТВОРЕННЯ ТА ВИКОРИСТАННЯ МОБІЛЬНОГО WEB-ДОДАТКУ ДЛЯ МОНІТОРИНГУ ОСНОВНИХ ПАРАМЕТРІВ ФУНКЦІОНУВАННЯ МАГАЗИНУ СПОРТТОВАРІВ

Грабовський Єгор Романович..... 11

ВИКОНАННЯ ПРОЄКТІВ ЯК ІНСТРУМЕНТ МАТЕМАТИЧНОГО МОДЕЛЮВАННЯ

Груздьева Катерина Ігорівна..... 13

ЦИФРОВІ ТЕХНОЛОГІЇ В БОТАНІЧНИХ САДАХ: РОЗРОБКА МОБІЛЬНОГО ДОДАТКУ ДЛЯ ПОКРАЩЕННЯ ДОСВІДУ ВІДВІДУВАЧІВ

Дембицька Анна Ігорівна..... 15

ПРОВІДНІ ТЕНДЕНЦІЇ У ГАЛУЗІ РОЗРОБКИ МОБІЛЬНИХ ЗАСТОСУНКІВ

Здебська Антоніна Анатоліївна..... 16

TELEGRAM-БОТ ДЛЯ ПАРСИНГУ РОЗКЛАДУ ЗАНЯТЬ З САЙТУ УНІВЕРСИТЕТУ І ЙОГО ІНТЕГРАЦІЇ В TELEGRAM

Коновал Євгеній Юрійович, Пігіда Данило Сергійович..... 18

МАТЕМАТИЧНІ МЕТОДИ ДОСЛІДЖЕННЯ ТА МОДЕЛЮВАННЯ КРИПТОСИСТЕМ З ВІДКРИТИМ КЛЮЧЕМ

Кононенко Ігор Олегович..... 20

МОБІЛЬНИЙ ДОДАТОК ДЛЯ МОНІТОРИНГУ ХАРЧУВАННЯ ЛЮДИНИ

Кравець Денис Віталійович..... 21

РОЗРОБКА МОБІЛЬНОГО ДОДАТКУ ДЛЯ ПЕРЕВІРКИ ПРАВОПИСУ УКРАЇНСЬКОЇ МОВИ

Максимів Олексій Андрійович..... 24

МЕТОДОЛОГІЧНІ ЗАСАДИ РОЗРОБКИ ГЕЙМДИЗАЙН ДОКУМЕНТАЦІЇ В КОНТЕКСТІ ОПТИМІЗАЦІЇ ІГРОВИХ ПРОЕКТІВ

Остапенко Дмитро Русланович 26

ВИКОРИСТАННЯ POWER BI ДЛЯ АНАЛІТИКИ РУХУ ТОВАРІВ ПРИ ВПРОВАДЖЕННІ СКЛАДСЬКОГО ОБЛІКУ КОМЕРЦІЙНОГО ПІДПРИЄМСТВА

Пінчук Андрій Григорович 27

РОЗРОБКА СИСТЕМИ УПРАВЛІННЯ ЗАПАСАМИ ТОРГОВЕЛЬНОГО ПІДПРИЄМСТВА

Попов Євгеній Станіславович 29

РОЗРОБКА ІНТЕРАКТИВНОГО МОДУЛЯ ДЛЯ ГРИ MINECRAFT З ПІДТРИМКОЮ ВЗАЄМОДІЇ ГРАВЦІВ ЧЕРЕЗ ЧАТ ПРЯМИХ ТРАНСЛЯЦІЙ

Посенко Данило Романович 30

РОЗРОБКА МЕТОДІВ ТА ЗАСОБІВ УПРАВЛІННЯ ІГРОВИМИ ПОДІЯМИ ЧЕРЕЗ ІНТЕГРАЦІЮ З ДОНАТ-СЕРВІСАМИ

Посенко Данило Романович 31

ДОСЛІДЖЕННЯ МЕТОДІВ ФАКТОРИЗАЦІЇ МНОГОЧЛЕНІВ ТА ЇХ ЗАСТОСУВАННЯ В КРИПТОГРАФІЇ

Самосєєв Євгеній Дмитрович 33

ВИКОРИСТАННЯ ГЕОЛОКАЦІЙНИХ СЕРВІСІВ ДЛЯ ВІЗУАЛІЗАЦІЇ ЗАБРУДНЕНОСТІ ТЕРИТОРІЇ РАДІОАКТИВНИМИ НУКЛІДАМИ

Свищо Максим Іванович 35

ВИДИ АПАРАТНО-ПРОГРАМНИХ КОМПЛЕКСІВ (АПК) МОНІТОРИНГУ ЯКОСТІ ПОВІТРЯ

Степанець Михайло Володимирович 37

ФОРМУВАННЯ РАХУНКІВ КІЛЬКОХ ВІДВІДУВАЧІВ РЕСТОРАНУ

Циба Володимир Олексійович 39

РОЗРОБКА ДОДАТКУ ДЛЯ ПЛАНУВАННЯ ОСОБИСТОГО БЮДЖЕТУ

Шемет Євгеній Ігорович 41

TF-IDF ДЛЯ ОЧИЩЕННЯ ТЕКСТОВИХ ДАНИХ У КЛАСИФІКАЦІЙНИХ ЗАДАЧАХ З ВИКОРИСТАННЯМ NLP

Шидловський Тимофій Максимович 42