КИЇВСЬКИЙ СТОЛИЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ БОРИСА ГРІНЧЕНКА
Факультет інформаційних технологій та математики
Кафедра комп'ютерних наук
Кафедра математики і фізики
Кафедра інформаційної та кібернетичної безпеки
ім. професора Володимира Бурячка

ISSN: 2664-2638 (Online)

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ – 2025

Збірник тез
XII Всеукраїнської науково-практичної конференції
молодих учених

15 травня 2025 року
м. Київ

Київ – 2025

УДК 004:378(082)
ББК 32.97:74.58я73
І-74

Схвалено Вченою радою факультету інформаційних технологій та математики Київського столичного університету імені Бориса Грінченка
(Протокол № 5 від 14.05.2025 р.)

Відповідальні за випуск:
М.М. Астаф'єва,
Д.М. Бодненко,
О.М. Глушак,
І.В.Машкіна,
О.В. Локазюк,
В.В. Прошкін,
С.М. Шевченко

Інформаційні технології – 2025: зб. тез XII Всеукраїнської науково-практичної конференції молодих учених, 15 трав. 2025 р., м. Київ / Київський столичний університет імені Бориса Грінченка; Відповід. за вип.: М.М. Астаф'єва, Д.М. Бодненко, О.М. Глушак, І.В. Машкіна, О.В. Локазюк, В.В. Прошкін, С.М. Шевченко. Київ : Київський столичний університет імені Бориса Грінченка, 2025. 362 с. ISSN: 2664-2638.

УДК 004:378(082)
ББК 32.97:74.58я73

Секція 1
ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ОСВІТІ ТА НАУЦІ

ВЕБ-СЕРВІС ДЛЯ ОРГАНІЗАЦІЇ ТА УПРАВЛІННЯ ОСВІТНІМ ПРОЦЕСОМ УНІВЕРСИТЕТУ

Адаменко В. О.
Вінницький національний технічний університет, м. Вінниця

У сучасному світі цифровізація дедалі активніше охоплює всі сфери діяльності, і система освіти не є винятком. Особливо актуальним є впровадження інформаційних технологій у вищих навчальних закладах, де постає необхідність автоматизації навчального процесу, забезпечення оперативної комунікації між усіма його учасниками та підвищення ефективності адміністрування. Веб-сервіси стають ключовим інструментом у реалізації цих завдань, дозволяючи поєднати функціональність, зручність і масштабованість в одному рішенні.

Заклади вищої освіти дедалі частіше інтегрують веб-сервіси [1] для реєстрації студентів, формування розкладу, ведення електронного журналу, управління курсами та оцінюванням. Такі рішення не тільки оптимізують роботу адміністрації та викладачів, а й покращують доступ студентів до навчальних матеріалів, спрощують контроль за успішністю та створюють прозоре освітнє середовище.

Метою цієї роботи є проєктування та реалізація веб-сервісу для організації та управління освітнім процесом університету. Сервіс має продемонструвати, як сучасні технології можуть сприяти підвищенню ефективності навчання, полегшенню адміністрування та вдосконаленню взаємодії між учасниками освітнього процесу.

Функціональні можливості системи

Серед функціональних можливостей системи передбачено реєстрацію та автентифікацію користувачів, зокрема студентів, викладачів та адміністрації, із забезпеченням входу до системи з авторизацією за роллю. Реалізовано модуль розкладу занять, що дозволяє переглядати розклад для викладачів і студентів, а також формувати його адміністраторам. Електронний журнал дозволяє викладачам вносити оцінки, а студентам переглядати свою успішність.

Система підтримує завантаження навчальних матеріалів, таких як презентації, документи та відеолекції, з можливістю каталогізації за предметами. Забезпечено функціонал тестування і контролю знань –

викладачі можуть створювати тести, студенти –проходити їх, а результати перевіряються автоматично. Адміністративні функції охоплюють додавання нових курсів, викладачів і студентів, а також генерацію звітів. Для забезпечення комунікації реалізовано механізми розсилки повідомлень і сповіщень, зокрема нагадування про тести або зміни в розкладі.

Використані технології

Серверна частина реалізована на основі фреймворку Spring Boot мовою програмування Java [2], що дозволяє створити надійний RESTful API та структурувати бізнес-логіку за принципами MVC. Клієнтську частину реалізовано з використанням React.js, що забезпечує швидкодію, реактивність і комфортну роботу у браузері.

Для зберігання даних використано PostgreSQL [3] – потужну реляційну СУБД із підтримкою складних зв'язків між таблицями. Аутентифікація та керування сесіями здійснюється за допомогою JWT-токенів, що дозволяє гарантувати безпеку і масштабованість [4]. Увесь застосунок контейнеризовано з використанням Docker, що спрощує процес розгортання та забезпечує стабільність незалежно від середовища. Система керування версіями Git та CI/CD-пайплайн через GitHub Actions забезпечують безперервну інтеграцію і контроль якості коду.

Вибір саме цих технологій дозволив реалізувати гнучку, безпечну і масштабовану систему, придатну для подальшого розширення функціоналу відповідно до потреб навчального закладу.

Висновки

У ході виконання роботи було спроєктовано та реалізовано веб-сервіс для організації та управління освітнім процесом університету. Сервіс охоплює всі основні аспекти взаємодії між студентами, викладачами та адміністрацією: забезпечує зручний доступ до навчальних матеріалів, автоматизує процес оцінювання, дозволяє ефективно формувати й змінювати розклад занять, а також підтримує комунікацію між учасниками освітнього процесу.

Результати роботи засвідчили, що веб-сервіси є потужним інструментом для оптимізації навчального процесу. Вони не лише зменшують адміністративне навантаження, а й забезпечують прозорість оцінювання, гнучкість у плануванні занять і підвищення загальної організованості освітньої діяльності. Впровадження такого сервісу створює надійне цифрове середовище, яке сприяє покращенню якості навчання, полегшує управління освітніми процесами та відповідає вимогам сучасної вищої освіти.

ДЖЕРЕЛА

1. Веб-сервіси. URL: https://osvita.if.ua/page/naipopuliarnishi-osvitni-platformi-dlia-organizatsiyi-distantsiinogo-navchannia

2. Joshua B. Effective Java Programming Language Guide. Boston: Addison-Wesley Professional, 2018. 412 p.

3. PostgreSQL. URL: https://www.postgresql.org.

4. Гаррісон Р., Шиєлдс П. Автентифікація та авторизація у вебі. Лондон: Leanpub, 2011. 254 с.

FIGMA ЯК ІНСТРУМЕНТ ДЛЯ ЕФЕКТИВНОЇ РОБОТИ ФАХІВЦІВ З РЕКЛАМИ ТА ЗВ'ЯЗКІВ З ГРОМАДСЬКІСТЮ

Аркушенко Б., Кравець К., Сивченко В., Вітова А., Кулибаба А.

Київський столичний університет імені Бориса Грінченка, м. Київ

Figma – це зручний онлайн-інструмент для дизайну інтерфейсів, за допомогою якого можна створювати макети, прототипи, іконки та багато іншого. Від моменту запуску у 2016 році він став популярним серед новачків і професіоналів завдяки простоті використання та можливостям спільної роботи у реальному часі. Цей інструмент дозволяє командам одночасно працювати над проєктами незалежно від їх місцезнаходження. Це дуже спрощує командну роботу, адже всі учасники можуть бачити зміни одразу й обмінюватися коментарями у макеті [2].

Головна фішка Figma – сервіс не потребує установки. Достатньо працювати у браузері, хоча є й десктопна та мобільна версії. Також доступні шаблони, плагіни та цифрова дошка FigJam, яка ідеальна для брейнштормів. Це універсальний інструмент для сучасних дизайн-завдань. Інструмент пропонує всі основні можливості для створення дизайнів: малювати фігури, працювати з текстами, додавати зображення, створювати кнопки чи іконки. Якщо ви часто використовуєте одні й ті ж елементи, наприклад, логотип чи стилізовану кнопку, можна зробити їх компонентами. Змінюєте один компонент – і всі його копії у макеті автоматично оновлено. Це економить час і гарантує, що все буде виглядати гармонійно.

Figma дозволяє не тільки створювати статичні макети, а й робити інтерактивні прототипи. Можна налаштувати переходи між екранами, додати прості анімації та подивитися, як усе буде виглядати у справжньому додатку чи на сайті. Це дуже допомагає, коли треба презентувати проєкт замовнику або протестувати ідею.

Ще одна функція – це бібліотеки стилів. Вони потрібні, щоб зберігати кольори, шрифти та інші елементи дизайну в одному місці. Якщо є брендбук або дизайн-система, їх легко організувати у бібліотеці, а потім використовувати у різних проєктах. Коли дизайн готовий, його легко передати розробникам. Figma дає можливість подивитися розміри елементів, експортувати картинки або шрифти тощо.

Структурований перелік задач, що виконує Figma:

- Макети веб-сайтів.
- Макети мобільних додатків.

- Дизайн іконок.
- Прототипи.
- Дизайн інтерфейсів для настільних програм.
- Створення банерів.
- Дизайн логотипів.
- Створення презентацій.
- Редагування фотографій.
- Розробка UX/UI дизайну.

Figma – це не просто інструмент, а справжній помічник для дизайнерів і команд. Ресурс робить процес створення проєктів швидким, простим і приємним. Щоб повноцінно оцінити можливості Figma, варто розглянути її основні переваги та недоліки.

Переваги та недоліки Figma для реклами [1]:

Переваги

- Швидке створення візуалізацій для клієнтів.
- Можливість тестувати макети для веб- та мобільних застосунків.
- Рекламісти можуть миттєво обмінюватися ідеями з дизайнерами, копірайтерами та клієнтами.
- Зручне налаштування дизайнів для соціальних мереж, банерів, вебсайтів тощо.
- Доступ до готових шаблонів для стандартних рекламних форматів.

Недоліки

- Figma не пропонує розширених інструментів для створення відео чи інтерактивного контенту, які часто потрібні в рекламі. Для нестандартних форматів реклами може знадобитися інтеграція з іншими сервісами.

Переваги та недоліки Figma для PR

Переваги

- Зручний інструмент для створення презентацій, інфографіки та макетів.
- Швидке створення прототипів сторінок для пресрелізів чи лендінгів.
- Ефективна співпраця з дизайнерами та розробниками в єдиному робочому просторі.
- Піарникам без дизайнерського досвіду легко створювати базові візуальні матеріали.

Недоліки

- Редагування текстів у Figma менш зручне, ніж у спеціалізованих текстових редакторах.
- Для створення динамічних відео чи інтерактивних матеріалів потрібні інші інструменти.

Figma позиціонує себе як сучасний багатофункціональний інструмент, що дозволяє фахівцям із реклами та зв'язків з громадськістю ефективно працювати над креативними проєктами. Figma також допомагає швидко та зручно створювати нові концепції, працювати над візуальними матеріалами для соціальних мереж, банерів чи публікацій, легко адаптуючи їх під різні формати. Завдяки зрозумілому інтерфейсу та продуманим інструментам, підготовка матеріалів стає значно простішою, залишаючи більше часу для творчості та розробки стратегії. Крім того, Figma дозволяє миттєво вносити зміни до дизайнів, що дуже зручно, коли потрібно швидко реагувати на запити клієнтів чи партнерів. Завдяки можливостям у створенні інтерактивних прототипів, використання бібліотек елементів та роботи із векторною графікою, значно полегшуються процеси проєктування. Figma ідеально підходить для створення інтерактивних презентацій, що важливо для роботи з громадськістю. Можливості коментування та версіонування, дозволяють прозоро та узгоджено працювати учасникам команди, а інструмент FigJam відкриває можливості роботи над ідеями та плануванням ще до створення прототипів.

Figma – це помічник для рекламістів та піарників, який працює з візуальними матеріалами і прототипами швидко та ефективно. Цей інструмент дозволяє дизайнерам та їх командам працювати разом незалежно від їх місцезнаходження, що значно підвищує продуктивність. З Figma легко створювати макети, інтерактивні прототипи та інші візуальні елементи, а також обмінюватися ідеями у режимі реального часу. Інтуїтивний інтерфейс і широкий набір функцій допомагають швидко реалізувати найсміливіші ідеї та забезпечують високу якість роботи.

ДЖЕРЕЛА

1. Figma: що це таке, для чого і кому потрібна [Електронний ресурс] - Режим доступу: https://cases.media/article/sho-take-figma-ta-dlya-kogo-vona-potribna?srsltid=AfmBOooSnq-Nonx0_EL3MwYx2AlE3Ec07HiL-iFNMLPhiP5NzHtZ-wfM2 (дата звернення 03.12.2024)

2. Figma – базовий інструмент для роботи дизайнерів [Електронний ресурс] - Режим доступу: https://kiev.itstep.org/blog/figma-is-a-basic-tool-for-designers (дата звернення 03.12.2024)

АНАЛІЗ ПОВЕДІНКОВИХ ПАТЕРНІВ СТУДЕНТІВ І ВИКЛАДАЧІВ ДЛЯ ВПРОВАДЖЕННЯ МЕТОДИКИ АВТОМАТИЗОВАНОГО ТЕСТУВАННЯ UX/UI ДИЗАЙНУ ОСВІТНІХ ЦИФРОВИХ ПЛАТФОРМ ІЗ ЗАСТОСУВАННЯМ МЕТОДІВ ШТУЧНОГО ІНТЕЛЕКТУ

Бажан Ю. П.

Державний університет інформаційно-комунікаційних технологій, м. Київ

У сучасній освіті цифрові платформи стають основним середовищем для навчання, викладання та організації освітнього процесу. Від якості UX/UI дизайну залежить ефективність взаємодії користувачів із платформами, швидкість засвоєння матеріалу, рівень задоволеності та адаптації. На жаль, багато існуючих рішень не враховують відмінності в поведінкових моделях студентів і викладачів, що призводить до фрустрації, втрати мотивації і зниження ефективності освітнього процесу [1]. Проблема ускладнюється тим, що традиційні підходи до тестування інтерфейсів орієнтуються на усередненого користувача і не враховують специфічних потреб кожної категорії.

У межах дослідження було створено базу поведінкових патернів студентів і викладачів. Аналіз проводився на основі clickstream-даних, теплових карт активності користувачів, записів сесій та опрацювання текстових коментарів за допомогою методів обробки природної мови (NLP) [2]. Для класифікації типових сценаріїв застосовано алгоритми машинного навчання, що дозволило виявити характерні моделі поведінки кожної групи користувачів.

Студенти виявили схильність до короткотривалих сесій, активного використання пошуку та швидкого переходу між розділами. Натомість викладачі частіше взаємодіяли з розширеними функціями управління контентом, аналітикою та налаштуваннями курсів.

Отримані дані показали, що навіть невеликі відмінності у дизайні можуть критично впливати на зручність використання. Наприклад, у студентів викликали труднощі багаторівневі меню без чіткої ієрархії, тоді як викладачі стикалися з недоступністю деяких функцій через нестачу інформаційних підказок. На основі аналізу було визначено найбільш критичні точки взаємодії з інтерфейсом, де виникає найбільше збоїв у користувацькому досвіді.

Для усунення виявлених недоліків запропоновано нову методику автоматизованого тестування UX/UI освітніх платформ. Особливістю підходу є адаптивність тестових сценаріїв до ролі користувача: окремо для студентів і окремо для викладачів. Система автоматично генерує тести, спрямовані на виявлення типових проблем –неінтуїтивної навігації, прихованих функцій, перевантаження екрана або нестачі доступності.

Такий підхід дозволяє не лише прискорити процес виявлення UX-проблем, а й зробити його більш персоналізованим і релевантним.

Запропонована методика дозволяє значно скоротити витрати часу на ручне тестування, мінімізувати суб'єктивність оцінювання та підвищити якість освітніх цифрових середовищ. Автоматизація тестування з урахуванням поведінкових особливостей користувачів сприяє підвищенню інклюзивності платформ та їх адаптивності до різних сценаріїв використання. Зокрема, завдяки цьому можна покращити доступність освітнього процесу для студентів з особливими освітніми потребами.

Таким чином, аналіз поведінкових патернів студентів і викладачів створює базу для побудови гнучких і адаптивних освітніх платформ, здатних краще відповідати очікуванням різних груп користувачів. Інтеграція моделей штучного інтелекту в процес тестування UX/UI відкриває нові перспективи для розвитку персоналізованого цифрового навчання, що базується на реальних потребах користувачів.

ДЖЕРЕЛА

1. Norman D. A. The Design of Everyday Things. New York: Basic Books, 2013. 384 p.
2. Krug S. Don't Make Me Think, Revisited: A Common Sense Approach to Web Usability. Berkeley: New Riders, 2014. 216 p.
3. Russell S., Norvig P. Artificial Intelligence: A Modern Approach. 4th ed. London: Pearson, 2021. 1152 p.

ГЕНЕРАТОРИ ЗОБРАЖЕНЬ ЗА ДОПОМОГОЮ ШІ

Баштова А., Кальян П., Литовка У., Бежевець А.,
Бекіров Е., Бодненко Д., Локазюк О.
Київський столичний університет імені Бориса Грінченка, м. Київ

Людство завжди прагнуло покращувати своє життя, автоматизувати складні завдання та зменшувати час на їх виконання. Ці потреби стали рушійною силою для створення технологій, які дозволяють вирішувати проблеми ефективніше. Однією з таких інновацій став штучний інтелект (ШІ) – технологія, яка змінила уявлення про можливості машин.

Розвиток ШІ відкрив нові горизонти для науки, бізнесу й суспільства, надаючи можливість вирішувати складні завдання з небаченою раніше швидкістю та ефективністю. Завдяки інтеграції машинного навчання, обробки природної мови та інших методів, системи ШІ здатні аналізувати великі обсяги даних, передбачати результати та оптимізувати процеси у різних сферах.

«Штучний інтелект (ШІ) – це технологія, яка дозволяє комп'ютерам виконувати завдання, що вимагають людського інтелекту» [1], такі як навчання, аналіз даних та ухвалення рішень

ШІ широко використовується в різних галузях, включаючи маркетинг, де він застосовується для персоналізації пропозицій, створення контенту та таргетингу реклами.

Генератори зображень на основі ШІ стають все популярнішими серед користувачів, причому найбільшу частку становлять ті, хто використовує Canva.

Canva є зручним інструментом для створення презентацій, але може мати проблеми з якістю зображень, особливо коли мова йде про людей або тварин.

Microsoft Bing також пропонує генератор зображень, який добре справляється зі створенням картинок за детальними описами, але може мати проблеми з вставленням тексту в зображення.

З метою аналізу даних щодо використання генераторів зображень нами проведено опитування серед студентів закладів вищої освіти України:

- Популярність генераторів зображень: 57% опитаних використовують генератори зображень ШІ.
- Розподіл використання генераторів: 37% використовують Canva, 11% - Microsoft Bing, 26,3% вважають обидва інструменти зручними.

Більшість опитаних вважають Canva більш зручним інструментом, ніж Microsoft Bing.

ШІ (штучний інтелект) –це технологія, яка дозволяє комп’ютерам і системам виконувати завдання, що зазвичай вимагають людського інтелекту, такі як розпізнавання мови, ухвалення рішень, навчання та аналіз даних[1, 2].

ШІ використовується в різних галузях, від медицини до транспорту, автоматизації й навіть у повсякденних застосунках, як-от віртуальні помічники

Специфіка штучного інтелекту (ШІ) у маркетингу та PR має безліч переваг і відкриває нові можливості для ефективної роботи.

Наприклад, Netflix чи Amazon використовують ШІ для персоналізації пропозицій, що значно підвищує лояльність клієнтів.

ШІ вже використовується для написання текстів, створення відео та графіки (наприклад, через генеративні моделі, як DALL·E або ChatGPT).

Рекламні платформи (Google Ads, Facebook Ads) використовують ШІ для таргетингу, визначення ключових слів і налаштування ставок(Рис.1).

	Canva	Bing
Плюси	Можливість обрати різні стилі(мінімаліз, яскраві, аніме і тд)	Безкоштовний Хороша передача кольорів Реалістичні зображення
Мінуси	Платна версія Неточність по заданих кольорах	3 спроби на день Один стиль Нереалістичні зображення людей

Рис. 1. Порівняльний аналіз Canva та Bing.

Результати опитування засвідчують наступне:

- 57% з опитуваних використовують генератор картинок ШІ.
- 37% використовували генератор в Canva.
- 11% використовували генератор Microsoft Bing.

Canva. Зручний застосунок для створення презентацій. Не завжди робить те, що від нього вимагають. Обличчя людей розмиті, додає зайві пальціі. Але якщо це не фото людей чи тварин, то справляється не погано.

На запитання: «Який спосіб ви вважаєте кращим/зручнішим?», отримано наступні відповіді реципієнтів:

- Canva - 61,4%
- Microsoft Bing - 12,3%
- Обидва зручні - 26,3%

Отже, Canva є більш популярним і зручним інструментом для створення зображень серед опитаних користувачів. Однак, обидва інструменти мають свої переваги та недоліки, і вибір того чи іншого залежить від конкретних потреб користувача.

ДЖЕРЕЛА

1. Штучний інтелект Електронний ресурс. URL: http://dspace.puet.edu.ua/handle/123456789/12911

2. Навчальний курс по штучному інтелекту (на базі Стенфордського курсу) Електронний ресурс. URL: https://web.archive.org/web/20120210055110/https://www.ai-class.com/.

МОЖЛИВОСТІ ЦИФРОВОГО МОДЕЛЮВАННЯ І ВІРТУАЛЬНИХ ЛАБОРАТОРІЙ У НАВЧАННІ ТЕОРІЇ ЕЛЕКТРИЧНИХ ТА МАГНІТНИХ КІЛ

Білак В. В., Гураль І. В.
Західноукраїнський національний університет, м. Тернопіль

Сучасна система вищої технічної освіти потребує впровадження ефективних цифрових інструментів, які сприяють не лише засвоєнню теоретичних знань, а й розвитку критичного мислення, дослідницьких та практичних навичок. Особливо актуальним це є для дисциплін з високим рівнем абстракції, таких як теорія електричних та магнітних кіл. Традиційні методи навчання часто не дають змоги наочно продемонструвати фізичні процеси, що відбуваються в електричних схемах. Саме тому важливим кроком є впровадження інформаційних технологій у навчальний процес [1].

Серед доступних програмних рішень NI Multisim вирізняється широким функціоналом для проєктування та аналізу електричних кіл. Його застосування на заняттях із дисципліни дозволяє:

- створювати схеми різної складності: від простих послідовних з’єднань до складних транзисторних каскадів;
- проводити якісний аналіз перехідних процесів та гармонічних коливань;
- здійснювати параметричні дослідження без використання фізичних лабораторій;
- оперативно змінювати вхідні умови експерименту та фіксувати результати.

NI Multisim підтримує симуляцію в реальному часі, що дає змогу студентам взаємодіяти з віртуальними приладами (осцилографами, мультиметрами, джерелами сигналів) подібно до роботи в реальній лабораторії [2].

Віртуальні лабораторії стали невід’ємною частиною технічної підготовки майбутніх інженерів, особливо в умовах гібридного чи дистанційного навчання. Таким чином вони забезпечують: гнучкість доступу до лабораторних установок у будь-який час; безпечне середовище для експериментів із високовольтним обладнанням; адаптивність – можливість виконання завдань на різних рівнях складності; індивідуалізацію навчальної траєкторії залежно від рівня підготовки студента.

Такий підхід не лише підвищує ефективність засвоєння матеріалу, а й сприяє розвитку навичок самостійної роботи, планування та аналізу результатів [3].

Інтеграція навчального середовища Moodle із системами симуляції відкриває можливості для створення адаптивних курсів з елементами

автоматизованої перевірки результатів. Наприклад, студенти можуть виконувати лабораторні завдання безпосередньо у Multisim, а результати подаються у вигляді скріншотів, цифрових вимірювань чи звітів. Програмні плагіни Moodle дозволяють інтегрувати тестові завдання, що містять симуляційні компоненти, та автоматично оцінювати їх за заданими критеріями [4].

Це дозволяє сформувати наскрізну систему зворотного зв'язку між викладачем і студентом, а також забезпечити об'єктивність оцінювання.

Використання цифрових технологій у навчанні електротехнічних дисциплін відповідає вимогам STEM-освіти, яка передбачає міждисциплінарне поєднання чотирьох ключових напрямів: науки (Science), технологій (Technology), інженерії (Engineering) та математики (Mathematics). Такий підхід спрямований не лише на передачу теоретичних знань, але й на формування практичних умінь, критичного мислення, аналітичних здібностей та навичок вирішення реальних прикладних завдань.

У контексті дисципліни «Теорія електричних та магнітних кіл» це означає, що студенти не просто опрацьовують формули і схеми, а занурюються в середовище моделювання, де можуть досліджувати динамічні процеси, проводити експерименти, оцінювати вплив параметрів на поведінку систем. Поєднання моделювання, числового аналізу та автоматизованого оцінювання результатів дозволяє будувати гнучкі, персоналізовані курси, що адаптуються до потреб кожного студента.

Інтеграція інформаційних технологій, зокрема NI Multisim, віртуальних лабораторій та систем тестування, дозволяє не лише покращити якість підготовки студентів у галузі теорії електричних та магнітних кіл, а й суттєво модернізувати навчальний процес. Ці інструменти створюють нові можливості для розвитку цифрової грамотності, практичних навичок та аналітичного мислення. Подальші дослідження доцільно зосередити на створенні модульних цифрових освітніх платформ, інтегрованих у єдину навчальну інфраструктуру.

ДЖЕРЕЛА

1. Молчанов О. В., Бородіна І. П. Використання електронних засобів навчання у вищій технічній школі // Інформаційні технології і засоби навчання. – 2021. – №4(84). – С. 22–30.

2. Franco S. Design with Operational Amplifiers and Analog Integrated Circuits. – McGraw-Hill Education, 2014. – 704 p.

3. Андрієнко Т. Л. Комп'ютерне моделювання електронних пристроїв у Multisim // Вісник ХНУРЕ. – 2019. – №1. – С. 118–123.

4. Bidwell J. Innovative Strategies for Integrating Simulations in Engineering Education. // Journal of STEM Education, 2020. – Vol. 21(3). – P. 45–52.

ВИКОРИСТАННЯ СЕРВІСУ *GOOGLE SLIDES* У РОБОТІ ПОВЕДІНКОВОГО СПЕЦІАЛІСТА

Богданова І., Головаченко Ю., Калюжна В., Радченко Н.
Київський столичний університет імені Бориса Грінченка, м. Київ

Корпорація Google розробила багато корисних онлайн-інструментів для роботи, навчання та інших цілей. Серед різноманітних багатьом відомих сервісів також є зручна та функціональна платформа для створення презентацій, відома як Google Slides. Дане дослідження має на меті розглянути питання використання сервісу Google Slides в роботі поведінкового спеціаліста.

Поведінкові спеціалісти (АВА-терапісти) працюють з дітьми, що мають проблеми розвитку, проблеми в поведінці та навчанні. Вони мають досконало та ретельно визначити наявні навички у дитини з ООП та відстежити відсутні навички, над якими планують працювати найближчим часом. Існує багато інструментів для діагностики аутизму та оцінювання мовленнєвих навичок дітей з аутизмом (ADOS, ЕСДМ, VB-MAPP, ABBLS, AFLS, CARS, CABS, M-CHAT).

Більшість з цих інструментів призначені для того, щоб дослідити, наскільки навички дитини з розладами аутистичного спектру розвинені в порівнянні з навичками його однолітків, що розвиваються типово. Для виконання цієї задачі необхідно безліч матеріалів, які неможливо придбати, скласти у коробки і все це розмістити в кабінеті фахівця через брак місця та економічної складової. Саме Google Slides може допомогти АВА спеціалісту реалізувати поставлену задачу.

Google Slides ефективний інструмент для візуалізації, тому його можна використовувати не лише для оцінювання навичок дитини, а також застосовувати під час поведінкового втручання для формування великої кількості навичок, серед них: візуальні навички, рецептивне мовлення, навички називання, інтравербальні навички та ін [1].

Сервіс Google Slides має досить простий та зрозумілий інтерфейс, тому в ньому легко розберуться користувачі з будь-яким рівнем підготовки. Він не потребує від користувача спеціального навчання.

В нашому центрі багато АВА спеціалістів, тому цей сервіс крисний ще й тим що надає групам користувачів можливість разом працювати з Google Slides та редагувати матеріали. Автор презентації може надати свої колегам різні рівні доступу (редактор, читач, коментатор), також може поділитися презентацією через посилання або публікацію на сайті, та зберегти її в різних форматах (PDF/PPTX/ODP). Використання сервісу допомагає спеціалісту економити час на підготовку до занять та прибирання матеріалу після його проведення.

Сервіс Google Slides пропонує безліч інструментів для налаштування дизайну презентацій. Він дозволяє редагувати макети, змінювати фон,

шрифт, колір, додавати картинки, відео, анімацію, таблиці, графіки тощо. Однією з важливих переваг сервісу є те, що він автоматично зберігає всі зміни, які користувач вносить у презентацію. Сервіс є безкоштовним, що надає йому особливого значення в умовах повномасштабного вторгнення.

Щоб зосередити увагу дитини на завданні ми переважно не використовуємо макети чи фони, які відволікають дитину від його виконання.

Google Slides дозволяє створювати інтерактивні та візуально привабливі презентації, які можуть включати текст, зображення, відео та навіть аудіофайли, що робить навчання більш динамічним і цікавим. Тому ми зупинимося на одній із наших презентацій, завданням якої є навчити дитину з ООП називати дію, яка відбувається в поточний час (https://docs.google.com/presentation/d/1eOYBNLwwR-6rqktuzJP2ampp4EOCvG1z/edit?usp=sharing&ouid=113310751187213822408&rtpof=true&sd=true).

Для дітей з ООП називання дієслів є досить складною навичкою і потребує інтенсивного вивчення. Саме для цього ми використовуємо інструмент вставлення коротких відео у презентацію. Під час демонстрації слайдів педагог натискає на кнопку «пуск» в результаті якої запускається відео і дитині легше зрозуміти яка саме дія зараз відбувається (Рис.1).

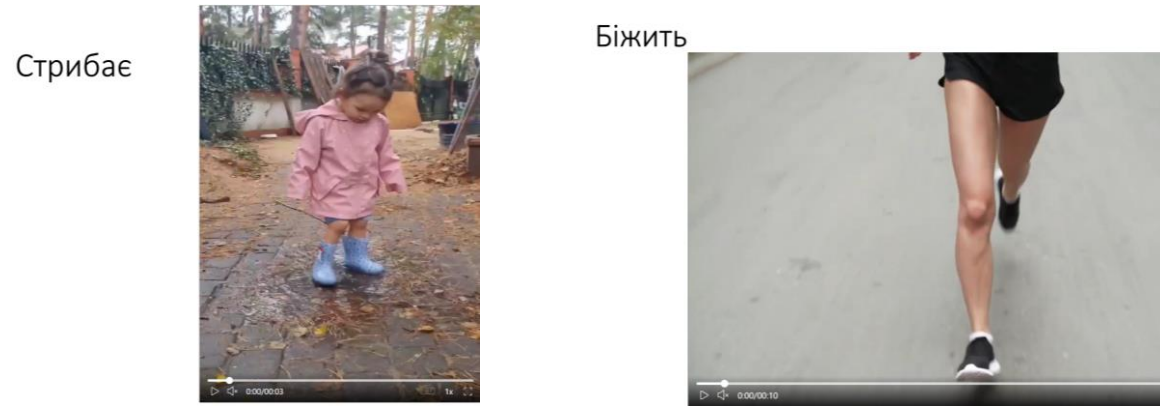


Рис.1. Вправа «Що робить?»

Такий формат донесення інформації до дітей з аутизмом підходить для створення більш інтерактивного навчального процесу, адже діти з ООП часто краще сприймають інформацію через зображення та відео. Завдяки цьому, діти можуть не лише чути дієслова, а й бачити, як ці дії виконуються в реальному часі. Також дуже важливо використовувати повторення: показувати одні й ті ж дії в різних контекстах та (або) з різними персонажами, щоб діти змогли асоціювати дієслова не з особою яка виконує дію, а з конкретними ситуаціями. Інтерактивне вивчення дієслів безперечно краще ніж їх вивчення на статичних друкованих картинках. Завдяки такому підходу, навчання стане не лише більш доступним, але й цікавим для дітей, що значно підвищить їх мотивацію до

корекційних занять. А в роботі поведінкового спеціаліста цей сервіс суттєво полегшує процес тестування та формування навичок.

Звичайно, Сервіс Google Slides не зможе діагностувати рівень сформованості навичок імітації, рухів дрібної та великої моторики, вокальної імітації, навичок прохання, комунікації, соціальної взаємодії, навичок письма, навичок догляду за собою. Не допоможе сервіс і з корекцією проблемних видів поведінки. Сервіс Google Slides не виключає використання друкованих матеріалів чи іграшок. Проте, він є дуже зручним засобом для діагностики величезної кількості навичок у дитини з розладами аутистичного спектру. Саме тому Google Slides вважається одним із найпопулярніших хмарних сервісів для створення і оформлення презентацій. Функціональний і простий у використанні, широкий вибір макетів і тем дизайну. Все це допомагає нам, АВА фахівцям, у нашій непростій роботі з дітьми з РАС. За допомогою цього інструменту спеціаліст може адаптувати матеріал під індивідуальні потреби кожної дитини з особливими освітніми потребами.

ДЖЕРЕЛА

1. Інноваційні технології формування життєвих компетентностей дітей з особливими освітніми потребами в системі краєзнавчої позашкільної освіти. Електронний ресурс. URL: https://st.kharkov.ua/wp-content/uploads/2025/01/METODYCHKA-2024-zbilsheni-zobrazhennia-1.pdf

2. Використання Google Slides у процесі дистанційного навчання. URL: https://surl.li/ksupry

3. Вебінар: 10 способів використання Google Презентацій під час змішаного навчання Електронний ресурс: URL: https://naurok.com.ua/webinar/10-sposobiv-vikoristannya-google-prezentaciy-pid-chas-zmishanogo-navchannya

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ЯК ІНСТРУМЕНТ РОЗВИТКУ ЕМОЦІЙНОЇ КОМПЕТЕНТНОСТІ МОЛОДІ: ЗАСТОСУНОК ПСИХОЛОГІЧНОЇ ПІДТРИМКИ НА ОСНОВІ ЕМОЦІЙНОГО ДИЗАЙНУ

Бондаренко А. О.

Київський столичний університет імені Бориса Грінченка, м. Київ

У серпні 2023 року понад половина студентів-медиків (59,6%) вказали на наявність симптомів тривожності; 58,8% зазначили про депресію і 62 ,5%, –про стресовий стан. Для порівняння: у 2019 році лише близько 23 % студентів вказали на виявлення подібних симптомів [1]. Не зважаючи на відсутність довгострокових досліджень можна зауважити значне збільшення психоемоційного навантаження серед молоді за вказаний період часу. У зв’язку з цим трендом, у межах бакалаврської

роботи було розроблено мобільний застосунок для надання психологічною підтримки з функціями емоційного щоденника і самодіагностики, а візуальна концепція додатку була натхненна мультфільмом Inside Out [4].

Архітектура застосунку реалізована на базі React Native та з використанням середовища Expo Snack. Інтерфейс застосунку адаптується до емоційного стану користувача через умовну логіку рендерингу.

На відміну від конкурентів, представлених на ринку, додаток орієнтований на індивідуальні емоційні потреби користувача. Залежно від обраної емоції, в режимі реального часу актуалізовуються відповідні функціональні модулі: самодіагностика за шкалами PHQ-9 та GAD-7, щоденник рефлексії, тематичні поради, а також навчальні матеріали. Такий підхід вибудовує персоналізовану взаємодію додатку і враховує актуальний емоційний стан користувача та рівень його залученості [2; 3].

Інтерфейс застосунку побудований на принципах емоційного дизайну Д. Нормана – з акцентом на вісцеральний, поведінковий і частково рефлексивний рівні сприйняття [5]. Образи персонажів із мультфільму Inside Out слугують не лише ілюстраціями, а також посередниками, які допомагають користувачу краще зрозуміти природу і суть пережитої емоції, а також спонукають виразити власні переживання у щоденнику рефлексій [4]. Наприклад, персонаж Страх звертається до користувача зі словами: «Я не ворог. Я – сигнал. Я приходжу не для того, щоб паралізувати, а щоб зупинити тебе на секунду і дати подумати: «А як зробити безпечніше?». «Такий спосіб взаємодії м’яко навчає користувача опановувати емоції, розуміти їх суть та призначення, що полегшує роботу з внутрішніми станами.

Застосунок охоплює ключові елементи психологічної самопідтримки, як трекінг емоцій, збереження відповідей, рефлексію та спостереження за динамікою емоційного стану. Разом із тим має освітній компонент, адже завдяки ненав’язливій взаємодії з персонажами користувач знайомиться з природою власних емоцій, вчиться їх розпізнавати, розуміє їх мету та опановує прості техніки для саморегуляції. Завдяки такому підходу додаток можна інтегрувати у навчальні модулі з психології, емоційного інтелекту або уроки з основ здоров’я. Також додаток буде помічником для педагогів і дитячих психологів.

Інноваційність розробки полягає в поєднанні адаптивної логіки подачі контенту, емоційно орієнтованого дизайну, а також наповненню навчальними елементами. Цей підхід створює універсальний і гнучкий інструмент, який стане у пригоді як і для особистого використання, так і для інтеграції в освітні процеси.

ДЖЕРЕЛА

1. Lushchak O. та ін. Prevalence of stress, anxiety, and symptoms of post-traumatic stress disorder among Ukrainians after the first year of Russian

invasion: a nationwide cross-sectional study // The Lancet Regional Health – Europe. – 2024. – Т. 36. – URL: https://www.thelancet.com/journals/lanepe/article/PIIS2666-7762(23)00192-8/fulltext

2. Wüllner S. та ін. Mobile applications in adolescent psychotherapy during the COVID-19 pandemic: a systematic review // Frontiers in Public Health. – 2024. – Т. 12. – № статті 1345808. – URL: https://www.frontiersin.org/articles/10.3389/fpubh.2024.1345808/full

3. Almuqrin A. та ін. Smartphone apps for mental health: systematic review of the literature and five recommendations for clinical translation. – 2025. – Т. 15, URL: https://bmjopen.bmj.com/content/15/2/e093932

4. Думками навиворіт [Електронний ресурс] // Вікіпедія : вільна енциклопедія. – 2024. – URL: https://uk.wikipedia.org/wiki/Думками_навиворіт

5. Норман Д. Емоційний дизайн: чому ми любимо (або ненавидимо) речі [Електронний ресурс]. – URL: https://www.goodreads.com/book/show/45890357

ВПЛИВ UNIVERSAL SENTENCE ENCODER НА РОЗВИТОК ОБРОБКИ ПРИРОДНОЇ МОВИ

Волков О. М., Савіцький Р. С.

Державний університет «Житомирська політехніка», м. Житомир

Модель Universal Sentence Encoder (USE) стала важливим етапом у розвитку обробки природної мови - Natural Language Processing (NLP), сприяючи суттєвому покращенню точності та швидкості виконання численних завдань, пов'язаних з аналізом тексту. USE надає можливість перетворювати тексти у вектори фіксованої довжини, які здатні захоплювати контекст і значення речень чи фраз [1], не прив’язуючись до конкретної лексики. Завдяки використанню глибоких нейронних мереж ця модель універсальна і здатна до адаптації в різноманітних умовах.

На зображенні теплової карти (Рис. 1) показано, як USE оцінює семантичну подібність між парами речень. Темно-червоні області відповідають високому рівню подібності, що свідчить про близьке за змістом формулювання речень, тоді як жовті та світлі тони вказують на значно нижчу семантичну спорідненість. Наприклад, речення «Мій телефон має чудову камеру.» та «Мій телефон дуже повільний.» демонструють високу подібність через схожість значення, тоді як «Коли у тебе день народження?» та «Яка температура буде завтра?» мають значно менший зв’язок через різний контекст.

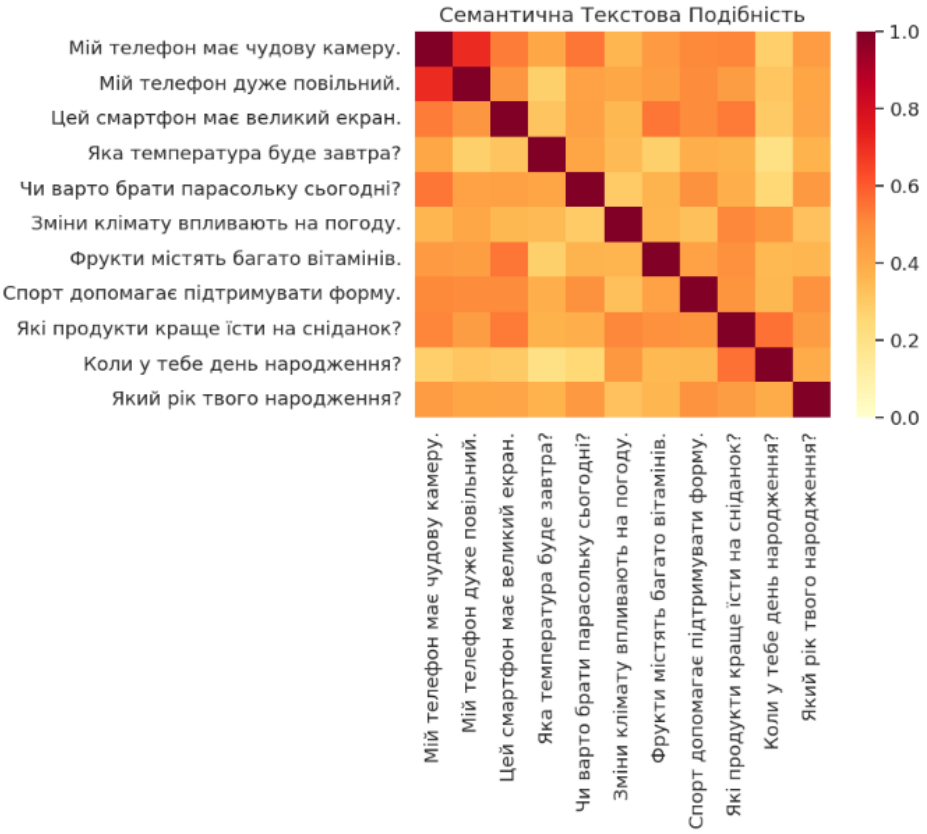


Рис. 1. Теплова карта схожості тексту [2; 3]

Створення семантичних векторів суттєво впливає на розвиток технологій обробки природної мови, зокрема це дає змогу покращити аналіз тексту, допомагаючи пошуковим системам, рекомендаційним алгоритмам і аналітичним платформам краще розуміти зміст і зв’язки між фразами. Крім того, технологія підвищує ефективність взаємодії з чат-ботами та віртуальними асистентами, оскільки дозволяє глибше розпізнавати наміри користувачів навіть у неоднозначних формулюваннях. Вона також відіграє ключову роль у міжмовній комунікації, спрощуючи автоматичний переклад текстів без втрати контексту.

Таким чином, Universal Sentence Encoder відкрив нові можливості для автоматизації та розвитку штучного інтелекту. Зображення теплової карти є лише одним із прикладів того, як модель візуалізує та аналізує семантичні зв’язки між текстовими даними, підкреслюючи її роль у створенні інноваційних рішень.

ДЖЕРЕЛА

1. Van O. Universal Sentence Encoder Explained & How To TensorFlow Tutorial [Електронний ресурс]. SPOT INTELLIGENCE, 10.01.2024. Режим доступу: https://spotintelligence.com/2024/01/10/universal-sentence-encoder-explained-how-to-tensorflow-tutorial/

2. Волков О.М. USE Colab Notebook [Електронний ресурс]. Режим доступу: https://colab.research.google.com/drive/10_dxZrV64a--u62QbUx9Z2oBdq2kuHmT#scrollTo=3wYFaEx35Ufw&line=29&uniqifier=1

3. Universal Sentence Encoder [Електронний ресурс]. TensorFlow, 10.03.2024. Режим доступу: https://www.tensorflow.org/hub/tutorials/semantic_similarity_with_tf_hub_universal_encode

ВИКОРИСТАННЯ ПРОГРАМИ PIVOT ANIMATOR У ЛОГОПЕДИЧНІЙ РОБОТІ

Гаврилюк О., Мошина В., Доропій С., Бодненко Д., Локазюк О.
Київський столичний університет імені Бориса Грінченка, м. Київ

Вступ. Логопе́дія – наука про порушення мовлення, методи їх попередження, виявлення й усунення засобами спеціального навчання й виховання. Логопедія вивчає причини, механізми, симптоматику, перебіг, структуру порушень мовленнєвої комунікації, системи корекційного впливу [1]. Також логопедію розглядають як галузь медицини та педагогіки, яка займається корекцією мовленнєвих порушень у дітей і дорослих. Важливу роль у логопедичній практиці відіграють інноваційні технології, які допомагають покращити процес навчання та зробити його більш цікавим і ефективним. Зараз вони є популярними через те, що багато занять перейшли саме на онлайн формат через вторгнення рф на територію України.

Основна частина. Одним із таких інструментів є програмне забезпечення Pivot Animator. Ця проста і доступна програма дозволяє створювати анімації, що можуть використовуватися для візуалізації різних аспектів логопедичної роботи, таких як артикуляційна гімнастика, вправи на розвиток моторики і засвоєння нових звуків. Також можна створювати певні загадки, мультики та, наприклад, демонстрації виконання вправ на моторику чи артикуляцію.

У своїй роботі ми розглянемо, як застосування Pivot Animator може стати дієвим методом в логопедичній практиці, особливо для дітей, які потребують додаткових мотиваційних стимулів і візуальної підтримки під час навчання.

Основні переваги Pivot Animator у логопедичній роботі:

1. **Простота у використанні**. Pivot Animator має інтуїтивно зрозумілий інтерфейс, що дозволяє легко створювати анімації навіть без спеціальних знань в області графіки чи програмування.
2. **Візуалізація вправ**. Програма дозволяє наочно демонструвати артикуляційні рухи, що допомагає дітям краще зрозуміти та засвоїти техніку виконання вправ.

3. **Мотивація дітей**. Анімаційні завдання роблять навчальний процес цікавішим і залучають дітей до активної участі, перетворюючи вправи на своєрідну гру.

4. **Гнучкість у створенні контенту**. Логопед може самостійно створювати різні анімації для конкретних потреб учня, адаптуючи матеріал під індивідуальні особливості.

5. **Доступність**. Pivot Animator є безкоштовним програмним забезпеченням, що робить його легкодоступним для використання як у навчальних закладах, так і вдома.

6. **Інтерактивність**. Програма дозволяє створювати динамічні сюжети й інтерактивні вправи, які можуть бути залучені в логопедичні заняття, допомагаючи дітям легше сприймати матеріал.

Водночас, можемо виділити такі недоліки як:

- **Обмежені інструменти анімації** – програма надає базові інструменти для створення анімацій, але можливості редагування, додавання складних ефектів і високоякісної графіки обмежені.
- **Відсутність підтримки інших форматів файлів** – Pivot Animator використовує власний формат .piv, який не підтримується іншими програмами. Експорт можливий тільки у форматах .gif та .avi, що обмежує варіанти використання анімацій.
- **Не простий інтерфейс** – для новачків програма може здатися трохи складною у використанні через мінімалістичний і не завжди інтуїтивний інтерфейс.
- **Обмеження на рівень деталізації** – оскільки програма створена для анімацій із простими паличковими фігурами, деталізовані персонажі або сцени неможливо створити.
- **Відсутність підтримки звуку** – у Pivot Animator не передбачено функцій для додавання звукових ефектів чи музики, що обмежує можливості створення повноцінних анімаційних кліпів.
- **Нестабільність і схильність до зависання** – деякі користувачі повідомляють, що програма може часом зависати або аварійно завершувати роботу, особливо на великих або складних проєктах.

Одним із основних завдань логопеда є розвиток артикуляційного апарату у дітей. Це включає виконання спеціальних вправ для м'язів язика, губ і щелеп, що допомагає покращити вимову. Використання анімації, створеної за допомогою Pivot Animator, дозволяє логопеду створювати прості, але ефективні візуальні інструкції для виконання артикуляційних вправ. Взагалі можна створювати будь-які фігури для виконання будь-яких завдань. (Рис. 1)

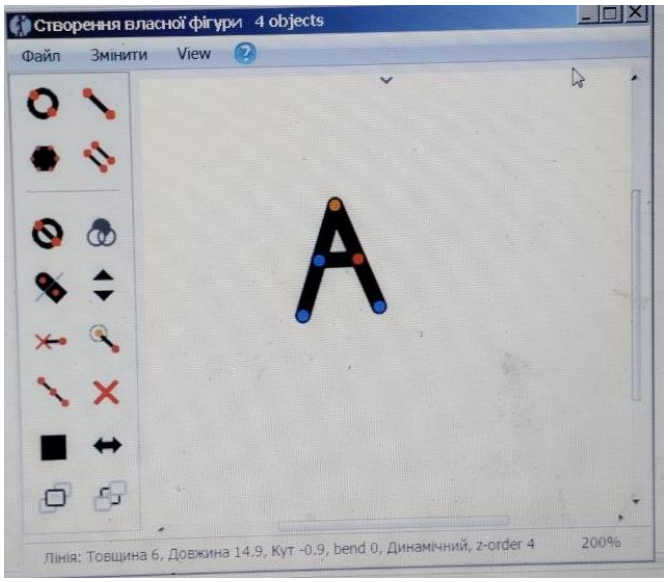


Рис. 1 Створення власних фігур для анімації. У даному проєкті це були літери алфавіту

Наприклад, можна анімувати рухи язика чи губ, що допоможе дитині зрозуміти, як правильно виконувати ті чи інші вправи. Такий підхід робить процес більш цікавим і допомагає дітям краще запам'ятовувати послідовність рухів (Рис. 2).

Крім артикуляційної гімнастики, Pivot Animator може бути корисним для розвитку дрібної моторики. Це важлива складова логопедичної роботи, оскільки дрібна моторика безпосередньо пов'язана з мовленням. За допомогою анімацій можна створювати інтерактивні вправи, які тренують рухи пальців рук, що сприяє покращенню моторних навичок і розвитку мовлення в дітей. Завдяки візуалізації та динаміці анімацій, діти легше сприймають завдання і краще їх виконують.

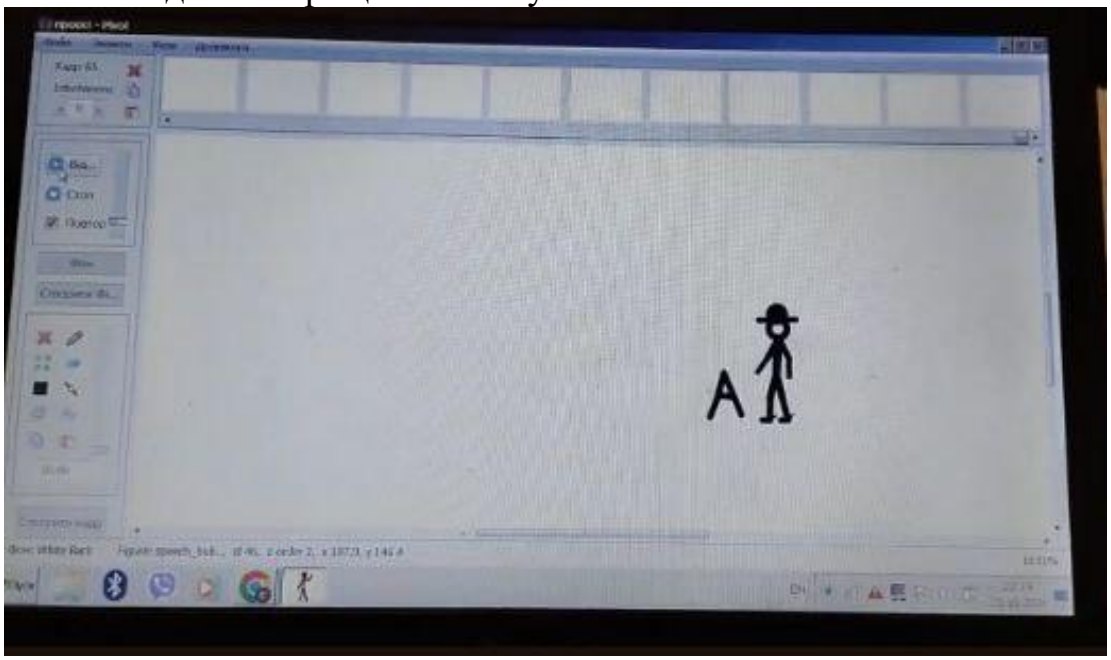


Рис. 2 Кадр із відео, на якому з допомогою візуальної підказки ми допомагаємо дитині згадати літери алфавіту

Нашою метою було створити відео для повторення алфавіту. Дана анімація містить більше тисячі кадрів, у якій з’являються літери під час різних ситуацій зі стандартними фігурами програми. Дитині необхідно називати літери, які вона бачить. Вкінці ж їй потрібно завершити алфавіт, так які він переривається. Таким чином ми граємося з дитиною і задіюємо максимальну кількість вищих психічних функцій. Основний вплив здійснюється на увагу, пам'ять, мислення та саме мовлення.

Важливим аспектом є мотивація учнів. Використання анімацій допомагає залучити дитину, зробити заняття більш цікавими й інтерактивними. Pivot Animator дозволяє створювати історії або ігрові ситуації, де мовленнєві вправи стають частиною захопливої гри, що значно підвищує інтерес до навчання. Дану програму можна використовувати й для занять у школі тощо.

Використання **Pivot Animator** у логопедичній роботі є доцільним та дієвим інструментом для покращення навчального процесу. Завдяки простоті, доступності та можливості створювати візуальні інструкції, програма допомагає дітям краще засвоювати артикуляційні вправи та розвивати мовленнєві навички. Анімаційні завдання не лише підвищують мотивацію учнів, але й роблять заняття більш інтерактивними та цікавими. Таким чином, Pivot Animator може стати важливим доповненням до традиційних методів роботи логопеда, сприяючи ефективнішому досягненню корекційних цілей.

ДЖЕРЕЛА:

1. Рібцун, Ю. В. Логопед. *Спеціальна педагогіка і психологія: сучас. термінол. словник*, 127-128. (2024).

2. Pivot Animator. [Електронний курс]. Режим доступу: https://pivotanimator.net/ Заголовок з екрану

3. Формат файлу PIV - анімація Pivot Animator - File Format Docs. [Електронний курс]. Режим доступу: https://docs.fileformat.com/uk/video/piv/

4. Pivot Animator Tutorials [Електронний курс]. Режим доступу: https://docs.fileformat.com/

5. Pivot Animator 4.2.6 [Електронний курс]. Режим доступу: https://daad.org.ua/7168-zavantazhiti-pivot-animator.html

ІНСТРУМЕНТАЛЬНІ ТА КОМУНІКАЦІЙНІ АСПЕКТИ ВІДДАЛЕНОГО УПРАВЛІННЯ КОМАНДАМИ В ІТ-ПРОЄКТАХ

Глинка Ю. Р., Вовк Р. Б.
Івано-Франківський національний технічний університет нафти і газу, м. Івано-Франківськ

У сучасних умовах стрімкої цифрової трансформації управління проєктами за участю розподілених та віддалених команд набуває дедалі більшого значення. Це зумовлено глобалізацією ринку праці, поширенням моделей гнучкої зайнятості та розвитком інформаційно-комунікаційних технологій. Усе більше організацій орієнтується на використання віддалених фахівців, що дозволяє розширити кадровий потенціал, оптимізувати витрати та забезпечити безперервність бізнес-процесів незалежно від географічного розташування учасників команди.

Під поняттям дистанційної роботи розуміється трудова діяльність, що виконується за межами традиційного офісного середовища із використанням електронних засобів комунікації та взаємодії. При цьому працівники залишаються штатними одиницями підприємства чи організації, а всі організаційно-правові аспекти їхньої взаємодії з роботодавцем зберігають чинність [1].

З активізацією використання віддаленого формату перед керівниками проєктів постають нові виклики, зокрема необхідність ефективної координації діяльності географічно розподілених команд. Основними завданнями управління у таких умовах є підтримка високого рівня продуктивності, забезпечення злагодженої взаємодії між учасниками, а також дотримання визначених термінів і бюджетів. Водночас такі умови потребують впровадження адаптивних підходів до планування, моніторингу виконання завдань, організації комунікацій та підтримки мотивації персоналу.

Формування віддалених команд супроводжується специфічними труднощами, пов’язаними з часовими та просторовими відмінностями, культурними бар’єрами, різними підходами до роботи й особистими особливостями учасників. Важливо не лише залучати висококваліфікованих фахівців, але й враховувати їхню здатність до самоорганізації, дисциплінованості, відповідальності, а також комунікаційні навички – здатність чітко формулювати думки, своєчасно реагувати на повідомлення, ефективно співпрацювати в асинхронному режимі.

На етапі формування команди вирішальне значення має правильний підбір кадрів і чіткий розподіл функціональних ролей. Визначення обов’язків і зон відповідальності зменшує ймовірність виникнення конфліктів, сприяє прозорості процесів та узгодженості дій.

Важливу роль відіграє впровадження регулярних комунікаційних практик –щоденних стендапів, тижневих зібрань, ретроспектив тощо. Вони допомагають підтримувати зворотний зв'язок, забезпечують прозорість дій кожного учасника та формують відчуття колективної відповідальності за результат. Окрім того, такі практики позитивно впливають на емоційний стан учасників, зміцнюють почуття належності до команди та довіру. Незважаючи на численні переваги, віддалений формат роботи не позбавлений недоліків. Зокрема, ускладненою є координація міжчасових зон, що потребує гнучкого планування графіків. Існує ризик втрати контексту через асинхронну комунікацію або нерозуміння, пов'язане з культурними розбіжностями. У деяких випадках відсутність фізичної присутності створює бар'єри у формуванні довіри, знижує ефективність контролю та ускладнює оперативне вирішення проблем.Окремо слід відзначити психологічні аспекти дистанційної роботи. В умовах розмиття меж між робочим та особистим життям працівники частіше стикаються з проблемами емоційного вигорання, зниженням мотивації та ізоляцією.

Технічна складова управління віддаленими командами також відіграє ключову роль. Застосування сучасних інструментів управління проєктами – таких як **Asana**, **Trello**, **Jira** – забезпечує можливість планування, постановки задач, контролю дедлайнів та пріоритетів, а також візуалізації проєктного прогресу. Їх інтеграція з платформами для обміну файлами (Google Drive, Microsoft Office, Dropbox) створює єдиний інформаційний простір для командної роботи.

Для забезпечення ефективного документообігу доцільним є використання хмарних сервісів – **Google Workspace**, **Microsoft 365**, **OneDrive**, які підтримують спільну роботу з документами в режимі реального часу. А сервіси типу **Miro** або **Mural** відкривають широкі можливості для візуального планування, мозкового штурму та командного аналізу ідей.

Таким чином, успішне управління розподіленими командами потребує комплексного підходу, що поєднує технологічні рішення з соціально-психологічними стратегіями. Ключовими факторами ефективної організації праці в дистанційному форматі є чітка структура ролей, злагоджена комунікація, постійна підтримка залученості та довіри, застосування інноваційних IT-інструментів, а також формування сприятливого мікроклімату в команді. Усі ці аспекти є передумовами досягнення високих результатів у реалізації проєктів незалежно від фізичного розташування їхніх учасників.

ДЖЕРЕЛА

1. Особливості корпоративного менеджменту в умовах віддаленої роботи. URL: https://nzlubp.org.ua/index.php/journal/article/view/382

МОЖЛИВОСТІ ТА ОБМЕЖЕННЯ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ОЦІНЮВАННІ ЕФЕКТИВНОСТІ ІТ-КОМАНД

Гловин Н. А., Вовк Р. Б.
Івано-Франківський національний технічний університет нафти і газу, м. Івано-Франківськ

У контексті цифрової трансформації, що охоплює всі аспекти соціально-економічного розвитку, штучний інтелект (ШІ) дедалі активніше інтегрується в процеси управління проєктами та розробки програмного забезпечення. Зокрема, технології ШІ все частіше застосовуються для аналізу ефективності роботи програмістських команд, автоматизації управлінських рішень, прогнозування термінів виконання задач, оптимізації ресурсів і оцінювання продуктивності окремих співробітників [1].

У сучасних умовах динамічного розвитку ІТ-галузі, організації стикаються з численними викликами, пов’язаними з необхідністю забезпечення ефективної командної роботи в умовах багатокомпонентних проєктів, розподілених команд і змінних вимог замовників. Застосування ШІ в цьому контексті розглядається як інструмент підвищення об'єктивності та швидкості управлінських рішень. Проте, незважаючи на потенційні переваги, широке використання алгоритмів оцінювання продуктивності супроводжується низкою технічних, соціальних та етичних обмежень.

Результативність функціонування ШІ-систем значною мірою залежить від якості вхідних даних і репрезентативності навчальних вибірок. Найчастіше алгоритми опираються на кількісні програмні метрики: кількість комітів у репозиторії, кількість виконаних завдань, швидкість виправлення помилок тощо. Однак ці показники не завжди адекватно відображають реальний внесок учасника команди. Наприклад, такі аспекти, як менторство, знання доменної області, рівень міжособистісної взаємодії або технічна складність виконаних завдань, часто залишаються поза межами аналітичного охоплення ШІ.

Більш того, алгоритми можуть відтворювати упередження, присутні в навчальних даних. Якщо система навчена на основі прикладів, де оцінювання ефективності базувалося на суб’єктивних чинниках, вона з великою ймовірністю відтворюватиме ці самі викривлення у майбутньому. Унаслідок цього створюється ризик несправедливого оцінювання, що безпосередньо впливає на мотивацію, залученість і психологічний стан працівників.

Особливу стурбованість викликає нездатність ШІ враховувати соціальний та емоційний контекст командної взаємодії. Алгоритми не можуть фіксувати вплив міжособистісних конфліктів, змін у пріоритетах

проєкту, або впливу лідерських якостей окремих співробітників. Крім того, у реальних умовах темп роботи команди може змінюватися під впливом зовнішніх факторів (нові вимоги замовника, внутрішні зміни в організації, технічні обмеження), що знижує валідність автоматизованих висновків [2].

Застосування систем ШІ без врахування вищезазначених чинників може призвести до ряду негативних наслідків:

- Орієнтація на метрики замість цілей: коли учасники команди знають, що їх оцінюють за певними показниками, вони можуть оптимізувати свою діяльність виключно під ці метрики, нехтуючи стратегічними цілями проєкту.
- Гейміфікація процесу: оцінювання перетворюється на своєрідну гру, де домінує змагання за кращі показники, а не командна ефективність.
- Психологічні ризики: сприйняття несправедливості або ігнорування індивідуального внеску може спричинити вигорання, зниження мотивації та підвищення плинності кадрів.

Щоб уникнути цих ризиків, доцільно впроваджувати гібридні моделі оцінювання, які поєднують аналітичний потенціал ШІ з експертною оцінкою менеджерів і колег. До таких підходів належать:

- Інтеграція кількісних та якісних показників.
- Механізми періодичного перегляду і коригування моделей.
- Урахування зворотного зв’язку від учасників команди.
- Підкреслення командних, а не індивідуальних, досягнень.

Окремої уваги заслуговують ресурсні аспекти. Розробка, навчання та супровід ШІ-систем потребують значних фінансових, часових та інтелектуальних інвестицій. Для малих та середніх підприємств витрати на інтеграцію таких рішень можуть виявитися економічно недоцільними.

Таким чином, застосування штучного інтелекту в системах оцінювання продуктивності ІТ-команд має значний потенціал, проте потребує виваженого та контекстно-залежного підходу. Недостатній облік етичних, психологічних та організаційних факторів може звести нанівець переваги автоматизації. Водночас інтеграція ШІ як інструменту підтримки (а не заміни) управлінських рішень –шлях до створення справедливої, ефективної та гуманної системи оцінювання в сучасних ІТ-командах.

ДЖЕРЕЛА

1. Яворський Р. Т., Шишковський С. В. Формування гнучкої системи менеджменту. Бізнес Інформ. 2023. № 10. С. 329–332.

2. Колесніков, А. П., Карапетян, О. М. Штучний інтелект: переваги та загрози використання. Ефективна економіка. 2023, №8.

ILLUSTRATOR ЯК ІНСТРУМЕНТ РЕКЛАМИ І PR

Грищук Д., Михайленко В., Коханевич В., Кравченко А.
Київський столичний університет імені Бориса Грінченка, м. Київ

Adobe Illustrator – універсальний стандарт у світі векторної графіки. Мета цієї роботи – дослідити функціонал Adobe Illustrator, його основні переваги та недоліки, а також провести порівняння з іншими популярними графічними редакторами. Ми прагнемо не лише розкрити ключові можливості цієї програми, а й допомогти зрозуміти, як і чому Illustrator став таким популярним, а також які альтернативи можуть бути цікавими для різних завдань.

Adobe Illustrator – професійний графічний редактор для створення та редагування векторної графіки від компанії Adobe [1]. Adobe Illustrator – найбільш розповсюджений векторний графічний редактор.Векторні зображення – ідеальні для сьогоднішнього цифрового простору: вони використовуються у веб-ілюструванні, створенні іконок і стикерів, завдяки своїм властивостям [2].

Функціонал Adobe Illustrator в рекламі та PR. Реклама сьогодні є важливо частиною бізнесу, адже вона допомагає привернути увагу до продуктів, послуг або брендів. Цифрова реклама також вимагає високої якості та креативності. За допомогою Adobe Illustrator можна створювати банери для соціальних мереж, де поєднуються яскраві кольори, динамічні композиції та текстові блоки, що привертають увагу. Ще однією важливою сферою використання Illustrator є створення інфографіки для реклами. Візуалізація складної інформації у формі діаграм, іконок або схем дозволяє краще донести основні ідеї до споживачів. Це особливо актуально для брендів, які прагнуть розповісти про свої досягнення або переваги продукту у зрозумілій і стильній формі. Реклама з унікальним текстовим оформленням виглядає більш професійно і запам’ятовується краще. Наприклад, створення унікального слогану з нестандартним шрифтом може стати візитною карткою бренду.

Чим Adobe Illustrator популярний у сфері реклами ?

1. Векторна графіка

Illustrator графічний векторний рдактор (зображення, які не втрачають якості при масштабуванні).

2. Гнучкість роботи з текстом

Illustrator дозволяє точно налаштовувати текст: змінювати шрифти, грати з обводками, створювати текстові ефекти, які підкреслюють стиль реклами.

3. Сумісність з програмами Adobe

Illustrator має функцію інтеграції з Adobe Photoshop, InDesign та After Effects.

4. Підтримка друкованих і цифрових форматів

Illustrator дозволяє експортувати роботи у формати, які потрібні для друку (PDF, EPS) та для цифрової реклами (PNG, SVG, JPEG).

5. Інструменти для створення макетів

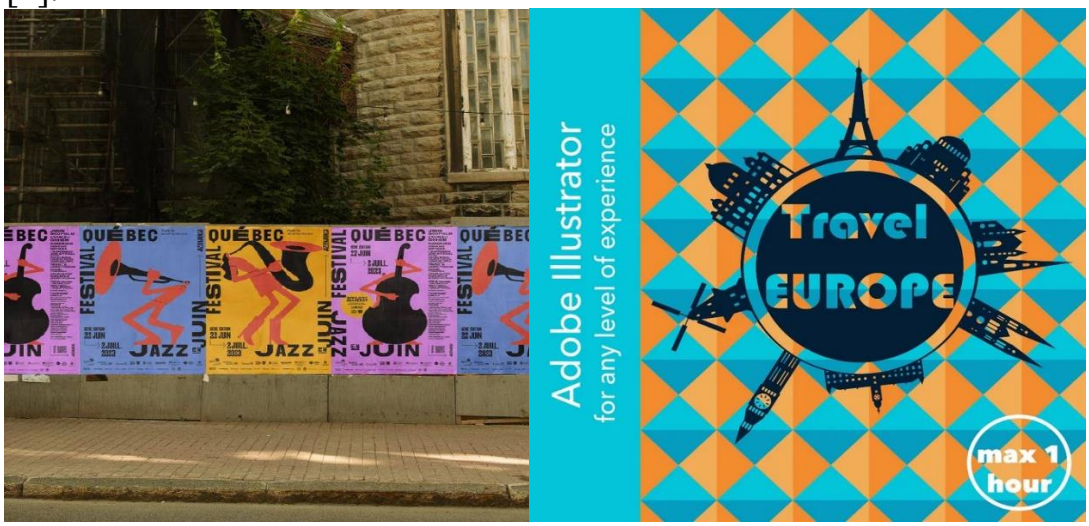
Інструменти роботи з шаблонами та сітками роблять процес створення макетів простим і точним, що важливо для реклами.

6. Підтримка кольорових профілів

Illustrator підтримує CMYK і Pantone, що забезпечує точність кольорів для друкованої реклами.

7. Ефекти та стилі

Можливість додавати тіні, градієнти, ефекти об'єму або блиску дозволяє створювати вражаючі візуальні елементи, які привертають увагу [4].



https://www.instagram.com/reel/C8eJe2tNh84/?igsh=MmpydG5oYXJnemk0
https://www.instructables.com/Creating-Advertisement-in-Adobe-Illustrator/

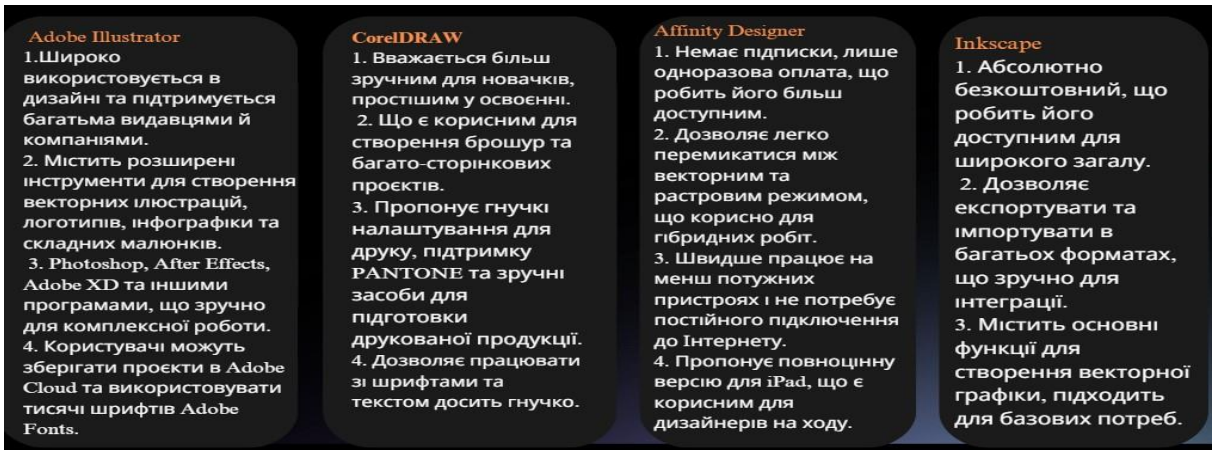
Ось приклад рекламних матеріалів, які створені в Adobe Illustrator: сучасний дизайн з використанням геометричних форм, яскравих градієнтів, інфографіки та чистої типографії.

Переваги	Недоліки
Векторна графіка Основна перевага Illustrator – векторна графіка, (зображення не втрачають якості при масштабуванні). Це особливо важливо для логотипів, іконок та ілюстрацій, що потребують високої роздільної здатності.	**Висока ціна** Illustrator є частиною Adobe Creative Cloud, що вимагає підписки, яка може бути дорогою для окремих користувачів і малих підприємств.
Інтеграція з продуктами Adobe Illustrator має функцію інтеграції з програмами Adobe: Photoshop, InDesign і After Effects, що спрощує роботу над комплексними проєктами, де потрібно використовувати кілька інструментів.	**Складність для новачків** Програма має круту криву навчання. Новачкам може бути важко зорієнтуватися в інтерфейсі та функціях без попереднього досвіду в графічному дизайні.

Різноманіття інструментів для малювання та редагування Illustrator пропонує широкий спектр інструментів для створення ліній, фігур, малювання пензлями, а також інструменти для точного редагування об'єктів. Він забезпечує високу деталізацію, дозволяючи художникам і дизайнерам експериментувати з різними стилями.	**Високі вимоги до системи** Для ефективної роботи Illustrator потрібні потужні комп'ютерні ресурси, що може бути проблемою для користувачів зі старими або менш потужними системами.
Широкі можливості для роботи з текстом Illustrator дозволяє легко працювати з текстом, що корисно для створення постерів, банерів, логотипів тощо. Інструменти для обтікання тексту навколо об’єктів, зміни кегля, інтерліньяжу та інших параметрів допомагають досягти бажаного результату.	**Обмежена підтримка растрових зображень** Illustrator переважно працює з векторною графікою. Хоча можна імплементувати растрові зображення, їх обробка обмежена в порівнянні з програмами, такими як Adobe Photoshop.
Розширені функції для створення логотипів та іконок Завдяки точності векторних інструментів, Illustrator ідеально підходить для створення графічних елементів, таких як логотипи та іконки, які потребують чітких ліній і точного пропорціонування.	**Кошти на оновлення** Оновлення програмного забезпечення можуть додати нові функції, але іноді вони також можуть вплинути на стабільність або вимагати нових навчань.
Шари та групування об'єктів Можливість використовувати шари та групувати об'єкти дозволяє легко організовувати і контролювати складні композиції, що особливо важливо при створенні великих проектів.	**Обмежена функціональність для анімації** Illustrator не призначений для створення анімацій, що може бути недоліком для дизайнерів, які потребують інтерактивності.
Активна підтримка та велика спільнота користувачів Adobe Illustrator має велику базу користувачів і спільноту, де завжди можна знайти навчальні матеріали, поради або готові шаблони.	**Продуктивність при великих проєктах** При роботі з великими файлами чи складними проєктами програма може зависати або сповільнюватися.

Порівняння застосунка Adobe Illustrator з іншими

Щоб оцінити його сильні та слабкі сторони, розглянемо порівняння Illustrator з іншими попул ярними програмами для векторної та графічної обробки, зокрема CorelDRAW, Affinity Designer, Inkscape та Adobe Photoshop.



Причини, чому варто обрати Illustrator.

1. Векторна графіка

Illustrator працює з векторними зображеннями, які можна масштабувати без втрати якості, що важливо для реклами, адже банери, білборди або інші макети можуть вимагати великого розширення.

2. Професійні інструменти для дизайну

Illustrator пропонує потужний набір інструментів для: *створення логотипів, іконок та ілюстрацій; роботи з текстом* ;*роботи з кольоровими схемами*

3. Інтеграція з продуктами Adobe

Illustrator – інтеграція Adobe Photoshop, InDesign та іншими програмами. Наприклад, ви можете створити графіку в Illustrator, а потім додати її в макет журналу чи реклами у Photoshop або InDesign.

4. Продуктивність і універсальність

Illustrator підходить для створення різних типів реклами:

1.*цифрової* (банери для сайтів, соціальних мереж);

2.*друкованої* (афіші, буклети, візитки);

3.*зовнішньої* (білборди, постери).

5. Експорт у різних форматах

Програма підтримує експорт у формати PDF, SVG, PNG, EPS та інші. Це дозволяє легко адаптувати дизайн для друку або використання в цифровому форматі.

6. Одна з перших програм для векторної графіки

Adobe Illustrator був випущений у 1987 році й став однією з перших програм для роботи з векторною графікою. Це зробило його революційним інструментом у світі дизайну.

7. Інструмент *«Перо»* – унікальна функція

8. Підтримка графіки для *VR* та *AR*

У сучасних версіях Illustrator можна створювати графіку для доповненої та віртуальної реальності, використовуючи інтеграцію з Adobe Aero.

9. Підтримка роботи з *3D*

Illustrator має інструменти для створення 3D-об’єктів, таких як екструзія, обертання або нанесення текстур. Це допомагає додати новий вимір у дизайни.

Adobe Illustrator **у рекламі**

Рекламний ілюстратор. Він створює візуальні матеріали для кампаній брендів: як правило це постери, банери, упаковка і брендинг. Йому необхідно привернути увагу аудиторії і передати ключові повідомлення брендів через візуальні образи [3].

Що можна створити в Illustrator?

1. Легко генерує нескінченні візерунки;
2. Миттєво генерує значки професійного рівня;
3. Миттєво додає розмір за допомогою інструменту Dimension;
4. Векторизує зображення;
5. Створює гарні персоналізовані написи.

Adobe Illustrator є ключовим інструментом у сучасному цифровому дизайні завдяки своїм широким можливостям. Програма здобула популярність серед дизайнерів та ілюстраторів завдяки своїй здатності створювати високоякісну векторну графіку, що зберігає чіткість і деталізацію незалежно від масштабу. Під час аналізу ми з’ясували, що Illustrator пропонує не лише базові інструменти для створення графіки, але й розширені функції, такі як інтеграція з іншими програмами, робота з текстом і градієнтами, а також підтримка різних форматів файлів. Попри його численні переваги, Illustrator має і недоліки, зокрема високу вартість підписки та певну складність для новачків. Проте, для професіоналів ці аспекти компенсуються багатим функціоналом і якістю, яку забезпечує програма.

ДЖЕРЕЛА

1.Створюйте шедеври за лічені секунди. url: https://openarchive.nure.ua/server/api/core/bitstreams/641d48b6-914f-47a4-b628-b2f1f0a6a3dd/content

2.Основи графіки в Adobe Illustrator.url: socrat.in.ua/en/courses/design/adobe-illustrator-essentials/

3.Чим займається ілюстратор: як розвинути необхідні навички та почати брати замовлення.url: https://genius.space/lab/chim-zajmayetsya-ilyustrator-yak-rozvinuti-neobhidni-navichki-ta-pochati-brati-zamovlennya/

4. Створіть банер із дизайном, який вирізнятиметься з решти.url: https://www.adobe.com/ua/products/illustrator/banner-design.html

ПЛАТФОРМА ДЛЯ АВТОМАТИЗАЦІЇ ПРОЦЕСІВ ДІЯЛЬНОСТІ КНИЖКОВОГО МАГАЗИНУ

Гутира С.Ю.
Київський столичний університет імені Бориса Грінченка, м. Київ

Сучасні книжкові магазини, як і багато інших сфер роздрібної торгівлі, стикаються з викликами цифрової трансформації. Автоматизація бізнес-процесів стає не просто трендом, а необхідністю для підвищення ефективності управління, оптимізації часу та покращення взаємодії з клієнтами. Запропонована онлайн-платформа спрямована на вирішення цих завдань, дозволяючи автоматизувати ключові аспекти діяльності книжкового магазину.

Досліджено, що однією з основних проблем традиційних магазинів є складність обліку асортименту та управління замовленнями. Ручна обробка даних призводить до помилок, втрати часу та зниження якості обслуговування. Запропоноване рішення передбачає створення інтегрованої системи, що забезпечує зручне керування каталогом товарів, замовленнями та оплатами, що дозволяє значно скоротити рутинні процеси та мінімізувати ризики неточностей.

Технологічна основа платформи будується на сучасному стеку веб-технологій. Для серверної частини використовується Node.js – з ним всі запити обробляються швидко та ефективно, а для фронтенду – React, який гарантує гнучкість та зручність інтерфейсу. База даних MongoDB використовується для зберігання інформації про книги, користувачів та історію замовлень, що дозволяє ефективно працювати з великими масивами даних. Інтеграція з платіжними системами робить процес оплати простим і безпечним для користувачів.

У практичній частині було розроблено основні функціональні модулі системи. Створено зручний каталог книг, де адміністратори магазину можуть додавати, редагувати та видаляти товари. Реалізовано систему обробки замовлень із можливістю змінювати їх статус і переглядати історію покупок. Для зручності було здійснено інтеграцію платіжних систем, що дозволяє здійснювати онлайн-оплату через різні методи (банківські картки та електронні гаманці). Для кращого розуміння взаємодії користувачів із системою була розроблена діаграма випадків використання, яка наочно демонструє основні сценарії взаємодії клієнтів та адміністраторів з платформою:

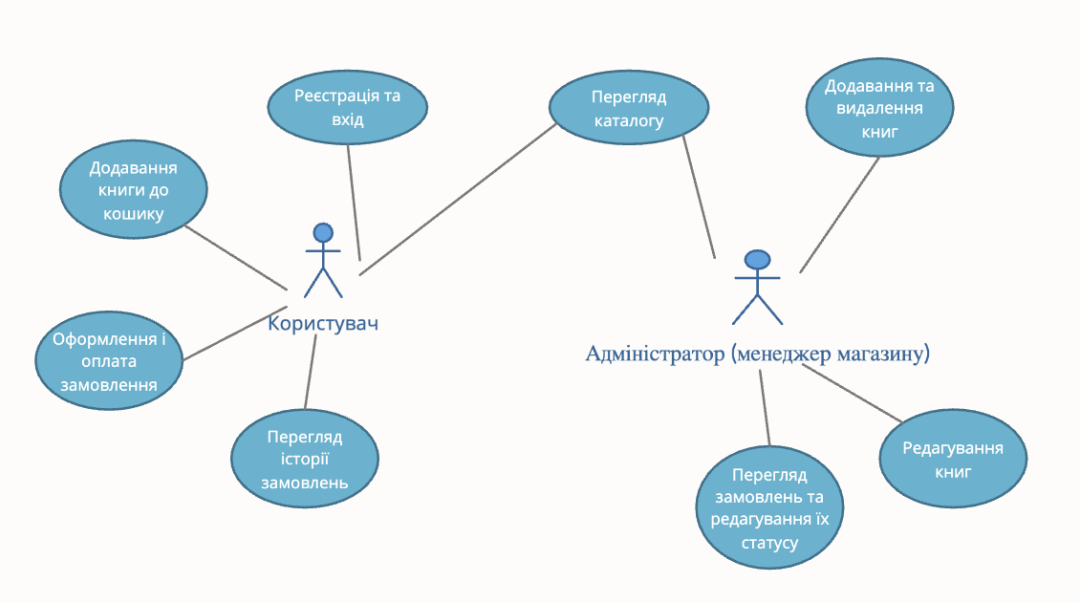


Рис. 1. Діаграма випадків використання

Отже, впровадження онлайн-платформи для автоматизації процесів книжкового магазину є важливим кроком у підвищенні його конкурентоспроможності. Діджиталізація бізнес-процесів дозволяє адаптуватися до сучасних умов ринку, покращити взаємодію з клієнтами та створити більш ефективну модель управління роздрібною торгівлею книгами.

ДЖЕРЕЛА

1. Ушенко Ю. О., Олар О. В., Галочкін О. В., Д'яченко Л. І. Сучасні технології розробки Web-додатків: фронтенд розробка: навч. посіб. (вид. електронне) / Чернівецький нац. ун-т ім. Ю. Федьковича. – Чернівці, 2022. – Режим доступу: https://archer.chnu.edu.ua/bitstream/handle/123456789/6760/%D0%A1%D1%82%D1%80%D0%B0%D0%BD%D0%B8%D1%86%D1%8B%20%D0%B8%D0%B7%20%D0%9F%D0%BE%D1%81%D1%96%D0%B1%D0%BD%D0%B8%D0%BA%20Web.pdf?sequence=1&isAllowed=y

2. Mohammed Abdala. Online E-Book Store Website Design // i-manager's Journal on Software Engineering. – 2011. – Т. 5, № 4. – С. 41–46. – DOI:10.26634/jse.5.4.1449. – Режим доступу: https://www.researchgate.net/publication/260907838_Online_E-Book_Store_Website_Design.

ХМАРНИЙ СЕРВІС «НАЦІОНАЛЬНА ОСВІТНЯ ПЛАТФОРМА ВСЕОСВІТА» ЯК КОМПЛЕКС КОРИСНИХ ІНСТРУМЕНТІВ У ПРОФЕСІЙНІЙ ДІЯЛЬНОСТІ ФАХІВЦЯ ІЗ ВТРУЧАННЯ ПРИ АУТИЗМІ

Драник Н. О., Здерчук А. Б., Ларіна Т. О., Шаповал Л. В.
Київський столичний університет імені Бориса Грінченка, м. Київ

Педагоги все частіше мають справу з викликами сьогодення, що спонукають їх до пошуку нових методів, способів, методик, інструментів роботи з дітьми. Окремим викликом для вчителя є забезпечення едукаційного процесу для дитини з особливими освітніми потребами.

Надважкі обставини, в яких опинилася Україна – пандемія, повномасштабне вторгнення РФ, дистанційне навчання, велика кількість переміщених осіб – виконання цього завдання стає ще складнішим і потребує суттєвої, структурованої та зручної підтримки.

Національна освітня платформа ВСЕОСВІТА https://vseosvita.ua/, на думку авторів, є одним із найпотужніших ресурсів, які надають широкий спектр інструментів для роботи з дітьми з особливими освітніми потребами.

Платформа ВСЕОСВІТА є надзвичайно розвинутим освітнім ресурсом, що виконує такі функції:

- стимулювання педагогів до творчості, інновацій, створення курсів, уроків, вебквестів, особливо стосовно візуалізації та адаптації освітніх матеріалів до особливих освітніх потреб учнів, при цьому здійснюється перевірка матеріалів на автентичність задля дотримання академічної доброчесності;
- надання можливості для навчання, підвищення кваліфікації, шляхом надання доступу до курсів власного виробництва, з можливістю додавання пройдених курсів до Європейської кредитної трансферно-накопичувальної системи, в тому числі навчання, яке стосується інклюзивної освіти, навчання дітей з особливими освітніми потребами;
- надання доступу учням до навчання з використанням матеріалів, курсів та інших освітніх інструментів, що дає їм широкий вибір матеріалів та забезпечує різноманітні освітні потреби;
- інтеграція з АІКОМ – автоматизованим інформаційним комплексом освітнього менеджменту, до якого платформа ВСЕОСВІТА приєдналася 07.05.2024 року, і це значно спрощує завдання навчальним закладам стосовно ведення електронної звітності.

Серед інших хмарних освітніх веб-ресурсів (таких, наприклад, як «На урок» https://naurok.com.ua/, LearningApps.org https://learningapps.org/) ВСЕОСВІТА вирізняється такими особливостями, як:

1) найбільш широкий діапазон освітніх інструментів та матеріалів для різних вікових груп і предметів – за форматом викладення, освітніми дисциплінами, додатковими освітніми науками;

2) більш гнучкий підхід до формату освітніх матеріалів – тести, вебквести, уроки, презентації, курси, візуальні матеріали;

3) для електронних посібників «конструктор тестів» та «конструктор уроків» було отримано гриф «Схвалено для використання в освітньому процесі» від Інституту модернізації змісту освіти Міністерства освіти і науки України[orcid.org/0000-0001-6083-2499];

4) приділено більше уваги співпраці між вчителями, поширенню та обговоренню питань освіти;

5) контроль дотримання академічної доброчесності авторами та підтвердження авторського права після першого опублікування розробок, відповідно до п. 1 ч. 1 ст. 9 Закону України «Про авторське право і суміжні права» від 01.12.2022 року №2811-IX.

Переваги платформи ВСЕОСВІТА:

1. Широкий функціонал, що дає можливість обрати найефективніші ресурси для конкретного учня або класу, а також сприяє поглибленню знань з різних тем.

2. Лекції та теоретичні матеріали у форматі тексту або презентацій відповідають програмі Міністерства освіти і науки України.

3. Забезпечено наявність розробок для найрізноманітніших освітніх потреб, що усуває проблему недостатнього забезпечення сучасної школи методиками та матеріалами для дітей з особливими освітніми потребами з-за необхідності проходження тривалої та складної експертизи у Державній науковій установі «Інститут модернізації змісту освіти» для отримання грифів Міністерства освіти і науки України.

4. Наявність інтерактивних завдань та ігор, які роблять навчання цікавішим і стимулюють учнів до активності.

5. Зручність використання: інтуїтивно зрозумілий інтерфейс, простота у використанні, категорії та фільтри полегшують пошук матеріалів за предметом, класом чи типом завдання, легко знайти тести та додаткові матеріали, які можна інтегрувати у свої уроки, є можливість зберігати прогрес і мати швидкий доступ до улюблених матеріалів завдяки особистому кабінету .

6. Адаптація до нових технологій - платформа дотримується актуальних освітніх тенденцій і намагається впроваджувати нові технології, як-от:

- використання гейміфікації для підвищення мотивації учнів;
- підтримка онлайн-тестів із миттєвою перевіркою та оцінюванням;
- можливість організації онлайн-уроків і заходів, що відповідає потребам дистанційного навчання в сучасних умовах.

7. Підтримка вчителів:

- доступ до методичних рекомендацій та готових планів уроків;

- можливість розробляти власні тести та ділитися ними з іншими педагогами;

- курси підвищення кваліфікації та вебінари, що допомагають вчителям постійно розвиватися.

8. Підтримка навчальних закладів у питанні планування та забезпечення процесу підвищення кваліфікації викладачів закладу.

9. Безкоштовний доступ до великої кількості якісних матеріалів, що дозволяє охопити широку аудиторію та сприяє зменшенню нерівності в доступі до якісної освіти.

Недоліки платформи ВСЕОСВІТА:

1. Не всі матеріали на платформі проходять жорстку перевірку на актуальність та відповідність шкільній програмі. Це може призвести до використання застарілих або неперевірених ресурсів, що впливають на якість навчання, та вимагає від педагогів додаткової уваги при виборі ресурсів для уникнення поширення некоректної інформації.

2. Технічні складнощі:

- завантаження сайту може бути повільним через перевантаження серверів під час пікових годин;

- можливі збої у функціонуванні тестів чи завдань, що викликає незручності для користувачів під час проведення контрольних робіт;

- виникає потреба у стабільному інтернет-з'єднанні, без якого доступ до матеріалів обмежується, що може знизити ефективність навчання та викликати розчарування в учнів і вчителів.

3. Не достатня інтерактивність: хоча платформа пропонує інтерактивні елементи, вони не завжди забезпечують достатню залученість:

- не всі завдання інтерактивні або динамічні, що може зменшувати інтерес учнів до матеріалу;

- відсутність можливостей для живого спілкування та миттєвої зворотної реакції з боку вчителів;

4. Інформаційне перевантаження: через великий обсяг матеріалів користувачі можуть зіткнутися з проблемою вибору. Учні та вчителі можуть губитися у великій кількості ресурсів, не знаючи, які з них є найрелевантнішими; виникає потреба у додаткових фільтрах та рекомендаціях, щоб спростити пошук найкращих матеріалів. Це може знижувати ефективність використання платформи та призводити до витрати часу на пошук.

Користь платформи ВСЕОСВІТА для роботи фахівця із втручання при аутизмі.

1. На платформі широко представлені приклади завдань і занять з адаптацією для дітей з особливими освітніми потребами. Потреба

візуальної підтримки для вивчення абстрактних понять виступає зручним джерелом спеціалізованих матеріалів.

2. Чимала підбірка курсів підвищення кваліфікації вебінарів, семінарів за запитом «аутизм», «ООП», «інклюзія».

3. Сервіс містить значну теоретичну базу стосовно аутизму, адже у вкладці «Методичні матеріали» знайшлось 264 безкоштовних матеріалів по цій темі.

ДЖЕРЕЛА

1. Кіпоренко С. С. Особливості використання хмарних технологій в освіті. *Економіка. Фінанси. Менеджмент: актуальні питання науки і практики: зб. наук. пр. ВНАУ*, 2019, № 4, с. 181-189.

2. Биков В. Ю., Гуржій А. М., Шишкіна М. П. Концептуальні засади формування і розвитку хмаро орієнтованого навчально-наукового середовища закладу вищої педагогічної освіти. *Modern Information Technologies and Innovation Methodologies of Education in Professional Training Methodology Theory Experience Problems*, 2018, №50, с.20-25.

3. Люлюкунова О. Цифровізація освітнього процесу. Дистанційне навчання. *ІІІ Всеукр. наук.-практ. конф. Дошкільна освіта: проблеми, пошуки, інновації*, Кривий Ріг, 2023, с. 375-381.

4. АІКОМ поповнила нова освітня інформаційна система «Всеосвіта», 2024. [Електронний ресурс]. Режим доступу: https://mon.gov.ua/news/aikom-popovnyla-nova-osvitnia-informatsiina-systema-vseosvita.

5. Конструктори тестів та уроків схвалено експертною комісією, 2021. [Електронний ресурс]. Режим доступу: https://mon.gov.ua/news/konstruktori-testiv-ta-urokiv-skhvaleno-ekspertnoyu-komisieyu.

ПЕРЕВАГИ ТА НЕДОЛІКИ ВЕБСИСТЕМ ДЛЯ МОНІТОРИНГУ ЗДОРОВ'Я

Душний Б.О. Черноволик Г.О.

Вінницький національний технічний університет, м. Вінниця

Порівняльний аналіз можливостей сучасних вебсистем для моніторингу здоров'я

Сучасні вебсистеми для моніторингу здоров'я використовують складні алгоритми аналізу даних, інтеграцію з носимими пристроями та персоналізований підхід для відстеження показників здоров'я користувачів. Вони забезпечують збір, обробку та візуалізацію даних про фізичну активність, харчування, сон, серцевий ритм та інші важливі показники.

Деякі системи фокусуються на профілактиці захворювань, пропонуючи рекомендації щодо здорового способу життя та нагадування

про необхідність медичних обстежень. Інші спеціалізуються на моніторингу конкретних медичних станів, наприклад, діабету або гіпертонії.

Важливими аспектами сучасних вебсистем моніторингу здоров'я є безпека даних, інтеграція з медичними інформаційними системами та адаптація до індивідуальних потреб користувачів різних вікових груп та станів здоров'я.

Серед популярних платформ можна виділити Apple Health, Google Fit і Samsung Health, кожна з яких має свої унікальні особливості, переваги та недоліки.

Apple Health (рис. 1) є інтегрованою платформою для моніторингу здоров'я від компанії Apple, яка об'єднує дані з різних пристроїв та додатків в єдиному інтерфейсі [1].

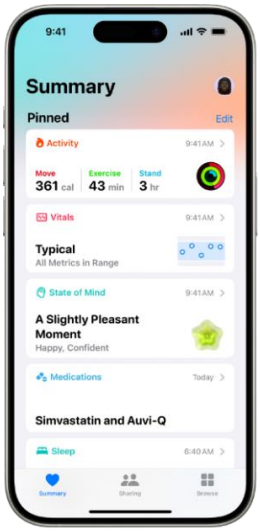


Рис.1. Приклад роботи вебсистеми Apple Health

Серед переваг даної вебсистеми слід виділити високу безпеку даних та конфіденційність, інтеграцію з великою кількістю сторонніх додатків та пристроїв, комплексний підхід до аналізу здоров'я, а також можливість створення медичної картки користувача. Однак система має і недоліки, зокрема: доступність лише для екосистеми Apple, відсутність розширеного аналізу даних без додаткових додатків та обмеженість у налаштуванні персоналізованих цілей.

Особливістю Apple Health є функція «Health Records», яка дозволяє користувачам інтегрувати свої медичні дані з різних медичних закладів, що підтримують цю функцію, створюючи комплексну картину здоров'я.

Наступною розглянемо вебсистему Google Fit (рис. 2), що представляє собою відкриту платформу для моніторингу здоров'я, доступну на різних пристроях і операційних системах [2]. До переваг цієї вебсистеми можна віднести кросплатформенність та доступність, інтуїтивно зрозумілий інтерфейс, систему кардіобалів для оцінки фізичної активності та безкоштовне використання базових функцій. Водночас

система має такі недоліки як менш детальний аналіз даних порівняно з конкурентами, обмежена інтеграція з медичними системами та потенційні проблеми з конфіденційністю даних.

Google Fit вирізняється своєю системою кардіобалів Heart Points, яка розроблена у співпраці з Всесвітньою організацією охорони здоров'я та заохочує користувачів до регулярної фізичної активності.

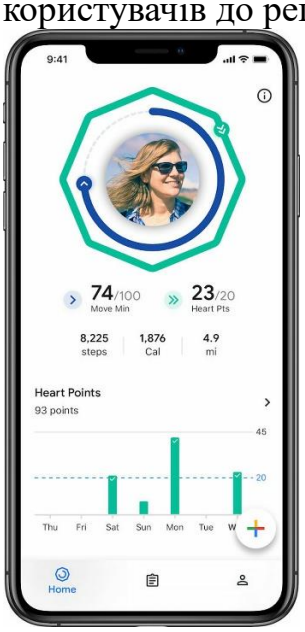


Рис. 2. Приклад роботи вебсистеми Google Fit

Рис. 3. Приклад роботи вебсистеми Samsung Health

Samsung Health (рис. 3) є комплексною платформою для моніторингу здоров'я, що пропонує широкий спектр функцій для відстеження різних аспектів здоров'я та фізичної форми [3]. Перевагами цієї системи є розширені функції моніторингу сну та стресу, соціальні елементи та змагання між користувачами, детальні звіти та візуалізація даних, а також наявність програм тренувань та харчування. До недоліків можна віднести надмірну кількість функцій, що може ускладнювати використання, оптимізацію переважно для пристроїв Samsung, відсутність деяких медичних функцій, доступних у конкурентів.

Samsung Health відрізняється своїм соціальним аспектом, дозволяючи користувачам змагатися з друзями у виконанні фізичних вправ, що додає елемент мотивації до здорового способу життя.

Встановлено, що згідно з проведеним аналізом, кожна з розглянутих вебсистем для моніторингу здоров'я має свої унікальні переваги та недоліки. Деякі з них пропонують більш глибоку інтеграцію з медичними системами, інші фокусуються на зручності використання та мотивації користувачів до здорового способу життя.

ДЖЕРЕЛА

1. Apple Health. URL: https://www.apple.com/ios/health/
2. Google Fit. URL: https://www.google.com/fit/
3. Samsung Health. URL: https://www.samsung.com/global/galaxy/apps/samsung-health/

ЗАСТОСУВАННЯ СПЕЦІАЛІЗОВАНИХ ПРОГРАМНИХ ЗАСОБІВ ДЛЯ ВІЗУАЛІЗАЦІЇ МОДЕЛЕЙ ВІДБИВНОЇ ЗДАТНОСТІ ПОВЕРХОНЬ

Завальнюк Є. К., Романюк О. Н.

Вінницький національний технічний університет, м. Вінниця

Разом із розвитком інформаційних технологій постійно підвищуються вимоги до якості та продуктивності рендерингу 3D-сцен. Для забезпечення високореалістичної й високопродуктивної 3D-візуалізації здійснюється розробка нових моделей рендерингу, зокрема, моделей відбиття світла від поверхонь. Моделі відбиття світла базуються, як правило, на основі двопроменевих функцій відбивної здатності (ДФВЗ), що визначають частку відбитого випромінювання у напрямку до спостерігача відносно напрямку падіння світла. Відповідно, якість кінцевої візуалізації залежить від якості тестування нових ДФВЗ.

Можна виокремити два напрямки тестування ДФВЗ: застосування широкопрофільних засобів 3D-моделювання й візуалізації (Blender, 3dsMax) і застосування спеціалізованих програмних засобів. Перевагами другого напрямку є більша швидкість налаштування параметрів, більш гнучке порівняння різних ДФВЗ на основі спеціальних метрик, відсутність зайвих параметрів візуалізації та зовнішніх чинників (наприклад, глобального освітлення), що можуть вплинути на чистоту досліджень. Окрім того, у повнофункціональних 3D-редакторах доступ до окремих функцій і параметрів візуалізації може бути обмежений. Розглянемо такі спеціалізовані засоби, як BRDF Explorer [1] і Idx3d [2]. BRDF Explorer – засіб для тестування ДФВЗ, розроблений Disney за допомогою мов C++, GLSL. Візуалізація сцени здійснюється на основі обраних у відповідних діалогових вікнах 3D-моделі та піксельного шейдера, де реалізовано визначену ДФВЗ. Також, можна додати карту зовнішнього середовища. Можливою є установка, як загальних параметрів візуалізації (зенітний і азимутальний кути падіння світла), так і характерних окремим ДФВЗ (шорсткість, коефіцієнт заломлення).

Можливість порівняння застосування кількох ДФВЗ на основі метрик якості зображень відсутня. Наявні додаткові графіки, наприклад, що візуалізують спекулярну пелюстку ДФВЗ у полярних і декартових координатах. Прямого інтерфейсу додання нових ДФВЗ немає, однак це можливо зробити шляхом створення відповідного текстового файлу з

розширенням .brdf у папці brdfs. Idx3d – 3D-рендерер, оригінально розроблений П. Васером на мові Java. Один із варіантів програми полягає у візуалізації двох 3D-сцен на основі обраних у списку ДФВЗ. Як правило, одна із моделей відбиття є еталонною, а інша – тестовою. При цьому, обчислюється метрика подібності зображень NMSE, а також час візуалізації. Можливою є установка коефіцієнта спекулярності поверхні, RGB-каналів альбедо матеріалу. Порівняємо засоби у таблиці 1.

Таблиця 1

Порівняння BRDF Explorer і Idx3d

Характеристика	BRDF Explorer	Idx3d
Розробник	Disney	Петер Васер
Наявність репозиторію коду в GitHub	Так	Так
Метричне порівняння якості візуалізації	Ні	Так
Зовнішнє додання нових ДФВЗ	Частково	Ні
Підтримка карт середовища	Так	Ні

Продемонструємо застосування BRDF Explorer (рис. 1а) і Idx3d (рис. 1б) для візуалізації модифікованої ДФВЗ Шліка. Дана модель запропонована авторами роботи [3] й дозволяє суттєво підвищити точність відтворення зони затухання відблиску. Використовується вираз

$$(2\cos(x)) / (1.25(n - n\cdot\cos(x) + 1.25\cdot\cos(x))^2),$$

де x – кут між нормаллю до точки поверхні та серединним вектором, n - коефіцієнт спекулярності поверхні.

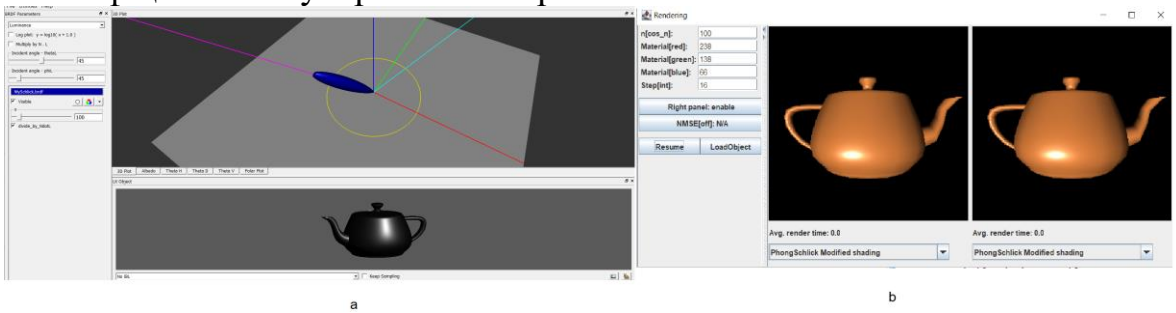


Рис. 1. Візуалізація запропонованої модифікованої моделі Шліка у BRDF Explorer (a) і Idx3d (b)

У результаті аналізу, запропоновано напрямки вдосконалення даних засобів: можливість одночасного порівняння кількох ДФВЗ (BRDF Explorer), вибору метрики якості зображень (Idx3d), візуалізації карти середовища (Idx3d), додання нових ДФВЗ через інтерфейс (BRDF Explorer, Idx3d), формування звітів з результатами (BRDF Explorer і Idx3d).

Отже, спеціалізовані засоби BRDF Explorer і Idx3d забезпечують більш ефективне тестування ДФВЗ порівняно із загальними 3D-засобами. Доцільним є їх вдосконалення, зокрема, у напрямках автоматичного оцінювання якості зображень та додання нових моделей відбиття.

ДЖЕРЕЛА

1. Aguilar D. BRDF Explorer. *GitHub*. URL: https://github.com/wdas/brdf/tree/main (дата звернення: 01.05.2025).

2. Borges A. IDX3D. *GitHub*. URL:https://github.com/AlessandroBorges/IDX3D (дата звернення: 01.05.2025).

3. Розробка модифікованої моделі Шліка для визначення спекулярної складової кольору / Є. К. Завальнюк та ін. *Інформаційні технології та комп'ютерна інженерія*. 2022. Т. 55, № 3. С. 4 – 12.

ЗАСТОСУВАННЯ ШІ ДЛЯ РОЗРОБКИ ТЕСТІВ ДО КУРСІВ ПЛАТФОРМИ LMS MOODLE

Ільїн О.О.

Київський національний університет будівництва і архітектури, м. Київ

Створення тестів в курсах LMS Moodle за допомогою стандартного підходу, тобто введення даних кожного окремого тестового завдання через браузер, є доволі кропіткою роботою, яка потребує значних затрат часу, уваги, технічної та розумової праці. Якщо є вже готовий файл із заздалегідь підготовленими тестовими завданнями, у авторському оформленні, така робота спрощується. В загальному випадку вона передбачає виконання рутинних операцій типу «copy/paste» по переносу окремих фрагментів тексту з файлу до відповідних полів у веб-браузері. Якщо підготовлених тестових завдань немає, приходиться створювати тестові завдання шляхом набору тексту у веб-браузері на сайті платформи, додаючи текст у відповідні поля, здійснювати однакові налаштування тощо. Для платформи Moodle вже існують сервіси на основі штучного інтелекту (ШІ) по генерації як контенту для курсів, так і тестових завдань [1-3]. Проте їх застосування може виявитись складним внаслідок кількох причин. Одна з них – необхідність втручатись в роботу LMS Moodle на рівні серверу: адміністратор платформи має встановити нові плагіни. Наступна причина – вимога щодо наявності ключа доступу до сервісу API OpenAI, який можна отримати як безкоштовно (але з суттєвими обмеженнями, які можуть взагалі унеможливити застосування сервісу API OpenAI в рамках даної задачі), так і оформивши платну підписку. В той же час існують більш загально доступні та безкоштовні веб-платформи штучного інтелекту у вигляді чат-ботів, таких як ChatGPT та інші (Gemini, Grok тощо). Їх застосування не має таких нюансів, але потребує іншого підходу, якому присвячена дане дослідження.

В Moodle вже інтегрований механізм імпорту тестових завдань з файлів текстового типу. Цей механізм як раз і дозволяє автоматизувати рутинні операції типу «copy/paste» під час наповненні курсів контентом різного характеру. Існує кілька типових схем розмітки тестів у зовнішніх файлах, з яких можна імпортувати дані у курси Moodle [4]: Aiken, Gift,

Moodle XML, WebCT та деякі інші. Максимального налаштування тестових завдань можна досягти використавши Moodle XML формат. Всі інші є більш простими за можливостями описати налаштування тестових завдань. З цих міркувань було обрано формат Aiken [5], який має дуже простий синтаксис розмітки і дозволяє описати тестові завдання з кількома варіантами відповіді. Приклад розмітки тестового завдання у форматі Aiken:

Яке основне призначення дашборда?

A. Аналіз даних у реальному часі

B. Зберігання великих обсягів даних

C. Розробка алгоритмів машинного навчання

D. Створення мережевих протоколів

ANSWER: A

Текст опису тестового завдання у форматі Aiken максимально вільний від сторонніх знаків розмітки, його дуже просто як читати людині, так і створювати навіть у «ручному» режимі набору тестів.

Основою методики автоматизації розробки тестових завдань за допомогою чат-боту ChatGPT є коректне написання запиту, який би включав як вказівку «розібрати» авторський формат оформлення тестових завдань, так і оформити їх у форматі файлу Aiken. Для вказання того, що контекст міститься у файлі на диску, рекомендується застосувати такій вміст запиту до ChatGPT: «Використовуючи зміст файлу [назва_файлу], зроби...». У відповідь ChatGPT попросить вказати файл для завантаження. Далі треба в якості дії, сформулювати ШІ задачу, результатом якої має стати набір тестових завдань, розмічених згідно формату файлу Aiken (деталі про формат див. у [5]). Як приклад результату досліджень ефективності подібних запитів, нижче наведений вже готовий запит до ChatGPT для розбору авторських тестових завдань та їх запису у формат Aiken у текстовий файл з кодуванням UTF-8.

<BEGIN CONTEXT >

У мене є файл з тестовими завданнями у такому форматі:

1. Текст питання на одному рядку.

2. Перелік варіантів відповідей, кожен варіант на новому рядку.

3. Вірна відповідь позначена знаком «+» на початку рядка, що містить варіант.

Використай цей контекст для створення тестових завдань у форматі Aiken.

<END CONTEXT >

<TASK>

Переробити цей формат у формат Aiken, збережи у файлі з кодуванням UTF-8 та дай файл для завантаження.

<END TASK>

<FORMAT>

- Дотримуйся стандарту Aiken:
  - Запитання на одному рядку
  - Відповіді позначені літерами (A, B, C, D)
  - Правильна відповідь вказується після «ANSWER:»
- Відповіді повинні бути у верхньому регістрі (наприклад, ANSWER: B).
- Між питаннями додавай порожній рядок.
- Не включати знак «+» у вірну відповідь.
<END FORMAT>

Цей запит має чітку структуру, створену спеціальними службовими словами, які «розуміє» ChatGPT. Вони містяться у трикутних дужках: <BEGIN CONTEXT >, <END CONTEXT >, <TASK>, <FORMAT> , <END FORMAT>. Технологія маркування окремих структурних елементів запиту такою розміткою доцільна, коли ми хочем мати чітку та логічну структуру у побудованому запиті. Це дозволяє точно контролювати формат відповіді та його особливості, коли передбачається багатократне використання цього запиту, що важливо для задач автоматизації. Як показали дослідження, запити такого формату є більш чіткими та передбачуваними у результаті своєї роботи під час виконання у ChatGPT в режимі чату та під час застосування через API для доступу до різних мовних моделей взагалі (OpenAI і т.п.) В останньому випадку треба врахувати, що службові команди можуть відрізнятись для різних мовних моделей. Також обов’язково зауважимо, що існує певна імовірність того, що запит може повернути результат, який відрізняється від очікуваного. Тому під час такого застосування сервісу ChatGPT необхідно контролювати результат його роботи.

ДЖЕРЕЛА

1. Mindfield Consulting. Moodle AI Plugins [Електронний ресурс]. Режим доступу: https://mindfieldconsulting.com/moodle-ai-plugins/?utm_source=chatgpt.com – Дата звернення: 25.04.2025.

2. Moodle. AI Solutions for Moodle [Електронний ресурс]. Режим доступу: https://moodle.com/us/news/ai-solutions-for-moodle/?utm_source=chatgpt.com – Дата звернення: 25.04.2025.

3. Moodle. OpenAI Chat Plugin [Електронний ресурс]. Режим доступу: https://moodle.org/plugins/block_openai_chat – Дата звернення: 25.04.2025.

4. Moodle. Import questions [Електронний ресурс]. Режим доступу: https://docs.moodle.org/405/en/Import_questions. Дата звернення: 25.04.2025.

5. Moodle. Aiken format [Електронний ресурс]. Режим доступу: https://docs.moodle.org/405/en/Aiken_format. Дата звернення: 25.04.2025.

СТВОРЕННЯ ОСВІТНІХ ПРОДУКТІВ У ЗАСТОСУНКУ WORDWALL ДЛЯ РОБОТИ З ДІТЬМИ З РОЗЛАДАМИ АУТИСТИЧНОГО СПЕКТРА

Іроні С., Ковалевська М., Шелудько О., Діденко М.
Київський столичний університет імені Бориса Грінченка, м. Київ

Для сучасних дітей використання інфомаційних технологій має вирішальне значення. Цифрові платформи дають можливість адаптувати, персоналізувати та гейміфікувати процес навчання. Розвиток дітей завжди пов'язаний з грою, бо саме цей вид діяльності є найбільш ефективним для досягнення найкращих результатів. Через гру діти пізнають світ, навчаються й розвиваються. Інтерактивні платформи дають можливість добирати ігри з урахуванням особливостей рівня розвитку та інтересів дитини. Щоб покращити навчальний процес, зробити його результативним, викладачі використовують різні застосунки. Вибираючи додаток фахівці звертають увагу на простоту використання, зрозумілий інтерфейс, інтерактивність, доступність на різних пристроях та можливість безоплатного користування. Платформа Wordwall відповідає цим вимогам і є прикладом інтерактивного, зручного та функціонального онлайн ресурсу, який став широко використовуватись у процесі навчання.

Метою Wordwall є забезпечення доступу до інтерактивного навчання учнів різних вікових категорій, з різними особливостями розвитку, в тому числі для дітей з РАС. Цей застосунок надає викладачам легкий і зручний спосіб створення інтерактивного контенту для навчання дітей з особливими освітніми потребами. Розробники створили інструмент доступний і зрозумілий для користувачів різного рівня володіння цифровими технологіями, щоб будь-який викладач міг створювати інтерактивні вправи за короткий проміжок часу.

Платформа Wordwall пропонує різноманітні формати завдань, включаючи кросворди, вікторини, сортування, пазли та інші. Інструмент також підтримує функцію створення завдань для друку, що дозволяє використовувати одні й ті ж матеріали як онлайн, так і офлайн. Завдяки налаштуванням рівня складності, Wordwall підходить для роботи з учнями будь-якого віку та рівня підготовки. Сервіс Wordwall достатньо зручний для групової роботи. Учням надаються посилання на вправу і вони в режимі реального часу виконують завдання. Сервіс надає можливість здійснювати рейтинг результатів, сформований у вигляді таблиці. Тобто учні можуть змагатися між собою, а також порівнювати свої досягнення з результатами інших учасників. Ігрові вправи використовуються: як тренажер при повторенні, як навчальні завдання та вікторини.

Таблиця 1

Аналіз переваг і недоліків сервісу Wordwall

Переваги:	Недоліки:
Можливість розробки інтерактивних ігор та завдань	Учні можуть захопитись формою, але не змістом
Широкий функціонал: типи завдань, інструментарій для створення, параметри доступу	Частина функціоналу, може бути на платній основі.
Зручний, зрозумілий сервіс	Обмежена кількість шаблонів в безкоштовній версії
Миттєва перевірка виконання вправ.	
Будь яке завдання можна зробити відкритим, загальнодоступним.	Якщо не зробити вправу відкритою то виконання завдання неможливо побачити за посиланням.
Велика бібліотека готових завдань	Безкоштовно можна створити лише 5 матеріалів
Крос-платформність створених завдань	Неможливо використовувати без інтернету
Надання доступу до вправи та можливість опублікувати її в соціальних мережах, Google Class, надіслати електронною поштою або отримати вбудоване посилання чи qr-код вправи	Якщо вправу не опублікувати, то її неможливо побачити за посиланням.
Має функцію конвертування інтерактивного завдання у форматах PDF	
Сервіс має україномовну версію	
Можливість вставити свої зображення з телефонної галереї, з бази комп'ютера.	Немає можливості вставити відео та анімацію
«Розумні» й швидкі налаштування параметрів додатка (встановлення темпу, таймера, кількості спроб, різноманітність тем тощо	Створення складних завдань потребує додаткових навиків та використання експертних систем

Приклади завдань Wordwall для роботи корекційними педагогами (процес навчання дітей з розладами аутистичного спектра)

Для розвитку когнітивної сфери фахівець повинен враховувати специфіку сприйняття інформації людьми з аутизмом. Кожна дитина з РАС унікальна, тому вправи мають бути адаптованими до рівня її розвитку, особистих інтересів і потреб. При створенні вправ важливо використовувати сильні сторони кожної дитини, а саме: переваги в

зоровому сприйнятті, високий рівень механічної пам’яті та інші. Щоб уникнути перевантаження, завдання повинні бути короткотривалими. Зображення для вправ треба вибирати без зайвих елементів, на світлому фоні, без гучного звукового супроводу.

Як приклад, додаємо кілька вправ для формування та розвитку академічних навичок у дітей з аутизмом. Вправи на повторення букв та складання слів простої структури (Рис. 1.)

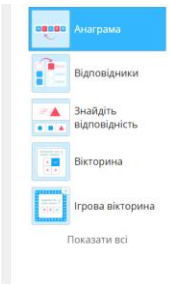


Рис. 1. Розвиток навички читання [1]

Вправа на розвиток розуміння прочитаного та на усні обчислення в межах десяти (Рис. 2). Вправа на Формування загальних понять (Рис. 3). Вправа для розвитку самостійності і планування (Рис. 4).

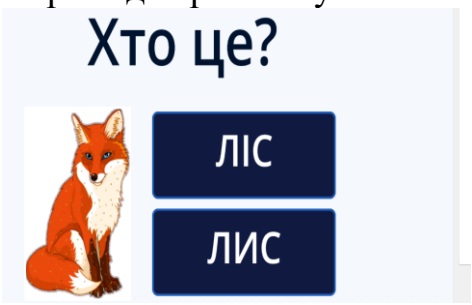


Рис. 2. а. Розвиток розуміння прочитаного;

Рис. 2. б. QR коди вправ;

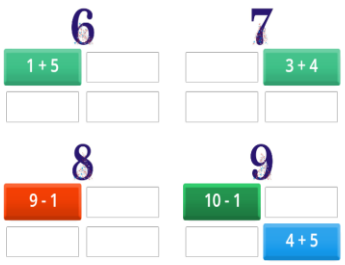
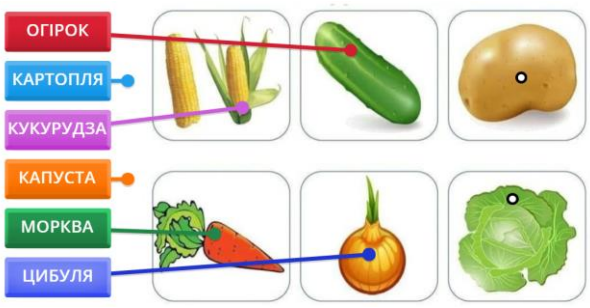


Рис. 2. в. Усні обчислення в межах 10 [2; 3]



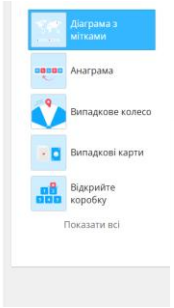


Рис. 3. Формування загальних понять. Овочі [4]

Рис.4. Вправа для розвитку самостійності і планування [5]

Такі вправи допомагають підтримувати інтерес до навчання, розвивають навички читання, усних обчислень та формування загальних понять. Також вдосконалюють навички самостійності, планування розпорядку дня чи окремої дії, допомагають в освоєнні навички соціальної взаємодії, що є важливою частиною розвитку когнітивної, та соціально-емоційної сфер дитини.

Отже, Wordwall є сучасним універсальним інструментом, який допомагає викладачам легко створювати та адаптувати навчальні завдання. Використання веб-сервісу Wordwall.net під час дистанційного навчання допомагає розвивати у учнів з особливими освітніми потребами: пізнавальну діяльність, мотивацію, самостійність, логічне мислення тощо.

ДЖЕРЕЛА

1. Розвиток навички читання. URL: https://wordwall.net/uk/resource/81349603
2. Усні обчислення в межах 10. URL: https://wordwall.net/uk/resource/81393998.
3. Усні обчислення в межах 10. URL: https://wordwall.net/uk/resource/81395405
4. Формування загальних понять. Овочі. URL: https://wordwall.net/uk/resource/81350786
5. Вправа для розвитку самостійності і планування. URL: https://wordwall.net/uk/resource/81484310
6. Wordwall: Веб-сайт. URL: https://wordwall.net/uk
7. Макаревич О. О. Гейміфікація як невід'ємний чинник підвищення ефективності елементів дистанційного навчання. Молодий вчений, 2015 URL: http://eprints.zu.edu.ua/17143/1/357.pdf
8. WordWall – простий спосіб для створення власних навчальних ресурсів URL: https://vchymo.com/app/application/WordWall#google_vignette.

ПОРІВНЯЛЬНИЙ АНАЛІЗ WATERFALL І AGILE ПІДХОДІВ У КОНТЕКСТІ КЕРУВАННІ ІТ-ПРОЄКТАМИ

Каричорт І. Б., Вовк Р. Б.
Івано-Франківський національний технічний університет нафти і газу, м. Івано-Франківськ

У сучасній практиці впровадження інформаційних технологій відсутній єдиний універсальний підхід, який би був однаково ефективним у контексті кожного конкретного проєкту чи організації. Сьогодні домінуючими підходами до розробки та впровадження ІТ-систем є каскадна модель (Waterfall) та гнучкі методології (Agile). Каскадна модель (Waterfall) є традиційним, лінійним та послідовним підходом до управління проєктами. У межах цієї моделі реалізація проєкту відбувається поетапно, причому перехід до наступного етапу можливий лише після завершення поточного. Типовими етапами Waterfall є: збір вимог, аналіз, проєктування, кодування, внутрішнє тестування, приймальні випробування, встановлення, впровадження, навчання та введення в експлуатацію. Такий підхід передбачає повне завершення кожної фази перед початком наступної, що забезпечує формальну структурованість проєкту [1].

Серед ключових переваг Waterfall моделі слід відзначити:

- чітке планування та проєктування, що ґрунтується на фіксованих припущеннях на початковому етапі;
- повна визначеність обсягу робіт;
- спрощене бюджетування;
- зручність контролю та моніторингу прогресу реалізації.

Водночас недоліками Waterfall є:

- жорсткість структури, що ускладнює внесення змін;
- низький рівень адаптації до змін у вимогах;
- верифікація відповідності вимогам здійснюється лише після завершення проєкту;
- необхідність великого обсягу документації;
- обмежене залучення замовника, що може призвести до незадовільних результатів;
- високі ризики при реалізації довготривалих проєктів з віддаленим у часі очікуваним результатом.

Методології Agile, на відміну від Waterfall, реалізують проєкт за допомогою поступових ітерацій, що забезпечує високу адаптивність до змін та гнучкість у прийнятті рішень. Основна ідея полягає в тому, щоб якнайшвидше створити базову версію програмного продукту, яка в подальшому поступово налаштовується відповідно до змінних вимог користувача [1].

До переваг Agile підходу належать:

- скорочений час до запуску базової версії продукту, що дозволяє паралельно реалізовувати складніші етапи;
- ефективне поетапне тестування та безперервне оновлення функціональності;
- прискорений життєвий цикл розробки;
- можливість оперативної перевірки припущень щодо функціональності;
- тісна взаємодія з користувачем на всіх етапах розробки;
- вища ймовірність задоволення кінцевого користувача за рахунок його активної участі;
- оптимізація витрат завдяки пріоритезації функцій.

Серед недоліків Agile варто виокремити:

- потребу у постійній та активній участі замовника;
- високі вимоги до кваліфікації та мотивації членів команди;
- складність точного оцінювання вартості проєкту на початковому етапі.

Таблиця 1

Порівняльна характеристика моделей Waterfall та Agile

Критерій	**Waterfall**	**Agile**
Підхід	Лінійний, послідовний	Ітеративний, інкрементний
Структура	Поділ на фази	Поділ на спринти
Сфера застосування	Великі проєкти	Невеликі або змінні проєкти
Взаємодія з клієнтом	Мінімальна	Постійна співпраця
Оцінка прогресу	Після завершення фази	Щоденні зустрічі, постійний моніторинг
Гнучкість змін	Обмежена	Висока, на будь-якому етапі
Тестування	Завершальний етап	Безперервне,

Отже, Waterfall передбачає ретельне початкове планування, чітке визначення бюджету та обсягів робіт, а також контроль на кожному етапі реалізації, що робить його ефективним у стабільному середовищі з фіксованими вимогами. Agile, у свою чергу, забезпечує адаптивність, швидке створення мінімально життєздатного продукту та ефективне тестування за рахунок поетапного поділу проєкту та тісної взаємодії з користувачем, що робить цей підхід придатним до динамічних умов та змінних вимог.

ДЖЕРЕЛА

1. Waterfall або agile реалізація - яку модель обрати? URL: https://quantum-int.com/news/waterfall-abo-agile-realizatsiya-yaku-model-obrati/

ЧОМУ FIVERR КОРИСНИЙ ДЛЯ РОБОТИ В СФЕРІ РЕКЛАМИ ТА PR?

Клобудська С., Циганкова К.,Тесля О., Майданюк І.,
Захаренко Т. Скрибка Д.
Київський столичний університет імені Бориса Грінченка, м. Київ

В сучасному світі кожна професія покращує свою роботу завдяки цифровим технологіям.Зокрема, професія рекламіста та PR-менеджера,яким необхідно завжди бути на зв’язку з клієнтом, швидко адаптуватись до нових трендів та застосовувати новітні технології.

Тож,у цій доповіді ми розповімо про корисний сервіс,який полегшить роботу працівників у сфері реклами та їхню комунікацію із замовниками.

1. Чому Fiverr? Fiverr – це глобальний онлайн-маркетплейс послуг фрілансерів, який охоплює приблизно 160 країн.

Платформа дозволяє продавати послуги та одночасно бути постачальником і клієнтом на ринку цифрового маркетингу.

Переваги та недоліки Fiverr для роботи в сфері реклами та PR

Переваги	**Недоліки**
Швидкий вибір послуг	Fiverr бере комісію 20%
Доступність	Конкуренція
Гнучкість	Платформа не проводить ретельну перевірку фрілансерів
Вбудована платіжна система	Виникають проблеми в комунікації із замовника та виконавця
Зручний інтерфейс	Повільне зростання на початку
Різні способи заробітку	
Широка аудиторія	
Різні способи заробітку	

2. Що потрібно для реєстрації:

- Після створення акаунту сайт пропонує обрати: отримати/надати послугу.
- Обравши «Надання фріланс послуг», вказуєте тип фрілансера> зазначаєте стиль в роботі> ознайомлюєтесь з можливостями в роботі> створюєте сторінку продавця.
- Необхідно заповнити дані в анкеті: ім'я та прізвище (англійською) та нікнейм, професійне портретне фото, короткий опис ваших здібностей, мови якими володієте та рівень їх знання.
- Вказати напрямок вашої діяльності, освіту та наявні сертифікати. В окремому вікні вписати посилання на соцмережі та вебсайт.
- Далі проходите етап безпеки облікового запису.

- Додаєте опис для вашого пакету послуг, перелік, необхідних для початку роботи над проектом, питань.
- Якщо ви є громадянином Америки, то необхідно заповнити додаткову форму.
- Тепер ваш профіль створений і можемо брати замовлення.

3. Можливості та користь для спеціальності «Реклама та зв'язки з громадськістю»

Графіка: на платформі можна створювати дизайни логотипів, сайтів, додатків, одягу, архітектури, 3D ілюстрацій, ігор та товарів.

Програмування та технології:можна створювати та обслуговувати сайти, використовувати ШІ, розробляти мобільні додатки, програмне забезпечення та ігри.

Цифровий маркетинг: налаштування реклами, аналітика, маркетингові стратегії, SEO (коригування HTML, тексту, структури сайту та зовнішніх факторів для покращення позицій у пошукових системах).

Написання та Переклад: створення статей, блогів, веб-контенту; написання рекламних текстів, слоганів, описів товарів; технічне написання; переклад з однієї мови на іншу, враховуючи документи, статті та веб-сайти; адаптація контенту для певної культури чи регіону; виправлення граматичних помилок і поліпшення стилю тексту.

Відео та анімація: анімація 2D/3D, логотипи, персонажі, рекламні ролики; відеомонтаж; рекламні відео; інфографіка.

Музика та Аудіо: створення музичних творів для фільмів, реклами, ігор та інших проєктів; професійний запис голосу для рекламних роликів, презентацій, аудіокниг; обробка аудіотреків для професійної якості звуку; створення звукового дизайну, ефектів та фонової музики.

Бізнес: Fiverr Business зв'язує вас із експертами-фрілансерами для будь-яких потреб бізнесу. Він допомагає оптимізувати роботу, співпрацювати з командою та досягати цілей в одному спільному робочому просторі.

Ви можете скористатися кадровими послугами, включаючи підбір персоналу: від написання оголошень про вакансії та збору резюме до перевірки кандидатів і проведення співбесід. Деякі консультанти допоможуть розробити організаційний план, визначити стратегію найму та знайти кандидатів, які відповідають культурі компанії, а юридичні кадровики можуть скласти трудові договори.

Фінансові послуги : фінансове консультування, бухгалтерські послуги, аналіз фінансових даних, курси та навчання, створення бізнес-планів, розробка фінансових інструментів, контент на фінансову тематику.

Послуги ШІ: доступ до глобальних експертів зі штучного інтелекту, безпечна платформа для транзакцій та гарантія якості. Всі послуги ШІ спрямовані на розширення можливостей бізнесу за допомогою передових рішень.

Особистісне зростання: Fiverr відкриває можливості для реалізації потенціалу та розвитку, з'єднуючи фрілансерів з клієнтами по всьому світу. Платформа дозволяє креативним людям заробляти на дизайні, копірайтингу, графічному дизайні та інших сферах; сприяє розвитку робочого досвіду, комунікації з іноземними партнерами та новим знайомствам; конкуренція на платформі мотивує до вдосконалення навичок через курси та вебінари.

Консультації: можна знайти фахівців для аналізу ринку, розробки бізнес-стратегії та фінансового планування для малих бізнесів та стартапів.

Рекламісти та піарники надають консультації з промоції та підвищення впізнаваності бренду, а SMM-спеціалісти допомагають оформити сторінки. Також, доступні послуги з написання резюме, супровідних листів, оптимізації профілів на LinkedIn та підготовки до співбесід для покращення кар'єрних перспектив.

Фотографія: на Fiverr можна знайти фотографів для зйомки подій, монтажу відео та професійних завдань. Вони допомагають рекламістам створювати постери й листівки. Майстри з обробки пропонують ретуш, корекцію кольору, видалення зайвого та художню обробку для персональних і комерційних фото.

5. Як відбувається замовлення.

1) Клієнт пише вам на платформі, що зручно, оскільки все обговорення знаходиться на одному сайті. Далі укладається контракт і пропонується кастомна пропозиція або стандартний пакет послуг. **Порада для фрілансерів:** відповідайте замовникам швидко та вчасно, оскільки в майбутньому ця інформація ввійде до статистики вашого профілю та вплине на ваш рейтинг, від якого залежить потік замовників.

2) Якщо клієнт купує вашу пропозицію без попереднього повідомлення, подякуйте йому та задайте додаткові питання. **Поради:** виконуйте роботу вчасно, враховуючи різницю в часі, та, у разі потреби, домовляйтесь про продовження дедлайну.

6. Badges. Значки «badges» відображають статус фрілансера. Їх отримують за позитивні відгуки, своєчасне виконання та стабільну якість.

Для новачків доступні базові значки, рівень 1 і 2 відображають успішність замовлень, а платинові і золоті свідчать про високі досягнення.

Значки підвищують довіру клієнтів, стимулюють замовлення, дозволяють встановлювати вищі ціни та мотивують фрілансерів покращувати якість роботи.

7. Як отримати відгук? Оскільки на Fiverr клієнт не зобов'язаний залишати відгук, то по завершенню роботи із замовником потрібно спонукати його до цього зазначивши, що ви були б дуже вдячні за зворотний зв’язок щодо якості виконання вашої замовлення.

8. Як вивести кошти. Для виведення коштів потрібно:

- Підключити **Payoneer** (зареєструватись можна як фізична особа чи ФОП)
- Заповнити податкову форму **W-9** (форма для американської податкової системи, адже, цей сайт працює зі штатів)

Fiverr гарантує отримання оплати, для цього там є всі необхідні функції. Тому рекомендує **НІКОЛИ** не виходити за межі платформи з потенційними клієнтами, не передавати персональні дані.

Отже, Fiverr – це чудовий варіант для інфлюенсерів, які прагнуть розвитку та розширення бази своїх клієнтів. Адже на платформі можна як розміщувати оголошення про свої послуги, так і шукати професіонала, який реалізує вам запит. Зокрема сайт багатофункціональний, що дає можливість працювати безпосередньо в ньому і вирішує проблему пошуку інших платформ та додатків для роботи.

ДЖЕРЕЛА

1. Scale your professional workforce with freelancers. URL: https://www.fiverr.com/
2. Як почати заробляти на Fiverr у 2024: ПОВНИЙ ГАЙД. URL: https://youtu.be/SNYlyEOd2A4?si=Lj-W8KoOExXKrKcl
3. Як фрилансити на Fiverr: від старту з нуля до черги з клієнтів URL: https://happymonday.ua/yak-frylansyty-na-fiverr

ФУНКЦІОНАЛЬНІ МОЖЛИВОСТІ ДОДАТКУ LEARNING APPS У РОБОТІ КОРЕКЦІЙНОГО ПЕДАГОГА

Козій Л., Літченко І., Пісоцька А., Чернявська Т.
Київський столичний університет імені Бориса Грінченка, м. Київ

Інформаційно-комунікаційна компетентність набуває особливого значення в умовах інформатизації суспільства, оскільки ефективність сучасної освіти значною мірою залежить від здатності педагогів інтегрувати цифрові технології в навчальний процес. Хоча Інтернет пропонує багато інтерактивних освітніх ресурсів, значна їх частина має недоліки: обмежений доступ, відсутність можливості редагування, невідповідність індивідуальним потребам учнів та складність створення власного контенту.

У цьому контексті перспективним інструментом є вебсервіс LearningApps.org, що належить до технологій WEB 2.0 і дає змогу створювати інтерактивні вправи для підтримки навчання. Платформа пропонує близько 30 шаблонів завдань, згрупованих за типами (вибір, розподіл, послідовність, заповнення, кросворди), які можна швидко адаптувати до різних методичних цілей. Створені завдання мають унікальні URL-адреси та сприяють підвищенню мотивації учнів завдяки доступності й візуальній привабливості.

Даний застосунок дає можливість використовувати створені вправи, а також конструювати власні. Для початку роботи потрібно пройти реєстрацію. Перш ніж створювати власні інтерактивні завдання, доцільно познайомитися з галереєю сервісу та переглянути напрацювання колег. Пошук можна здійснювати за вказаними критеріями: автор, тематика, вік. Режим «Створення вправ» розкриває для педагога багато нових можливостей. Використовуючи шаблони, можна розробляти вправи, які відповідатимуть індивідуальним особливостям учня/дитини, рівню знань, а також враховувати їх корекційне спрямування.

Онлайн ресурс *LearningApps* в професійній діяльності корекційного педагога може сприяти активації пізнавальної діяльності у дітей з особливими потребами.

Таблиця 1

Аналіз переваг і недоліків LearningApps

Переваги	**Недоліки**
Використання вправ інших авторів	Відсутня можливість коригувати вправи інших авторів
Самостійна розробка завдань	Завдання можна створити лише за шаблоном
Можливість завантажувати власні зображення	Зображення не повинні перевищувати задані параметри
Створення власної колекції	
Можливість використання за посиланням	
Використання для індивідуальної та групової роботи	

Для дитини з аутизмом, формування базових навичок – це одне з основних завдань спеціального педагога. Тому, використовуючи застосунок *LearningApps* для розвитку ключових компетентностей, можна формувати соціальні, функціональні, комунікативні навички, та підвищувати рівень когнітивної сфери.

У дітей з розладами аутичного спектру сильний візуальний канал для отримання інформації. Вправи, які розроблені у застосунку, мають унаочнений дидактичний матеріал, який допомагає втримати в полі зору цілісність завдання, також, що не менш важливо для дітей даної категорії, знизити рівень тривожності, адже дитина знає і бачить, що на неї чекає, може контролювати ситуацію, виконувати завдання у власному темпі.

Для розвитку базових функціональних навичок можна використовувати шаблон «класифікація». Завдання можна розробляти безпосередньо для конкретної дитини, щоб закріпити сформовані вміння, або працювати над формуванням нових. Під час виконання завдання «Сам – з допомогою» дитина з розладами аутичного спектра за проханням

групує малюнки, закріплюючи правила, що можна і потрібно робити самостійно, а що тільки в присутності, або за допомогою дорослих https://learningapps.org/watch?v=pzq10h7w324 (Рис.1).

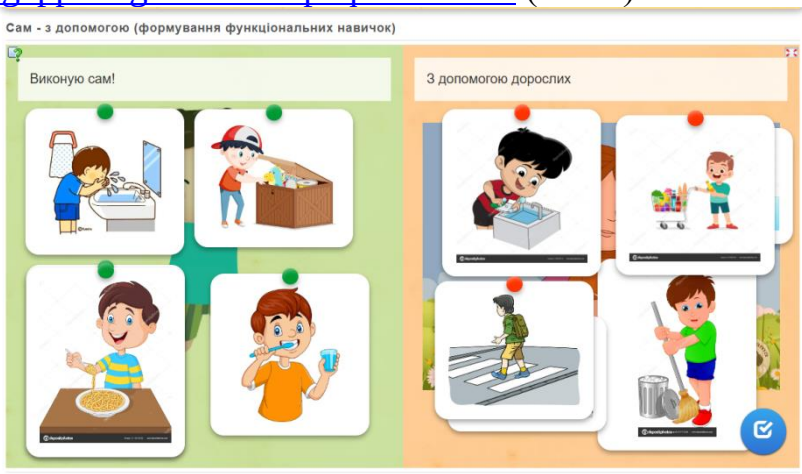


Рис. 1. Вправа «Сам – з допомогою»

Для розвитку когнітивної сфери, з використанням цього ж шаблону, створено вправу, яка спрямована на розвиток навичок класифікації https://learningapps.org/watch?v=p4z1ckarj24 (Рис. 2). Суть виконання даного завдання заключається в тому, щоб розмістити подані овочі та фрукти у відповідні кошики. Дана вправа сприяє розвитку вміння класифікувати, стійкості та розподілу уваги. Після правильного виконання завдання дається вербальне заохочення. Не менш важливо для дитини з розладами аутичного спектра проговорювати назву кожного малюнка, таким чином ми допоможемо розвинути мовлення і запам’ятати назви предметів.

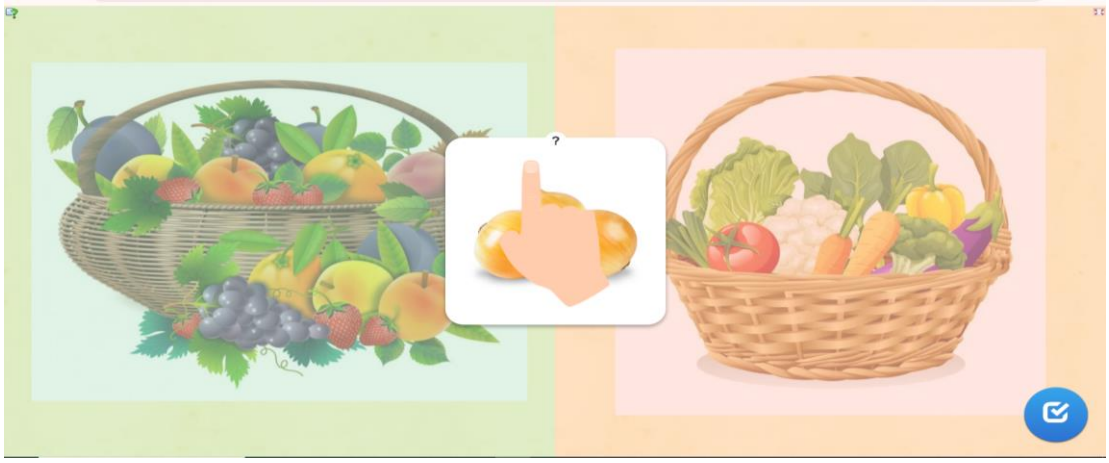


Рис. 2. Вправа «Овочі-фрукти»

З метою проведення дослідження узагальнення змістового матеріалу дитиною молодшого шкільного віку можна використати завдання на групування предметів за функціональним призначенням https://learningapps.org/watch?v=pwo07n5on24 (Рис. 3).

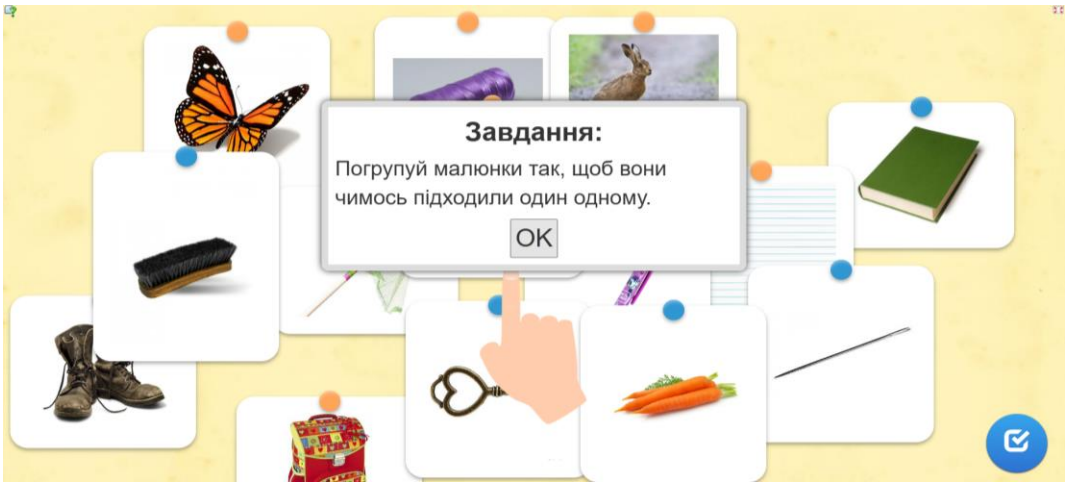


Рис. 3. Вправа на узагальнення змістового матеріалу за функціональним призначенням

Під час виконання демонструються малюнки, які потрібно об’єднати в пари. Якщо вправа виконується самостійно, то це чудовий результат. Якщо виконується самостійно, але з помилками або з допомогою педагога то це говорить про недостатній рівень сформованості вміння узагальнювати.

У наступному завданні «Гра-праця» використовуються малюнки, які потрібно об'єднати у дві групи так, щоб у кожній з них вони підходили один до одного. Для розробки цієї вправи використано шаблон «Пазл» https://learningapps.org/watch?v=p6yxcnw1k24 (Рис. 4)

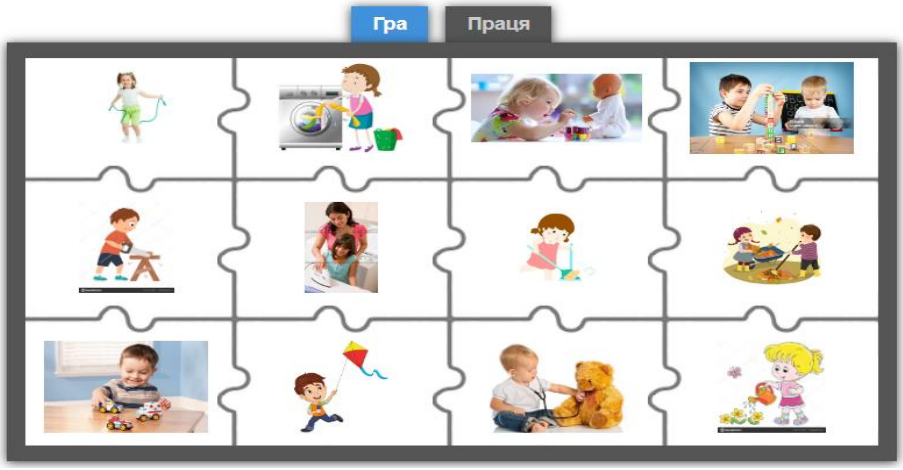


Рис. 4. Вправа «Гра-праця»

Наведене завдання може бути використане для розвитку логічного мислення та зв’язного мовлення.

За допомогою шаблону «Послідовність» створено вправу, яка допомагає розвивати логічне мислення. Для цього потрібно уважно розглянути малюнки і розмістити їх в послідовності, даючи відповідь на запитання «Що було спочатку? Що потім?». Дитина виконує завдання, вибудовуючи малюнки, відповідно до послідовності подій. https://learningapps.org/watch?v=p7t1d5ejk24 (Рис.5)

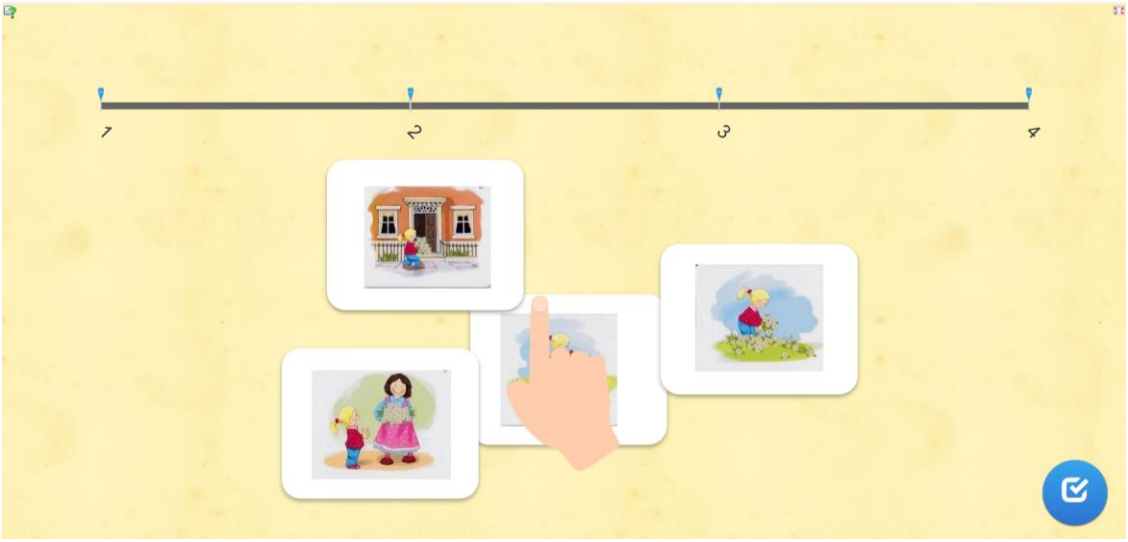


Рис. 5. «Послідовність подій»

Додаток *Learning Apps* – це платформа з великою кількістю освітніх інтерактивних завдань, ігор та активностей, доступних педагогам та учням безкоштовно. Використання Learning Apps допомагає підвищити ефективність корекційної допомоги, зробивши його більш захоплюючим, різноманітним та ефективним. Працюючи з дітьми з розладами аутичного спектра, завдяки різноманітними шаблонам, візуальному супроводу під час виконання завдань, педагог може досягти бажаного результату, заохочувати дітей до співпраці, сприяти розвитку когнітивних функцій, комунікативних, соціальних, функціональних навичок, працездатності, допомагати дітям самостійно вивчати та закріплювати матеріал.

ДЖЕРЕЛА

1. Руденко, О. В. (2025). Актуальність використання інформаційно-комунікаційних технологій в освітньому процесі. ББК 74 О 75, 136.

2. Лисак, Н. А. (2025). Можливості та напрями використання сервісів Learning Apps та Learning UA. Послідовність створення інтерактивних вправ і завдань. ЕКСПЕРТ, 475.

3.LearningApps.org 2025 [Електронний ресурс]: – Режим доступу: https://learningapps.org

ВИКОРИСТАННЯ ВЕБ-СЕРВІСУ PREZI У ТВОРЧІЙ ДІЯЛЬНОСТІ ФАХІВЦІВ З РЕКЛАМИ І ЗВ'ЯЗКІВ З ГРОМАДСЬКІСТЮ

Коломієць С., Івашина О., Стецько К., Касимбаєва К., Конюхова М.

Київський столичний університет імені Бориса Грінченка, м. Київ

У сучасному світі медіа та журналістика швидко адаптуються до нових технологічних змін, що відкривають безліч можливостей для створення та подачі інформації. Одним із таких інструментів, який значно

змінив підхід до створення презентацій та мультимедійного контенту, є онлайн-платформа Prezi.com. Це інноваційний та потужний інструмент для створення інтерактивних, нелінійних презентацій, що дозволяє створювати вражаючі, динамічні та візуально привабливі матеріали.

Prezi відразу здобула популярність завдяки своїй унікальній особливості: замість традиційних слайдів, використовується нескінченний простір для розміщення інформації. Користувачі можуть створювати презентації, у яких можна переміщатися між різними блоками контенту, створюючи ефект безперервного перегляду, що набагато ефективніше сприймається аудиторією, порівняно з класичними слайд-шоу. Prezi дозволяє інтегрувати текст, зображення, відео та графіку в єдиний простір, що дає змогу журналістам та медіа-організаціям створювати мультимедійні матеріали, які значно краще привертають увагу та утримують інтерес глядачів.

Основні функції Prezi:

- Створення інтерактивних презентацій: користувачі мають змогу створювати унікальні та динамічні презентації, використовуючи готові шаблони та змінюючи теми й кольори;
- Інтеграція мультимедійного контенту: можна додавати зображення, відео, аудіофайли, графіки та діаграми;
- Ефект зуму та нелінійна навігація: користувач може збільшувати та зменшувати певні частини слайдів, що дозволяє створювати ефект занурення в тему. Нелінійна структура дає змогу переходити до будь-якої частини презентації за бажанням, що підходить для інтерактивних виступів і відповідає потребам аудиторії;
- Спільна робота над презентаціями: користувачі можуть запрошувати інших для спільного редагування презентації в режимі реального часу;
- Налаштування доступу та безпека: презентації можуть бути публічними або приватними, з можливістю обмеження доступу. Це важливо для конфіденційних презентацій або тих, які призначені для вузької аудиторії;
- Інтеграція з іншими інструментами: Prezi легко інтегрується з популярними платформами для співпраці та комунікації, такими як Microsoft Teams, Slack та інші. Це забезпечує зручний спосіб обміну презентаціями та збереження продуктивності в робочому процесі.

Серед основних переваг та недоліків веб-сервісу Prezi варто виокремити (Таблиця 1):

Таблиця 1

Переваги	**Недоліки**
Цікаві анімовані ефекти	Малий пакет локалізації
Гнучкість налаштування	Безкоштовна версія дозволяє створювати презентації без додаткової функціональності
Можливість співпраці кількох користувачів над спільним проєктом	При реєстрації на пробний пакет потрібно вказувати платіжну інформацію
Зручний конструктор, що дозволяє легко змінювати послідовність усіх елементів, додавати векторну графіку, свої зображення та відеоматеріал	Готова презентація забирає багато дискового простору
Обширний вибір кастомізації	Наразі є стартапом, а не повноцінним стабільним сервісом

Сервіс Prezi є дуже корисним у діяльності фахівців з реклами і зв'язків з громадськістю, а саме для створення:

- Презентацій продуктів і послуг – демонстрація характеристик, переваг, та прикладів використання товару або послуги за допомогою інтерактивних переходів і масштабування;
- Рекламних концепцій – візуалізація ідей та стратегій рекламних кампаній для переконливого представлення клієнтам чи партнерам;
- Матеріалів для заходів – ефектні презентації для конференцій чи промо-івентів, що привертають увагу завдяки унікальній подачі;
- Навчальних матеріалів для рекламістів – спрощене пояснення маркетингових стратегій або рекламних процесів.

Підсумовуючи, можна сказати, що Prezi –це сучасний та ефективний інструмент для створення інтерактивних і динамічних презентацій, що вирізняється своїми унікальними можливостями. Завдяки підтримці мультимедійного контенту, ефектам масштабування та нелінійній навігації, платформа забезпечує високий рівень інтерактивності та гнучкості. Prezi є ідеальним вибором для тих, хто прагне інноваційно підходити до подання інформації, особливо в рекламі, маркетингу чи журналістиці.

ДЖЕРЕЛА

1. Хмарний сервіс Prezi – плюси та мінуси. [Електронний ресурс] - Режим доступу: https://prezi.com/p/fmjlwtb2shyu/prezi/ (дата звернення: 16.11.2024)

2. Веб-застосунок, за допомогою якого можна створити інтерактивні презентації з нелінійною структурою. Режим доступу: https://vchymo.com/app/application/Prezi (дата звернення: 16.11.2024)
3. Prezi. [Електронний ресурс] - Режим доступу: https://www.google.com/url?q=https://uk.wikipedia.org/wiki/Prezi&sa=U&sqi=2&ved=2ahUKEwiR3dDqjOaJAxXwAxAIHVBDJhwQFnoECCwQAQ&usg=AOvVaw3U5RcOqKdr1dr49zGiKX5b (дата звернення: 16.11.2024)

ВИКОРИСТАННЯ СИСТЕМИ КЕРУВАННЯ КОНТЕНТОМ БЛОГУ В ОСВІТНЬОМУ СЕРЕДОВИЩІ

Коляда В. С.
Державний університет інформаційно-комунікаційних технологій, м. Київ

Сучасні інформаційні технології активно інтегруються в освітній процес, формуючи нові підходи до взаємодії між викладачем і студентом. Розроблена система керування контентом блогу, яка дозволяє створювати, редагувати, переглядати та реагувати на публікації, може бути використана як ефективний інструмент для підвищення мотивації студентів та оперативне отримання зворотного зв'язку від викладача.

Мета дослідження: Впровадити та оцінити ефективність системи керування блогу, реалізованої на Java Spring Boot для підвищення мотивації студентів та оперативного зворотного зв'язку під час вивчення технічних дисциплін.

Результати експерименту: Під час пілотного тестування (група з 30 студентів протягом 4 тижнів) отримано:

1) 85% учасників підтвердили, що ведення блогу допомогло краще засвоювати матеріал;
2) Активність (пости, лайки) зросла на 40% порівняно з традиційними формами взаємодії;
3) Середня швидкість виправлення помилок у звітах лабораторних робіт зросла з 3 днів до 1,5 днів.

Інтерактивна платформа сприяє підвищенню залученості студентів через можливість обговорення матеріалів, оцінювання («лайки») та ведення особистих блогів. Це створює умови для реалізації концепції активного навчання, що, згідно з дослідженням [1], «відкриває нові форми взаємодії між учасниками освітнього процесу, сприяє розвитку навичок співпраці, критичного мислення та вирішення проблем».

Інтеграція цифрових інструментів у навчальний процес та підвищення вимог до володіння інформаційно-комунікаційними технологіями вимагають системного підходу до професійного розвитку викладачів [2]. Це може стати проблемою, але це дасть бажаний результат.

Приклад застосування: Студенти групи ПЗ-31 публікували звіти лабораторних робіт(див. рис. 2) з дисципліни «Бази даних» у вигляді блог-постів. Викладач оцінював роботи, що дозволило:

1) Швидко виявляти типові помилки (SQL-ін’єкції, неправильні запити);
2) Надавати персоналізовані рекомендації;
3) Підвищити середню оцінку за лабораторні роботи на 15%.

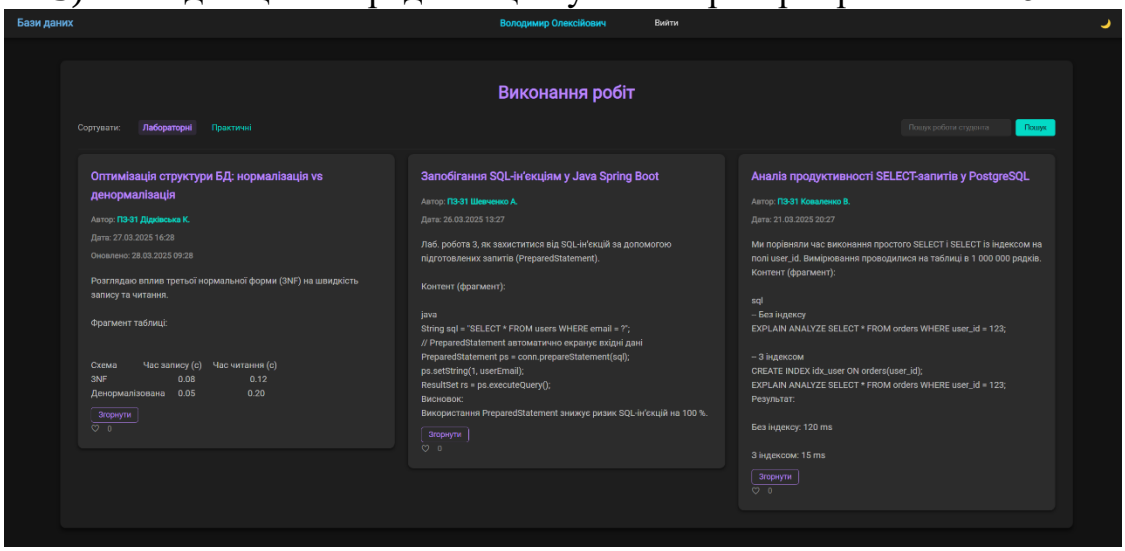


Рис. 1. Фрагмент публікацій

Схема взаємодії (рис. 2):

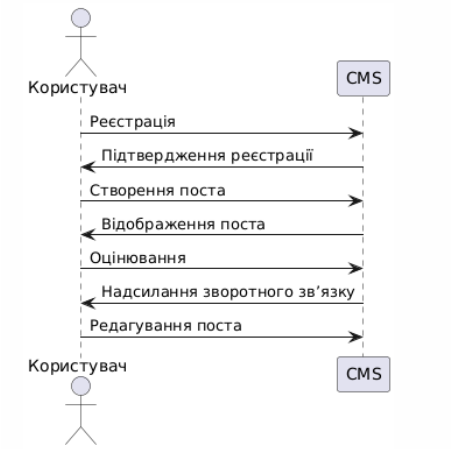


Рис. 2. Схема взаємодії користувача з системою

ДЖЕРЕЛА

1. Освіта для цифрової трансформації суспільства / В. Кременя та ін. Київ : ТОВ «Юрка Любченка», 2024. Т. 1. 526 с. URL: https://lib.iitta.gov.ua/id/eprint/742488/1/Монографія_т1_ел.pdf.

2. Гуменний О. Д., Федоренко О. І. Система розвитку цифрової компетентності викладачів професійно-теоретичної підготовки закладів професійної освіти в міжкурсовий період // Професійна освіта. 2025. DOI: 10.5281/zenodo.14848762. URL: https://lib.iitta.gov.ua/id/eprint/744609/1/Гуменний%2Вта%2Він%2В2.pdf.

ФУНКЦІОНАЛЬНІ МОЖЛИВОСТІ ДОДАТКУ TIKTOK У ПРОФЕСІЙНІЙ ДІЯЛЬНОСТІ РЕКЛАМІСТА

Лаврик М.
Київський столичний університет імені Бориса Грінченка, м. Київ

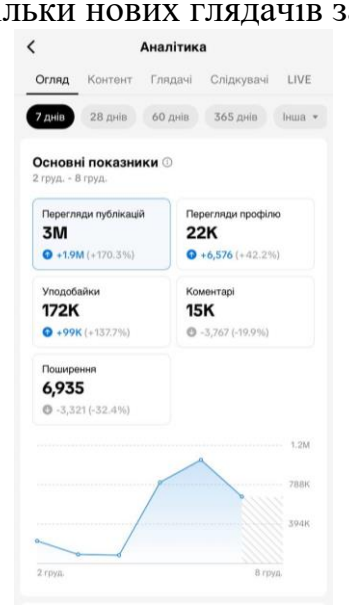
TikTok – це платформа для створення коротких роликів, популяризації брендів та трендів у маси, завдяки цьому додатку ми з легкістю можемо прорекламувати будь-який товар із мінімальним бюджетом.

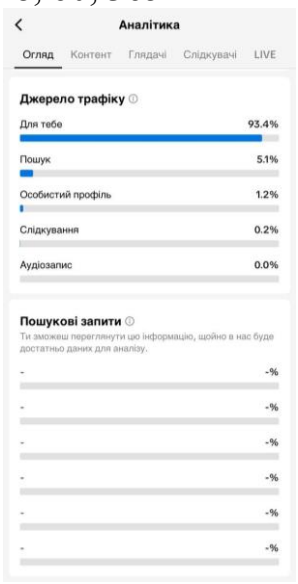
Цільова аудиторія: таких обмежень немає, тому що платформа дуже популярна серед усіх вікових категорій, але найчастіше можна помітити дітей, підлітків та молоді, а саме від 5 до 30 років. 16+ (відкривається можливість знімати ролики), 18+ (проведення прямих ефірів). Діти використовують для перегляду роликів, ну а молоді ж найчастіше для просування.

Можливості для реклами: в ТікТок можна як монтувати, так і просувати товар. Просування є платне та безкоштовне. Нещодавно творці внесли оновлення у вигляді «TikTok Studio» для перегляду аналітики, цільової аудиторії та іншого. Почнімо зі статистики.

Аналітика: *є основні показники, в них входять:* перегляди публікацій, перегляди профілю, уподобання, коментарі та поширення. Переглянути можна за 7, 28, 60, 365 (Рис. 1, 2).

Також можна подивитись джерело трафіку та пошукові записи, тобто як ваш профіль знайшли. Контент*:* перегляд топових публікацій, скільки нових глядачів за 7, 28, 60, 365 та інший період днів (Рис. 3).





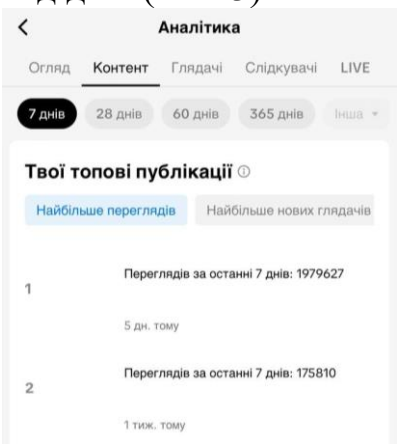


Рис. 1 Рис. 2 Рис. 3

Глядачі: у даній функції можна побачити, яка кількість глядачів, аналітика віку, статі та розташування вашої цільової аудиторії (Рис. 4). Також ми побачимо найактивніші години активності аудиторії.

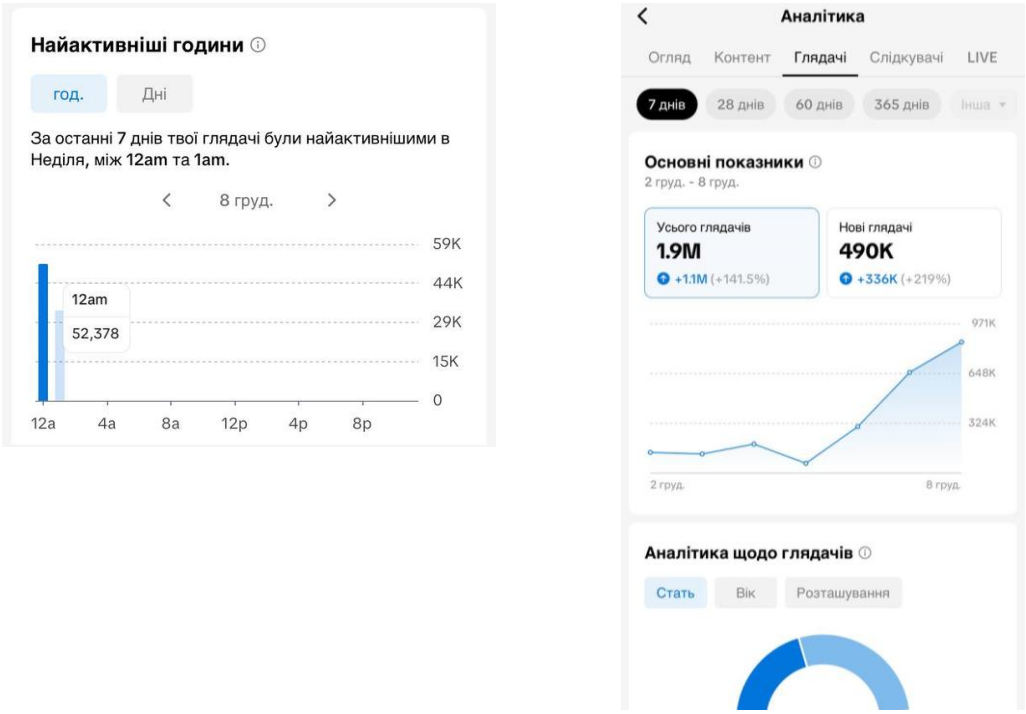


Рис. 4

Слідкувачі: скільки всього аудиторії, чистий приріст кількості, який дає можливість дізнатись накрученні підписники чи дійсно потейційні покупці (Рис. 5).

Просування: просувати можна заради переглядів відео, підписників та переглядів профілю, здійснити продажі та залучити потенційних клієнтів (Рис. 6).

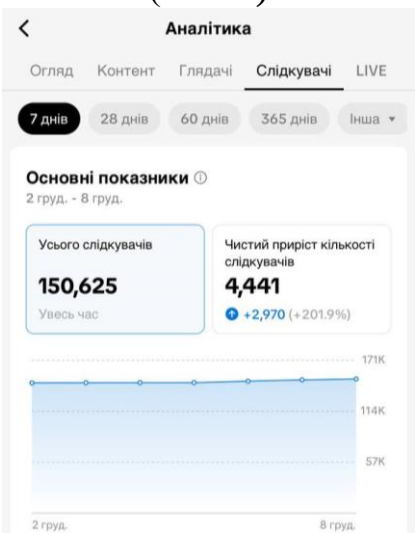


Рис. 5

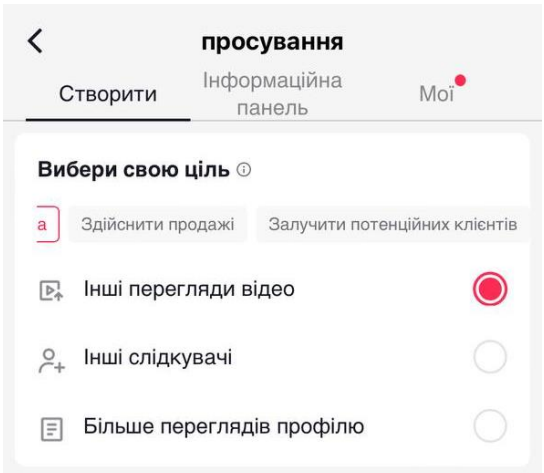


Рис. 6

Інформаційна панель: оглянути результати просування, вартість реклами, покази відео, нових слідкувачів, перегляди профілю та історію замовлень (Рис. 7).

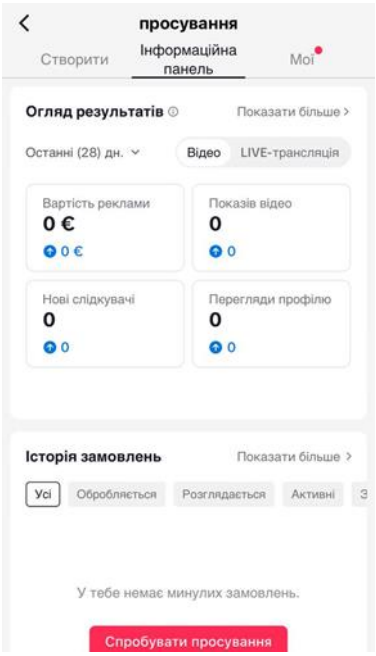


Рис. 7

Також можна безкоштовно просувати свій товар через звичайні відео, монтувати їх у програмі. Далі спробуємо порівняти переваги та недоліки, а результати представити у Таблиці 1.

Таблиця 1

Переваги	**Недоліки**
Хороший трафік	Жорсткі правила спілки
Зручний інтерфейс	Інколи обмежений вибір функціоналу інструментів
Широкий вибір інструментів	
Простий та зрозумілий інтерфейс	

TikTok – це незамінний застосунок для просування та залучення клієнтів. Він адаптований для різної аудиторії, матеріального стану. Зараз майже всі сидять в ТікТок, тому просунути свій товар набагато легше та зробити це можна різними способами.

ДЖЕРЕЛА

1. Головна TikTok [Електронний ресурс]. Режим доступу до ресурсу: https://www.tiktok.com/uk-UA/ (дата звернення 20.11.2024 р.)

2. Вікіпедія TikTok [Електронний ресурс]. Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/TikTok (дата звернення 20.11.2024 р.)

КОМПЛЕКСНИЙ ПІДХІД ДО УПРАВЛІННЯ РИЗИКАМИ В ІТ-ПРОЄКТАХ В УМОВАХ НЕВИЗНАЧЕНОСТІ

Лазебнік Ю. В., Вовк Р. Б.
Івано-Франківський національний технічний університет нафти і газу, м. Івано-Франківськ

Ефективне управління ризиками в інформаційно-технологічних проєктах передбачає врахування як потенційних негативних впливів (загроз), так і позитивних (можливостей). Успішна реалізація ІТ-проєктів вимагає високої здатності до адаптації в умовах постійної невизначеності, що набуває особливої актуальності в контексті воєнних дій, економічної нестабільності та динамічних змін ринку.

Фундаментом процесу ідентифікації ризиків слугує модель RIO-RIT-REO-RET, яка дозволяє класифікувати ризики за джерелом (внутрішні або зовнішні) та за характером впливу (загроза чи можливість). Даний підхід органічно поєднується з методикою SWOT-аналізу, що забезпечує всебічне охоплення ризикового простору проєкту. SWOT-аналіз дозволяє виявляти потенційні ризики шляхом оцінювання сильних та слабких сторін проєкту, а також аналізу зовнішніх можливостей і загроз [1]. У контексті моделі: RIO відповідає внутрішнім можливостям, RIT –внутрішнім загрозам, REO –зовнішнім можливостям, а RET –зовнішнім загрозам, що забезпечує системну і структуровану оцінку.

Оцінка ризиків здійснюється за ймовірністю їх виникнення (у діапазоні від 0 до 1) та рівнем впливу на бюджет, строки, обсяг і якість. Загальна формула для кількісної оцінки ризику представлена як добуток ймовірності на суму вагових коефіцієнтів впливу:

$$D = P \times (Vb + Vt + Vs + Vq),$$

де P –ймовірність настання події, Vb, Vt, Vs, Vq –оцінки впливу на бюджет, строки, обсяг та якість відповідно. Для ранжування ризиків використовується шкала критичності: високий (0,7–1,0), середній (0,4–0,6), низький (до 0,3). На основі отриманого ранжування ідентифікуються ризики, що потребують управлінського втручання [2].

Інтегроване управління ризиками включає формування інформаційної бази, що складається з довідкової, аналітичної та операційної частин. Це забезпечує накопичення знань, моніторинг ризиків та адаптацію моделей до специфіки конкретного ІТ-проєкту.

Профілактика ризиків передбачає реалізацію заходів на трьох рівнях: індивідуальному (для окремих завдань), груповому (для підрозділів) та загальному (на рівні всього проєкту). Такий підхід дозволяє знизити ймовірність ескалації ризиків і оптимізувати використання ресурсів.

Важливою складовою є впровадження сучасних інструментів та програмних засобів для моніторингу, ідентифікації та оцінки ризиків. Автоматизація даних процесів сприяє зниженню впливу людського фактора та підвищенню точності прогнозування. Серед типових технологічних ризиків слід виокремити інфраструктурні проблеми (відмова серверів, помилки в ПЗ, кіберзагрози), що можуть мати критичні наслідки. Їхнє своєчасне виявлення дозволяє не лише уникнути збоїв, але й спланувати модернізацію інфраструктури та впровадження інноваційних технологій з метою забезпечення стабільності функціонування проєкту.

Крім технічних та економічних аспектів, управління ризиками повинно охоплювати й управління очікуваннями зацікавлених сторін. Ігнорування цього чинника може спричинити хибну оцінку ризиків і негативно вплинути на хід реалізації проєкту. Систематична комунікація та коригування стратегій з урахуванням потреб стейкхолдерів сприяє досягненню цілей проєкту. Гнучкість управління є ключовим чинником успішної реалізації ІТ-проєктів в умовах змінного середовища, зокрема у разі економічної чи політичної турбулентності. Застосування принципів гнучких методологій сприяє адаптації до нових умов та оперативному коригуванню стратегії, що забезпечує збереження конкурентоспроможності. Людський фактор залишається важливим елементом ризик-менеджменту. Комунікаційні помилки, недостатня кваліфікація та психоемоційні навантаження можуть призводити до зростання ризиків. У зв’язку з цим доцільним є впровадження програм безперервного навчання, підвищення кваліфікації та формування культури управління ризиками в організації. Аналіз попередніх ІТ-проєктів, як успішних, так і невдалих, забезпечує цінну емпіричну базу для формування стратегій управління. Вивчення типових помилок та запозичення кращих практик дозволяє істотно знизити рівень ризиків у майбутніх проєктах.

Узагальнюючи, управління ризиками в ІТ-сфері є складним багатовимірним процесом, що вимагає застосування системного підходу, міждисциплінарних знань та сучасних технологічних рішень. Вчасна ідентифікація ризиків, математичне моделювання, використання програмного забезпечення, належна комунікація та гнучкість у прийнятті рішень є ключовими чинниками забезпечення стабільності та успіху ІТ-проєктів в умовах невизначеності.

ДЖЕРЕЛА

1. How can you use SWOT analysis to identify project risks? // LinkedIn.URL: https://surl.lu/gbnetl

2. Risk Assessment Calculation Formula // SafetySection.com. URL: https://surl.li/cbkqmb

ВИКОРИСТАННЯ СЕРВІСІВ ЗІ ШТУЧНИМ ІНТЕЛЕКТОМ ПРИ ВИКЛАДАННІ МАТЕМАТИКИ

Локазюк О. В., Сидоренко А. Б., Гнилуша М. О.
Київський столичний університет імені Бориса Грінченка, м. Київ

Сервіси зі штучним інтелектом (ШІ) дають нові можливості для покращення навчального процесу: для викладачів та вчителів проводити навчальні заняття з математики продуктивно та ефективно, а для студентів та учнів краще засвоювати навчальний матеріал. Наведемо приклади застосування: платформи Khan Academy або Sokratic автоматично підлаштовуються під рівень здобувача та дають рекомендації щодо тем, які варто повторити; Desmos або GeoGebra підтримують візуалізацію функцій і геометричних об’єктів; ChatGPT, Wolfram Alpha, Mathway – можуть генерувати та розв'язувати завдання різного рівня складності тощо.

За допомогою сервісів зі штучним інтелектом для викладача (вчителя) можна візуалізувати математичні поняття, персоналізувати навчання здобувачів, генерувати велику кількість завдань, автоматично перевіряти виконані завдання, розвивати критичне мислення учнів та студентів, підтримувати інклюзивну освіту.

Познайомимося з деякими прикладами з візуалізацією геометричного матеріалу з використанням вказаних нижче сервісів, які можуть бути ефективними при вивченні, наприклад, просторових фігур та стереометрії загалом. Дані сервіси допоможуть розвинути просторову уяву та наочно показати тяжкий для сприйняття матеріал.

Розглянемо використання ресурсу Tripo 3D (Рис. 1) на прикладі побудови правильних многогранників:

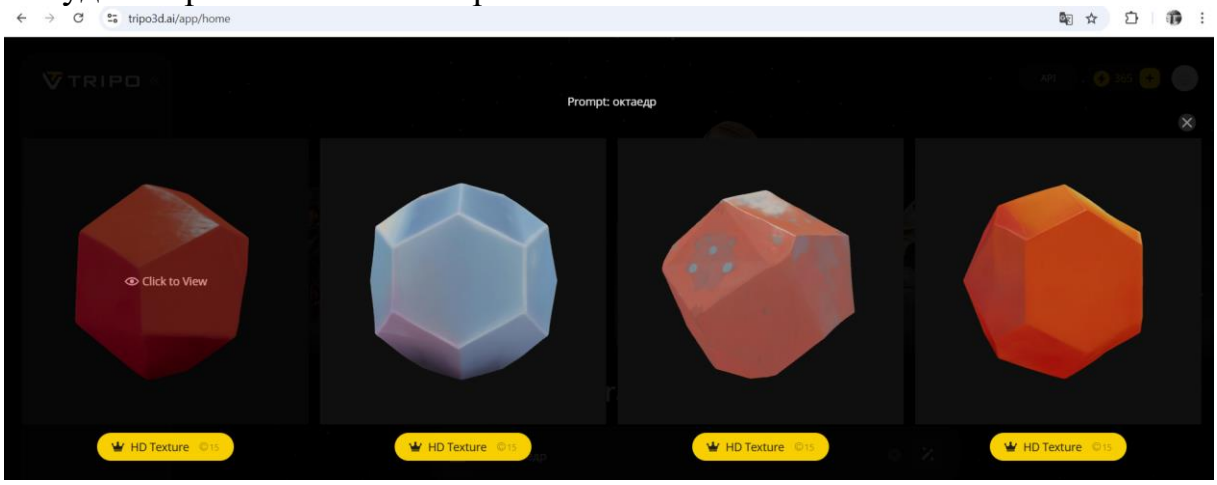


Рис. 1. Правильні многогранники. Додекаедр

Наведемо приклад побудови тетраедра за допомогою ресурсу Tripo 3D (Рис. 2):

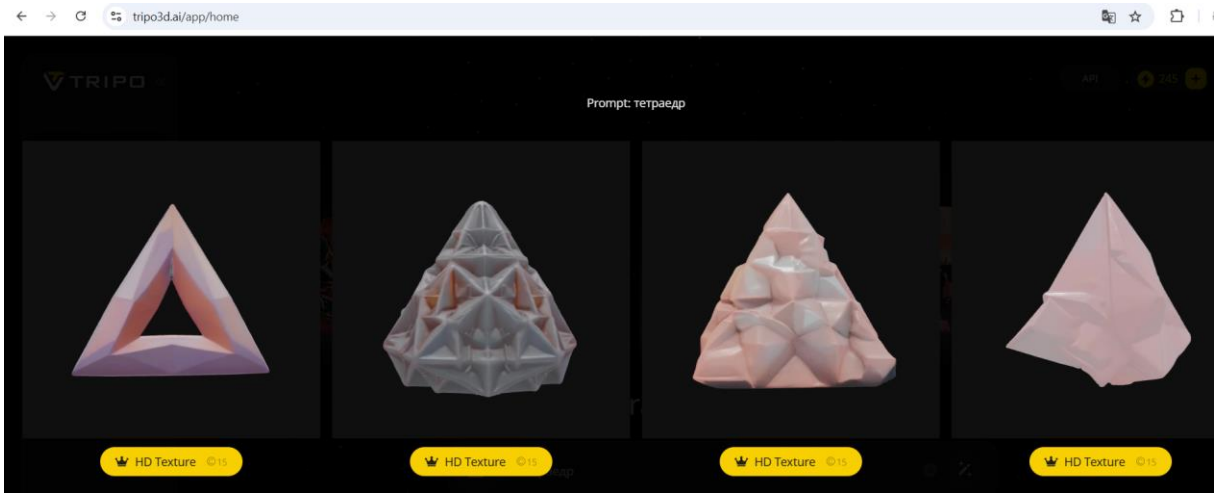


Рис. 2. Правильні многогранники. Тетраедр

Побудова многогранника за допомогою онлайн-ресурсу Assemblrworld (Рис. 3):

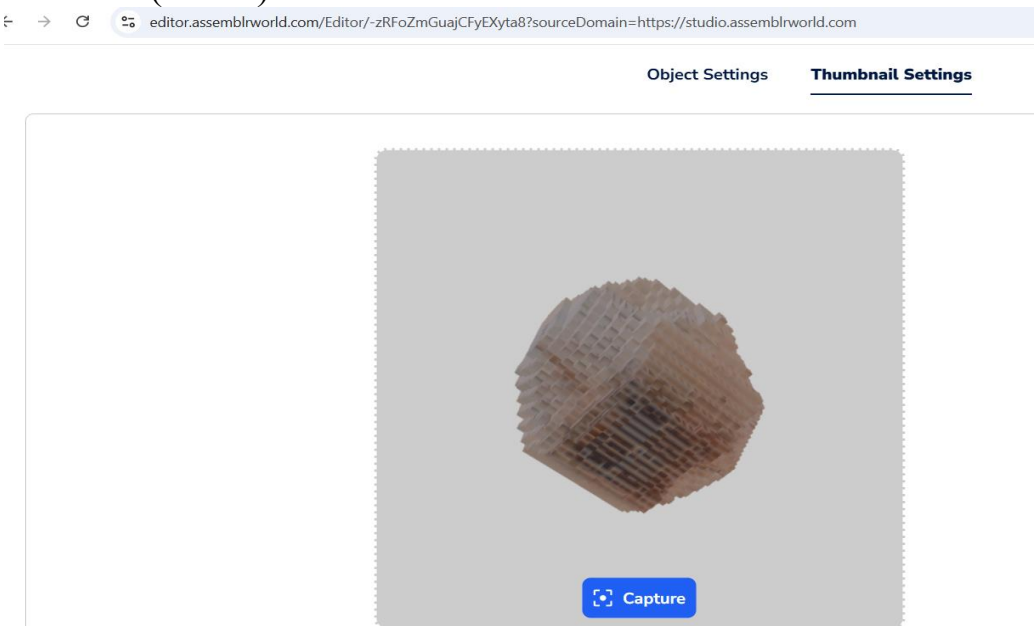


Рис. 3. Правильні многогранники

Зазначені сервіси є доступними за посиланнями нижче [1; 2]. За допомогою вказаних інструментів можна змоделювати певні ситуації та продемонструвати матеріал наочно.

Технології віртуальної реальності (VR), штучний інтелект (AI) відкривають нові можливості для навчання, сприяючи досягненню навчальних цілей завдяки унікальному поєднанню інтерактивності, візуалізації та занурення.

ДЖЕРЕЛА

1. Електронний ресурс. Tripo 3D / Режим доступу https://www.tripo3d.ai/app/home

2. Електронний ресурс. Assemblrworld / Режим доступу https://editor.assemblrworld.com

ІТЕРАЦІЙНІ МОДЕЛІ ТА БЕЗПЕРЕРВНА ІНТЕГРАЦІЯ ЯК ОСНОВА УПРАВЛІННЯ РИЗИКАМИ В ІТ-ПРОЄКТАХ

Мурава О. І., Вовк Р. Б.
Івано-Франківський національний технічний університет нафти і газу, м. Івано-Франківськ

Гнучкі методології розробки програмного забезпечення являють собою сукупність фреймворків та підходів, що орієнтовані на часті ітерації, інтенсивну комунікацію та адаптивність на всіх етапах життєвого циклу проєкту. На відміну від традиційних методів управління проєктами, які передбачають суворе дотримання заздалегідь визначеного плану, Agile-методології ґрунтуються на принципах безперервного надання цінності, інтеграції зворотного зв'язку та адаптації до змін [1].

У сфері управління ІТ-проєктами часто виникають виклики, пов'язані з невизначеністю вимог, затримками у розробці, неефективною комунікацією між командами та високими ризиками невдачі. Традиційні методи управління не завжди забезпечують достатній рівень адаптивності для врахування динамічних змін ринку та технологічного середовища. Застосування гнучких підходів, таких як Agile, Scrum та Kanban, сприяє ефективному управлінню ризиками, покращенню командної взаємодії та забезпеченню стабільності процесу розробки.

Одним із ключових аспектів управління ризиками в ІТ-проєктах є застосування ітераційного підходу (Iterative Model) та адаптивного планування. Невизначеність вимог і можливість їхніх змін на різних етапах розробки є типовими проблемами, з якими стикаються команди. Використання Agile-методологій дозволяє забезпечити поступову реалізацію проєкту, мінімізуючи потенційні ризики та підвищуючи рівень гнучкості. Зокрема, Scrum передбачає структурований підхід до управління проєктами, що базується на розподілі роботи на короткі ітерації (спринти), які тривають від одного до чотирьох тижнів і завершуються створенням конкретного функціонального інкременту продукту [2].

Такий підхід дає змогу оперативно реагувати на зміну вимог замовника, уникати значних фінансових та часових витрат, що можуть виникнути через помилки на пізніх стадіях розробки, а також поступово вдосконалювати кінцевий продукт відповідно до актуальних потреб користувачів.

Однією з ключових причин неуспішності ІТ-проєктів є недостатня взаємодія між учасниками команди, відсутність регулярного обміну інформацією та несвоєчасне виявлення проблемних аспектів розробки. Гнучкі методології передбачають систематичне обговорення процесів і результатів роботи, що сприяє підвищенню прозорості та оперативному реагуванню на виклики проєкту. Зокрема, ефективна комунікація

забезпечується через такі механізми: щоденні стендапи (Daily Stand-ups), огляди спринтів (Sprint Review) та ретроспективи (Sprint Retrospective).

Впровадження цих практик сприяє підвищенню ефективності командної роботи, мінімізації ризиків, пов'язаних із несвоєчасним виявленням проблем, та забезпеченню високої адаптивності процесу розробки. Ще одним важливим аспектом управління ризиками є визначення пріоритетності завдань у процесі розробки програмного забезпечення. У межах гнучких методологій застосовується концепція мінімально життєздатного продукту (Minimum Viable Product, MVP), що передбачає створення базової версії продукту з критично необхідним функціоналом для початкового тестування гіпотез. Основна мета MVP – забезпечити швидкий вихід на ринок, отримати первинний зворотний зв'язок від користувачів та здійснити необхідні коригування перед масштабуванням [3].

Для ефективного визначення пріоритетів застосовуються різні методи, зокрема: MoSCoW (Must-have, Should-have, Could-have, Won't-have) та Kano Model. Застосування цих підходів дозволяє командам зосередитися на реалізації найбільш значущих функцій, уникати зайвих витрат ресурсів та своєчасно адаптувати продукт відповідно до вимог користувачів.

Окремим джерелом ризиків у процесі розробки є технічні помилки, які можуть накопичуватися через недостатнє тестування та несвоєчасну інтеграцію змін. Для їх мінімізації широко застосовується підхід безперервної інтеграції (Continuous Integration, CI) та безперервного розгортання (Continuous Deployment, CD), що дозволяє автоматизувати процеси тестування, компіляції та впровадження змін у виробниче середовище [4].

Отже, дослідження засвідчують, що застосування гнучких методологій управління розробкою програмного забезпечення (Agile, Scrum) сприяє ефективному зниженню ризиків в IT-проєктах, забезпечуючи адаптивність до змін, прозорість процесів та зменшення невизначеності. Автоматизація CI/CD, моніторинг і аналіз ризиків дозволяють своєчасно ідентифікувати проблеми та оперативно впроваджувати коригувальні заходи. Ітераційний підхід та механізми зворотного зв'язку мінімізують фінансові та часові витрати, підвищуючи ефективність управління проєктами та забезпечуючи стабільний розвиток програмного продукту.

ДЖЕРЕЛА

1. Що таке гнучкі методології? URL: https://surl.li/hixeft

2. Що таке Scrum? URL: https://surl.li/zofkdi

3. Розробка MVP: Як швидко перевірити ідею та мінімізувати ризики? URL: https://surl.li/gspmtb

4. Що таке безперервна інтеграція та безперервна доставка? URL: https://surl.li/afwclb

РОЛЬ СИСТЕМ УПРАВЛІННЯ ПРОЄКТАМИ У ТРАНСФОРМАЦІЇ ОСВІТНЬОГО ПРОЦЕСУ

Онищук В. І., Вовк Р. Б.
Івано-Франківський національний технічний університет нафти і газу, м. Івано-Франківськ

Системи управління проєктами (Project Management Systems, PMS) набули широкого розповсюдження в корпоративному середовищі, зокрема у сфері бізнесу та інформаційних технологій. Останніми роками спостерігається зростання інтересу до використання таких інструментів в освітньому процесі, що зумовлено потребою у підвищенні ефективності організації навчання, розвитку командної роботи та формуванні професійних навичок здобувачів освіти.

У контексті цифровізації освіти впровадження сучасних інформаційних технологій сприяє вдосконаленню якості навчального процесу. Одним із перспективних напрямів такого вдосконалення є інтеграція систем управління проєктами, які широко використовуються в IT-компаніях та інших організаціях, у практику освітньої діяльності. Застосування PMS у навчанні забезпечує підвищення організованості, дисципліни та розвиток навичок проєктного менеджменту, які є затребуваними на сучасному ринку праці.

Системи управління проєктами надають широкі функціональні можливості для планування, делегування та контролю виконання завдань у команді. До найпоширеніших платформ належать Trello, Jira, Asana, YouTrack, Microsoft Project тощо. Ці системи забезпечують можливість розподілу завдань, встановлення термінів їх виконання, структурування задач шляхом декомпозиції, моніторингу прогресу та підтримки комунікації між учасниками проєкту.

У контексті освітнього середовища PMS можуть бути ефективно використані для реалізації навчальних проєктів, написання курсових і дипломних робіт, організації командної взаємодії в межах лабораторних завдань та групових проєктів. Також можливе застосування PMS для особистого планування навчальної діяльності студентів, а також для оптимізації роботи викладачів у процесі підготовки та реалізації навчальних програм.

Основні переваги впровадження систем управління проєктами в освітній процес полягають у наступному:

- Підтримка командної роботи: PMS забезпечують структуровану взаємодію між учасниками освітнього процесу,

оптимізуючи розподіл обов'язків та контроль за дотриманням термінів виконання завдань.

- Розвиток навичок управління проєктами: використання таких систем сприяє формуванню у студентів компетентностей, пов'язаних із плануванням, організацією та реалізацією проєктної діяльності.
- Підвищення прозорості контролю: викладачі отримують змогу оперативно відслідковувати прогрес виконання завдань, здійснювати оцінювання та надавати зворотний зв'язок.
- Гнучкість та доступність: більшість систем управління проєктами мають веб-інтерфейси та мобільні додатки, що дозволяє працювати з будь-якого пристрою та в будь-який час.

Сучасні платформи дистанційного навчання, зокрема Moodle, Google Classroom та Microsoft Teams, частково підтримують інтеграцію з PMS, що відкриває нові можливості для автоматизації управління освітнім процесом. Така інтеграція дозволяє об'єднати навчальні ресурси, завдання та систему оцінювання в єдиний цифровий простір.

Разом з тим, ефективність впровадження систем управління проєктами залежить від низки чинників, серед яких – правильний вибір платформи та методології її використання. Наприклад, Trello відзначається простим інтерфейсом і зручністю для широкого кола користувачів, у той час як Jira є доцільною для викладання технічних дисциплін та впровадження гнучких підходів (Agile, Scrum). Практика використання PMS у провідних університетах підтверджує їхню ефективність у формуванні проєктного мислення у студентів. Водночас існують певні виклики, що супроводжують інтеграцію PMS у навчальний процес. До них належить потреба у попередньому навчанні як здобувачів, так і викладачів, що може ускладнити початкові етапи впровадження. Крім того, обмеженість технічних ресурсів та недостатня мотивація окремих викладачів або освітніх установ можуть стати перешкодою для повноцінної реалізації проєктного підходу. Також слід враховувати, що не всі навчальні дисципліни передбачають проєктну чи командну діяльність, отже використання PMS доцільне лише в певних умовах.

Отже, інтеграція систем управління проєктами в освітній процес сприяє підвищенню ефективності навчання, активізації взаємодії між учасниками освітнього середовища та розвитку професійних компетентностей у студентів. Поєднання PMS із системами дистанційного навчання створює нові умови для оптимізації організації освітнього процесу, забезпечуючи його відповідність сучасним вимогам цифрової економіки.

ДЖЕРЕЛА

1. Сазерленд Д. Scrum. Навчись робити вдвічі більше за менший час. Харків : КСД, 2016. 280 с.

2. Agile Project Management Course (Google) | Coursera . – [Електронний ресурс]. – Режим доступу: https://surl.li/gdgbjc

ПЕДАГОГІЧНІ AI АГЕНТИ: ПРОЕКТУВАННЯ ТА ІМПЛЕМЕНТАЦІЯ

Остапенко Д. А.
Київський столичний університет імені Бориса Грінченка

Активне впровадження цифрових рішень у сфері освіти та прогрес у штучному інтелекті сприяють появі інноваційних підходів до навчання, орієнтованих на індивідуальні потреби студентів, в якому ключову роль починають відігравати педагогічні AI агенти (англ. *Pedagogical AI Agents*). Вони функціонують як віртуальні наставники, що здатні не лише подавати навчальний матеріал, а й адаптувати його до індивідуальних потреб здобувача освіти, надавати рекомендації, аналізувати прогрес і забезпечувати зворотний зв’язок [1].

Основні принципи проектування педагогічних AI агентів

Створення педагогічного агента зі штучним інтелектом базується на інтеграції знань із когнітивної психології, теорії навчання, інформаційних технологій та принципів етичної взаємодії між людиною й машиною [2; 3]. До ключових частин освітнього агента належать системи персоналізації знань, модулі предметної інформації, педагогічні алгоритми та зручні інтерфейси для взаємодії зі здобувачами освіти:

- Модель учня (student model): база знань про індивідуальні особливості, стиль навчання, рівень підготовки [1, с. 137];
- Модель знань (domain model): структура предметного матеріалу;
- Педагогічна стратегія (pedagogical model): правила та алгоритми подання матеріалу і взаємодії [3];
- Інтерфейс користувача (UI/UX): канал комунікації зі студентом (текстовий, голосовий, візуальний) [2, с. 14–15].

Архітектура агентів часто реалізується на базі когнітивних фреймворків (наприклад, Open Learner Model, Bayesian Knowledge Tracing), а для реалізації взаємодії використовуються мовні моделі (GPT, BERT) та нейронні мережі [1–3].

Імплементація та виклики

У процесі впровадження AI агентів у навчальний процес постають наступні виклики:

1. Якість навчальних даних. AI агент залежить від точності та обсягу даних щодо навчального матеріалу та користувача [4].
2. Персоналізація. Адаптація до рівня, стилю і темпу навчання кожного студента потребує гнучких алгоритмів і складних моделей [3].

3. Безпека та етика. Надання рекомендацій і збору даних має ґрунтуватися на прозорих, етично виправданих підходах [5].

4. Оцінювання ефективності. Необхідне створення методик оцінювання впливу AI агентів на навчальні результати [2; 4].

У межах експериментальної платформи буде реалізовано прототип AI агента, який проводить діагностику знань у вигляді діалогу та генерує індивідуальні завдання. Агента буде протестовано у середовищі Moodle із використанням API-інтеграції з мовною моделлю GPT-4 [3, с. 23–24]. Результати попереднього тестування свідчать про зростання зацікавленості студентів та підвищення успішності на 12–15 % [4].

Педагогічні AI агенти мають значний потенціал для трансформації освітнього процесу. AI агенти демонструють значний потенціал у підвищенні ефективності освіти завдяки гнучкості, автоматизації та індивідуальному підходу до навчання [1; 2; 5]. Подальші дослідження зосереджені на покращенні моделей адаптації, забезпеченні етичної взаємодії та розробці відкритих платформ для інтеграції ШІ агентів у систему освіти.

ДЖЕРЕЛА

1. Woolf B. P. Building Intelligent Interactive Tutors: Student-Centered Strategies for Revolutionizing E-Learning. Burlington : Morgan Kaufmann, 2009. 381 p.

2. Holmes W., Bialik M., Fadel C. Artificial Intelligence in Education: Promises and Implications for Teaching and Learning. Boston : Center for Curriculum Redesign, 2019. 56 p.

3. Luckin R., Holmes W., Griffiths M., Forcier L. B. Intelligence Unleashed: An Argument for AI in Education. London : Pearson Education, 2016. 48 p.

4. Aleven V., McLaughlin E. A., Koedinger K. R. Toward meta-adaptive tutors: A new approach to improving adaptive learning technology // *International Journal of Artificial Intelligence in Education*. 2017. Vol. 27(1). P. 146–179.

5. Kunda M. Teaching Artificial Intelligence to Think Like a Student: Implications for Cognitive Modeling // *AI Magazine*. 2020. Vol. 41(2). P. 12–24.

ІНТЕГРОВАНА ІНФОРМАЦІЙНА ПЛАТФОРМА ДЛЯ СПОРТСМЕНІВ І ТРЕНЕРІВ

Писарєв В. Д.

Київський столичний університет імені Бориса Грінченка, м. Київ

У сучасному спортивному середовищі зростає потреба в ефективному управлінні тренувальним процесом, моніторингу результатів

спортсменів і організації змагань. Рішенням цієї проблеми можуть стати інтегровані цифрові платформи, що об'єднують ці функції в єдиному середовищі. З огляду на вимоги до безпеки даних та прозорості процесів, використання блокчейн технології стає важливим для досягнення необхідного рівня захисту інформації та забезпечення довіри до результатів. Блокчейн дозволяє забезпечити незмінність та прозорість записів, що є критично важливим для спортивних досягнень, результатів змагань та тренувальних процесів.

Застосування блокчейн технологій у спортивних інформаційних системах вимагає вирішення кількох важливих задач. По-перше, необхідно розробити систему, яка дозволить динамічно і безпечно обробляти спортивні дані та результати змагань у реальному часі. По-друге, важливо створити алгоритми для інтеграції цієї технології в існуючі процеси моніторингу та організації спортивних змагань, що дозволить мінімізувати вплив людського фактору та покращити управлінську ефективність. Метою цієї роботи є розробка моделі інтегрованої платформи для спортсменів та тренерів з використанням блокчейн технологій, що забезпечить ефективну обробку даних, автоматизацію процесів та підвищення прозорості та безпеки.

Для реалізації запропонованої платформи буде використано принципи децентралізації даних, що забезпечить їх безпеку та доступність для всіх учасників (спортсменів, тренерів, організаторів змагань). Кожен результат тренування або змагання буде фіксуватися в блокчейн реєстрі, що дозволить отримати незмінну інформацію про спортивні досягнення спортсменів та результати змагань. Окрім цього, платформа автоматизує процеси реєстрації спортсменів, організації змагань, формування тренувальних планів і розрахунку результатів, що зменшить навантаження на адміністраторів і підвищить ефективність роботи спортивних організацій.

Процес створення цієї платформи передбачає кілька етапів:

1. Аналіз існуючих рішень: Оцінка поточних цифрових платформ, що використовуються для управління спортивною діяльністю, та визначення недоліків, які можуть бути виправлені за допомогою блокчейн технологій.

2. Розробка архітектури системи: Визначення ключових компонентів платформи, таких як інтерфейси для користувачів, бази даних для зберігання результатів та механізми інтеграції з існуючими спортивними платформами.

3. Розробка алгоритмів для обробки даних: Створення ефективних алгоритмів, що забезпечать автоматичне внесення результатів у блокчейн, їх обробку, збереження та доступ до них.

4. Інтеграція блокчейн технології: Впровадження протоколів блокчейн для забезпечення незмінності даних, захисту від

несанкціонованого доступу та забезпечення їх прозорості для усіх учасників.

5. Прототипування та тестування: Створення прототипу платформи та його тестування на контрольній групі користувачів для оцінки ефективності системи та можливих шляхів для покращення.

Для розв'язання проблеми планування і обробки спортивних даних, буде застосовано блокчейн як основний метод для зберігання та верифікації результатів. Завдяки дистрибуційній природі блокчейн технології, дані будуть зберігатися в кількох вузлах, що забезпечить їх захист та доступність для користувачів без потреби в централізованих серверах. Крім того, алгоритми для обробки даних будуть забезпечувати швидке і ефективне збереження результатів та доступ до них у реальному часі. Для реалізації цієї системи використовуватиметься мова програмування Python для розробки інтерфейсів користувачів, реалізації алгоритмів обробки даних та інтеграції з блокчейн платформами.

Перші етапи експерименту передбачають тестування платформи на обмежених обсягах даних (20 спортсменів, 30 тренерів), щоб оцінити ефективність роботи системи. Далі обсяги будуть збільшуватися до 50 спортсменів та 100 тренерів, 100 спортсменів та 200 тренерів для перевірки стабільності і масштабованості системи.

Запропонована інтегрована платформа з використанням блокчейн технології дозволить досягти високої ефективності в управлінні спортивною діяльністю, забезпечить безпеку даних та дозволить забезпечити прозорість результатів змагань і тренувань. Застосування блокчейн допоможе зменшити ризики фальсифікацій, підвищити довіру до результатів і забезпечити автоматизацію процесів. Розробка ефективного рішення для таких платформ сприятиме розвитку спортивної індустрії та підвищенню якості управління тренувальними процесами.

ДЖЕРЕЛА

1. He N. Blockchain Use Cases in the Sports Industry: A Systematic Review // *International Journal of Networked and Distributed Computing*. 2024. Vol. 12. C. 17–40. URL: https://link.springer.com/article/10.1007/s44227-024-00022-3

2. Demirci N. The Future of Blockchain Technology in the Sports Industry // *Journal of Sports Industry & Blockchain Technology*. 2024. DOI: 10.5281/zenodo.12599715.

ВИКОРИСТАННЯ WOLFRAM|ALPHA В ПОЄДНАННІ З GOOGLE DOCUMENTS У НАВЧАЛЬНОМУ ПРОЦЕСІ

Пономаренко С., Малюк С., Жирнов Д., Супрун А., Бодненко Д.
Київський столичний університет імені Бориса Грінченка, м. Київ

Хмарні сервіси забезпечують доступ до даних через Інтернет. Основні категорії:

- IaaS: обчислювальні ресурси.
- PaaS: платформи для розробки.
- SaaS: готове програмне забезпечення.
- DevOps: автоматизація та моніторинг етапів розробки ПЗ.

Переваги хмарних сервісів: доступність, економія витрат, гнучкість і масштабованість, автоматизація процесів, швидкість інтегрування, спільна робота.

Wolfram|Alpha – це потужна система, що дозволяє розв'язувати математичні задачі, аналізувати дані та надавати відповіді на запити завдяки інтеграції алгоритмів і великої бази знань. Вона підтримує обробку природної мови (поки що тільки англійська мова), візуалізацію результатів та покрокові рішення, що робить її ефективним інструментом для навчання та досліджень.

Історія Wolfram|Alpha

- Mathematica (1987) – основа для Wolfram|Alpha.
- Wolfram|Alpha (2009): система, що обчислює відповіді на основі бази знань і алгоритмів.
- Постійна інтеграція нових джерел даних та алгоритмів.

Переваги Wolfram|Alpha:

- Обробка природної мови для запитів.
- Показ покрокового рішення..
- Широкий спектр тем: математика, фізика, статистика тощо.
- Візуалізація даних (графіки, діаграми).
- Доступ до даних в реальному часі.
- Інтеграція з платформами через API.
- Доступ до базових функцій безкоштовний.
- Pro функціонал

Недоліки Wolfram|Alpha:

- Обмеження безкоштовної версії.
- Залежність від Інтернету.
- Можливі помилки через некоректні запити.
- Обмежена підтримка мов.
- Складність інтеграції.

Wolfram|Alpha + Google Documents

- Google Documents – хмарний текстовий редактор із підтримкою розширень, включаючи Auto-LaTeX Equations.

- LaTeX – інструмент для високоякісного оформлення документів.
- Переваги Auto-LaTeX Equations:

Відтворення формул.

Автоматичне підбирання розмірів і кольорів.

Можливість редагування формул.

Хмарні сервіси змінюють підхід до роботи в математиці, забезпечуючи ефективність, доступність і якісне оформлення. Використання Wolfram|Alpha у поєднанні з Google Documents стимулює розвиток аналітичного мислення, дозволяє автоматизувати обчислення та підвищує якість освіти.

ДЖЕРЕЛА

1. Кіяновська, Н. М., & Зіонос, Н. О. (2024). Використання систем комп'ютерної математики на заняттях вищої математики в технічних університетах. І-57 Інноваційні практики наукової освіти: матеріали IV Всеукраїнської, 384

2. Lyubchyk, O., & Kryvenko, I. (2024). Використання сервісів google на заняттях з дисципліни «Медична Інформатика» для студентів з поглибленим вивченням англійської мови. Continuing Professional Education: Theory and Practice, 80(3), 84-102.

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ВИЗНАЧЕННЯ РИТМУ СЕРЦЕБИТТЯ

Присяжнюк В. В., Романюк О. Н.

Вінницький національний технічний університет, м. Вінниця

Принципи роботи штучного інтелекту для визначення серцебиття базуються на аналізі неявних змін кольору шкіри обличчя, які викликані коливаннями кровонаповнення під час серцевих скорочень. Ці зміни настільки малі, що їх складно вловити людським оком, проте вони можуть бути зафіксовані звичайною камерою [1]. Штучний інтелект, зокрема нейронні мережі, здатен навчитися розпізнавати ці слабкі сигнали на основі великої кількості відеозаписів, що містять обличчя людей та відповідні мітки частоти серцебиття.

Робота таких систем зазвичай починається з попередньої обробки відео, де з кадрів автоматично виділяється ділянка обличчя, а також визначаються ключові зони шкіри, які найкраще передають пульсації – наприклад, лоб або щоки. Далі ці області аналізуються покадрово для побудови часових рядів зміни кольору або яскравості пікселів. Ці ряди є вхідними даними для моделей машинного навчання, які далі обробляють інформацію та виокремлюють з неї характерний ритм пульсу.

Навчання таких моделей відбувається на заздалегідь підготовлених датасетах, де для кожного відео точно відомі реальні значення серцебиття (отримані, наприклад, за допомогою контактного пульсоміра). Під час навчання нейронна мережа поступово навчається співвідносити зміни у відео з відповідними значеннями пульсу. Після завершення навчання модель може обробляти нові відео й визначати серцебиття в режимі реального часу.

Отже, принцип роботи штучного інтелекту для визначення серцебиття полягає у перетворенні візуального сигналу в біофізіологічну інформацію завдяки глибокому аналізу даних, автоматичному виділенню ознак та здатності адаптуватися до умов реального середовища. Це робить такі системи перспективними для створення точних, зручних і повністю безконтактних методів [2] моніторингу здоров’я.

Штучний інтелект активно впроваджується в різні галузі, де необхідний безконтактний, зручний та точний моніторинг серцебиття. Однією з ключових сфер застосування є :

1) Медицина – зокрема для дистанційного нагляду за пацієнтами, раннього виявлення серцевих патологій, а також у реанімаційних відділеннях, де важливий постійний контроль життєвих показників без прямого контакту з пацієнтом. ШІ-системи здатні працювати у фоновому режимі, автоматично фіксуючи відхилення пульсу або ритму.

2) Телемедицина – завдяки камерам у смартфонах, ноутбуках чи інших пристроях пацієнти можуть передавати свої біосигнали лікарям без необхідності фізичного візиту. Це особливо актуально в умовах віддалених районів або для людей з обмеженою мобільністю.

3) Фітнес і спорт – ще одна популярна сфера, де ШІ допомагає вимірювати пульс під час тренувань без носіння спеціальних пристроїв. Це дозволяє створювати персоналізовані тренувальні плани, відслідковувати навантаження і контролювати відновлення організму [3].

4) Психофізіології і емоційного моніторингу визначення пульсу застосовується для оцінки рівня стресу, збудження чи тривоги. Це використовується у дослідженнях взаємодії людини з комп’ютером, у навчальних системах або навіть у маркетингу – для вивчення реакцій споживачів на різні стимули.

5) Системи безпеки та спостереження –де на основі біометричних параметрів можна ідентифікувати людину, виявляти її стан (наприклад, втому чи знерухомлення) або оперативно реагувати на потенційні загрози[4].

6) Розумний транспорт – системи в автомобілях, які аналізують стан водія за допомогою камери, здатні виявити ознаки сонливості або серцевих проблем під час руху та активувати захисні функції авто.

Отже, використання штучного інтелекту для визначення серцебиття є універсальним і багатогранним рішенням, яке охоплює як охорону

здоров’я, так і інші галузі, де важливо мати доступ до точного, зручного та безконтактного моніторингу фізіологічного стану людини.

ДЖЕРЕЛА

1. W. Wang, A. C. den Brinker, S. Stuijk, and G. de Haan, «Algorithmic principles of remote PPG,» *IEEE Transactions on Biomedical Engineering*, vol. 64, no. 7, pp. 1479–1491, Jul. 2017.

2. M. Chen and A. P. Sarwal, «DeepPhys: Video-Based Physiological Measurement Using Convolutional Attention Networks,» in *Proceedings of the European Conference on Computer Vision (ECCV)*, Munich, Germany, 2018, pp. 356–373.

3. D. McDuff, S. Gontarek, and R. W. Picard, «Remote measurement of cognitive stress via heart rate variability,» in *Proceedings of the 36th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, Chicago, IL, USA, 2014, pp. 2957–2960.

4. Z. Zhang, «Photoplethysmography-Based Heart Rate Monitoring in Physical Activities via Joint Sparse Spectrum Reconstruction,» *IEEE Transactions on Biomedical Engineering*, vol. 62, no. 8, pp. 1902–1910, Aug. 2015.

ФУНКЦІОНАЛЬНІ МОЖЛИВОСТІ ДОДАТКУ ADOBE PHOTOSHOP В ПРОФЕСІЙНІЙ ДІЯЛЬНОСТІ РЕКЛАМІСТА

Пукаленко Ю. О.

Київський столичний університет імені Бориса Грінченка, м. Київ

Вступ. Кожного дня ми бачимо рекламні банери, буклети, постери та інші види рекламних оголошень, йдучи до школи, на роботу чи відпочинок з друзями. Велика їх кількість розміщена в метро чи автобусах. Це все – результат роботи рекламістів. Їх основна мета – залучити якнайбільшу кількість аудиторії через яскраву рекламу, що легко запам’ятовується.

Розвиток графіки протягом останнього десятиліття зазнав значних змін, і одним із ключових чинників цього процесу стало широке використання різноманітних технологічних можливостей. Зокрема використання різних графічних редакторів, найпопулярнішим з яких є **Adobe Photoshop**.

Adobe Photoshop – це програмне забезпечення для створення цифрових зображень і дизайну, яке дозволяє перетворювати фотографії, графіку та ілюстрації у високоякісний власний вміст. Можна редагувати та створювати за допомогою шарів, пензлів, інструментів штучного інтелекту на основі найновішої моделі Adobe Firefly Image [1].

Цільова аудиторія. Переважно молодь віком від 18-35 років. Вікове обмеження - 4+ (від розробника). Основні користувачі – фотографи,

графічні дизайнери, аніматори, монтажери; використовують для роботи в галузях виробництва, медицини, архітектури, при проведенні наукових досліджень [2].

Можливості для реклами. В *Adobe Photoshop* можна редагувати та створювати рекламні банери, оголошення, буклети та інший цифровий контент. Його використовують для оформлення веб-сторінок, що допомагає залучити аудиторію до продукту, забезпечує віртуальну комунікацію. З допомогою нього можна виправляти недоліки зображення, створювати колажі, змінювати кольори, додавати ефекти і працювати з шарами для досягнення виразності зображення.

Серед головних переваг та недоліків сервісу Adobe Photoshop варто відмітити основні, які представлено у таблиці 1:

Таблиця 1

Переваги та недоліки сервісу Adobe Photoshop

Переваги	**Недоліки**
Стабільний та надійність	Потребує багато оперативної та дискової пам’яті
Універсальний	Можливий повільний запуск програми
Адекватна кольоропередача	Платна підписка
Простий та зрозумілий інтерфейс	Складність навчання і освоєння програми
Широкий вибір інструментів	

Photoshop став незамінним інструментом у багатьох сучасних професіях. З роками ця програма розвивалася і тепер доступна не лише професійним дизайнерам і розробникам, а й стане в нагоді навіть новим користувачам. В наш час оволодіння базовими знаннями графічного редагування є важливим для професіоналів у всіх галузях.

ДЖЕРЕЛА

1. Головна Adobe - Adobe Photoshop [Електронний ресурс] - Режим доступу до ресурсу: https://www.adobe.com/apps/all/all-platforms/pdp/photoshop?source=apps (дата звернення 18.10.2024)

2. Вікіпедія Adobe Photoshop [Електронний ресурс] - Режим доступу до ресурсу: https://uk.m.wikipedia.org/wiki/Adobe_Photoshop (дата звернення 18.10.2024)

ПІДБІР ПУБЛІКАЦІЙ З ВИКОРИСТАННЯМ CONTENT-BASED ТА COLLABORATIVE-BASED ФІЛЬТРАЦІЇ

Радківська А. В., Савіцький Р. С.
Державний університет «Житомирська політехніка», м. Житомир

У сучасних інформаційних системах персоналізовані рекомендації відіграють ключову роль у покращенні користувацького досвіду та підвищенні залученості аудиторії. Вибір відповідного методу підбору рекомендацій значною мірою залежить від характеру даних, доступних у базі, та вимог до ефективності обробки інформації. PostgreSQL як одна з найпопулярніших реляційних систем керування базами даних, пропонує широкий набір засобів для реалізації рекомендаційних алгоритмів. Серед них особливого значення набувають контентно-орієнтовані та колаборативні методи, які використовують різні принципи обробки та зберігання даних для формування релевантних пропозицій.

Content-based фільтрація працює з характеристиками самих публікацій. У базі даних зберігається текстовий вміст, теги, категорії, а також метаінформація, яку можна використовувати для пошуку схожих записів [1]. PostgreSQL дозволяє ефективно реалізовувати цей метод за допомогою повнотекстового пошуку через tsvector, а також порівняння наборів тегів та інших метаданих публікацій, що аналізуються. Основна ідея – аналіз уже оцінених або переглянутих користувачем публікацій і пошук нових на основі спільних ознак. Однією з головних переваг є автономність підходу, що працює без потреби в даних про інших користувачів, оскільки ґрунтується на характеристиках контенту, що дозволяє рекомендувати публікації на основі їх змісту. Фільтрування засноване на взаємодії з контентом робить систему ефективною для нових користувачів або публікацій, оскільки не потребує взаємодії з іншими користувачами. Крім того, рекомендації, що ґрунтуються на content-based filtering, зазвичай досить точно задовольняють інтереси користувача завдяки добре категоризованому контенті. Однак, мінусом є проблема обмеженого різноманіття рекомендацій. Що не дозволяє користувачеві розширити своє коло споживаного контенту.

Collaborative filtering, навпаки, фокусується на аналізі взаємодій користувачів. База містить історію переглядів, лайків або оцінок, які формують зв’язки між користувачами та контентом [2]. PostgreSQL використовується для збереження зв’язків у вигляді реляційних таблиць, а пошук схожих користувачів або публікацій здійснюється через агрегацію даних та обчислення подібності (наприклад, через косинусне схожість або кореляцію). Метод не враховує вміст самих публікацій, але дозволяє знаходити популярний або персоналізований контент на основі поведінки схожих користувачів. Це дозволяє знаходити нові публікації, що можуть бути цікавими користувачу, навіть якщо вони не були безпосередньо схожі

на ті, які він раніше переглядав. Колаборативний фільтр також не потребує детальної категоризації контенту, що знижує потребу в складних метаданих [3]. Однак цей підхід має свої мінуси, зокрема проблему «холодного старту», коли нові користувачі або нові публікації не мають достатньо взаємодій для коректного формування рекомендацій [4].

Основна різниця між підходами полягає у джерелі даних для рекомендацій: контентний аналізує властивості самих публікацій, тоді як колаборативний – взаємодії користувачів між собою та з контентом. Обидва підходи мають свої переваги та обмеження, тому на практиці нерідко застосовуються гібридні методи, що поєднують контентно-орієнтоване та колаборативне фільтрування для підвищення точності та різноманітності рекомендацій. Використання PostgreSQL у цьому контексті забезпечує гнучкість та ефективність, дозволяючи реалізовувати складні алгоритми аналізу даних та формування персоналізованих пропозицій.

ДЖЕРЕЛА

1. Pazzani M. J., Billsus D. Content-Based Recommendation Systems // The Adaptive Web: Methods and Strategies of Web Personalization. Springer, 2007.
2. Collaborative Filtering // Encyclopedia of Machine Learning and Data Mining. Springer, 2017.
3. Sarwat M., Mokbel M. Collaborative Filtering // Encyclopedia of Database Systems. Springer, 2018.
4. Evelyn Eve. Collaborative filtering in recommender system: an overview [Електронний ресурс]. Medium, н.д. Режим доступу: https://medium.com/@evelyn.eve.9512/collaborative-filtering-in-recommender-system-an-overview-38dfa8462b61.

РОЗРОБКА СМАРТ-КОНТРАКТІВ ДЛЯ АВТОМАТИЗАЦІЇ БІЗНЕС-ПРОЦЕСІВ

Радука О. О.
Київський столичний університет імені Бориса Грінченка, м. Київ

Цифровізація стрімко розвивається, а смарт-контракти стали важливим інструментом цифрової трансформації. Аналіз сучасного стану теми показав активне зростання інтересу до впровадження смарт-контрактів у 2020–2024 рр. У публікаціях [1; 2; 5] простежуються як теоретичні підходи, так і прикладні реалізації – у логістиці, енергетиці, торгівлі та сфері цифрової економіки. При цьому відзначається недостатнє висвітлення практичних аспектів інтеграції смарт-контрактів у реальні бізнес-системи [4]. Американський криптограф Нік Сабо визначив смарт-

контракти як комп’ютерні протоколи, що автоматично виконують операції відповідно до закладених алгоритмів.

Основними перевагами смарт-контрактів є:

- усунення посередників;
- автоматичне виконання умов;
- чітка регламентація процесу;
- неможливість зміни коду після створення.

Це сприяє зниженню витрат на транзакції та скороченню судових спорів. Водночас смарт-контракти мають ряд недоліків:

Залежність від зовнішніх джерел даних, що може призводити до недостовірності інформації.

Автоматичне виконання без можливості внесення змін у разі виникнення непередбачених обставин.

Потенційні помилки в коді, які неможливо виправити після запуску контракту.

Відсутність правового регулювання та складність визначення застосовного права для міжнародних угод.

Відсутність механізмів захисту прав сторін у разі збоїв або шахрайства.

Особливу увагу слід приділити відповідальності за порушення зобов’язань у смарт-контрактах.

Поетапна методологія впровадження смарт-контрактів, охоплює п’ять стадій:

- підготовку (аналіз потреб, бізнес-процесів і технічної інфраструктури);
- проєктування (використання BPMN/UML, побудова логіки контрактів);
- розробку (Solidity, створення тестового середовища);
- впровадження (інтеграція через API, навчання персоналу);
- моніторинг та вдосконалення (тестування, оцінка ефективності) [3; 4].

Таким чином, смарт-контракти мають значний потенціал, проте їх використання потребує доопрацювання та правового регулювання. Оптимальним рішенням на сьогодні може стати гібридна модель, де частина умов існуватиме у цифровому форматі, а частина – у традиційній письмовій формі.

Перспективи застосування смарт-контрактів в освіті та науці полягають у можливості автоматизації академічної сертифікації, цифрової ідентифікації, управління грантовими проектами та валідації даних [6].

ДЖЕРЕЛА

1. Wallis K., Stodt J., Jastremskoj E., Reich C. Agreements between Enterprises digitized by Smart Contracts in the Domain of Industry 4.0

[Електронний ресурс] // arXiv. 2020. Режим доступу: https://arxiv.org/abs/2007.14181

2. Горбачук В. М., Ніколенко Д. І., Пустовойт М. М., Годлюк В. В., Рибачок Д. О. Смарт-контракти в енергетиці. Використання блокчейн технологій в енергетиці [Електронний ресурс] // ResearchGate. 2024. Режим доступу: https://www.researchgate.net/publication/382183240

3. Трішин Ф. А., Трач О. Р. Процесний підхід у формуванні системи управління якістю бізнес-процесів в операційній діяльності на туристичних підприємствах України // Food Industry Economics. 2022. Т. 14, № 4. Режим доступу: https://www.researchgate.net/publication/369601389

4. Таранюк Л. М. Теоретико-методологічні засади управління вибором напрямів реінжинірингу бізнес-процесів промислових підприємств // Вісник СумДУ. Серія: Економіка. 2015. № 1. С. 13. Режим доступу: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=VSU_ekon_2015_1_13

5. Шевчун М. Б. Моделювання результативного управління логістичними процесами підприємства торгівлі // Бізнес Інформ. 2021. С. 234–241. – Режим доступу: http://jnas.nbuv.gov.ua/uk/article/UJRN-0001269641

6. Бавико О. Є. Цифровізація бізнес-процесів як елемент стратегії сталого смарт-розвитку підприємницьких структур // Економічний журнал Одеського політехнічного університету. 2023. № 2(24). С. 15–23. Режим доступу: https://economics.net.ua/ejopu/2023/No2/15.pdf

ФУНКЦІОНАЛЬНІ МОЖЛИВОСТІ ТА ПОРІВНЯЛЬНИЙ АНАЛІЗ ІНСТРУМЕНТІВ УПРАВЛІННЯ ПРОГРАМНИМИ ПРОЄКТАМИ

Романишин В. І., Вовк Р. Б.

Івано-Франківський національний технічний університет нафти і газу, м. Івано-Франківськ

Програмне забезпечення для управління проєктами являє собою спеціалізований інструментарій, призначений для підтримки бізнес-процесів, пов’язаних із плануванням, реалізацією та контролем виконання робіт. Такі системи інтегрують уніфікований набір функціональних модулів, що охоплюють планування завдань, управління ресурсами та бюджетами, а також забезпечують взаємодію між членами проєктної команди [1].

Сучасні інструменти для управління проєктами повинні забезпечувати широкий функціональний спектр, зокрема:

- Планування завдань, яке включає створення списків задач, пріоритезацію, встановлення термінів та контроль за їх дотриманням.
- Управління ресурсами, що передбачає ефективний розподіл як людських, так і матеріальних ресурсів із урахуванням навантаження.
- Моніторинг і звітність, які дають змогу відстежувати хід виконання проєкту та формувати аналітичну звітність.
- Управління бюджетом, що включає прогнозування фінансових витрат, їх контроль і забезпечення доцільності реалізації проєкту.
- Забезпечення командної взаємодії через інтеграцію чатів, спільного редагування документів, що сприяє оперативному прийняттю рішень.
- Контроль версій, який дозволяє зберігати історію змін і відновлювати попередні версії проєктних артефактів.

Крім того, більшість систем управління проєктами обладнані інструментами автоматизації, зокрема шаблонами завдань, нагадуваннями та інтеграцією з іншими сервісами, що підвищує загальну продуктивність. Також значну роль відіграє безпека: захист від несанкціонованого доступу, резервне копіювання даних і контроль доступу з боку адміністратора є критично важливими для збереження цілісності інформації [2].

Ефективне управління програмними проєктами вимагає використання спеціалізованих інструментів, функціональні можливості яких повинні відповідати потребам конкретного проєкту. Розглянемо три поширених рішення:

- Jira (Atlassian) є одним з найбільш розповсюджених інструментів для управління проєктами, що реалізуються відповідно до гнучких методологій (Agile). Система підтримує Kanban і Scrum, дозволяє налаштовувати робочі процеси, інтегрується з Git, Slack та іншими сервісами, а також містить розширений аналітичний функціонал [3].
- Worksection –веб-платформа, орієнтована на малі та середні компанії, яка забезпечує контроль над завданнями, строками виконання та бюджетами. Інструмент підтримує календарне планування, діаграми Ганта, Kanban-дошки та засоби інтеграції з іншими продуктами [1].
- ClickUp –хмарний сервіс із широкими можливостями кастомізації, який підтримує автоматизацію бізнес-процесів, управління ресурсами, документообіг і контроль часу. Він орієнтований на команди, які працюють за гнучкими підходами, і дозволяє налаштовувати індивідуальні статуси завдань та використовувати тайм-трекери [1].

Вибір конкретного програмного забезпечення залежить від таких факторів, як методологія управління, масштабність проєкту, інтеграційні можливості, вартість і функціональні характеристики. Для великих і складних проєктів доцільним є використання Jira або ClickUp, які надають гнучкі можливості налаштування процесів та інтеграції. Для невеликих команд або стартапів доцільним є використання Worksection, який поєднує

простоту інтерфейсу з функціональністю, необхідною для управління обмеженими ресурсами. Інтеграція з іншими системами (Git, Slack, Google Drive тощо) є одним з ключових критеріїв вибору, оскільки забезпечує безперебійну взаємодію в межах міждисциплінарних команд. Також важливу роль відіграє цінова політика: Jira використовує модель ліцензування, ClickUp і Worksection пропонують безкоштовні пакети для малих команд, що робить їх доступними для широкого кола користувачів.

Проведений аналіз показує, що кожен із розглянутих інструментів має власні переваги. Jira є оптимальним рішенням для команд, що дотримуються Agile-методологій і мають потребу в потужній інтеграційній підтримці. ClickUp забезпечує високу гнучкість у налаштуванні робочих процесів, тоді як Worksection вирізняється простотою використання та орієнтацією на бізнеси з обмеженими ресурсами. Незважаючи на широкий вибір доступних рішень, універсальна платформа, що б однаково ефективно підтримувала всі проєктні методології, на сьогодні відсутня. Тому доцільним є не лише ретельний вибір програмного забезпечення, а й розгляд можливості комбінованого використання декількох інструментів з метою підвищення загальної ефективності управління проєктами.

ДЖЕРЕЛА

1. 10 найкращих програм для управління проєктами для малогобізнесу 2024. URL: https://surl.li/qrxabo

2. Метод машинного навчання в управлінні програмними проєктами. URL: https://vottp.khmnu.edu.ua/index.php/vottp/article/view/344.

3. Jira | Issue & Project Tracking Software | Atlassian. URL: https://www.atlassian.com/software/jira.

ТАЙМ-МЕНЕДЖМЕНТ ЯК ІНСТРУМЕНТ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ УПРАВЛІННЯ ІТ-ПРОЄКТАМИ

Романова Ю. С., Вовк Р. Б.

Івано-Франківський національний технічний університет нафти і газу, м. Івано-Франківськ

Раціональне управління часом у межах ІТ-проєктів є однією з ключових умов дотримання встановлених строків розробки, оптимального використання ресурсів і зниження ризиків, пов’язаних із затримками. Недостатньо ефективне управління часовими ресурсами здатне призводити до перевантаження співробітників, підвищеного рівня стресу та професійного вигорання. Це особливо актуально в умовах багатозадачності, коли працівники одночасно залучені до кількох ініціатив із жорсткими дедлайнами [1].

Сучасні ІТ-проєкти, зокрема ті, що реалізуються за гнучкими методологіями (Agile, Scrum), передбачають чітке планування робочих

завдань у межах ітерацій (спринтів), що, у свою чергу, потребує високої дисципліни в тайм-менеджменті. Планування часових витрат дозволяє формувати реалістичні графіки виконання, вчасно виявляти відставання та оперативно вживати коригувальні заходи.

Серед інструментів, що сприяють ефективному плануванню та реалізації ІТ-проєктів, варто виділити системи управління завданнями, зокрема Jira, YouTrack та Trello. Перші дві пропонують широкі функціональні можливості для структурування завдань, встановлення строків, відстеження прогресу та проведення ретроспектив. Trello, попри обмежений функціонал, залишається зручним інструментом для невеликих команд або проєктів. У великих командах також застосовуються діаграми Ґанта, контрольні точки (milestones), метод критичного шляху (CPM) та метод критичного ланцюга (CCM), який враховує обмеженість ресурсів і забезпечує більш точне планування тривалості проєкту [2].

Окрему роль у забезпеченні ефективного використання часу відіграють системи трекінгу, які дозволяють контролювати продуктивність розробників, формувати регулярні звіти, порівнювати запланований і фактичний час виконання завдань. Це сприяє виявленню вузьких місць, накопиченню історичних даних і підвищенню точності майбутніх оцінок. Централізована система обліку часу значно знижує адміністративне навантаження на менеджерів, забезпечуючи прозорість проєктного процесу. Поєднання таких систем із методикою *Pomodoro* сприяє підвищенню продуктивності, дозволяючи спеціалістам чергувати інтенсивну роботу з короткими перервами, що, своєю чергою, допомагає знизити ризик професійного вигорання.

Одним із найбільш надійних підходів до оцінювання часових витрат є аналіз історичних даних з попередніх проєктів зі схожими характеристиками. Такий аналіз дає змогу формувати реалістичні прогнози, уникати необґрунтованих припущень, виявляти ризики на ранніх етапах. Додатково застосовується оцінювання на основі віх (milestone-based estimation), яке полягає в розбитті проєкту на логічні етапи з чітко визначеними цілями. Це дозволяє своєчасно коригувати ресурсне забезпечення. На завершальних етапах життєвого циклу ІТ-проєкту (тестування, деплой) питання дотримання строків набуває особливої актуальності, оскільки можливі затримки можуть мати каскадний ефект на суміжні проєкти та графіки релізів. Для цього впроваджуються буферні часові зони (*time buffers*) і попередній аналіз ризиків.

Управління зацікавленими сторонами також є невід’ємною складовою ефективного тайм-менеджменту. Йдеться про підтримку регулярної комунікації з усіма учасниками проєкту, отримання зворотного зв’язку, що дає змогу оперативно реагувати на зміни. Проведення неформальних зустрічей, командоутворювальних заходів (*team buildings*)

сприяє покращенню міжособистісної взаємодії та формуванню здорового мікроклімату в команді.

У контексті залучення спільних ресурсів –коли спеціалісти паралельно беруть участь у кількох проєктах –постає потреба в ретельній координації графіків. Тайм-менеджмент у такому випадку виконує роль балансування навантаження. Важливими інструментами тут є регулярні синхронізаційні зустрічі (*sync meetings*), системи планування ресурсів (*resource scheduling*), які забезпечують візуалізацію поточного навантаження кожного члена команди та дозволяють ухвалювати обґрунтовані рішення щодо перерозподілу завдань у динамічному середовищі.

Отже, ефективне управління часом в ІТ-проєктах –це не лише організаційна навичка, а цілісна система, що поєднує інструменти, методології, дані, командну взаємодію та аналітику. Її головна мета –не лише забезпечити своєчасне завершення проєкту, а й досягти цього з оптимальним використанням ресурсів, збереженням якості та високим рівнем задоволеності замовника. В умовах зростаючої складності цифрових продуктів та конкуренції на ринку, здатність ефективно керувати часовими ресурсами стає ключовим фактором успішності організацій.

ДЖЕРЕЛА

1. Time Management Tools to Boost Productivity. Udemy. URL: https://blog.udemy.com/time-management-tools.

2. Getting $#!t Done: How to Manage Your Time as a Remote Dev. Arc Talent Career Blog. URL: https://surl.li/emjfkl.

ВИКОРИСТАННЯ ІНТЕРАКТИВНОГО СЕРВІСУ «WORDWALL» У ПРОФЕСІЙНІЙ ДІЯЛЬНОСТІ ВЧИТЕЛЯ УКРАЇНСЬКОЇ МОВИ Й ЛІТЕРАТУРИ

Свиридченко І. М.

Київський столичний університет імені Бориса Грінченка, м. Київ

В освітній професійній діяльності вчителя-словесника важливим є не лише грамотне орієнтування в означеній інформації чи застосування її на практиці, а й обов’язкове зацікавлення своїм предметом учнів сучасними й нестандартними способами. Саме великої популярності набрали інноваційні засоби навчання – інтерактивні завдання, вправи, ігри, квести тощо з використанням цифрових платформ чи онлайн-застосунків.

Так, одним із найбільш відомих і корисних сервісів є інтерактивна платформа «Wordwall», що дозволяє створювати такі завдання, які запам’ятаються аудиторії і привернуть увагу до певної теми чи загалом до заняття, допомагають формувати ключові компетентності; до того ж

система оптимізована до використання людьми, які не мають навичок високого рівня в програмуванні, тому розроблювання вправ не займатиме багато часу. Цим і зумовлюється **актуальність** дослідження.

Метою роботи є демонстрація корисності цифрового застосунку на уроках української мови і літератури для виконання колективних, групових чи самостійних завдань в ігровій формі.

Специфіка сервісу. «Wordwall» – це зручний і швидкий ресурс, за допомогою якого учитель розроблює завдання за певною темою на основі вже наявних шаблонів. Є можливість створювати інтерактиви за такими формами: відповідники (перетягувати головні слова до визначень), вікторина (надавати відповіді на запитання з кількома варіантами), випадкові карти (на карті з'являтиметься запитання, на яке учні відповідають усно), флешкартки (на фронтальній стороні знаходиться запитання, а коли перевернути – відповідь), доповнити речення (перетягування слів на порожні місця в реченні), сортування за групами (перетягування елементів до груп згідно із завданням), випадкове колесо (за допомогою колеса фортуни можна дізнатися випадковий елемент), кросворд та багато інших. Під час виконання певних завдань модератор може встановлювати функцію відліку часу, а потім результат відобразиться у рейтинговій таблиці із зазначенням витрачених хвилин кожного учня, який вказав своє ім'я.

Переваги і недоліки сервісу «Wordwall»

Переваги	Недоліки
Інтерактивний підхід. За допомогою цієї платформи можна залучити до виконання вправ велику кількість учнів, змотивувати активну участь та забезпечити групову чи самостійну роботу.	Обмежені можливості для застосування користувачами безкоштовної версії. Так можна створювати лише 5 завдання на 30 днів.
Універсальне спрямування. Платформа дозволяє користуватися різним віковим групам, людям з різним рівнем знань, а також створювати завдання для багатьох тематик і форм роботи.	Вузький асортимент шаблонів для безкоштовної версії не дозволяє постійно застосовувати сервіс, адже одноманітні завдання можуть швидко набриднути аудиторії.
Мобільне використання. Платформа доступна всім учням з будь-якого гаджету з доступом до мережі.	Обмеження з візуальним контентом. Немає можливості додавати відеофайлів до розроблених завдань.
Велика кількість можливостей для створення власних навчальних ресурсів.	

Порівняння сервісів «Wordwall» і «LearningApps»

Критерій	Wordwall	LearningApps
Різноманітність завдань і шаблонів	+	+
Доступність усіх шаблонів у безкоштовній версії	–	+ (немає платної версії)
Можливість додавання інших візуальних елементів (фото, відео, аудіо)	+ (окрім відео)	+
Різнокольоровість шаблонів, візуальні елементи	+	–
Необов'язковість реєстрації для створення власних завдань	–	+
Збереження результатів виконаних завдань учнями	+	–

Використання інтерактивної платформи «Wordwall» у професійній діяльності учителя-словесника. За допомогою онлайн-сервісу «Wordwall» на уроках української мови і літератури легко використовувати різноманітні засоби навчання – тестування чи опитування, ігри на знання граматики чи синтаксису, розширення словникового запасу, літературні квести й ігри для запам'ятовування сюжету чи аналізу образів персонажів. Сервісом «Wordwall» варто послуговуватися не лише під час занять, а й, наприклад, для домашнього опрацювання чи проведення позакласної роботи – мовних або літературних конкурсів, вікторин, брейн-рингів, квестів, олімпіад тощо з метою підвищення мотивації і рівня зацікавленості одним із найважливіших профілів навчання у школі, а також як один з методів дотримання положень мовної політики України – усебічне поширення української мови серед громадян і сприяння її якісному вивченню.

Щодо інших аспектів учительської професійної діяльності, то ресурс цілком придатний для застосування на педрадах, колегіумах, конференціях тощо. Можна залучати й інших колег до інтерактивної діяльності й взаємодії з усіма учасниками освітнього процесу. Наприклад, за шаблоном «Випадкове колесо» розробити систему запитань для пізнання емоційного стану колег на педраді чи рівня їх обізнаності з певними положеннями інтерактивного й продуктивного навчання тощо.

Цифровий сервіс «Wordwall» – платформа, що допомагає урізноманітнити навчальний процес за допомогою інтерактивних завдань, які можна розробити самостійно відповідно до теми заняття. Це сприяє підвищенню інтересу учнів до навчання, а також дозволяє напрацювати певні навички розрізнення тих чи інших елементів теорії. Також така інтерактивна взаємодія допомагає формувати ключові компетентності – вільне володіння українською мовою, інформаційно-цифрова компетентність, розвиток ініціативності, критичного мислення,

застосування емоційного інтелекту – та розвивати сучасне освітнє середовище. Великою перевагою сервісу є можливість створювати завдання в ігровій доступній формі для будь-якого учня з використанням мінімум часу.

ДЖЕРЕЛА

1. LerningApps. Інтерактивні навчальні модулі. URL: https://learningapps.org/index.php?category=100&s= (дата звернення: 25.11.2024).

2. Wordwall. Інтерактивні завдання і вправи. URL: https://wordwall.net/uk (дата звернення: 25.11.2024).

ВИКОРИСТАННЯ ДОДАТКУ TIK TOK В РЕКЛАМІ ТА PR

Стрілець Д. , Панченко А., Гайсін Р., Герасименко В., Захожа В.
Київський столичний університет імені Бориса Грінченка, м. Київ

TikTok – це культурний феномен, який змінив спосіб, у який люди створюють, споживають і поширюють контент. Завдяки своїй інтерактивній природі додаток відкриває широкі можливості для реклами та PR. Бренди можуть не лише демонструвати свої продукти, але й активно взаємодіяти зі своєю аудиторією; популярність TikTok стала невід'ємною частиною сучасного медіа-ландшафту.

Історія додатку

Розроблений компанією ByteDance,TikTok був вперше запущений у Китаї в 2016 році під назвою Douyin; у 2018 році відбулося злиття з платформою Musically, що значно сприяло міжнародній популярності TikTok. Сьогодні додаток доступний понад 150 країнах і має активну аудиторію. Завдяки інноваційним інструментам для створення коротких відео TikTok входить в топ найпопулярніших соціальних мереж на планеті Земля.

Характеристика додатку. TikTok має багато функцій, які роблять його привабливим для користувачів. Широкий вибір фільтрів, спецефектів і музичних треків можна використовувати для створення коротких відео. Штучний інтелект працює на основі вподобань і активності користувачів, щоб персоналізувати стрічку «Для вас». TikTok заохочує творчість через виклики та тренди, які швидко поширюються серед спільноти. Простий та інтуїтивно зрозумілий інтерфейс робить платформу доступною для тих, хто ніколи раніше не користувався такими додатками. TikTok –чудове середовище для самовираження, розваг і взаємодії з глобальною аудиторією.

Порівняння з іншим додатком

Кожна соціальна мережа має свої особливості та аудиторію. Старшим віковим групам подобаються естетичні пости, фотографії та

відео в соціальних мережах.Корисний для текстових повідомлень, групових обговорень і таргетованої реклами, але втрачає популярність серед молодого покоління. Існує платформа для тривалого інформативного чи розважального відеоконтенту, де автори можуть детально висвітлювати теми. TikTok особливо привабливий для молоді та творчих людей через його швидкий темп споживання, легкість створення відео та здатність швидко генерувати тренди. Користувачі можуть вибрати спосіб взаємодії на кожній платформі.

Переваги	Недоліки
Велика аудиторія. Це мільярди переглядів щодня, що дає шанс брендам отримати увагу навіть без великих витрат на рекламу.	**Молода аудиторія.** Більшість користувачів TikTok –це підлітки та молодь до 30 років, що обмежує можливості для роботи з іншими цільовими групами
Швидке поширення. Завдяки вірусному потенціалу відео можуть стати популярними буквально за лічені години.	**Швидкоплинність контенту.** Нові тренди постійно змінюються, і брендам доводиться швидко адаптуватися до змін. .
Можливості для креативності. TikTok дозволяє створювати неформальний контент, який добре сприймається молодою аудиторією.	**Вимоги до креативності.** Контент повинен бути цікавим та унікальним, інакше його просто не помітять.
Залученість користувачів. Відео тут активно коментують, лайкають та репостять, що сприяє підвищенню впізнаваності брендів	**Проблеми з конфіденційністю.** TikTok неодноразово критикували за зберігання і використання даних користувачів.

Специфіка використання в професійній діяльності

Підвищення впізнаваності бренду та залучення користувачів є одними з найважливіших завдань сучасного маркетингу. Для досягнення цих цілей бренди використовують різні стратегії, інструменти та формати.

1.Аудиторію можна охопити через ефективний канал комунікації. Ключовим інструментом формування довіри до бренду є просування продукту. Співпраця з лідерами громадської думки чи експертами у своїй галузі завдяки їхній лояльній аудиторії.

- Є високий рівень автентичності.
- Охоплення нових сегментів споживачів.
- Ефективною є взаємодія з нішевою аудиторією.
- Природність інтеграції бренду можна підтримувати шляхом створення унікального контенту.

2.Прямі трансляції дозволяють брендам безпосередньо взаємодіяти зі своєю аудиторією.

- Цей формат можна використовувати Презентувати новинки.
- У режимі реального часу відповідайте на запитання аудиторії.
- Під час трансляції проводите акції, знижки або ексклюзивні пропозиції.

- Довіра створюється демонстрацією людського обличчя бренду.
- Взаємодія з брендом є значущою для глядачів, оскільки вони отримують відчуття особистого контакту.

3. У креативних кампаніях використовуються нестандартні підходи.

Відео, яке показує продукти по-іншому, допомагає виділитися. Креативних кампаній може бути більше однієї.

Сюжет міні-серіалу пов'язаний з твором.

У відео можна використовувати віртуальну реальність або інтерактивні елементи.

Увагу аудиторії можна привернути гумором або емоційними історіями.

Нові формати дозволяють брендам бути ближчими до своєї аудиторії та залишати незабутній емоційний слід.

Поєднання цих стратегій допомагає будувати довгострокові відносини з клієнтами.

TikTok- це новітня платформа, яка докорінно змінює підхід до реклами та PR. Її успіх базується на унікальному поєднанні креативності,простотивикористання та потужного вірусного ефекту. TikTok відкриває безмежні можливості для бізнесу,але також вимагає швидкої адаптації до трендів, розуміння аудиторії та нестандартного підходу до створення контенту. За допомогою TikTok бренди можуть не тільки підвищити впізнаваність, але й встановити живий контакт зі своєю цільовою аудиторією. Успіх на цій платформі залежить від уміння бути автентичним, слідувати трендам і створювати контент, який викликає емоції та бажання поділитися з іншими. TikTok - це простір, де швидкість і креативність можуть дати важливі результати для компаній у постійно мінливому цифровому світі.

ДЖЕРЕЛА

1. TikTok -феномен сучасних соціальних мереж [Електронний ресурс] URL: https://icyeast.org/a-tiktok-fenomen-suchasnyh-socialnyh-merezh

2. Instagram як платформа для таргетованої реклами: секрети успіху [Електронний ресурс] URL: https://www.volynpost.com/news/244786-instagram-iak-platforma-dlia-targetovanoi-reklamy-sekrety-uspihu

3. TikTok Advertising: повний огляд рекламних функцій платформи [Електронний ресурс] URL: https://sendpulse.ua/blog/tiktok-advertising

4. Офіційний сайт TIKTOK [Електронний ресурс] URL: https://www.tiktok.com/uk-UA/

ВИКОРИСТАННЯ ДІАГРАМИ ПРЕДМЕТНОЇ ГАЛУЗІ ДЛЯ СТВОРЕННЯ МОДЕЛІ ПРЕДМЕТНОЇ ГАЛУЗІ СИСТЕМИ З ОПИТУВАННЯ СТУДЕНТІВ

Тимошенко М.О.
Державний університет інформаційно-комунікаційних технологій, м. Київ

У сучасному інформаційному середовищі зростає потреба в інтегрованих системах збору та аналізу даних для покращення організації навчального процесу. Застосування діаграми предметної галузі дозволяє побудувати ефективну модель, що відображає структуру та динаміку опитувань серед студентів. Такий підхід сприяє оптимізації процесу аналізу отриманих даних, забезпечуючи як якісну обробку інформації, так і своєчасне прийняття управлінських рішень [1; 2].

Постановка задачі

Задачею дослідження є розробка методології створення моделі предметної галузі для системи з опитування студентів із застосуванням діаграми предметної галузі. Основними завданнями є:

аналіз існуючих підходів до моделювання предметної галузі;

розробка діаграми для візуалізації основних об’єктів, їх властивостей та взаємозв’язків(див. рис. 1);

інтеграція розробленої діаграми у загальну модель інформаційної системи.

Мета дослідження

Метою дослідження є визначення та обґрунтування ключових можливостей використання діаграми предметної галузі для побудови моделі системи опитування студентів. Це передбачає розробку концептуальної схеми, що:

- забезпечить точне відображення предметної області;
- дозволить адаптувати систему до змін у навчальному процесі;
- оптимізує збір і аналіз даних для прийняття ефективних управлінських рішень.

Результати дослідження

У процесі дослідження було здійснено порівняльний аналіз існуючих методів моделювання. Основні результати включають:

- створення діаграми предметної галузі, яка включає такі компоненти: анкети, відповіді, профілі студентів та результати аналізу;
- розробку алгоритму інтеграції розробленої діаграми в архітектуру інформаційної системи;

апробацію моделі на базі прототипу, що демонструє ефективність підходу.

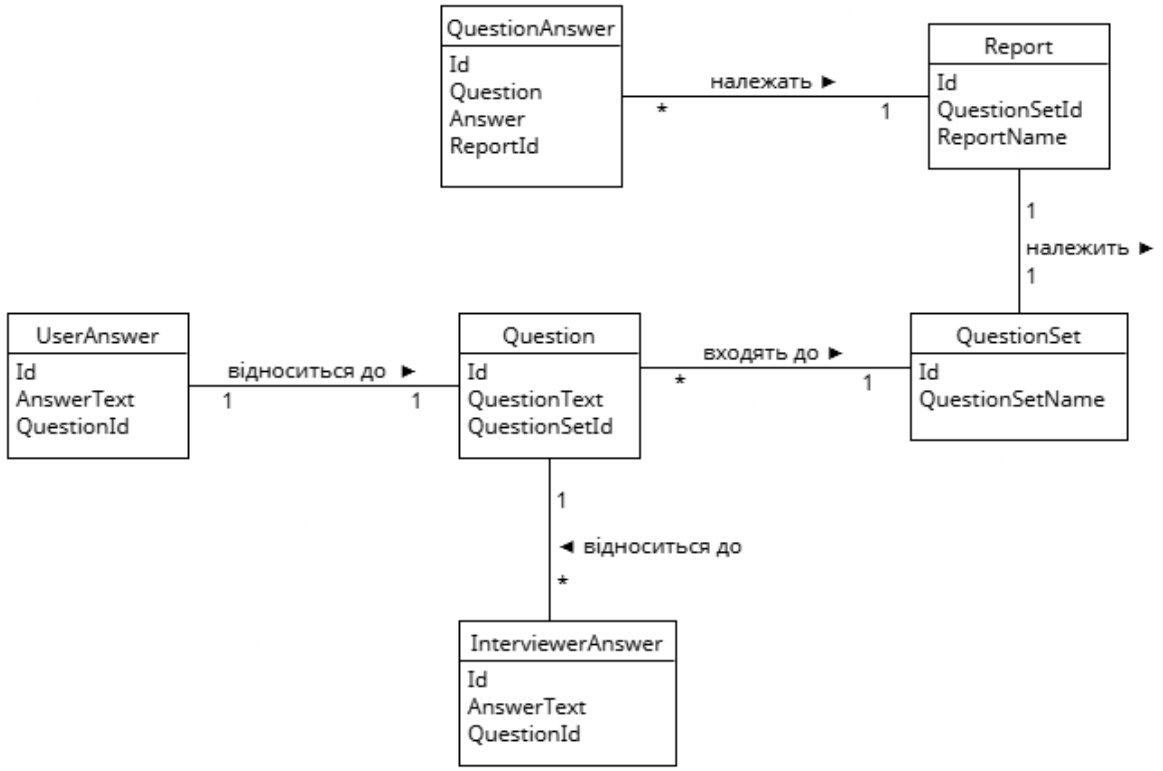


Рис. 1. Діаграма прецедентів функціональності застосунку

Висновки та перспективи

Отримані результати підтверджують доцільність застосування діаграми предметної галузі для створення системи опитування студентів, що сприяє:

- підвищенню структурованості й прозорості обробки даних;
- швидкому доступу до аналітичної інформації;
- можливості подальшої інтеграції системи з іншими інформаційними платформами навчального закладу.

Подальші дослідження можуть бути спрямовані на адаптацію моделі до специфічних вимог окремих навчальних установ та розширення функціональних можливостей системи.

ДЖЕРЕЛА

1. Zachman, J. A., *A Framework for Information Systems Architecture*, Harper & Row, 1987.

2. Dennis, A., Wixom, B. H., & Tegarden, D., *Systems Analysis and Design*, Wiley, 2015.

3. Сивенко В. М., *Методи моделювання інформаційних систем*, Київ: Наукова думка, 2012.

4. Петрова Л. І., *Основи системного аналізу в управлінні освітою*, Харків: ХНУ ім. В. Н. Каразіна, 2018.

СТВОРЕННЯ АВТОМАТИЧНОГО РИГГІНГУ 3D ПЕРСОНАЖУ ЗА ДОПОМОГОЮ ПЛАТФОРМИ MIXAMO

Христенко А. В.
Київський столичний університет імені Бориса Грінченка, м. Київ

Термін «риггінг» прийшов з морської справи. Це система канатів, тросів і ланцюгів на судні. Іншими словами, риггінг – це такелаж [1].

Риг потрібен для налаштування і керування 3D-моделлю. Початково 3D-модель нерухома. Це манекен, яким неможливо керувати. Ригер натомість встановлює в цю модель суглоби, кістки та дозволяє керувати її кінцівками імітуючи рух [1].

Ригінг, а тим більш анімація це експертне направлення у 3D якому вчаться не один місяць чи ріг. Але проект Mixamo компані Adobe має широкий функціонал легкий для сприйняття інтерфейс та інструментарій, що дозволяє досить легко і швидко оживити модель власного персонажу.

Mixamo – Це сайт для автоматичної генерації скелету для моделей персонажів (гуманойдів), створений компанією Adobe, а також велика бібліотека готових анімацій.

На першому етапі користувач взаємодіє з вебінтерфейсом Mixamo для ініціалізації процесу автоматичного ріґґінгу. Платформа приймає тривимірні моделі у таких форматах: **FBX (Filmbox)** – бінарний або ASCII-формат, який підтримує сітку, текстури, анімацію та структури скелету. **OBJ (Wavefront Object)** – геометричний формат, орієнтований виключно на опис полігональної сітки без підтримки анімації. **ZIP-архів** - повинен містити сітку моделі у FBX або OBJ-форматі разом із супровідними файлами текстур (наприклад, у форматах .PNG, .JPG, .TGA тощо).

Для забезпечення коректного ріґґінгу необхідно дотримуватись таких умов: **Модель повинна мати гуманоїдну анатомічну структуру**, тобто включати тулуб, голову, дві руки та дві ноги, розташовані симетрично відносно центральної осі. Позиціонування персонажа повинно відповідати T-позі або A-позі, що означає. Модель повинна бути суцільною: усі геометричні частини мають бути з'єднані або об'єднані в одну сітку (mesh), без окремих, плаваючих об'єктів. Наявність нормалей та UV-розгортки є бажаною, хоча не обов’язковою умовою для базового ріґґінгу. Масштаб і орієнтація моделі повинні бути стандартизованими: рекомендовано вирівнювання по вертикальній осі (звичайно Y або Z, залежно від програмного середовища).

Після розміщення користувачем анатомічних маркерів, Mixamo ініціює етап **автоматизованого ріґґінгу**, відбувається побудова внутрішньої скелетної структури та розрахунок вагових коефіцієнтів для управління деформацією сітки (skin weighting). Цей процес здійснюється

без участі користувача, з використанням комбінації шаблонного фітингу, процедурного генератора кісток та алгоритмів машинного навчання.

На основі макетів платформа реконструює **стандартизовану структуру скелету**, яка відповідає загальноприйнятій гуманоїдній ієрархії. Вона зазвичай включає: **Центральний стовбур (spine):** таз (hips), нижня спина, середина спини, груди та шия. **Верхні кінцівки (arms):** плечі, передпліччя, зап'ястки. **Нижні кінцівки (legs):** стегна, гомілки, стопи. **Голова (head):** шия і череп.

Ієрархія будується за принципом батьківсько-дочірніх зв'язків, що забезпечує коректну передачу трансформацій від кореня до кінцевих ефекторів. Після побудови кісткової структури виконується процес **скінінгу** – визначення ступеня впливу кожної кістки на довколишні вершини сітки (vertices). Mixamo застосовує алгоритм **heat map skinning** або аналогічний метод, який враховує: евклідову відстань від кістки до вершини, топологію сітки, анатомічну зону впливу (визначену маркерами).

Після успішного завершення ріґґінгу користувач отримує **уніфіковану скелетну модель**, яка: містить структуру кісток з унікальними іменами, сумісними з бібліотекою Mixamo має скінінг, що забезпечує коректну деформацію сітки є придатною для негайного застосування анімацій.

ДЖЕРЕЛА

1. Немченко О. Rigger в Pingle Studio - Що треба знати про ригінг у геймдеві та як опанувати цей фах: поради спеціаліста. - Режим доступу: https://gamedev.dou.ua/blogs/rigger-in-gamedev-industry/

2. Mixamo. Офіційний сайт. - URL: https://www.mixamo.com

3. Adobe Systems. Офіційний сайт - URL: https://www.adobe.com/ua

ВПЛИВ МЕТОДОЛОГІЙ AGILE ТА WATERFALL НА ЕФЕКТИВНІСТЬ ПРОЄКТІВ РОЗРОБКИ ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Цап Д. І., Вовк Р. Б.

Івано-Франківський національний технічний університет нафти і газу, м. Івано-Франківськ

Розробка вбудованого програмного забезпечення (ПЗ) супроводжується низкою специфічних викликів, зокрема обмеженими апаратними ресурсами, необхідністю забезпечення високої надійності та суворими вимогами до продуктивності. У цьому контексті вибір відповідної методології розробки, такої як каскадна модель (Waterfall) або гнучкі методології (Agile), відіграє ключову роль у досягненні успішних результатів. Обидва підходи мають свої переваги та обмеження, що

потребує адаптації методів управління розробкою до конкретних особливостей проєкту.

Каскадна модель (Waterfall) є традиційним лінійним та послідовним підходом до розробки програмного забезпечення. Вона передбачає суворе дотримання етапності процесу, де кожна стадія має бути завершена перед переходом до наступної. Основною перевагою цього підходу є його передбачуваність, можливість детального планування та контроль за відповідністю кінцевого продукту початковим вимогам. Однак жорсткість моделі обмежує можливість внесення змін у процесі розробки, що може бути критичним недоліком у динамічних проєктах [1].

Натомість Agile-методології передбачають ітеративний підхід до розробки, що забезпечує гнучкість і можливість адаптації до змінних вимог. Використання цього підходу сприяє паралельному виконанню різних етапів розробки, що дозволяє мінімізувати витрати на внесення змін і прискорює процес адаптації до нових умов. Крім того, Agile орієнтований на регулярний зворотний зв’язок із зацікавленими сторонами, що сприяє створенню продукту, який максимально відповідає очікуванням користувачів [2].

У сфері розробки вбудованого ПЗ вибір між цими методологіями визначається специфікою проєкту. Каскадна модель може бути ефективною у випадках, коли вимоги до системи є чітко визначеними та стабільними, а можливість змін обмежена. Це особливо актуально для вбудованих систем, що працюють у критичних умовах, де будь-яке відхилення може призвести до небажаних наслідків. Водночас гнучкі методології можуть бути доцільними у ситуаціях, коли необхідно швидко адаптувати систему до змінних вимог або поступово вдосконалювати функціональність програмного забезпечення.

Гнучкі методології розробки, зокрема Agile, забезпечують високу адаптивність до змінних вимог, що є особливо важливим для динамічних проєктів. Використання коротких ітераційних циклів розробки дозволяє командам регулярно отримувати зворотний зв’язок від замовників і користувачів та відповідним чином коригувати функціональність програмного забезпечення. Це має критичне значення у випадках, коли вимоги до вбудованого ПЗ змінюються внаслідок оновлення виробничих процесів або необхідності інтеграції з новими апаратними рішеннями. Однією з ключових переваг Agile є здатність до швидкого внесення змін та виправлення помилок, що особливо актуально для високодинамічних проєктів, де специфікації можуть уточнюватися на всіх етапах розробки [2]. Водночас застосування каскадної моделі (Waterfall) може бути виправданим у випадках, коли всі вимоги до системи відомі заздалегідь і їхня зміна може спричинити значні витрати на переробку коду.

Разом із тим, розробка вбудованого ПЗ у межах Agile передбачає певні виклики, зокрема потребу у частому тестуванні та інтеграції. Це

може створювати додаткове навантаження на ресурси, особливо у випадку систем реального часу, де кожна ітерація вимагає фізичного тестування на цільовій апаратній платформі. У свою чергу, Waterfall передбачає проведення повного циклу тестування лише після завершення всіх етапів розробки, що може мінімізувати витрати на тестування, однак призводить до підвищених ризиків виявлення критичних помилок на пізніх етапах життєвого циклу [1]. Останнім часом активно досліджуються підходи до поєднання Agile та Waterfall у гібридні методології, що дозволяють поєднати переваги обох моделей. Зокрема, на етапах планування проєкту та визначення основних вимог застосовується каскадна модель, тоді як розробка окремих компонентів та їх інтеграція реалізуються за принципами Agile.

Отже, вибір між Agile та Waterfall у розробці вбудованого програмного забезпечення залежить від специфіки проєкту, вимог замовника та апаратних обмежень. Обидві методології мають свої переваги та недоліки, а їх правильне комбіноване застосування може суттєво підвищити ефективність процесу розробки. В умовах жорстких ресурсних обмежень та високих вимог до продуктивності все більшого поширення набувають змішані підходи, що дозволяють адаптувати процес розробки до конкретних потреб системи.

ДЖЕРЕЛА

1. Agile проти Waterfall – різниця між методологіями. *Guru99*. URL: https://www.guru99.com/uk/waterfall-vs-agile.html.

2. Вимоги до програмного забезпечення: Agile vs Waterfall Methodology - Visure Solutions. *Visure Solutions*. URL: https://visuresolutions.com/uk/посібник-з-відстеження-управління-вимогами/вимоги-до-програмного-забезпечення-agile-vs-waterfall/.

SCRUM ЯК ІНСТРУМЕНТ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ УПРАВЛІННЯ НЕВЕЛИКИМИ ПРОЄКТАМИ

Шнурок В. С., Вовк Р. Б.

Івано-Франківський національний технічний університет нафти і газу, м. Івано-Франківськ

Освітній проєкт – це цілеспрямована, структурована ініціатива, орієнтована на забезпечення освітнього процесу та розвитку компетентностей учасників шляхом їхньої активної взаємодії та практичного досвіду. Такі проєкти можуть реалізовуватися в рамках формальної освіти, корпоративного навчання або громадських ініціатив, сприяючи набуттю актуальних знань та навичок.

У сучасних умовах, що характеризуються високою динамічністю змін і необхідністю адаптації до нових викликів, зростає популярність гнучких методологій управління проєктами. Однією з найбільш ефективних серед них є Scrum, що дозволяє оптимізувати процес організації роботи команди, забезпечуючи швидке реагування на зміни та поступове вдосконалення продукту. Цей підхід є особливо актуальним у керуванні маломасштабними проєктами, які характеризуються обмеженими ресурсами та стислими часовими рамками, що зумовлює необхідність підвищення ефективності всіх етапів розробки [1].

Scrum – це фреймворк, заснований на принципах Agile-підходу, у межах якого реалізація проєкту здійснюється через короткі ітеративні цикли – спринти. Такий підхід сприяє адаптивності команди, зменшенню ризиків та регулярному постачанню якісного продукту. В межах Scrum визначаються три ключові ролі [2]:

1. Власник продукту (Product Owner) – відповідає за управління беклогом, визначення пріоритетів і забезпечення роботи команди над найбільш цінними завданнями.
2. Scrum-майстер (Scrum Master) – забезпечує дотримання принципів методології, усуває перешкоди в роботі команди.
3. Команда розробників (Developers) – безпосередньо займається виконанням завдань, створенням продукту та його поступовим удосконаленням.

Застосування методології Scrum у малих проєктах має низку переваг:

1. Гнучкість та адаптивність – можливість швидкого реагування на зміни у вимогах або зовнішніх умовах.
2. Оптимізація комунікацій – регулярні зустрічі та відкритий обмін інформацією підвищують ефективність командної взаємодії та сприяють оперативному вирішенню проблем.
3. Фокус на створенні цінності – постійний зворотний зв’язок від стейкхолдерів забезпечує розробку продукту, який відповідає реальним потребам користувачів.
4. Прозорість процесів – чітко визначені ролі, етапи та артефакти методології Scrum спрощують управління проєктом і підвищують ефективність його реалізації.

Впровадження методології Scrum може супроводжуватися низкою викликів, що обумовлені як організаційними, так і психологічними факторами. Зокрема, необхідність трансформації управлінських процесів та перегляду корпоративної культури може викликати опір змін на різних рівнях організації. Крім того, недостатній рівень підготовки учасників команди щодо принципів Agile-підходу може призводити до зниження ефективності впровадження методології. Для мінімізації цих ризиків рекомендується здійснювати попереднє навчання персоналу, залучати досвідченого Scrum-майстра, адаптувати методологію відповідно до

специфіки організації та використовувати спеціалізовані інструменти управління проєктами (наприклад, Jira, Trello) [3].

Одним із ключових аспектів успішного функціонування Scrum-команд є налагодження ефективної комунікації між їхніми учасниками та стейкхолдерами. Оскільки не всі зацікавлені сторони можуть мати достатній рівень обізнаності щодо принципів гнучкого управління, це може спричиняти непорозуміння або некоректну інтерпретацію завдань. Наслідком таких бар'єрів стає уповільнення процесу розробки та ускладнення досягнення поставлених цілей. Окремого розгляду потребує питання масштабування Scrum у контексті невеликих проєктів. У таких командах часто спостерігається поєднання кількох ролей одним учасником, що може спричиняти конфлікти інтересів та надмірне навантаження на окремих спеціалістів. Для оптимізації роботи в таких умовах необхідно здійснювати ретельний аналіз ресурсів і, за потреби, адаптувати фреймворк, дотримуючись його основних принципів, але допускаючи певні модифікації відповідно до специфіки проєкту.

Отже, використання гнучких методів планування, а також регулярна оцінка ефективності процесів сприяють вчасному виявленню проблемних аспектів і забезпеченню їх коригування, що підвищує результативність впровадження Scrum у малих командах.

ДЖЕРЕЛА

1. Що таке Скрам (Scrum) 2025. SCRUM це методологія ? Brain Rain. URL: https://surl.li/nvpeuc .

2. Tatiana D. Scrum, як найпопулярніша методологія Agile (про Agile, частина Medium. URL: https://surl.li/dsxjfs.

3. Методологія Scrum, що допоможе організувати роботу команди та підвищити її продуктивність. Webpromo. URL: https://surli.cc/bsyzbu .

WORDWALL: ОПИС ПРОГРАМИ ТА ЇЇ МОЖЛИВОСТЕЙ У ДІЯЛЬНОСТІ ЛОГОПЕДА

Ярошевська А., Дробович В., Бурдейна Л., Кривошеіна Я., Галенко В.
Київський столичний університет імені Бориса Грінченка, м. Київ

Сучасна логопедія потребує інноваційних методів, щоб підвищити ефективність роботи з дітьми, які мають порушення мовлення. Особливе значення мають цифрові технології, адже вони дозволяють легко адаптувати потрібний матеріали під індивідуальні потреби кожної дитини, підвищуючи їхню мотивацію до навчання. З огляду на це, постає питання вибору ефективних інструментів, які можуть бути застосовані в практиці логопеда.

Одним із таких інструментів є платформа Wordwall, що відзначається універсальністю та простотою у використанні. Вона дозволяє створювати інтерактивні завдання, які відповідають різним інтересам та рівням підготовки дитини. Даний сервіс відповідає вимогам сучасної логопедичної практики, адже надає можливість легко адаптувати навчальні матеріали, створюючи вправи для розвитку всіх сторін мовлення.

З огляду на актуальність питання використання платформи Wordwall у логопедичній практиці, нами було виокремлено такі завдання:

1. Проаналізувати функціональні можливості платформи Wordwall з точки зору її застосування в логопедичній практиці.

2. Дослідити переваги та недоліки використання Wordwall для створення інтерактивних завдань, які сприяють розвитку мовленнєвих навичок у дітей з порушеннями мовлення.

3. Оцінити зручність використання Wordwall на різних пристроях у контексті логопедичних занять, як у класі, так і в дистанційному форматі.

Wordwall – це універсальний навчальний ресурс, що сприяє підвищенню мотивації учнів. Завдяки йому можна організувати диференційоване та індивідуальне навчання через створення різних типів вправ, таких як інтерактивні та друковані. Основною перевагою є простота у використанні, що дозволяє вчителям швидко створювати матеріали без спеціальних технічних навичок. Wordwall підтримує використання як на комп'ютерах, так і на мобільних пристроях [1].

Для кого буде корисний Wordwall:

- ✓ Вчителі та викладачі
- ✓ Учні
- ✓ Батьки
- ✓ Логопеди та спеціалісти корекційної освіти

Таблиця 1

Порівняльна таблиця переваг та недоліків WORDWALL

Переваги	Недоліки
Зручність у створенні завдань за допомогою готових шаблонів	Обмежені функції без платної підписки (мало шаблонів у безкоштовній версії)
Адаптація вправ під будь-яку тему (вікторини, пошук слів, анаграми, лабіринти)	Обмежені можливості для налаштування та персоналізації завдань
Інтеграція з пошуковими системами (пошук зображень через Bing)	Малий вибір типів завдань (обмежений набір інтерактивних форматів)
Розвиток мовлення (навчання лексики, граматики, комунікативних навичок)	Відсутність інструментів для одночасної співпраці між викладачами або учнями

Підходить для індивідуальної та групової роботи	Мова інтерфейсу може бути некоректно локалізована
Можливість редагування та адаптації завдань відповідно до потреб учнів	Платформа працює тільки онлайн, що залежить від інтернет-з'єднання
Контроль знань учнів через інтерактивні завдання	
Підвищення мотивації завдяки ігровому формату	
Сумісність з різними пристроями (комп'ютери, планшети, телефони, інтерактивні дошки)	
Спрощена організація навчальних матеріалів (збереження в папках, спільне використання)	
Сучасний підхід до навчання, альтернатива традиційним методам [3, с.75-76]	

Можливості у створенні ігор та вправ

Wordwall має багато шаблонів, які дозволять урізноманітнити будь-який матеріал(Рис.1).

Рис. 1. Приклади використання Wordwall в роботі логопеда

Приклади використання можна побачити, перейшовши за посиланнями, приведеними нижче:

1) Відповідники- http://surl.li/cjqeqt
2) Вікторина - http://surl.li/nwulfd
3) Випадкові карти - http://surl.li/cncbjw
4) Флеш-картки - http://surl.li/zplbyl
5) Доповніть речення - http://surl.li/rdlcqu
6) Сортування за групами - http://surl.li/vuvmdq
7) Знайти відповідність - http://surl.li/ryvafi
8) Випадкове колесо - http://surl.li/ymjcab
9) Відкрийте коробку - http://surl.li/tzyreb

10) Анаграми - http://surl.li/mrgbuq
11) Наведіть порядок-http://surl.li/wossso
12) Вікторина «Виграй або програй»- http://surl.li/qkwfxk

В результаті дослідження проведено аналіз платформи Wordwall та її можливостей у контексті логопедичної діяльності. Платформа є потужним інструментом для створення інтерактивних завдань, що сприяють розвитку мовленнєвих навичок у дітей з порушеннями мовлення.

Wordwall є зручним у використанні інструментом для логопедів завдяки простим у застосуванні шаблонам, що дозволяють створювати різноманітні інтерактивні завдання. Платформа підвищує мотивацію учнів завдяки ігровому підходу до навчання, що робить процес навчання більш захопливим і продуктивним.

Важливим аспектом є сумісність платформи з різними пристроями (комп'ютери, планшети, телефони), що дозволяє використовувати її як у класичному, так і в дистанційному форматі занять. Серед недоліків варто відзначити обмежені можливості безкоштовної версії платформи, що знижує доступ до більш широкого спектра шаблонів та інструментів [2].

Таким чином, Wordwall може стати важливим інструментом у роботі логопедів, проте для повноцінного використання усіх його можливостей необхідно розглянути варіант платної підписки.

ДЖЕРЕЛА

1. Освітня платформа «Вчимо» // [Електронний ресурс] - Режим доступу: **https://vchymo.com/app/application/WordWall**.
2. Вигівська Н. С. Педчитання на тему: «Використання онлайн іструменту WordWall під час проведення уроків виробничого навчання» - Полтавський професійний ліцей, Міністерство освіти і науки України - 2024.

ВИКОРИСТАННЯ СОЦІАЛЬНОЇ МЕРЕЖІ FACEBOOK У ТВОРЧІЙ ДІЯЛЬНОСТІ ФАХІВЦІВ З РЕКЛАМИ І ЗВ'ЯЗКІВ З ГРОМАДСЬКІСТЮ

Ятленко Ю. В., Лемещенко Є. А., Гаргуша П. В., Брик А. А., Лановенко Д. В.
Київський столичний університет імені Бориса Грінченка, м. Київ

У сучасному світі багато людей прагнуть розвиватися у творчих напрямках, створюючи сучасний особистий контент, який є оригінальним, якісним і привертає увагу. Для цього чудово підходить така платформа, як Facebook. Facebook – це багатофункціональна соціальна мережа, яка служить не тільки для спілкування, але й для професійного використання. Платформа дозволяє створювати контент для реклами, взаємодіяти з аудиторією, аналізувати дані та впроваджувати маркетингові стратегії [1].

Facebook надає всі необхідні інструменти для роботи з текстом, зображеннями, відео, опитуваннями, прямими трансляціями тощо. Вона також інтегрується з іншими популярними сервісами, такими як Instagram і Messenger, що робить її ще більш зручною для роботи в команді та масштабування проектів. Facebook є потужною платформою для комунікації, реклами та створення контенту. Ця соціальна мережа використовується не лише для особистого спілкування, а й для професійних цілей у сфері реклами, PR та маркетингу.

Основні функції та інструменти Facebook:

- групи та спільноти: створення груп для обговорення PR-кампаній, обміну досвідом і пошуку партнерів.
- Facebook Pages (Сторінки): можливість брендам, компаніям чи особам створювати сторінки для просування своїх послуг або продуктів.
- реклама та таргетинг: інструменти для налаштування рекламних кампаній з широким вибором параметрів (геолокація, інтереси, вік, стать тощо).
- інтеграція контенту: можливість інтегрувати фото, відео, опитування, прямі трансляції та статті, що сприяє залученню аудиторії.

Основні можливості Facebook:

Контент різного типу:

- текстові публікації.
- зображення та відео.
- прямі трансляції.
- опитування та інтерактивні формати.
- Інструменти для командної роботи: можливість спільного управління сторінками та розподіл ролей серед команди (адміністратор, модератор, редактор).
- Аналіз даних: інструменти аналітики для вимірювання охоплення, залучення та ефективності контенту.
- Реклама та таргетинг: широкі можливості для налаштування реклами, орієнтованої на конкретну аудиторію.
- Хмарне зберігання: уся інформація та дані зберігаються у хмарі, що дозволяє працювати з будь-якого пристрою.

Використання в професійній діяльності:

- Управління PR-кампаніями: Facebook використовується для створення подій, управління спільнотами та поширення інформації серед цільової аудиторії.
- Просування бренду: завдяки зручним рекламним форматам можна ефективно просувати продукти та послуги.
- Інтерактивна взаємодія: прямі трансляції, опитування та інші інструменти сприяють створенню інтерактивного контенту, що залучає користувачів.

Відмітимо деякі головні переваги та недоліки Facebook та представимо їх у таблиці 1.

Таблиця 1

Головні переваги та недоліки Facebook

Переваги:	*Недоліки:*
Хмарне збереження даних: Вся інформація доступна з будь-якого пристрою, синхронізується між акаунтами	Необхідність постійного інтернет-з'єднання: Для роботи з контентом або спілкування у Facebook потрібен стабільний доступ до мережі
Інструменти аналізу: Детальна аналітика (охоплення, залучення, кількість кліків) дозволяє вимірювати ефективність кампаній	Конкуренція за увагу: Велика кількість контенту у стрічці потребує унікальності реклами для залучення аудиторії
Спільна робота: Командна взаємодія через облікові записи адміністраторів сторінок	Платний доступ до ефективного охоплення: Безкоштовні методи просування обмежені; для значного охоплення потрібні інвестиції у рекламу
Глобальна аудиторія: Facebook дозволяє охопити користувачів з усього світу	

Популярність Facebook як інструменту у сфері реклами та PR зростає завдяки його багатофункціональності та можливості роботи з глобальною аудиторією. Це зручна платформа для створення, управління та просування контенту, яка має потужні інструменти для аналітики та налаштування рекламних кампаній.

ДЖЕРЕЛА

1. Що таке Facebook? [Електронний ресурс]. Режим доступу: https://uk.wikipedia.org/wiki/Facebook (дата звернення 18.11.2024 р.)

Секція 2
АПАРАТНЕ І ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ПРОЄКТУВАННЯ ІНФОРМАЦІЙНОЇ ВЕБ-ПЛАТФОРМИ ДОКУМЕНТООБІГУ АГЕНЦІЇ НЕРУХОМОСТІ

Андрущенко Є. Є
Київський столичний університет імені Бориса Грінченка, м. Київ

Сучасні агенції нерухомості мають в роботі велику кількість документів, що містять дані про договори оренди, об'єкти нерухомості, купівлі-продажу та клієнтів. Методи документообігу, такі як паперові архіви чи електронні таблиці, є малоефективними, застарілими та схильними до помилок, також такі методи ускладнюють оперативний доступ до необхідної інформації.

У зв'язку з цим виникає потреба у створенні централізованої інформаційної веб-платформи документообігу для агентств нерухомості, яка дозволить автоматизувати процеси зберігання, пошуку, редагування та спільного доступу до документів. Така система покликана підвищити ефективність роботи агентства, знизити ризики втрати даних і покращити взаємодію між співробітниками та клієнтами [1].

Мета роботи є розробка веб-платформи для управління документами агенції нерухомості, що забезпечить автоматизацію процесів та підвищення рівня безпеки а також буде використовувати нові методи роботи з документами, що покращить роботу з ними та підвищить рівень безпеки.

Для досягнення цієї мети необхідно вирішити наступні завдання:

1) Створити єдину систему для роботи з документами, де їх можна буде зберігати, передавати та переглядати.
2) Додати блокчейн для фіксації угод, щоб усі зміни зберігалися в захищеному реєстрі, який неможливо підробити.
3) Використовувати цифровий підпис, щоб підтверджувати справжність документів і надавати їм юридичну силу.
4) Налаштувати рівні доступу для користувачів, щоб лише уповноважені особи могли переглядати чи змінювати документи.
5) Автоматизувати створення звітів і контроль змін, щоб можна було відстежувати, хто і коли редагував документи.

Для виконання роботи необхідно реалізувати структуровану систему документообігу, яка включатиме модель класів та архітектурну схему. Це

дозволить забезпечити зручне управління документами, контроль доступу, безпечне зберігання та аудит змін.

Модель класів:

1) User (користувач): містить інформацію про роль, права доступу користувача. [3]

2) Document (документ): включає дані: (назва, автор, статус, дата створення).

3) Transaction (операція): відображає зміни, внесені до документа.

4) AuditLog (журнал дій): реєструє всі операції користувачів.

5) EncryptionService (служба шифрування): забезпечує захист даних.

6) BlockchainModule (модуль блокчейн-реєстрації угод) відповідає за збереження інформації про угоди у розподіленому реєстрі, що забезпечує їхню незмінність та прозорість [2].

Структурна схема системи складається з наступних компонентів:

1) Клієнтський рівень: веб-інтерфейс (Angular).

2) Серверний рівень: Spring Boot (Java).

3) База даних: PostgreSQL реляційна БД з підтримкою складних зв’язків між сутностями

4) Система контролю доступу: рольова модель RBAC [3].

5) Модуль блокчейн-реєстрації угод: Цей компонент інтегрує блокчейн у документообіг, щоб забезпечити захист від змін і шахрайства [2].

Запропонована інформаційна веб-платформа дозволяє автоматизувати процеси документообігу агенції нерухомості, підвищити безпеку та надійність зберігання даних. Використання блокчейн-реєстрації угод забезпечує прозорість операцій та захист від підробок, а цифровий підпис гарантує достовірність документів. Даний підхід сприяє підвищенню ефективності роботи агенції та спрощенню взаємодії між сторонами угоди.

ДЖЕРЕЛА

1) Гілюта М.І. Розробка інформаційної веб- платформи на основі технологій C # для автоматизації документообігу транспортного підприємства: дипломна робота на здобуття освітнього ступеня «магістр» за спеціальністю «121 –інженерія програмного забезпечення» / М.І. Гілюта . –Тернопіль: ТНТУ, 2019. –125 с. https://elartu.tntu.edu.ua/handle/lib/30658

2) Когут Ю. Технології блокчейн та криптовалюта: ризики та кібербезпека. Сідкон, 2022.

3) Role Mining in Business: Taming Rose-Based Access Control Administration. World Scientific Publishing Co Pte Ltd, 2012.

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ В ІНТЕЛЕКТУАЛЬНОЇ СИСТЕМИ МОНІТОРИНГУ ВНЕСКУ РОЗРОБНИКІВ У ПРОГРАМНІ ПРОЕКТИ

Беро В. Ф.
Державного університету інформаційно-комунікаційних технологій, м. Київ

Із розвитком інформаційних технологій, зокрема платформ для колективної розробки програмного забезпечення, зросла потреба в захищених інструментах для збору та аналізу даних про активність учасників проєктів [2]. Особливої актуальності набуває питання забезпечення безпеки даних під час використання таких інструментів, оскільки йдеться про доступ до акаунтів розробників, історії комітів та внутрішньої структури проєктів [1; 2].

Метою даного дослідження є розробка та впровадження заходів для забезпечення конфіденційності інформації в програмному забезпеченні «Інтелектуальна система моніторингу внеску розробників у програмні проєкти». Для досягнення цієї мети було застосовано підхід, що включає як технологічні рішення, так і організаційні механізми. Зокрема, передбачено ізоляцію середовища виконання за допомогою Docker-контейнерів, захист конфіденційних даних через використання змінних середовища та шифрування, а також контроль доступу до API за допомогою токенів авторизації.

Розробка продукту передбачає використання наступних технічних засобів і методів захисту:

– Контейнеризація за допомогою Docker. Забезпечує ізоляцію виконання компонентів системи, обмежуючи доступ до системних ресурсів та файлової системи хоста [2].

– Використання .env. Використання змінного середовища .env для безпечного зберігання конфігураційних параметрів, токенів доступу до API Git та облікових даних message-broker [1; 2].

– Використання RabbitMQ. Використання брокера повідомлень RabbitMQ для розподілу завдань між мікросервісами, з можливістю обмеження доступу до черг через політики безпеки [2].

– Оновлення. Регулярне оновлення залежностей та Docker-образів з урахуванням актуальних патчів безпеки [2].

– Bearer Token. Авторизація на основі токенів для обмеження доступу до зовнішнього та внутрішнього API системи, а також реалізація механізмів перевірки автентичності користувача [1].

– Хешування паролів до системи. Для збереження облікових даних застосовується алгоритм хешування з додаванням унікальної солі за допомогою бібліотеки «bcrypt», що ускладнює атаки метою перебору [3].

Методологія дослідження.

Дослідження базується на системному аналізі сучасних методів забезпечення інформаційної безпеки в десктопних програмних системах, з особливим акцентом на ізоляцію середовища виконання, безпечне зберігання конфігураційних даних та захищену взаємодію з API зовнішніх сервісів. Використання Docker-контейнерів, Flask API, message-брокера [1; 2].

Результати та переваги реалізації.

Контейнеризація забезпечила ізоляцію процесів і захист від доступу до системних ресурсів хост-машини. Зберігання токенів і паролів у Docker Secrets або .env-файлах з обмеженим доступом мінімізувало ризики витоку облікових даних. Авторизація доступу до API за допомогою токенів. Крім цього, автоматизоване оновлення даних та логування взаємодій із зовнішніми сервісами дозволяє вчасно виявляти підозрілу активність або технічні збої.

Розроблений набір заходів захисту даних є критично важливою складовою роботи інтелектуальної системи моніторингу. Впровадження ізоляції середовища виконання, авторизації через токени, захищеного зберігання конфігураційних файлів, системного моніторингу та логування взаємодій забезпечує комплексний захист на всіх рівнях. Подальше вдосконалення безпеки системи може включати реалізацію двофакторної автентифікації (2FA) [1], розмежування прав доступу до окремих компонентів системи.

ДЖЕРЕЛА

1. Grinberg, M. (2018). Flask Web Development: Developing Web Applications with Python. O’Reilly Media.

2. Turnbull, J. (2014). *The Docker Book: Containerization is the new virtualization*. James Turnbull.

3. Хешування паролів: використання солі та bcrypt. [Електронний ресурс]. Режим доступу: https://drukarnia.com.ua/articles/kheshuvannya-paroliv-vikoristannya-soli-ta-bcrypt

РОЗРОБКА СИСТЕМИ МОНІТОРИНГУ ЗДОРОВ'Я

Білан М. П.

Київський столичний університет імені Бориса Грінченка, м. Київ

У сучасних умовах стрімкого розвитку цифрових технологій важливим завданням є розробка ефективних систем для моніторингу та прогнозування стану здоров’я людини. Такі системи дозволяють здійснювати безперервне спостереження за фізіологічними параметрами організму, аналізувати дані в реальному часі та прогнозувати можливі відхилення.

Метою цієї роботи є створення системи, яка інтегрує сенсорні пристрої, засоби передачі даних, алгоритми обробки інформації та методи прогнозування з використанням штучного інтелекту. Основна увага приділяється зручності використання, точності прогнозування та захисту персональних даних користувача.

Архітектура системи включає в себе такі компоненти: сенсорний модуль для збору фізіологічних даних (пульс, тиск, рівень кисню в крові), модуль передачі даних (Bluetooth/Wi-Fi), серверну частину для зберігання та аналізу даних, а також клієнтський застосунок для візуалізації інформації.

Алгоритми прогнозування базуються на методах машинного навчання, зокрема використовується градієнтний бустинг, рекурентні нейронні мережі (RNN) та метод опорних векторів (SVM). Тренування моделей здійснюється на основі анонімізованих медичних даних, що дозволяє підвищити точність прогнозів

Впровадження такої системи може бути корисним як для хронічних пацієнтів, людей похилого віку, так і для спортсменів і звичайних людей. Вона забезпечує раннє виявлення проблем, зменшує навантаження на лікарів та підвищує ефективність медичного обслуговування.

Подальші дослідження передбачають вдосконалення алгоритмів прогнозування, інтеграцію з медичними базами даних та оптимізацію інтерфейсу користувача.

ДЖЕРЕЛА

1. **Müller, M., & Maier, M. (2017).** *Health Monitoring Systems for Chronic Patients: An Overview of State-of-the-Art and Future Trends*. Journal of Health Technology, 23(3), 345-358.

2. **Thompson, J., & Roberts, L. (2019).** *Wearable Sensors and Their Application in Health Monitoring*. Journal of Biomedical Engineering, 12(5), 210-223.

3. **Raj, R., & Kumar, S. (2021).** *Artificial Intelligence in Health Monitoring Systems: A Review of Techniques and Applications*. IEEE Transactions on AI in Healthcare, 8(4), 101-112.

4. **Kumar, A., & Sharma, V. (2020).** *Predictive Models for PTSD Detection in Military Personnel: A Review of Approaches and Algorithms*. Journal of Military Medicine, 45(2), 55-68.

5. **Zhao, X., & Lin, Y. (2022).** *Data Privacy and Security in Health Monitoring Systems: A Comprehensive Survey*. Security and Privacy in Health Technologies, 5(1), 18-33.

6. **Lee, J., & Kim, M. (2021).** *Telemedicine and Remote Monitoring: A Solution for Military Health*. Journal of Military Health, 39(3), 104-118.

7. **Sun, W., & Zhang, L. (2018).** *Machine Learning Algorithms for Health Monitoring and Early Diagnosis*. International Journal of Medical Informatics, 123(2), 45-58.

8. **Vasilenko, O., & Panchenko, D. (2020).** *Integration of Wearable Devices with Artificial Intelligence for Health Monitoring Systems*. International Journal of Computational Health, 14(4), 78-89.

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ СИСТЕМИ ТА ЇХ ЗАХИСТ В ЕЛЕКТРОННІЙ КОМЕРЦІЇ: АРХІТЕКТУРНІ РІШЕННЯ ТА НОРМАТИВНО-ПРАВОВІ АСПЕКТИ

Бондаренко Д.
Київський столичний університет імені Бориса Грінченка, м. Київ

Інформаційно-комунікаційні системи (ІКС) є базовою технологічною платформою сучасної електронної комерції, відіграючи вирішальну роль у забезпеченні безперервної цифрової взаємодії між продавцем і покупцем незалежно від їхньої фізичної локалізації. Завдяки розвитку ІКС стало можливим здійснення комерційних транзакцій у реальному часі, що істотно прискорює обмін товарами, послугами та інформацією на глобальному ринку.

Інтенсивне зростання обсягів онлайн-торгівлі обумовлює зростання ризиків, пов’язаних із витоком персональних і фінансових даних користувачів, що, у свою чергу, вимагає дотримання суворих стандартів безпеки, визначених як міжнародними нормами, так і національним законодавством. Актуальні кіберзагрози, такі як фішинг, SQL-ін’єкції, атаки типу «відмова в обслуговуванні» (DoS), XSS-атаки, вимагають від розробників онлайн-магазинів впровадження комплексних заходів захисту [1].

Стійкість і безпека вебресурсів, що мають відкритий доступ до Інтернету, є критичними факторами їхньої надійної роботи. Це передбачає створення багаторівневих систем захисту, здатних ефективно протидіяти як зовнішнім, так і внутрішнім загрозам безпеки.

Архітектурні рішення сучасних онлайн-магазинів дедалі частіше ґрунтуються на концепції SPA (Single Page Application), що передбачає побудову односторінкових застосунків із використанням сучасних вебтехнологій:

- **Фронтенд**: реалізується на базі фреймворку React.js, який забезпечує створення динамічного, інтерактивного інтерфейсу користувача та оптимізує взаємодію із сервером.

- **Бекенд**: побудований на платформі Node.js із використанням ORM Sequelize для ефективної роботи з базами даних та побудови безпечних API.
- **База даних**: використовується PostgreSQL – одна з найбільш надійних і масштабованих систем управління базами даних з відкритим кодом.

Комплексна система безпеки охоплює всі рівні архітектури та включає:

- **На рівні фронтенду**: впровадження протоколу HTTPS для шифрування даних при передачі, застосування політик CORS для обмеження доступу до API лише з авторизованих джерел, захист від XSS-атак шляхом санітизації введених даних і використання спеціалізованих бібліотек, таких як DOMPurify, а також мінімізація та обфускація JavaScript-коду для ускладнення його зворотної інженерії[2].
- **На рівні бекенду**: забезпечення аутентифікації та авторизації користувачів за допомогою сучасних протоколів безпеки (JWT, OAuth 2.0), захист від SQL-ін'єкцій через параметризовані запити, реалізація механізмів обмеження частоти запитів (rate limiting) і контролю доступу (middleware), а також впровадження систем журналювання подій (Winston, Morgan) для забезпечення аудиту та моніторингу безпекових інцидентів [3;4].
- **На рівні бази даних**: застосування технологій шифрування (наприклад, Transparent Data Encryption, шифрування окремих полів), реалізація принципу мінімізації прав доступу користувачів (principle of least privilege), регулярне створення резервних копій баз даних і моніторинг активності для своєчасного виявлення аномалій.

Відповідно до чинного законодавства України, функціонування інтернет-магазинів вимагає:

- Повного інформування споживача про товар та продавця.
- Можливості укладення електронних договорів відповідно до вимог закону.
- Реєстрації на державному порталі «е-покупець» для отримання статусу перевіреного продавця, що покликано підвищити рівень довіри покупців і забезпечити прозорість торгівлі.

Попри численні переваги електронної комерції, серед яких варто відзначити оперативність обслуговування, можливість персоналізованих пропозицій, оптимізацію витрат і розширення ринків збуту, існують певні ризики. Серед них – ймовірність придбання неякісної продукції, шахрайські схеми, проблеми з логістикою та необхідність забезпечення постійного вдосконалення захисту інформаційних систем.

Комплексний підхід до захисту інформації онлайн-магазинів дозволяє не лише відповідати чинним нормативно-правовим вимогам, але й створює умови для підвищення довіри споживачів, зміцнення репутації

бренду та забезпечення довгострокової стабільності бізнесу в умовах цифрової трансформації суспільства.

ДЖЕРЕЛА

1. ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements. International Organization for Standardization, 2013.

2. Mozilla Foundation. HTTPS and TLS [Електронний ресурс]. – Режим доступу: https://developer.mozilla.org/en-US/docs/Web/Security/HTTP_strict_transport_security.

3. OWASP Foundation. Cross Site Scripting (XSS) [Електронний ресурс]. – Режим доступу: https://owasp.org/www-community/attacks/xss/.

4. Auth0. JWT Handbook [Електронний ресурс]. – Режим доступу: https://auth0.com/learn/json-web-tokens/.

ЗАСТОСУВАННЯ СУЧАСНОГО СТЕКУ ТЕХНОЛОГІЙ У СЕРВІСІ ДОСТАВКИ ЇЖІ

Василевський С. О.

Київський столичний університет імені Бориса Грінченка, м. Київ

У сучасному світі онлайн-доставка їжі стала важливою складовою повсякденного життя, однак цей сектор стикається з рядом проблем, що впливають на якість обслуговування, зручність користування та ефективність бізнес-процесів [1, с. 1–3].

Однією з головних проблем є безпека платежів і захист персональних даних. Онлайн-оплати мають бути захищені від шахрайства та хакерських атак, які загрожують як користувачам, так і бізнесу [2]. Також важливо забезпечити стабільну роботу веб-платформи та мобільного додатку – збої, повільне завантаження чи погана оптимізація для мобільних пристроїв можуть знижувати кількість замовлень і задоволеність клієнтів.

Сервіси доставки повинні ефективно взаємодіяти з партнерами, синхронізуючи меню, наявність товарів і статуси замовлень у реальному часі. Без цього можливі помилки, як-от замовлення недоступних страв або неточні терміни доставки [2]. Важлива й персоналізація сервісу: збереження улюблених позицій, зручне відстеження замовлень і персоналізовані рекомендації – їх відсутність знижує конкурентоспроможність платформи.

Отже, метою роботи стала розробка веб-застосунку, що надає користувачеві можливість швидко та зручно замовляти їжу з актуальною інформацією про меню, ціни та час доставки. Для цього обрано сучасні технології, що забезпечують високу продуктивність, безпеку та масштабованість. Для створення динамічного, відзивчивого інтерфейсу

використовується бібліотека React, яка завдяки віртуальному DOM дозволяє швидко оновлювати вміст сторінки. Авторизацію реалізовано через JWT-токени, що забезпечує безпечний доступ до ресурсів без передачі логіна і пароля з кожним запитом. Технологія WebSockets дозволяє миттєво оновлювати статуси, відображати зміни та реалізовувати чати. Передача платіжних даних здійснюється через захищені HTTPS-запити. Як веб-сервери використовуються Apache та Nginx – вони забезпечують ефективну обробку запитів і балансування навантаження. Інфраструктура базується на AWS: EC2 для розгортання серверів, RDS для реляційних баз даних, що дозволяє легко масштабувати систему під потреби проєкту.

Було створено діаграму класів UML для моделювання системи:

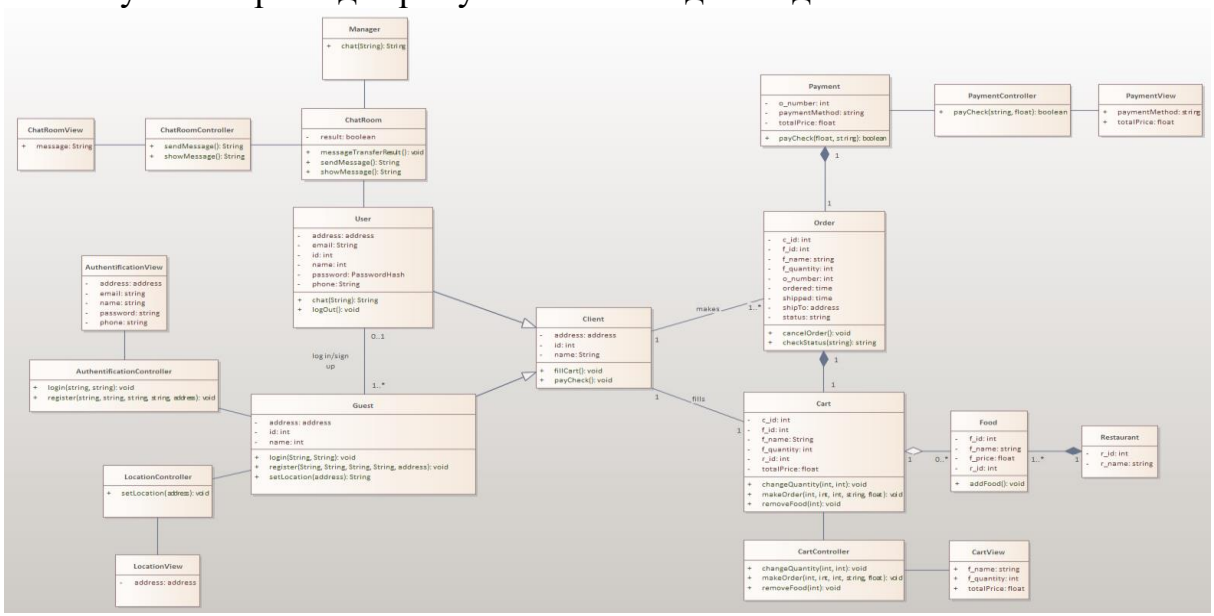


Рис.1. Діаграма класів

Діаграма класів відображає модель системи для онлайн-замовлення їжі, включаючи користувачів, замовлення, оплату та управління чатом. Основними класами є User, Guest, Client, які взаємодіють із замовленнями (Order), кошиком (Cart) та оплатою (Payment). Client може створювати замовлення та оплачувати їх. Cart дозволяє змінювати кількість товарів та оформляти замовлення. Food та Restaurant представляють їжу та ресторани. AuthenticationController та LocationController керують реєстрацією та місцезнаходженням користувачів.

Дана робота запропонувала новий стек технологій для ефективного веб-застосунку замовлення їжі. У результаті можна помітити, що застосунок відзначається зручним та адаптивним інтерфейсом, швидкою та безпечною обробкою замовлень, а також інтеграцією реального часу для покращення взаємодії між клієнтами, кур'єрами та адміністраторами. Завдяки масштабованій інфраструктурі він здатний ефективно працювати

при зростаючому навантаженні, забезпечуючи стабільність і надійність сервісу.

ДЖЕРЕЛА

1. Stanford University. URL: https://web.stanford.edu/~leinav/teaching/Collison.pdf (date of access: 30.03.2025).

2. Izraylevych I. How to Build a Meal Ordering and Delivery Platform?. Medium. URL: https://igorizraylevych.medium.com/how-to-build-a-meal-ordering-and-delivery-platform-bca418008c46 (date of access: 30.03.2025).

РОЗРОБКА АВТОМАТИЗОВАНОГО ІНСТРУМЕНТА ДЛЯ ІНТЕГРАЦІЇ ДАНИХ З РІЗНИХ ДЖЕРЕЛ З МЕТОЮ АНАЛІЗУ ТА ВІЗУАЛІЗАЦІЇ

Гусак С. Л.

Київський столичний університет імені Бориса Грінченка, м. Київ

У сучасних умовах глобалізації фінансових ринків, які характеризуються високою непередбачуваністю, критично важливим стає оперативний доступ до актуальних фінансових даних. Дослідження показують, що своєчасна фінансова інформація значно покращує здатність інвесторів приймати ефективні рішення та реагувати на ринкові зміни [1]. Ефективне управління інвестиціями вимагає не лише фінансової грамотності, але й оперативного доступу до актульних даних, що підтверджується дослідженнями про вплив фінансової обізнаності на прийняття інвестиційних рішень [2; 3].

Саме тому необхідним рішенням є автоматизація об’єднання даних з різних джерел в одному місці для їх аналізу.

Розроблений автоматизований інструмент забезпечує інвесторів можливістю отримати зручний інструмент для аналізу даних, що надходять з різних джерел, зокрема ExchangeRate-API, Yahoo Finance та Binance. Інструмент реалізує повний цикл ETL-процесу (Extract-Transform-Load), який включає отримання даних через API-запити, очищення структурування із застосуванням бібліотеки pandas, отримання даних про котирування акції відбувається через бібліотеку yfinance. Усі дані зберігаються в уніфікованому вигляді у форматі .csv, після чого завантажуються у базу даних Supabase (на базі PostgreSQL).

Для забезпечення швидкого та стабільного доступу до даних створено REST API з використанням фреймворку FastAPI. Кінцевим користувачам надано зручний веб-інтерфейс, розроблений за допомогою технології Streamlit. Інтерфейс дозволяє переглядати графіки цін на акції, валютних курсів, вартості криптовалюти, використовувати різні типи діаграм, а також таблиці для порівняльного аналізу. Оновлювати дані

можна через натискання кнопки «Оновити» без необхідності перезапуску застосунку.

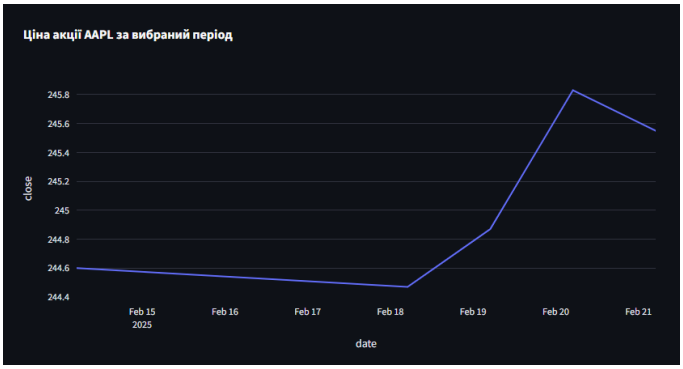


Рис. 1. Графік ціни на акції AAPL реалізований у Streamlit

Проведене порівняння існуючих рішень на ринку продемонструвало обмеженість популярних платформ, таких як Yahoo Finance або Investing.com у безкоштовних версіях, що суттєво звужує можливості інвесторів. Дослідження також свідчать, що більшість інвесторів мають обмежений доступ до детальної, якісної фінансової інформації, що впливає на якість ухвалення рішень [4].

Створення власного інструменту дозволяє уникнути цих обмежень, забезпечуючи повний контроль над процесом інтеграції та аналізу даних.

Розроблена система має суттєву практичну цінність, оскільки дозволяє інвесторам ефективніше керувати своїми активами, оперативно реагувати на зміни ринку та знижувати фінансові ризики. У перспективі планується розширення функціоналу системи шляхом інтеграції нових фінансових джерел та удосконалення аналітичних інструментів.

ДЖЕРЕЛА

1. Garrity J., O'Donnell J. B., Sanders G. C. Continuous Auditing and Data Mining – 2015.

2. Ahmed Z., Ramakrishnan S., Noreen U. Financial literacy as competitive advantage for individual investors' decision making // Advanced Science Letters. – 2017. – Vol. 23. – C. 8988–8993.

3. Zhang Y., Lu X., Xiao J. Does financial education help to improve the return on stock investment? Evidence from China // Pacific-Basin Finance Journal. – 2023.

4. Desoky A. The perceived importance of electronic sources of financial information to individual investors in Egypt: an empirical investigation // Afro-Asian Journal of Finance and Accounting. – 2010. – Vol. 2, № 1. – C. 70–87.

ЕФЕКТИВНІСТЬ ВИКОРИСТАННЯ PEER-TO-PEER ТЕХНОЛОГІЙ У СТРІМІНГОВИХ СЕРВІСАХ

Демченко Д. О., Савіцький Р. С.
Державний університет «Житомирська політехніка», м. Житомир

Онлайн-сервіси з відео за запитом (VOD) та прямими трансляціями (Live Streaming) постійно збільшують обсяги даних, що передаються користувачам, особливо під час масових подій –спортивних змагань, концертів чи запуску нових серіалів [1]. Для забезпечення стабільної якості зображення традиційно використовуються CDN (Content Delivery Network), витрати на які можуть складати відчутну частину бюджету компаній. За даними Sandvine, світовий інтернет-трафік відеоконтенту щороку зростає в середньому на 30–40%, тож пошук економічно вигідних технологій передавання даних стає критично важливим [2].

Використання P2P-моделі у стрімінгових сервісах дає можливість розподілити навантаження між користувачами: частина контенту поширюється безпосередньо з пристрою на пристрій, зменшуючи потребу у CDN та центральних серверах [3]. Таким чином знижуються витрати на оренду чи утримання інфраструктури – як мережевої, так і серверної.

Інтеграція P2P-механізмів у VOD та Live-стрімінгові сервіси може знизити сукупні витрати на серверну інфраструктуру та оренду пропускної здатності від 30% до 70% залежно від масштабу події [4]. За даними аналітичних звітів відомих CDN-провайдерів, розподіл навантаження між користувачами суттєво скорочує витрати на CDN-ресурси при масових онлайн-трансляціях, а у пікові періоди здатний зменшити використання серверних потужностей на 40–70% [5]. Перехід на P2P-підхід для масштабних трансляцій може окупитися протягом одного-двох років після впровадження завдяки зниженню обсягів традиційного трафіку на центральних серверах і, відповідно, зменшенню витрат на оренду чи утримання CDN.

Для конкретного прикладу розглянемо сервіс, який передає приблизно 100 ТБ (терабайтів) відеоданих на місяць. Припустимо, що середня вартість CDN-трафіку становить $0.05 за 1 ГБ (тобто $50 за 1 ТБ), то місячні витрати на доставку контенту будуть орієнтовно $5,000. Якщо P2P-технологія дозволяє скоротити використання CDN на 50%, то обсяг «централізованого» трафіку зменшується з 100 ТБ до 50 ТБ, а витрати –з $5,000 до $2,500 на місяць. Річна економія у такому сценарії складе близько $30,000 (без урахування додаткових витрат на розробку та підтримку P2P-рішень).

Незважаючи на економічну вигоду при використанні P2P рішень для відео стрімінгу, потрібно враховувати виклики й обмеження технології:

− початкові витрати на інтеграцію P2P-рішень у внутрішню інфраструктуру;

– нестабільність користувацьких вузлів (коливання швидкостей, відсутність гарантованого аптайму);

– необхідність додаткових механізмів безпеки та захисту контенту в розподілених мережах.

Впровадження P2P-рішень потребує попередньої технічної підготовки та фінансових інвестицій, потенційні довгострокові переваги у вигляді значних заощаджень на трафіку, підвищення масштабованості та конкурентоспроможності сервісу виправдовують ці витрати. У контексті стрімінгових платформ, які активно нарощують аудиторію, P2P-технології стають одним із найбільш перспективних напрямів оптимізації інфраструктурних витрат.

ДЖЕРЕЛА

1. Cisco Annual Internet Report (2018–2023) White Paper URL: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html (дата звернення 21.01.2025)

2. The Global Internet Phenomena Report January 2024 URL: https://www.sandvine.com/phenomena (дата звернення 21.01.2025)

3. Dehui Wei1, Jiao Zhang, Haozhe Li. Swarm: Cost-Efficient Video Content Distribution with a Peer-to-Peer System, 2024. URL: https://arxiv.org/pdf/2401.15839 (дата звернення 21.01.2025)

4. P2P Delivery Saves Network Bandwidth URL: https://www.hivestreaming.com/resources/p2p-efficiency-really-matters-save-network (дата звернення 21.01.2025)

5. Zhihui Lu, Ye Wang, Yang Richard Yang An Analysis and Comparison of CDN-P2P-hybrid Content Delivery System and Model. *JOURNAL OF COMMUNICATIONS, VOL. 7, NO. 3, MARCH 2012*. URL: https://www.jocm.us/uploadfile/2013/0416/20130416034901618.pdf (дата звернення 21.01.2025)

ТЕХНОЛОГІЇ СТВОРЕННЯ E-COMMERCE ПЛАТФОРМ

Дмитрієв В. Г., Рельке А. А.

Вінницький національний технічний університет, м. Вінниця

Сучасні технології електронної комерції активно розвиваються, пропонуючи бізнесу інноваційні можливості для розбудови онлайн-торгівлі. Ключовою основою для створення e-commerce платформ є хмарні сервіси, як-от AWS, Azure та Google Cloud, які забезпечують гнучку інфраструктуру, що автоматично масштабується залежно від навантаження. Це дозволяє бізнесу ефективно розподіляти обчислювальні ресурси та оптимізувати витрати на IT-інфраструктуру [1].

Мікросервісна архітектура трансформувала підхід до розробки онлайн-магазинів, забезпечуючи декомпозицію складних систем на незалежні компоненти. Така структура дозволяє командам розробників працювати паралельно над різними функціональними модулями, як-от системою пошуку, кошиком, обробкою замовлень чи персоналізованими рекомендаціями. Застосування контейнеризації та оркестрації за допомогою технологій Docker і Kubernetes забезпечує надійне розгортання та управління мікросервісами у різних середовищах.

Сучасні JavaScript-фреймворки – React, Angular, Vue.js – значно покращили користувацький досвід в e-commerce платформах [2]. Вони забезпечують швидке відображення інтерфейсу та миттєву реакцію на дії користувача, що критично важливо для конверсії відвідувачів у покупців. Технологія прогресивних веб-додатків (PWA) дозволила створювати e-commerce платформи, що функціонують подібно до нативних мобільних додатків, забезпечуючи швидкодію навіть при нестабільному інтернет-з'єднанні.

API-орієнтована архітектура є фундаментальним принципом розробки сучасних e-commerce платформ, що уможливлює безперешкодну інтеграцію з платіжними системами, логістичними сервісами, CRM та ERP-системами. REST API та GraphQL технології забезпечують ефективний обмін даними між різними компонентами екосистеми електронної комерції, створюючи єдиний безшовний процес для користувача.

Технології машинного навчання та аналізу даних стали невід'ємною частиною e-commerce платформ, забезпечуючи персоналізацію контенту, рекомендаційні системи та аналітику поведінки користувачів [3]. Вони дозволяють прогнозувати попит, автоматизувати ціноутворення та створювати персоналізовані маркетингові кампанії, що значно підвищує ефективність онлайн-продажів.

Безпека e-commerce платформ реалізується через впровадження протоколів шифрування, токенізації платіжних даних та багатофакторної автентифікації. Технології блокчейн поступово інтегруються в e-commerce системи для забезпечення прозорих і безпечних транзакцій, а також для реалізації програм лояльності на основі токенів [4].

У перспективі розвиток технологій створення e-commerce платформ спрямований на ще глибшу інтеграцію з Інтернетом речей, голосовими помічниками та системами штучного інтелекту, що забезпечить більш інтуїтивний та персоналізований процес онлайн-шопінгу.

Сучасні технології створення e-commerce платформ відкривають широкі можливості для розвитку онлайн-торгівлі, забезпечуючи ефективні рішення для бізнесу різного масштабу. Хмарні сервіси та мікросервісна архітектура формують гнучку інфраструктуру, що дозволяє оптимально розподіляти обчислювальні ресурси та швидко масштабувати e-commerce

системи відповідно до зростання бізнесу. Прогресивні веб-технології та JavaScript-фреймворки суттєво покращують користувацький досвід, створюючи інтуїтивно зрозумілі інтерфейси з миттєвою реакцією на дії користувача. API-орієнтована архітектура забезпечує безперешкодну інтеграцію з різними сервісами та системами, формуючи цілісну екосистему електронної комерції. Комплексне застосування цих технологій створює основу для розбудови конкурентоспроможних e-commerce платформ, здатних задовольнити потреби як продавців, так і покупців у динамічному цифровому середовищі.

ДЖЕРЕЛА

1. Романюк О. Н., Романюк О. В., Чехместрук Р. Ю. Комп'ютерна графіка: електронний навчальний посібник. Вінниця : ВНТУ, 2023. 147 с. URL: https://ir.lib.vntu.edu.ua/handle/123456789/37689 (дата звернення: 28.04.2025).
2. Developer JavaScript frameworks URL: https://developer.mozilla.org/en-US/docs/Learn_web_development/Core/Frameworks_libraries (дата звернення: 29.04.2024).
3. Denovo Що таке Machine Learning? URL: https://denovo.ua/resources/what-is-machine-learning (дата звернення: 29.04.2024).
4. Debut Infotech Blockchain in Ecommerce: The Future of Online Shopping URL: https://www.debutinfotech.com/blog/blockchain-in-ecommerce (дата звернення: 29.04.2024).

ТЕХНОЛОГІЧНІ АСПЕКТИ ВПРОВАДЖЕННЯ ІНТЕЛЕКТУАЛЬНИХ ТРАНСПОРТНИХ СИСТЕМ У МІСЬКІЙ ІНФРАСТРУКТУРІ НА ОСНОВІ IOT, AI ТА ХМАРНИХ ТЕХНОЛОГІЙ

Довженко Н. М.[1,2], Іваніченко Є. В.[1], Мазур Н. П.[1]
[1] Київський столичний університет імені Бориса Грінченка, м. Київ
[2] Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м. Київ

Сучасні інтелектуальні транспортні системи (ITC) ґрунтуються на впровадженні передових технологій, таких як штучний інтелект (AI), Інтернет речей (IoT) та аналіз великих даних (Big Data). Використання IoT-пристроїв, зокрема сенсорів, камер спостереження, лічильників трафіку та GPS-трекерів, дозволяє збирати, обробляти та аналізувати великі масиви інформації в реальному часі. Своєю чергою це сприяє оперативному реагуванню на зміну дорожніх умов, ефективному управлінню

транспортними потоками та підвищенню рівня інформаційної безпеки під час передачі критичних даних [1; 2].

Однак обробка таких значних обсягів інформації потребує не лише потужних інструментів зберігання, аналітики та інтелектуальних алгоритмів для прийняття швидких управлінських рішень у режимі реального часу, але й надійних засобів захисту даних на всіх етапах їх обробки. Архітектура інтелектуальної транспортної системи (Рис. 1) базується на багаторівневій структурі збору, обробки та аналізу даних для ефективного управління міським транспортом[1; 3].

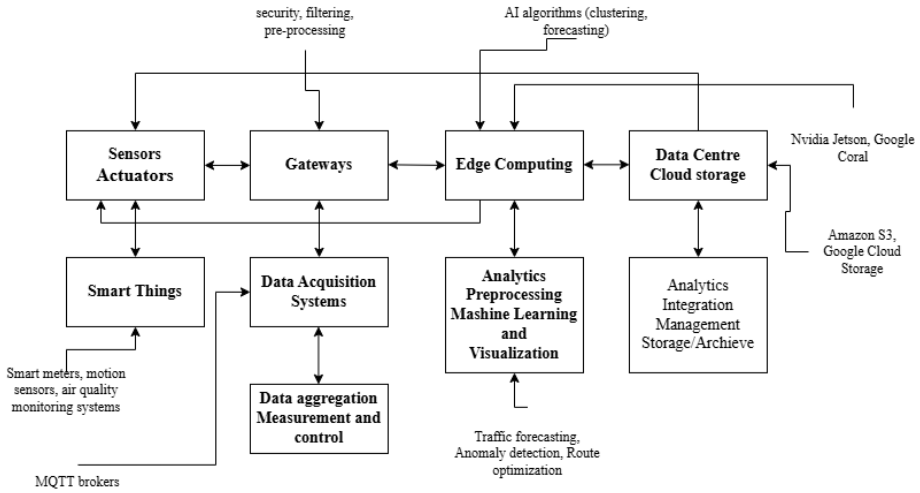


Рис.1. Архітектура інтелектуальної транспортної системи

Перший етап «Збір і підготовка даних». Інфраструктура IoT включає датчики, виконавчі пристрої та розумні об'єкти (Smart Things), що фіксують інформацію про транспортні потоки, якість повітря та інші параметри. Зібрані дані надходять до шлюзів, де проходять первинну обробку (фільтрацію, безпеку, попередню аналітику).

Другий етап «Обробка, аналітика та передача даних». Дані передаються до периферійних обчислювальних систем (Edge Computing), де застосовуються алгоритми машинного навчання для прогнозування трафіку, виявлення аномалій та оптимізації маршрутів.

Третій етап «Інтеграція даних і управління». Оброблені дані спрямовуються в хмарне середовище (Data Centre/Cloud Storage), де відбувається довгострокове зберігання, аналітика та інтеграція.

Четвертий етап «Реакція та виконання рішень». Інформація використовується для динамічного керування транспортними потоками – адаптації світлофорів, маршрутизації транспорту та оновлення дорожніх повідомлень.

П’ятий етап «Підсумковий аналіз і оптимізація». Система аналізує накопичені дані для вдосконалення управління трафіком, оптимізуючи маршрути на основі аварійної статистики та довгострокових тенденцій (пікові години, небезпечні ділянки).

Таким чином, побудова інтелектуальної транспортної системи в умовах «розумного міста» є складним, але необхідним завданням. Забезпечення безперервної інтеграції IoT-пристроїв, використання хмарних технологій для зберігання та обробки великих даних, застосування сучасних методів AI для прогнозування та управління трафіком, впровадження механізмів захисту інформації, а також ефективна й безпечна комунікація між компонентами системи в режимі реального часу дозволять суттєво підвищити ефективність роботи міської транспортної інфраструктури та задовольнити зростаючі потреби урбаністичних середовищ [1; 2].

ДЖЕРЕЛА

1. Довженко, Н., Мазур, Н., Складанний, П., Костюк, Ю., Рзаєва, С. (2024). *Інтеграція IoT та штучного інтелекту в інтелектуальні транспортні системи.* Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(26), 430–444. https://doi.org/10.28925/2663-4023.2024.26.708

2. Dovzhenko N., Barabash O., Ausheva A., Ivanichenko Y., Obushnyi S.. *Comprehensive Analysis of Efficiency and Security Challenges in Sensor Network Routing.* CEUR Workshop Proceedings, Volume 3550, Cybersecurity Providing in Information and Telecommunication Systems, CPITS-II 2023. Pp. 275-280.

3. Dovzhenko N., Haidur H., Brzhevska Z., Ivanichenko Y., Nesterova O. *Method of Sensor Network Functioning under the Redistribution Condition of Requests between Nodes.* CEUR Workshop Proceedings. Volume 3421, Cybersecurity Providing in Information and Telecommunication Systems, CPITS 2023. Pp. 278–283.

ПОРІВНЯННЯ RS485 ТА RJ45 В КОНТЕКСТІ ПРОТОКОЛУ ПЕРЕДЕАЧІ ДАНИХ MODBUS

Ємельянов В. Б.

Державний університет інформаційно-комунікаційних технологій, м. Київ

При виборі технології комунікації для роботи додатку який збирає та аналізує дані з аналізаторів мережі, виникають питання відповідоності кожної технології до вимог частки ринку на яку орієнтуєтсья додаток і компанія яка його виробляє.

Для реалізації програмного забезпечення, що збирає та аналізує дані з мережевих аналізаторів, важливо обрати ефективний і доступний спосіб фізичного з’єднання пристроїв, сумісний з протоколом Modbus [1]. Найпоширенішими варіантами для реалізації Modbus є RS485 (Modbus RTU) [2; 3] та RJ45 (Modbus TCP) [4; 5]. Задачею дослідження є порівняння цих двох інтерфейсів у контексті реального проєкту – розробки

універсального програмного забезпечення для роботи з бюджетними аналізаторами, поширеними на ринку України. Провести техніко-економічне порівняння фізичних інтерфейсів RS485 і RJ45 у контексті передачі даних за протоколом Modbus, визначити доцільність використання одного з них у розробці програмного забезпечення для мережевих аналізаторів.

У ході розробки реального комерційного проєкту для компанії було виявлено такі ключові особливості:

1. Вартість: 100 метрів 8-жильної витої пари (кабель під RJ45) коштує значно дорожче, ніж аналогічна довжина кабелю для RS485. Крім того, Ethernet-адаптери та комутатори мають вищу ціну в порівнянні з простими RS485-конвертерами.

2. Дальність передачі: RS485 забезпечує передачу даних на відстань до 1200 метрів без ретрансляторів, тоді як стандарт RJ45 (Ethernet) обмежений 100 метрами без активного обладнання.

3. Сумісність: більшість бюджетних аналізаторів, присутніх на ринку України, мають вбудований порт RS485, а моделі з Ethernet (RJ45) або відсутні, або значно дорожчі. Тобто RS485 – універсальніший варіант.

4. Стабільність та кількість підключень: RS485 дозволяє побудову шини з 32 пристроїв без хабів або маршрутизаторів. RJ45 потребує більш складної мережевої інфраструктури.

5. Простота підключення: RJ45 забезпечує простоту через стандартизований роз’єм «одним клацанням», що зручно для швидкого монтажу та обслуговування, особливо для користувачів без досвіду.

Враховуючи ці фактори, у розробці було прийнято рішення на користь RS485, оскільки клієнти прагнуть мінімізувати витрати та використовувати наявне обладнання.

Інтерфейс RS485 продемонстрував себе як економічно доцільніше, універсальне та стабільне рішення для передачі даних за протоколом Modbus у промислових умовах. Його використання дозволяє спростити логістику, знизити витрати та забезпечити надійний зв’язок на великих відстанях.

Надалі передбачається розвиток програмного забезпечення з підтримкою обох протоколів (Modbus RTU та Modbus TCP), що дозволить охопити більший сегмент ринку пристроїв.

ДЖЕРЕЛА

1. Modbus Plus protocol overview / D. Reynders та ін. Practical Industrial Data Communications. 2004. С. 336–339. URL: https://doi.org/10.1016/b978-075066395-3/50026-7 (дата звернення: 30.04.2025).

2. Frenzel L. E. RS-485. Handbook of Serial Communications Interfaces. 2016. С. 117–119. URL: https://doi.org/10.1016/b978-0-12-800629-0.00028-0 (дата звернення: 30.04.2025).

3. Soto C. Modbus RTU Design : Begin to Set up and Interface: Modbus Rtu Implementation Guide. Independently Published, 2021.

4. Rutronik introduce the new UTS RJ45 connector. Microelectronics International. 2009. Т. 26, № 1. URL: https://doi.org/10.1108/mi.2009.21826aad.007 (дата звернення: 30.04.2025).

5. Coutu M. Technicians Guide to Modbus TCP. Independently Published, 2020.

ВЕБ-СЕРВІС ДЛЯ АНАЛІЗУ РИНКУ НЕРУХОМОСТІ

Зайцев І. В.

Київський столичний університет імені Бориса Грінченка, м. Київ

У сучасному суспільстві, що стрімко розвивається в умовах цифровізації, аналіз ринку нерухомості набуває особливої актуальності. Завдяки використанню сучасних інформаційних технологій, зокрема web-сервісів, з’являється можливість оперативного збору, аналізу та прогнозування даних про ринок нерухомості. Це дозволяє інвесторам, агентствам та кінцевим користувачам приймати більш зважені рішення при купівлі, продажу або оренді об’єктів нерухомості [1; 2].

Ефективний аналіз ринку сприяє оптимізації операцій, підвищенню прозорості та зниженню ризиків, пов’язаних з інвестиціями. Розробка web-сервісу на платформі Ruby on Rails забезпечує не лише високу продуктивність і безпеку, але й можливість масштабування системи при роботі з великими обсягами даних. Сучасні рішення часто орієнтовані виключно на агрегацію та візуалізацію інформації, тоді як інтеграція інтелектуальних алгоритмів для прогнозування ринкових тенденцій залишається малоефективною. У дослідженнях, наприклад, Сірманс та ін. [3] було показано, що застосування гедонічного аналізу дозволяє отримати більш точну оцінку вартості нерухомості, а класична робота Geltner та ін. [4] демонструє комплексний підхід до аналізу комерційного ринку.

Метою дослідження є розробка web-сервісу для аналізу ринку нерухомості, який забезпечить автоматизований збір, обробку та прогнозування даних з використанням сучасних алгоритмів аналізу та візуалізації.

Об’єкт дослідження – ринок нерухомості як економічна система, що включає процеси купівлі, продажу та оренди житлових і комерційних об’єктів.

Предмет дослідження – інструменти, технології та алгоритми для збору, аналізу та прогнозування ринкових даних, а також інтеграція цих методів у web-сервіс на базі Ruby on Rails.

Для досягнення поставленої мети необхідно виконати наступні завдання:

- Провести аналіз сучасних методів збору та обробки даних про нерухомість.
- Визначити ключові параметри, що впливають на динаміку змін вартості об’єктів нерухомості.
- Розробити алгоритми прогнозування ринкових тенденцій з використанням статистичних методів та технологій машинного навчання.
- Спроектувати архітектуру web-сервісу на базі Ruby on Rails із забезпеченням масштабованості та високої продуктивності.
- Провести тестування системи на реальних даних для оцінки точності прогнозів та зручності користування.

Запропонований сервіс вирізняється інтеграцією модулів аналітики та прогнозування, що дозволяє в режимі реального часу оновлювати інформацію та надавати користувачам рекомендації для прийняття оптимальних інвестиційних рішень.

ДЖЕРЕЛА

1. Ruby on Rails Guides. (n.d.). https://guides.rubyonrails.org/
2. Ruby, S., Thomas, D., & Hansson, D. (2019). *Agile Web Development with Rails 6*. Pragmatic Bookshelf. Retrieved from https://pragprog.com/titles/rails6/agile-web-development-with-rails-6/
3. Sirmans, G. S., MacPherson, J. M., & Zietz, E. N. (2005). The Composition of Residential Property Values: A Hedonic Analysis. *Journal of Real Estate Finance and Economics, 30*(4), 435–466.
4. Geltner, D., Miller, N. G., Clayton, J., & Eichholtz, P. (2007). *Commercial Real Estate: Analysis and Investment*. John Wiley & Sons

РОЗРОБКА ЧАТ-БОТА З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ПІДТРИМКИ КОРИСТУВАЧІВ У ЗАКЛАДАХ ГРОМАДСЬКОГО ХАРЧУВАННЯ

Ільяш Н. С.
Київський столичний університет імені Бориса Грінченка, м. Київ

Автоматизація обслуговування клієнтів є важливою складовою цифрової трансформації бізнесу. Використання чат-ботів у сфері громадського харчування сприяє підвищенню ефективності обслуговування, зменшенню навантаження на персонал, прискоренню обробки замовлень та покращенню взаємодії з клієнтами [1].

Метою дослідження є розробка інтелектуального чат-бота для автоматизації підтримки клієнтів у закладах громадського харчування.

Автори визначили завдання дослідження:

– Проаналізувати потреби клієнтів закладів громадського харчування.

– Дослідити існуючі рішення та визначити їхні переваги та недоліки.
– Обрати оптимальні технології для реалізації чат-бота.
– Розробити модуль обробки природної мови (NLP).
– Інтегрувати чат-бот із системами замовлення та базами даних.
– Провести тестування та оцінити ефективність розробленого рішення.

Об’єкт дослідження – чат-бот для підтримки користувачів у закладах громадського харчування.

Предмет дослідження – методи штучного інтелекту та обробки природної мови (NLP) для розробки чат-бота.

Для досягнення поставленої мети використовувалися такі методи дослідження. як:

– Аналіз літератури – дослідження наукових джерел, присвячених розробці чат-ботів та застосуванню штучного інтелекту.
– Порівняльний аналіз – вивчення існуючих чат-ботів для закладів громадського харчування.
– Проєктування – розробка архітектури чат-бота, бази знань та інтеграційних модулів.
– Експериментальний метод – тестування розробленого чат-бота в реальних умовах [4].

Було розроблено чат-бот, що включає наступні функціональні можливості:

– Автоматичний прийом замовлень у чаті.
– Надання відповідей на поширені запитання клієнтів.
– Рекомендації щодо вибору страв та напоїв.
– Обробка скарг і пропозицій клієнтів.
– Збір зворотного зв’язку та аналіз даних про замовлення.

Розроблений чат-бот ефективно справляється з прийомом замовлень, наданням інформації про меню та акції, а також обробкою зворотного зв’язку клієнтів. Тестування підтвердило відповідність системи заявленим вимогам, а також виявило можливості для подальшого покращення, такі як розширення функціоналу за рахунок інтеграції з платіжними сервісами та CRM-системами закладів громадського харчування [3].

Отже, дослідження підтвердило, що використання чат-ботів у сфері громадського харчування є ефективним способом автоматизації клієнтського обслуговування та значно підвищує рівень обслуговування клієнтів. Впровадження такого рішення сприяє підвищенню рівня сервісу, прискоренню комунікації з клієнтами та оптимізації витрат бізнесу. Аналіз наукової літератури та існуючих рішень підтвердив, що інтеграція штучного інтелекту дозволяє покращити якість комунікації та мінімізувати витрати підприємств на персонал [2]. Таким чином, результати роботи

демонструють перспективність використання чат-ботів у ресторанному бізнесі та їхню здатність покращувати клієнтський досвід.

ДЖЕРЕЛА

1. Андрющенко В. А., Петроченко С. О. Основи створення чат-ботів з використанням платформи Dialogflow. Інформаційні технології. 2021. №2. С. 18-25.
2. Гудименко О. В. Штучний інтелект: основи теорії і практики. Київ: Наукова думка, 2018. – 348 с.
3. Jurafsky D., Martin J. H. Speech and Language Processing. 3rd edition. Pearson, 2019.
4. Таненко Ю. Л., Семенов А. П. Використання Telegram API для створення чат-ботів. Збірник наукових праць студентів. 2021. №6. С. 45-50.

РОЗРОБКА WEB-САЙТУ ДЛЯ ПРОВЕДЕННЯ ЕЛЕКТРОННИХ ГОЛОСУВАНЬ З ВИКОРИСТАННЯМ БЛОКЧЕЙН ТЕХНОЛОГІЙ

Іщук М.О
Державний університет інформаційно-комунікаційних технологій, м. Київ

Електронне голосування відіграє важливу роль у сучасному суспільстві, надаючи низку переваг порівняно з традиційними методами. Електронне голосування дозволяє громадянам голосувати з будь-якого місця, де є доступ до інтернету, що особливо важливо для людей з обмеженими можливостями; швидко підрахувати результати голосування, що зменшує час очікування та ризик помилок. Слід відмітити також економічну складову електронного голосування: зменшуються витрати на організацію виборів, пов'язані з друком бюлетенів, роботою виборчих комісій та іншими логістичними аспектами. Однак, важливо враховувати потенційні ризики, пов’язані з кібербезпекою та необхідністю забезпечення таємниці голосування. Цим і підтверджується розробка web-сайту для проведення електронних голосувань з використанням блокчейн технологій. У сучасному світі, де довіра до традиційних систем голосування зменшується, блокчейн стає новою віхою у забезпеченні прозорості, захисту даних та відсутності фальсифікацій.

Блокчейн –це розподілений реєстр, або децентралізована база даних, яка забезпечує незмінність, прозорість та безпеку збереження інформації [1]. Архітектура блокчейн додатку представлено на рис. 1.

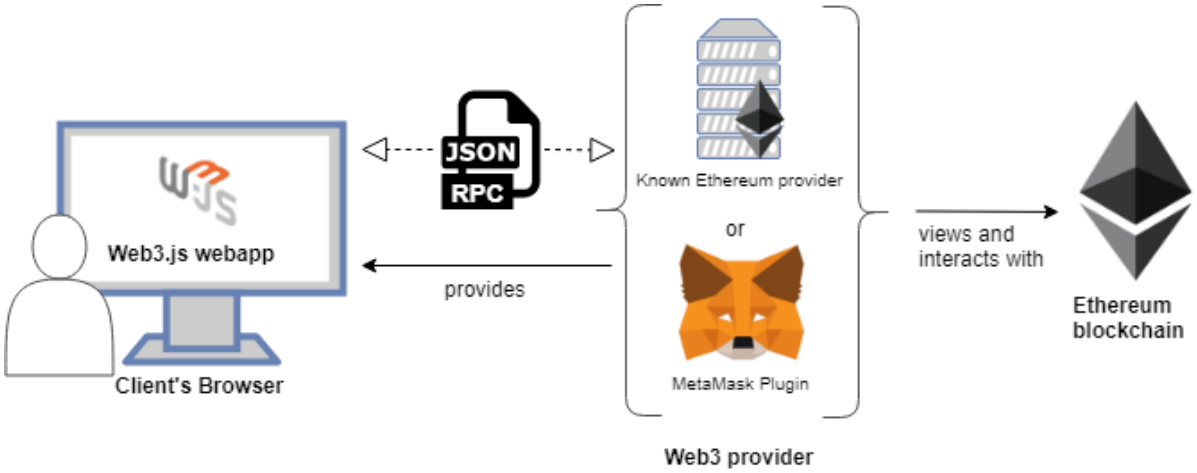


Рис.1. Архітектура блокчейн додатку [2]

У центрі взаємодії перебуває браузер користувача, в якому виконується клієнтський додаток, реалізований із використанням Web3.js. Основна роль Web3.js у цій системі –надання API, через яке клієнтський застосунок надсилає запити до блокчейн-мережі. Ці запити оформлюються у форматі JSON-RPC –легковагового протоколу віддаленого виклику процедур, що дозволяє уніфіковано взаємодіяти з вузлом Ethereum (Ethereum node).

Інтеграція бібліотеки Web3.js з мовою програмування TypeScript забезпечує типобезпечне програмування при створенні децентралізованих додатків (DApp), що взаємодіють з блокчейном Ethereum. TypeScript надає сувору типізацію, що дозволяє розробникам виявляти помилки ще до виконання коду, покращуючи надійність і знижуючи кількість помилок при роботі з Web3 API. При використанні Web3.js у TypeScript-проєктах потрібно врахувати, що типи для Web3 не повністю охоплюють весь API, тому розширення типів є обов'язковим кроком.

Web3-провайдер виконує критично важливу роль –він є посередником між клієнтським додатком, який працює у браузері користувача, та Ethereum-блокчейном. У контексті електронного голосування на базі блокчейну, правильний вибір і використання Web3-провайдера напряму впливає на безпеку, функціональність та зручність застосунку. Провайдери реалізують функціональність комунікації з мережею Ethereum, зокрема забезпечують надсилання транзакцій, читання стану блокчейну, підписання повідомлень та взаємодію зі смарт-контрактами.

React реалізує компонентно-орієнтований підхід, що дозволяє модульно побудувати інтерфейс голосування: кожен елемент UI –форма голосування, статус голосу, таймери, результати –створюється як незалежний компонент, який можна повторно використовувати та легко тестувати. Завдяки цьому забезпечується висока гнучкість розробки та зменшується складність підтримки проєкту.

У підсумку, блокчейн Ethereum є остаточним пунктом усіх транзакцій та запитів, здійснених через клієнтський застосунок. Він виконує роль децентралізованого сховища, у якому зберігаються всі дані у незмінному вигляді, забезпечуючи таким чином прозорість, достовірність і відмовостійкість системи. Така архітектура дозволяє реалізувати повноцінні децентралізовані рішення, зокрема у сфері електронного голосування, де критичним є питання довіри, верифікації та збереження анонімності.

ДЖЕРЕЛА

1. Ковальчук Л.В., Кудін А.М., Кучинська Н.В. Вступ до технології блокчейн та криптовалют. Київ. КПІ ім. Ігоря Сікорського. 2022.
2. Ethereum Book on Github. URL:https://github.com/ethereumbook/ethereumbook/issues/376

ВИВЕДЕННЯ ВИСНОВКІВ (INFERENCE) МАШИННОГО НАВЧАННЯ НА КОРИСТУВАЦЬКИХ ПРИСТРОЯХ

Карлов Є. О.
Київський столичний університет імені Бориса Грінченка, м. Київ

За останні роки відбулося стрімке зростання інтеграції технологій машинного навчання та штучного інтелекту у смартфони, планшети, вбудовані пристрої та інші користувацькі платформи. Завдяки вдосконаленим алгоритмам та потужності сучасних пристроїв все більше додатків можуть здійснювати виведення висновків (inference) без необхідності постійного з’єднання з серверною інфраструктурою [1].

Переваги виведення висновків (inference) машинного навчання на користувацьких пристроях:

- Безпека користувацьких даних. Локальне виконання обчислень дозволяє зменшити передачу чутливої інформації через мережу, що сприяє покращенню захисту приватності.
- Швидкість виконання. Оскільки обчислення проводяться безпосередньо на пристрої, затримки, пов’язані з мережею, значно зменшуються, що забезпечує миттєве реагування.
- Незалежність від Інтернету. Застосунки можуть функціонувати в режимі офлайн, що є особливо важливим у зонах з поганим або відсутнім доступом до мережі.
- Безкоштовність. Використання локальних ресурсів може знизити витрати на серверну інфраструктуру та передачу даних, що робить рішення більш економічно ефективними для кінцевих користувачів.

Недоліки виведення висновків (inference) машинного навчання на користувацьких пристроях:

- Збільшений розмір застосунку. Вбудовані моделі машинного навчання часто займають значну частину пам’яті, що може призводити до збільшення розміру застосунку.
- Збільшене навантаження на пристрій. Інтенсивні обчислення можуть спричиняти перевантаження пристрою, що впливає на його продуктивність та енергоефективність, особливо при тривалому використанні.

Для виведення висновків (inference) на користувацьких пристроях розробники використовують спеціалізовані інструменти, що дозволяють оптимізувати модель для роботи в умовах обмежених ресурсів та надають набір засобів розробки для різних мов програмування. До найбільш популярних відкритих технологій можна віднести LiteRT від Google, Core ML від Apple та ExecuTorch від Linux Foundation [2].

Для ефективного виконання завдань машинного навчання, зокрема виведення висновків (inference), та зменшення навантаження на центральний і графічний процесори, на сучасні пристрої виробники вбудовують спеціальні процесори: NPU (Neural Processing Unit). Серед провідних компаній, які інтегрують NPU у свої настільні рішення, варто відзначити Apple з чипами серії M, AMD з лінійкою Ryzen AI та Intel з процесорами Core Ultra. Також NPU мають топові моделі мобільних процесорів Snapdragon від Qualcomm, Exynos від Samsung і Tensor від Google [3].

Виведення висновків (inference) машинного навчання безпосередньо на користувацьких пристроях має значні переваги та забезпечує перспективу подальшої інтеграції передових технологій машинного навчання та штучного інтелекту в щоденне життя користувачів, незважаючи на виклики, які дедалі ефективніше долаються розробниками апаратних рішень.

ДЖЕРЕЛА

1. Nandanwar A. Revolutionizing Consumer Electronics with the power of AI Integration. URL: https://moschip.com/blog/semiconductor/revolutionizing-consumer-electronics-with-the-power-of-ai-integration/ (date of access: 16.04.2025).
2. How can you optimize machine learning models for devices with limited resources? URL: https://www.linkedin.com/advice/1/how-can-you-optimize-machine-learning-models-devices-7v8zc (date of access: 16.04.2025).
3. Martindale J. NPU Explained: Why Neural Processing Units Are the Future of AI. URL: https://www.lifewire.com/what-is-a-neural-processing-unit-npu-11704394 (date of access: 16.04.2025).

РОЗРОБКА ПРОГРАМИ ДЛЯ ANDROID ДЛЯ ЗАПОБІГАННЯ КІБЕРБУЛІНГУ

Кліщ А. Р.
Державний університет інформаційно-комунікаційних технологій, м. Київ

Сучасний цифровий світ створює нові виклики, серед яких особливо гострою проблемою став кібербулінг. В Україні, за даними ЮНІСЕФ [1], понад 40% підлітків 12–17 років стикалися з різними формами психологічного тиску в Інтернеті. Найпоширенішими проявами є публічне приниження у соцмережах, розповсюдження компромату та систематичні образи у месенджерах. Як зазначають експерти Центру громадського здоров'я [2], лише 15–20% постраждалих звертаються за допомогою через страх осуду або незнання дій.

У відповідь на цю проблему було розроблено Android-додаток, що поєднує інформаційний ресурс, самодіагностику та швидкий доступ до служб допомоги. Реалізація здійснена мовою Kotlin із використанням Android SDK, що забезпечує сумісність із більшістю пристроїв.

Ефективна профілактика кібербулінгу, як зазначає «Київстар» [3], включає освітню, діагностичну та оперативну складові. Додаток містить опис видів кібербулінгу, алгоритми дій, тест на рівень агресивності (20 питань), а також інтеграцію з гарячою лінією (0 800 500 225).

Рис.1. Результати тестування Android-додатку проти кібербулінгу

У результаті тестування серед 100 користувачів, 82% позитивно оцінили інтерфейс, а 78% зазначили, що краще розуміють природу кібербулінгу. Це підтверджує важливість таких цифрових рішень у боротьбі з проблемою.

ДЖЕРЕЛА

1. ЮНІСЕФ Україна. Кібербулінг: як захистити свою дитину. URL: https://www.unicef.org/ukraine/cyberbullying

2. Центр громадського здоров'я. Кібербулінг: що робити? URL: https://phc.org.ua/news/kiberbuling-scho-robiti-koli-vas-abo-vashu-ditinu-ckuyut-v-interneti

3. Київстар. Кібербулінг: що це таке і як захистити свою дитину. URL: https://kyivstar.ua/uk/cybersecurity/kiberbuling-shcho-ce-ta-yak-uberegty-dytynu

АНАЛІЗ ВЕБ-ДОДАТКІВ УПРАВЛІННЯ АВІАКОМПАНІЄЮ ТА ПРОДАЖУ КВИТКІВ

Кобилко М. П., Вакалюк Т. А

Державний університет «Житомирська політехніка», м.Житомир

У сучасному світі технології стали невід'ємною частиною багатьох галузей, в тому числі і авіації. Система управління авіакомпанією є важливим інструментом для забезпечення ефективної роботи авіаперевезень. Вона охоплює багато функцій, що включають як оперативне управління рейсами, так і обслуговування пасажирів.

Враховуючи важливість зручності для користувачів, було здійснено аналіз сервісів для бронювання квитків на прикладі сайтів трьох популярних авіакомпаній: Wizz Air**,** Lufthansa та Ryanair**.**

Сайт авіакомпанії Wizz Air [1] має інтерфейс, що орієнтований на швидкий пошук та бронювання квитків. Користувач з першої сторінки має можливість обрати напрямок, дату та кількість пасажирів для пошуку необхідного рейсу. Система швидко генерує результати, що вказує на оптимізований пошуковий механізм, імовірно із застосуванням попередньо кешованих маршрутів. Також з переваг можна зазначити динамічну зміну ціни, що адаптується до попиту. Однак, функціональна логіка побудована таким чином, що на кожному кроці бронювання користувачу пропонуються багаточислені додаткові послуги, наприклад - підписка на клубні програми, це значно ускладнює навігацію.

Ryanair [2] – ще одна популярна система бронювання квитків на рейси. Перевагами Ryanair є простий та зручний інтерфейс, варіативність у виборі додаткових послуг, можливість перегляду доступних рейсів та вибору місць на борту.

З недоліків можна зазначити, що навіть при відмові від додаткових послуг іноді відбувається їх повторна пропозиція, при тому, відсутній будь-який спосіб пропустити цей етап.

Lufhansa [3] – сайт авіакомпанії з більш комплексною системою управління для пасажирів з додатковими послугами та можливостями. Сайт має різноманітний функціонал, що включає вибір валюти, мови та

навіть пропозицій залежно від геолокації користувача. Даний веб-сервер містить адаптивність під різні пристрої: десктопна і мобільна версії, інтерфейс яких динамічно адаптується під роздільну здатність, при цьому зберігаючи повну функціональність.

Крім того, на відміну від Wizz Air чи Ryanair, де етап платежу часто змішується з додатковими пропозиціями, тут оплата винесена в окремий завершальний блок з підтвердженням усіх даних та можливістю їх редагування.

Перевагами Lufhansa також можна зазначити системи накопичення миль та програми лояльності, що стимулюють повторні покупки.

Після аналізу наявних веб-платформ авіаперевізників, можна сформулювати основні вимоги до системи управління майбутньої авіакомпанії, а саме до клієнтської сторони. Враховуючи всі переваги та недоліки наявних рішень, пропонуються наступні характеристики до розроблюваного майбутнього програмного забезпечення:

1. Зрозумілі, чіткі та послідовні етапи бронювання квитків з можливістю повернення до попереднього кроку без втрати введених раніше даних.
2. Простий та інтуїтивно зрозумілий інтерфейс, який має забезпечувати швидкий доступ до основних функцій.
3. Створення особистого кабінету користувача при реєстрації з можливістю перегляду історії бронювань, збереження напрямків та персональних даних.
4. Забезпечення високої швикості роботи та стабільності. Адже це є важливим кроком для оптимізації запитів та збереження часу завантаження.
5. Інтеграція з різними платіжними системами та забезпечення підтримки банківських карток та цифрових гаманців.

Майбутнє програмне забезпечення має бути зручним для користувачів. Також є важливим аби система ефективно підтримувала всі внутрішні процеси авіакомпанії.

ДЖЕРЕЛА

1. Wizz Air [Електроний ресурс]. – Режим доступу: https://www.wizzair.com/uk-ua
2. Rynair [Електроний ресур]. – Режим доступу: https://www.ryanair.com/ua/uk
3. Lufhansa [Електроний ресурс]. – Режим доступу: https://www.lufthansa.com/ua/en

АРХІТЕКТУРНІ ПІДХОДИ ДО ПОБУДОВИ СИСТЕМИ УПРАВЛІННЯ АВІАКОМПАНІЄЮ

Кобилко М. П., Вакалюк Т. А

Державний університет «Житомирська політехніка», м.Житомир

У наш час, в епоху цифрових інновацій, інформаційні технології відіграють важливу роль в організації та оптимізації усіх процесів в авіаційній індустрії. Ця сфера є складною та усі механізми авіакомпанії вимагають високоточності та відсутності будь-яких помилок. Створення автоматизованих рішень сприяє підвищенню ефективності та якості обслуговування пасажирів.

Одним з оптимальних підходів до реалізації подібних систем є реалізація багаторівневої архітектури у веб-застосунку. Наприклад, клієнт-серверну модель, що реалізована відповідно до шаблону MVC (Model-View-Controller) [1], із застосуванням REST API та технологічно стеку Spring [2].

Система управління авіакомпанії забезпечує керування різними складовими, такими як: рейси, літаки та їх конфігурації, аеропорти, працівники та пасажири тощо. Функціонально програма поділяється на три частини та містить адміністративний модуль, клієнтський інтерфейс та модуль для пілотів і стюардес.

Адміністративний блок дозволяє додавати нові літаки та їх конфігурації. Це визначає розміщення сидінь, що враховується під час генерації квитків для кожного рейсу. Адміністратор також має можливість додавати аеропорти, створювати та редагувати рейси, призначати робітників та літаки на рейси (після чого відбувається автоматична генерація квитків). Зі сторони пасажирів можливий перегляду рейсів та купівлі квитків на них. А зі сторони робітників – перегляд своїх призначень на рейс та розклад.

Архітектура побудована згідно з шаблоном Model-View-Controller (MVC), що дозволяє логічно розділити компоненти системи за функціональним призначенням: моделями, контролерами та інтерфейсом для пасажира.

Контролери (Controller) відповідають за маршрутизацію HTTP-запитів та обробку взаємодії між клієнтом і сервером.

Модель (Model) описує об'єкти, які відображають структуру таблиць у базі даних. Взаємодія з ними здійснюється через репозиторії Spring Data JPA - інструмент, який спрощує запити, абстрагуючи їх від низькорівневого SQL-коду. За необхідності є можливість написати власні запити, що забезпечує гнучкість у реалізації складніших операцій.

Також використовується ORM-фреймворк Hibernate для перетворення об'єктів на реляційні таблиці та навпаки [3, с. 19].

Саме він реалізує об’єктно-реляційне відображення, забезпечуючи ефективну інтеграцію з реляційною СУБД.

Представлення (View) реалізується на клієнтській стороні системи, де отримуються дані від сервера через REST API.

Особливу увагу слід приділити підтримці високого рівня безпеки. Розділення ролей (адміністратор, працівник, пасажир) в системі відбувається через механізми автентифікації та авторизації, з обов’язковим шифруванням даних. Для цього в архітектурі веб-додатку використовуються Spring Security, що відповідає за управління доступом до різних частин системи. Також реалізується шифрування паролів і захищає чутливі дані під час їх передачі через HTTPS, що гарантує безпечну комунікацію між клієнтом і сервером.

Для підвищення безпеки автентифікації та авторизації також використовуються JWT (JSON Web Tokens). Сервер генерує створення JWT токена після успішної автентифікації користувача у веб додатку. Він містить необхідну інформацію про користувача та його роль у системі. А також підписується за допомогою секретного ключа і передається в заголовку HTTP запитів при кожному доступі до ресурсів. Використання JWT також дозволяє уможливлює безперервну ідентифікацію без необхідності зберігання сесій на сервері.

Також слід зазначити, що для забезпечення стабільності та надійності системи використовується автоматизоване тестування. Наприклад unit-тести та інтеграційні тести. Це дозволяє своєчасно виявляти помилки на ранніх етапах розробки. При введенні нових змін у систему, можна гарантувати швидку та безпомилкову інтеграцію оновлень без порушень стабільності роботи системи.

Таким чином, клієнт-серверна модель з використанням архітектури MVC та REST API забезпечує чітке розділення обробки даних на сервері та відображення інтерфейсу на клієнтській стороні. Завдяки чому, у майбутньому можна реалізувати систему лояльності для клієнтів, програму знижок для працівників чи динамічну зміну ціни на квитки залежно від попиту тощо. Чітке розділення компонентів у проєкті дозволяє локалізовано змінювати або доповнювати окремі частини системи без впливу на її загальну функціональність.

ДЖЕРЕЛА

1. MVC [Електроний ресурс]. – Режим доступу: https://developer.mozilla.org/en-US/docs/Glossary/MVC

2. Spring Boot Documentation [Електроний ресурс]. – Режим доступу: https://spring.io/

3. Tudose, C. Java Persistence with Spring Data and Hibernate / C. Tudose, C. Bauer, G. King, G. Gregory. –Revised and extended new ed. – Shelter Island: Manning Publications Co., 2023.

РОЗРОБКА МОДЕЛІ ПРЕДМЕТНОЇ ГАЛУЗІ ЗАСТОСУНКУ ДЛЯ ПІДТРИМКИ НАВЧАННЯ ПРОФЕСІЙНИХ ОЦІНЮВАЧІВ КАВИ

Козачок К. Ю.
Державний університет інформаційно-комунікаційних технологій, м. Київ

У сучасних умовах розвитку кавової індустрії зростає потреба у професійній підготовці дегустаторів кави (Q-грейдерів), які відіграють ключову роль у контролі якості продукту. Цей процес вимагає ефективних цифрових рішень для навчання, тестування та оцінювання. Створення спеціалізованого застосунку дозволить автоматизувати ці етапи, підвищити точність оцінювання знань і забезпечити єдиний підхід до підготовки фахівців у галузі сенсорної оцінки кави[3].

Постановка задачі.

Процес навчання професійних оцінювачів кави потребує якісної цифрової підтримки, яка б охоплювала підготовку, оцінювання та аналіз результатів. Для побудови такого застосунку необхідно розробити модель предметної галузі, яка б відображала ключові сутності, зв'язки та функціональність, пов'язані з навчанням, тестуванням і оцінюванням студентів.

Мета дослідження.

Метою дослідження є створення інформативної моделі предметної галузі у вигляді діаграми для майбутнього застосунку, що підтримує процеси навчання та оцінювання знань професійних дегустаторів кави (Q-грейдерів).

Результати дослідження.

В результаті було побудовано діаграму предметної галузі, яка описує взаємозв'язки між основними сутностями системи. Зокрема, діаграма включає такі ключові елементи[1-2]:

- **CoffeeTest** – тестові матеріали, що охоплюють інформацію про каву.
- **Coffee** – об'єкти оцінювання, які мають текстовий опис і назву.
- **Question** – питання, що пов'язані з кавовими тестами й входять до складу білетів.
- **Ticket** – білети, які формуються з питань і призначаються студентам.
- **Answer** – варіанти відповідей до питань, серед яких зазначено правильний.
- **Evaluation** – оцінки, які формуються оцінювачем на основі відповідей на питання.
- **Report** – звіт про результати, що формується для кожного білету.
- **Student** – студенти, що проходять тестування.

- **Evaluator** – оцінювачі, які перевіряють відповіді студентів.
- Додаткові сутності (**TicketCreator**, **QuestionCreator**) відповідають за створення вмісту для тестів.

Дана діаграма дозволяє наочно відобразити структуру та логіку роботи системи підтримки навчання дегустаторів кави, встановити коректні зв'язки між об'єктами та забезпечити підґрунтя для розробки бази даних і логіки майбутнього застосунку.

Структуру інформаційної моделі навчального застосунку для оцінювачів кави можна подати у вигляді діаграми предметної області, яка демонструє основні сутності системи та взаємозв'язки між ними (див. рис. 1).

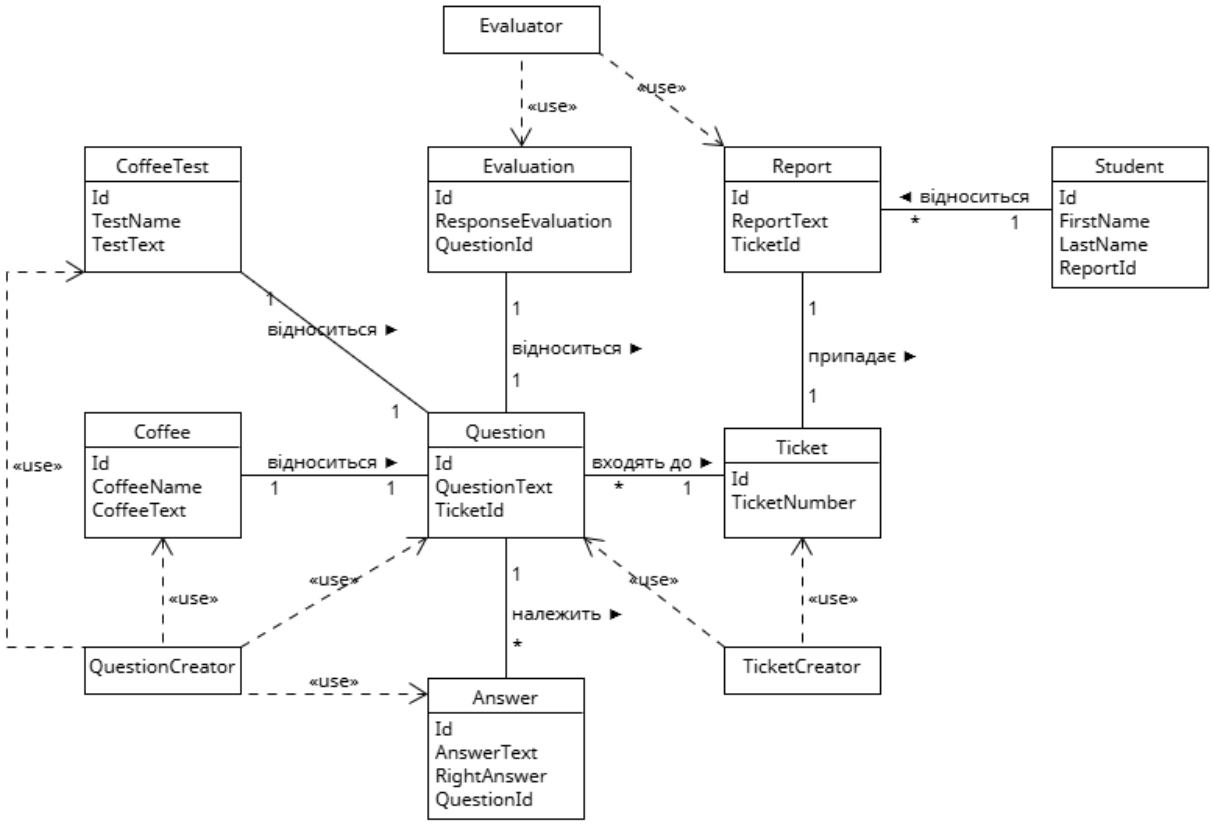


Рис. 1. Діаграма предметної області застосунку

Розроблена модель предметної галузі дозволяє точно описати процеси взаємодії між студентами, оцінювачами, білетами, запитаннями та оцінками. Надалі ця модель може бути використана для проєктування бази даних, створення веб- або мобільного застосунку для тестування, аналітики та сертифікації оцінювачів кави. Перспективи подальшої роботи полягають у реалізації застосунку, що базується на створеній моделі та впровадженні його у навчальний процес.

ДЖЕРЕЛА

1. UMLetino - *Online UML Tool*. URL: https://www.umletino.com/umletino.html
2. Unified Modeling Language - *Overview*. URL: https://www.uml-diagrams.org.
3. Specialty Coffee Association - *Coffee Taster's Flavor Wheel*. URL: https://sca.coffee/research/coffee-tasters-flavor-wheel.

РОЗРОБКА ФУНКЦІОНАЛЬНОСТІ ЗАСТОСУНКУ ДЛЯ ПІДТРИМКИ НАВЧАННЯ ПРОФЕСІЙНИХ ОЦІНЮВАЧІВ КАВИ

Козачок К. Ю.

Державний університет інформаційно-комунікаційних технологій, м. Київ

У наш час зростає потреба в сучасних засобах підтримки професійного навчання, зокрема в галузі спеціалізованих дегустаційних практик. Для професійних оцінювачів кави важливо мати доступ до структурованої інформації, систематичних тренувань та інструментів для перевірки знань. Застосунок із відповідною функціональністю дозволяє автоматизувати та покращити процес навчання, забезпечуючи інтерактивну взаємодію між викладачем і студентом, а також підтримку навчальних матеріалів і тестування [1].

Постановка задачі

Задачею дослідження є розробка функціональності застосунку, який підтримує навчання професійних оцінювачів кави шляхом автоматизації процесів тестування, оновлення матеріалів та видачі квитків для оцінки.

Мета дослідження

Визначення ключових вимог до функціональності застосунку, його архітектури та засобів реалізації для ефективного навчання професійних оцінювачів кави.

Результати дослідження

Розроблена функціональність застосунку включає кілька програмних модулів, представлених на діаграмі прецедентів (див. рис. 1). Діаграма прецедентів – це інструмент UML, який відображає взаємодію між користувачами (акторами) та системою через конкретні сценарії використання (прецеденти) [2; 3].

На діаграмі представлено два типи користувачів: викладач та студент. Викладач може управляти інформацією щодо сортів кави, методів тестування, а також формувати квитки для оцінки. Студент має можливість проходити тестування. Система включає модулі:

- **Управління інформацією про сорти кави** – дозволяє викладачу додавати та редагувати дані про каву.

- **Управління інформацією щодо методів тестування** – забезпечує оновлення методик оцінки.
- **Формування квитка** – генерує квитки для оцінки, які включають завдання для студента.
- **Проходження тестування** – дозволяє студенту виконувати завдання з оцінки кави.

Модуль **TicketCreator** відповідає за створення квитків і є частиною підсистеми формування квитків.

Вказану функціональність можна представити у вигляді прецедентів взаємодії користувачів із системою, які зображені на діаграмі (див. рис. 1).

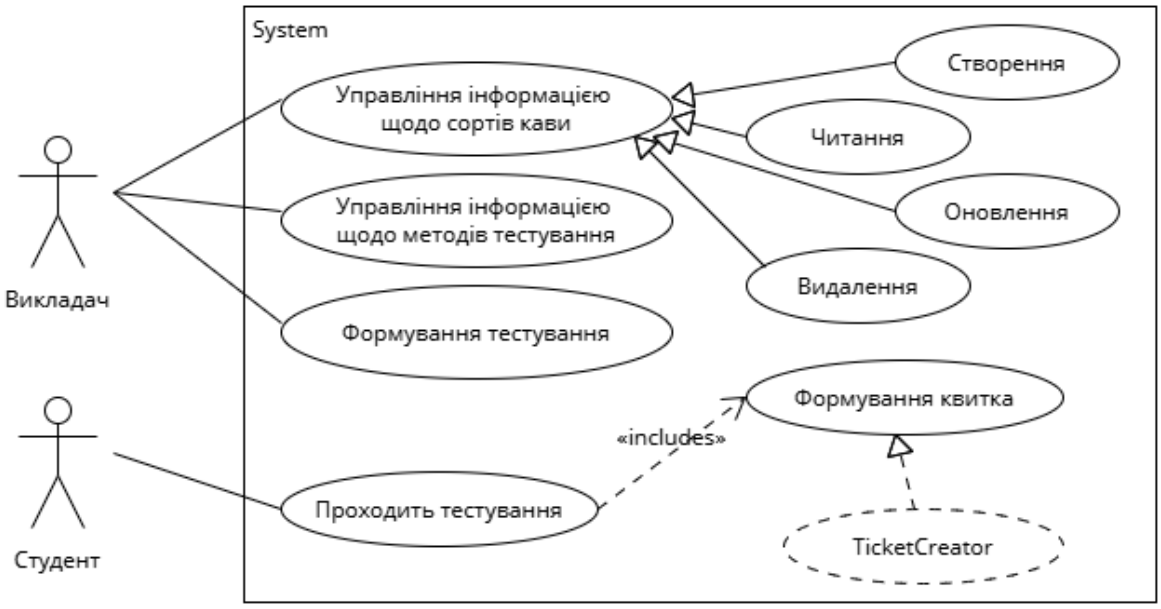


Рис. 1. Діаграма прецедентів функціональності застосунку

Розроблена функціональність застосунку дозволяє автоматизувати процес навчання професійних оцінювачів кави, що підвищує ефективність підготовки. Використання модульної архітектури забезпечує гнучкість та можливість подальшого розширення функціоналу, наприклад, додавання аналітики результатів тестування.

ДЖЕРЕЛА

1. UMLetino - *Online UML Tool*. URL: https://www.umletino.com/umletino.html
2. Unified Modeling Language - *Overview*. URL: https://www.uml-diagrams.org.
3. Specialty Coffee Association - *Coffee Taster's Flavor Wheel*. URL: https://sca.coffee/research/coffee-tasters-flavor-wheel.

ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ РОЗВ'ЯЗАННЯ ЗАДАЧ ШТУЧНИМ ІНТЕЛЕКТОМ ГРАФІЧНИМ СПОСОБОМ

Комар Д.
Київський столичний університет імені Бориса Грінченка, м. Київ

ШІ, такі моделі, як GPT-4o та Gemini Pro 2.5, добре вирішують стандартні завдання, такі як написання коду для функцій чи алгоритмів. Дослідження, наприклад, на платформі CodeSignal, показують, що ШІ часто перевершує середніх розробників, але не досягає рівня топ-20% спеціалістів. Для графічних розв'язків, таких, як блок-схеми, і не поширених середовищ, рідкісних мов програмування, ШІ має обмеження.

Метою даного проєкту є дослідження на скільки добре з побудовою блок-схеми впорається ШІ (ChatGPT, Gemini) при розв'язанні базових задач із програмування.

Основні завдання

- Обрати типові задачі з програмування базового рівня.
- Ввести умови задач у ШІ-системи.
- Проаналізувати результати.
- Перевірити код за допомогою тестів.
- Визначити сильні та слабкі сторони підходу.

При реалізації, для перевірки було обрано задачі: «Сума двох чисел», «Високосний рік», «Середнє з трьох», «Масив – Гора». На кожному етапі оцінювались:

- якість блок-схем (ASCII або графічні);
- точність логіки програм;
- кількість пройдених тестів;
- здатність ШІ враховувати контекст та уточнення користувача.

Алгоритм роботи

1. Формулювання задачі.
2. Введення задачі до ШІ.
3. Аналіз згенерованих схем і коду.
4. Запуск тестів.
5. Корекція на основі зворотного зв'язку.
6. Повторна перевірка.

№	Задача	Спроба 1	Спроба 2	Спроба 3	Результат
1	Сума двох чисел	Блок-схема некоректна	ASCII-схема після запиту	Код правильний	Розв'язано
2	Високосний рік	Некоректний код	Неправильна блок-схема	Не розв'язано	Не розв'язано
3	Середнє з трьох	Пройдено 4/9 тестів	Після тестів –частково правильно	Результат неповний	Не розв'язано

4	Масив – Гора	Алгоритм правильний	Gemini –8/11 тестів	Блок-схема умовна	Частково
5	Діапазон чисел	Без циклу	ASCII схема з помилкою	Цикл враховано, схема працює	Розв’язано
6	Діапазон з кроком	Ігноровано від’ємний крок	Код виправлено, схема ні	Схема після прикладів не коректно відображає відповідь	Частково
7	Макс. кількість 1 підряд	Немає оновлення лічильника	Цикл працює, схема недосконала	Тест пройдено, схема слабка	Частково
8	Розрахунок решти	Лише один крок у схемі	Додано цикл, але без логіки	Отримали працюючий код, але без блок-схеми	Не розв’язано

Проведений аналіз показав, що сучасні ШІ-системи, зокрема ChatGPT та Gemini, демонструють низький рівень ефективності при розв’язуванні базових задач із програмування саме графічним способом. Проведений аналіз восьми базових задач з програмування виявив неоднорідний та загалом низький рівень ефективності сучасних ШІ-систем, а саме ChatGPT та Gemini, у їхньому розв'язанні.

Хоча в окремих випадках спостерігалися певні успіхи (наприклад, задача «Сума двох чисел» після уточнення та часткове розв'язання задачі «Масив – Гора»), а також «Діапазон чисел» більшість спроб продемонстрували значні труднощі у досягненні коректного та повного розв'язання.

ДЖЕРЕЛА

1. AI vs. human engineers: Benchmarking coding skills head-to-head – CodeSignal. CodeSignal. URL: https://codesignal.com/blog/engineering/ai-coding-benchmark-with-human-comparison (дата звернення: 01.05.2025).

2. OpenAI. ChatGPT. URL: https://chat.openai.com (дата звернення: 01.05.2025).

3. Google. Gemini. URL: https://gemini.google.com (дата звернення: 01.05.2025).

ЗБІР І АНАЛІЗ ОСВІТНІХ ДАНИХ ДЛЯ ПОДАЛЬШОЇ NLP-КЛАСИФІКАЦІЇ ЗА CSTA K–12

Коновал Є. Ю., Яскевич В. О.
Київський столичний університет імені Бориса Грінченка, м. Київ

У сучасному освітньому середовищі велике значення має відповідність навчальних матеріалів затвердженим стандартам, зокрема CSTA K–12, які визначають структуру викладання комп'ютерних наук у школі. Для розробки ефективних систем автоматичного аналізу текстів потрібен якісний датасет. Саме процес збору, структурування та попереднього аналізу даних є критичним етапом у створенні систем NLP-класифікації освітніх матеріалів відповідно до цих стандартів.

Мета проекту

Зібрати, структурувати та проаналізувати текстові освітні матеріали з відкритих онлайн-ресурсів із прив'язкою до стандартів CSTA K–12 для подальшого використання у навчанні NLP-моделі, яка буде класифікувати тексти за відповідними стандартами.

Основні завдання

- Пошук і відбір освітніх матеріалів, що мають зв'язок із CSTA K–12.
- Структурування матеріалів у вигляді датасету (заголовок, опис, код стандарту).
- Первинний аналіз і очищення даних.
- Створення CSV-файлу з анотованими прикладами.
- Підготовка даних до подальшого використання в NLP-моделях класифікації(форматування тексту, видалення спец. символів і т.д.).

Опис реалізації

Для збору освітніх матеріалів використовувалися відкриті ресурси, зокрема:

- офіційна бібліотека ресурсів CSTA [1],
- каталог навчальних програм Code.org [2],
- платформа Teachers Pay Teachers [3].

На основі отриманих прикладів було сформовано датасет, у якому кожен запис включає:

- назву завдання,
- короткий опис діяльності,
- код освітнього стандарту CSTA K–12 (наприклад, «1A-CS-01»).

Використано Python-бібліотеку Pandas [4] для формування та збереження датасету у форматі CSV. Загальна кількість тестових прикладів 120 записів, розподіл стандартів категорії Grades K-2 (Ages 5-7) зображений на рис 1.

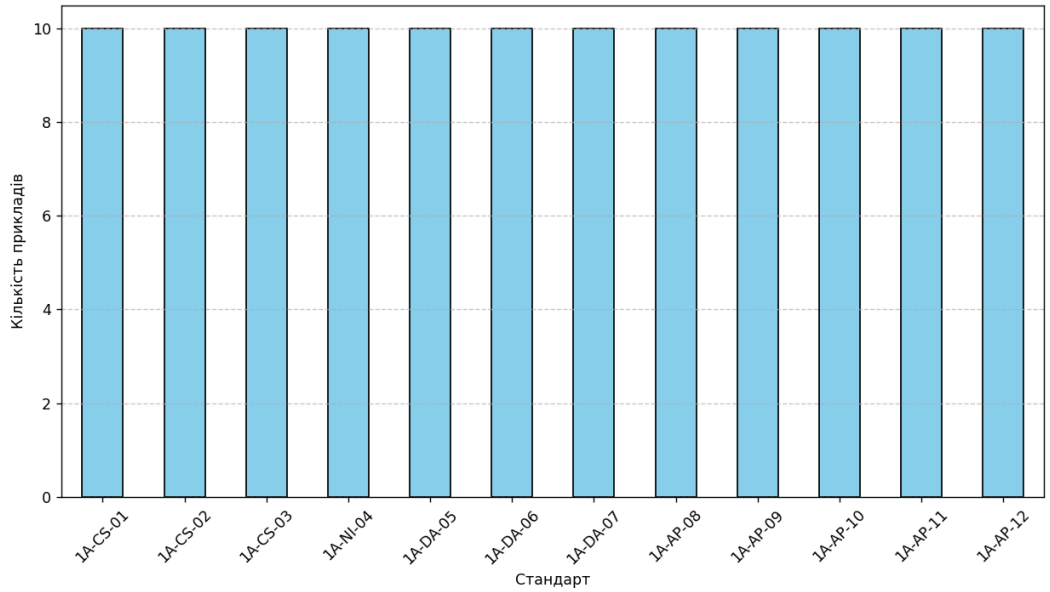


Рис. 1. Кількість прикладів на кожен стандарт

Алгоритм роботи

1. Збір текстових даних із вебсайтів.
2. Ручна анотація прикладів кодами стандартів.
3. Побудова структурованого датафрейму (title, descriptionSnippet, STANDART).
4. Збереження у форматі CSV для подальшої обробки.
5. Передача датасету в NLP-модель для класифікації нових освітніх прикладів.

Ретельний процес збирання та аналізу освітніх текстів є підґрунтям якісного навчання NLP-моделі. Створений датасет із зразками, анотованими відповідно до CSTA K–12, дає змогу будувати системи, здатні автоматично класифікувати свіжі освітні матеріали. У майбутньому цей підхід може бути масштабований та застосований для підтримки вчителів під час підготовки навчального контенту.

ДЖЕРЕЛА

1. CSTA Resource Library. URL: https://csteachers.org/resources-library/
2. Code.org Curriculum Catalog. URL: https://studio.code.org/catalog
3. Teachers Pay Teachers –CSTA Cybersecurity Resources. URL: https://www.teacherspayteachers.com/browse/pdf/under-5?search=CSTA%20cyber%20security
4. Pandas Documentation. URL: https://pandas.pydata.org/docs/

ПІДТРИМКА МУЛЬТИМОВНОСТІ В REACT ВЕБ-ДОДАТКАХ НА ПРИКЛАДІ КОМПОНЕНТА LANGUAGESWITCHER

Кравець А. В.
Київський столичний університет імені Бориса Грінченка, м. Київ

Згідно з дослідженням [1], багатомовність веб-сайтів є критично важливою в сучасному глобалізованому світі, оскільки вона дозволяє значно розширити охоплення аудиторії, забезпечує рівний доступ до інформації незалежно від рідної мови користувача, демонструє культурну інклюзивність і повагу до різноманіття, надає компаніям конкурентну перевагу на міжнародних ринках та допомагає відповідати нормативним вимогам багатьох регіонів щодо надання інформації різними мовами.

Для мультимовності в React використовують різні бібліотеки: React-intl, i18next[2], LinguiJS, Polyglot.js, LocalizeJS, Crowdin.

Було обрано бібліотеку i18next у зв'язку з її гнучкістю та широкими можливостями розширення. Бібліотека підтримує не лише React, а й інші фреймворки, що робить її універсальним рішенням. Крім того, інтеграція з react-i18next дозволяє легко використовувати переклади у компонентах за допомогою хуку useTranslation, що дозволяє оптимізувати кодову базу.

Розроблений компонент LanguageSwitcher забезпечує перемикання мов і збереження вибору користувача під час використанні хуку useTranslation з бібліотеки react-i18next для роботи з мультимовним інтерфейсом та хуку useLocalStorage для збереження вибраної мови між сеансами. Зміна мови здійснюється через виклик i18n.changeLanguage(lang), а графічне представлення реалізовано за допомогою кнопок, які відображають активний стан залежно від обраної мови.

Структура зберігання і підключення текстів:

```
/src
        /translations
          en.json
          ua.json
        /i18n
          i18n.js
```

Бібліотека i18next використовує формат JSON для зберігання даних мов. У JSON-файлах дані організовані як об'єкти з ключами та відповідними значеннями, де ключі представляють ідентифікатори рядків, а значення –їх переклади. Для прикладу приведено ua.json та en.json відповідно:

```
{ «welcome»: «Ласкаво просимо»,
  «navigation»: {«home»: «Головна»}
}
```

```
{ "welcome": "Welcome",
  "navigation": {"home": "Home"}
}
```

Підключення мультимовності до компонентів виглядає таким чином:

```
import { useTranslation } from 'react-i18next';
import useLocalStorage from '../services/hooks/use-localstorage';
export function LanguageSwitcher() {
   const { i18n } = useTranslation();
   const [language, setLanguage] = useLocalStorage('language', 'en');
   const switchLanguage = (lang) => {
      i18n.changeLanguage(lang);
      setLanguage(lang);
   };
   return (
      <div>
         <button onClick={() => switchLanguage('en')}>English</button>
         <button onClick={() => switchLanguage('ua')}>Українська</button>
      </div>
   );
}
export default LanguageSwitcher
```

Підключення перекладу до компонентів виглядає таким чином:

```
import { useTranslation } from 'react-i18next';

export function HomePage() {
   const { t } = useTranslation();

   return (
      <div>
         <h1>{t('welcome')}</h1>
         <nav>
            <a href=«/»>{t('navigation.home')}</a>
         </nav>
      </div>
   );
}
```

Запропонований копмпонент є ефективним керуванням мовними налаштуваннями в React-додатках, зберігаючи вибір користувача між сеансами. Використання бібліотеки i18next та локального сховища робить реалізацію компонента простим та надійним.

ДЖЕРЕЛА

1. Nicoletta C., Frédéric B., Philippe B., Khalid C., Christopher C., Thierry D., Sara G., Hitoshi I., Bente M., Joseph M., Hélène M., Jan O., Stelios P. [Електронний ресурс] // ACL Anthology. Режим доступу: https://aclanthology.org/2022.lrec-1.227.pdf.
2. react-i18next: Інтернаціоналізація для React / React Native [Електронний ресурс]. Режим доступу: https://react.i18next.com/
3. React: The library for web and native user interfaces [Електронний ресурс] // Meta Open Source. Режим доступу: https://react.dev/
4. Window localStorage Property [Електронний ресурс] // W3Schools. Режим доступу: https://www.w3schools.com/jsref/prop_win_localstorage.asp
5. Reusing Logic with Custom Hooks [Електронний ресурс] // React Documentation. Режим доступу: https://react.dev/learn/reusing-logic-with-custom-hooks#extracting-your-own-custom-hook-from-a-component

СУЧАСНІ ПІДХОДИ ДО АВТОМАТИЗАЦІЇ РЕГРЕСІЙНОГО ТЕСТУВАННЯ З ВИКОРИСТАННЯМ ЕМУЛЯЦІЇ ДІЙ КОРИСТУВАЧА

Кравчун О. М, Перепелюк С. А, Яновський О. М., Яцина О. Г.
Західноукраїнський національний університет, м. Тернопіль

Автоматизація регресійного тестування є критично важливою складовою забезпечення якості програмного продукту в умовах швидкого розвитку програмної інженерії. Постійні зміни у кодовій базі потребують системної перевірки функціоналу, що вже був реалізований раніше. Регресійне тестування дозволяє виявити неочікувані дефекти, спричинені новими змінами, і запобігти їх появі у продуктивному середовищі [1].

Імітація взаємодії з інтерфейсом користувача (UI) є особливо актуальною в умовах, коли система повинна відображати поведінку реального користувача. Тестові сценарії в цьому випадку охоплюють такі дії, як заповнення форм, натискання кнопок, переходи по сторінках тощо. Це дозволяє перевірити не лише функціональність, а й зручність та стабільність інтерфейсу.

Інструменти автоматизації UI-тестів, такі як Selenium, Selenide, Playwright чи Cypress, дозволяють моделювати подібні сценарії з високим ступенем наближеності до реального використання [2]. Особливо важливо те, що такі тести легко інтегруються в середовища CI/CD, підтримують кросбраузерне тестування та масштабуються відповідно до зростання проєкту.

Серед широкого спектра доступних фреймворків для Java-проєктів особливої уваги заслуговує бібліотека Selenide. На відміну від «чистого» Selenium, який вимагає значних зусиль на налаштування, обробку тайм-аутів та організацію очікувань, Selenide надає вищий рівень абстракції. Він дозволяє зосередитися безпосередньо на логіці тестування, спрощує написання і підтримку тестів, а також має зручні механізми логування та генерації звітів [3].

Платформа підтримує інтеграцію з JUnit, TestNG та Allure, що дозволяє ефективно організувати тестовий процес у рамках розробки за методологіями Agile або DevOps.

Автоматизоване тестування інтерфейсу також дозволяє ефективно реалізовувати підхід «тестування як документація». Завдяки застосуванню фреймворків із підтримкою Behavior-Driven Development (BDD), таких як Cucumber або JBehave, можливим стає створення тестових сценаріїв, які читаються як природна мова. Це особливо корисно для спільної роботи між розробниками, тестувальниками та бізнес-аналітиками. У поєднанні з Selenide це дозволяє створювати тести, які водночас є і технічно точними, і бізнес-зрозумілими.

У таблиці 1 представлено ключові характеристики інструментів емуляції дій користувача.

Таблиця 1

Порівняльна характеристика інструментів, що реалізовують імітацію дій користувача

Критерій / Інструмент	Selenium	Selenide	Playwright	Katalon/TestProject
Поріг входу	Високий	Середній	Низький	Дуже низький
Підтримка браузерів	Висока	Висока	Висока	Середня
Швидкість виконання	Середня	Дуже висока	Висока	Середня
CI/CD інтеграція	Так	Так	Так	Частково
Гнучкість	Висока	Висока	Висока	Обмежена

Ще одним аспектом є стабільність тестів. У великих автоматизованих проєктах нестабільні (flaky) тести є значною проблемою. Тут Selenide демонструє ефективність завдяки вбудованим механізмам smart waits, які дозволяють автоматично обробляти затримки у завантаженні елементів інтерфейсу, знижуючи ймовірність помилкових спрацювань.

Масштабованість також має важливе значення. Завдяки інтеграції з хмарними платформами, такими як BrowserStack або Selenoid, Selenide дозволяє запускати UI-тести паралельно на різних конфігураціях браузерів та ОС. Це істотно підвищує ефективність кросбраузерного тестування.

Автоматизоване регресійне тестування, що ґрунтується на моделюванні користувацьких дій, дозволяє ефективно забезпечити якість програмного забезпечення при частих оновленнях. Із наведеної таблиці та проведеного аналізу в контексті Java-проєктів найбільш придатним інструментом виявився Selenide, який поєднує в собі гнучкість, зручність використання та високу стабільність виконання тестів. Надалі доцільним є поглиблення досліджень у напрямку поєднання UI-автоматизації з методами тестування API та впровадження інтелектуальних засобів генерації тестів.

ДЖЕРЕЛА

1. Dustin, E. Effective Software Testing: 50 Specific Ways to Improve Your Testing. Addison-Wesley, 2002. – 272 p.

2. Koskela, L. Test Driven: TDD and Acceptance TDD for Java Developers. Manning Publications, 2007. – 250 p.

3. Vinogradov, A. Selenide: concise UI tests in Java. [Online]. Available: https://selenide.org

ВИКОРИСТАННЯ МЕТОДІВ МАШИННОГО НАВЧАННЯ ТА ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ РОЗРОБКИ НОВИННОГО БОТА

Кривошеєв І. С.

Київський столичний університет імені Бориса Грінченка, м. Київ

Інформаційні технології стрімко розвиваються, і одним із напрямків їх використання є автоматизація збору та аналізу новинних даних. Завдяки методам машинного навчання (ML), штучного інтелекту (AI) та обробки природної мови (NLP) можна значно покращити швидкість та якість створення новинних повідомлень, автоматизувати обробку великих масивів текстових даних та забезпечити персоналізовану подачу контенту. Новинні боти використовуються в месенджерах, на веб-сайтах та в мобільних додатках, надаючи актуальну інформацію в режимі реального часу [1; 2; 6].

Метою дослідження була розробка новинного бота з використанням методів машинного навчання та штучного інтелекту для автоматизації збору та генерації новинних повідомлень Автор проаналізував декілька новинних за їх функціональними можливостями та технологіями, завдяки яким воони реалізовані. Результати аналізу узагальнені в таблиці 1.

Автор розробив прототип новинного бота, в якому за допомогою методів AI та ML реалізовані наступні функції [4; 5; 3]:

– Збір даних: веб-скрейпінг новинних порталів за допомогою BeautifulSoup та Scrapy, використання API новинних сервісів для отримання актуальної інформації.

– Аналіз тексту: розпізнавання та аналіз новинних заголовків за допомогою NLP, тематичний аналіз новин з використанням методів класифікації (наприклад, Naive Bayes або SVM).

– Генерація новинних повідомлень: створення коротких анотацій за допомогою нейронних мереж (LSTM або трансформерів), підсумовування тексту для отримання основних тез.

– Персоналізація новин: рекомендація новин на основі вподобань користувача за допомогою алгоритмів колаборативної фільтрації, автоматичне налаштування контенту відповідно до інтересів.

– Публікація новин: інтеграція з месенджерами (Telegram, Viber) або веб-платформами для доставки новин.

Таблиця 1

Порівняння ботів, за їх функціональністю та видом навчання

Назва бота	Використані технології	Функціональні можливості
Cyborg (Bloomberg)	VL, NLP	Аналіз фінансових звітів та перетворення їх на новини [2]
Bertie (Forbes)	ML, NLP	Генерація заголовків, пропозиція трендових тем для новин [2]
Heliograf (The Washington Post)	ML, NLP	Автоматизація створення коротких новинних статей зі структурованих даних [2]
JAMES (The Times of London)	ML, AI	Персоналізація новинного контенту на основі аналізу поведінки та інтересів користувачів [2]
Lynx Insight (Reuters)	ML, AI	Аналіз великих масивів даних для надання інформації для журналістських розслідувань [2]
Claim Hunter (Newtral)	ML, NLP	Транскрибація аудіоконтенту, виявлення тверджень, які потребують перевірки фактів [2]
Reuters (News Tracer)	ML, AI	Швидке виявлення термінових новин та перевірка їхньої достовірності [2]

Розроблений прототип новинного бота демонструє можливість автоматичної генерації коротких новинних зведень на основі аналізу ключових подій. Отже, прототип новинного бота забезпечить оперативне інформування користувачів про актуальні події та новини з використанням методів машинного навчання та штучного інтелекту.

ДЖЕРЕЛА

1. Висоцька В., Чирун Л., Чирун С., Романчук Р., Свищ Д. Інтелектуальна система передбачення фейкових новин на основі технологій NLP та машинного навчання // Наукові журнали та конференції. – 2024. – Випуск 16. – С. 325-347. science.lpnu.ua
2. Штучний інтелект в журналістиці // Блог про штучний інтелект. – 2021. shtychniyintellekt.blogspot.com
3. Що редакції думають про впровадження штучного інтелекту // Медіамейкер. – 2024. mediamaker.me
4. Ворочек О.Г., Соловей І.В. Використання мовних моделей штучного інтелекту для генерації публікацій у соціальних мережах // Вісник Житомирського державного технологічного університету. – 2024. – №1(93). – С. 128-134. library.ztu.edu.ua
5. Степенко С.М. Використання методів машинного навчання для виявлення фейкових новин // Магістерська дисертація. – Київ: НТУУ «КПІ», 2023. – 85 с. ai.kpi.ua
6. Розуміння ключових відмінностей між машинним навчанням і штучним інтелектом // Codelabs Academy. – 2024. codelabsacademy.com

JIRA, TRELLO ТА ASANA ЯК ЗАСОБИ РЕАЛІЗАЦІЇ ГНУЧКИХ ПІДХОДІВ ДО УПРАВЛІННЯ ІТ-ПРОЄКТАМИ

Кушнір В. М, Вовк Р. Б.

Івано-Франківський національний технічний університет нафти і газу,
м. Івано-Франківськ

У контексті сучасного цифрового середовища, де ефективне управління проєктами є критичним чинником успішності, особливого значення набувають інструменти, призначені для автоматизації процесів планування, моніторингу виконання завдань та забезпечення командної взаємодії. До найбільш поширених платформ, що використовуються у сфері розробки програмного забезпечення, належать Jira, Trello та Asana. Ці програмні засоби підтримують сучасні підходи до управління проєктами, зокрема Agile, Scrum і Kanban, та забезпечують розширені можливості для інтеграції, налаштування і візуалізації робочих процесів. Завдяки цьому команди отримують змогу ефективно організовувати завдання, відстежувати прогрес їх виконання, а також підтримувати прозору комунікацію незалежно від масштабу проєкту.

Jira, розроблена компанією Atlassian, є потужним інструментом для управління програмними проєктами, орієнтованим передусім на гнучку розробку. Її головною перевагою є висока гнучкість у налаштуванні, що дозволяє адаптувати систему відповідно до специфіки конкретної команди або проєкту. Платформа підтримує реалізацію таких методологій, як Agile та Scrum, зокрема через механізм спринтів –фіксованих часових інтервалів,

протягом яких команда виконує певний обсяг робіт. Такий підхід сприяє структурованості, прозорості процесів і оперативному реагуванню на зміни.

Крім того, у Jira реалізовано функціонал дашбордів та звітності, що дозволяє здійснювати глибокий аналіз ефективності: зокрема, оцінювати швидкість розробки, продуктивність у межах окремих спринтів, відповідність вимогам тощо. Проте, незважаючи на значний функціональний потенціал, система має певні обмеження. Зокрема, складність початкового налаштування та перенавантаженість інтерфейсу можуть створювати труднощі для нових користувачів. Крім того, доступ до повного функціоналу передбачений переважно у платних версіях, що може бути неприйнятним для невеликих команд. Використання хмарної версії також зумовлює необхідність стабільного інтернет-з'єднання.

Для команд, які надають перевагу простоті та швидкому старту, ефективним рішенням є Trello – ще один продукт Atlassian, побудований на принципах методології Kanban. Основу інтерфейсу складають візуальні дошки з картками завдань, що переміщуються між колонками відповідно до етапів виконання («To Do», «In Progress», «Done»). Такий підхід сприяє зручному візуальному контролю за процесом та не вимагає тривалого навчання. Серед переваг Trello – інтуїтивно зрозумілий інтерфейс, підтримка інтеграцій з популярними сервісами (Slack, Google Drive, Dropbox), а також можливість розширення функціональності за допомогою Power-Ups (автоматизація, календарі, аналітика тощо) [1].

Водночас, функціональні обмеження Trello можуть бути критичними для великих проєктів, які потребують розгалуженої структури завдань із залежностями. Безкоштовна версія передбачає обмежену кількість Power-Ups, що ускладнює довготривале використання у складних проєктах.

Іншим популярним інструментом є Asana [2], яка поєднує простоту інтерфейсу з широкими можливостями для планування, організації та моніторингу завдань. Платформа підтримує роботу за методологіями Agile та Scrum, зокрема реалізацію спринтів, ієрархічну структуру завдань (основні й підзадачі), а також розширені засоби візуалізації – зокрема діаграми Ганта, що дозволяють наочно відображати часові рамки та залежності. До ключових функціональних можливостей Asana належить контроль за дедлайнами, аналіз прогресу виконання завдань у реальному часі, а також інтеграція з зовнішніми сервісами (Slack, Google Drive, Dropbox).

Користувачам надається можливість вибору формату представлення інформації –у вигляді списків, канбан-дощок або діаграм Ганта, що забезпечує адаптивність платформи до різних стилів роботи. Водночас, деякі розширені функції, зокрема аналітика та таймлайни, доступні лише у платних версіях. Крім того, новим користувачам може бути складно одразу опанувати повний спектр можливостей платформи.

Таким чином, ефективне управління проєктами в IT-сфері передбачає використання спеціалізованих інструментів, які забезпечують планування, контроль, комунікацію та адаптивність до змін. Jira, Trello та Asana є прикладами таких інструментів, що мають власні переваги та обмеження. Jira орієнтована на складні проєкти з високим рівнем кастомізації, Trello є зручним рішенням для малих команд і швидкого старту, а Asana забезпечує гнучке планування з ефективною візуалізацією завдань. Вибір відповідного інструмента залежить від специфіки проєкту, технічних вимог і організаційних особливостей команди, що у підсумку сприяє підвищенню продуктивності та якості керування проєктним циклом.

ДЖЕРЕЛА

1. Як використовувати Jira, Trello, Asana та Worksection для управління проєктами. URL: https://worksection.com/ua/blog/how-to-use-jira-trello-asana-worksection-for-pm.html

2. Asana vs Jira: Який інструмент для управління проектами підійде вашій команді? URL: https://www.chanty.com/blog/uk/asana-vs-jira-uk/

БАГАТОРОЗРЯДНА ЦИФРОВА ІНДИКАЦІЯ У ВБУДОВАНИХ СИСТЕМАХ

Кушнір О. В.

Київський столичний університет імені Бориса Грінченка, м. Київ

У сучасних вбудованих системах багаторозрядна цифрова індикація є основним засобом взаємодії користувача з пристроєм. Особливої актуальності вона набуває в малопотужних системах, де обмежені ресурси мікроконтролера, кількість доступних виводів, обсяг оперативної пам’яті та потреба в енергоефективності змушують інженера шукати баланс між зручністю інтерфейсу та апаратними можливостями.

Семисегментні індикатори залишаються найпоширенішими пристроями індикації завдяки простоті реалізації, зручності візуального сприйняття та невеликій вартості. Однак саме реалізація багаторозрядної індикації (від 4 до 8 цифр) створює найбільше труднощів в умовах обмеженого числа GPIO-виводів. Для вирішення цієї проблеми найчастіше застосовується динамічне мультиплексування, яке дозволяє керувати кількома розрядами через спільні лінії даних. Такий підхід знижує апаратну складність індикаторної системи, однак вимагає точного розрахунку частоти оновлення і адаптації програмного керування [1]. Якщо ж апаратні ресурси дозволяють, доцільно використовувати індикаторні драйвери, наприклад MAX7219, який керує 8-розрядними модулями через SPI-інтерфейс. У документації описано можливість каскадування до 8 пристроїв, що відкриває шлях до створення табло з 64

розрядами без перевантаження основного процесора [2]. Подібні рішення знайшли широке застосування в промислових системах, де важливе компактне і стабільне відображення даних.

Для малопотужних систем, таких як Arduino Uno або ATtiny, часто застосовуються послідовнісні регістри 74HC595, які дозволяють мінімізувати кількість потрібних ліній керування за рахунок послідовної передачі даних. Однак це створює потребу в оптимізації коду, особливо в багаторозрядних реалізаціях. В умовах обмежених ресурсів контролера доцільно поєднувати мультиплексування із застосуванням таблиць символів у Flash-пам’яті, що дозволяє зменшити затримки при відображенні інформації [3].

У більш продуктивних мікроконтролерах, таких як ESP32, реалізацію багаторозрядної індикації можна винести на апаратний рівень, використовуючи апаратні таймери або DMA-контролери. За допомогою ESP-IDF розробник отримує доступ до низькорівневих ресурсів, що дозволяє забезпечити стабільне оновлення індикації незалежно від навантаження основної програми. Технічний посібник компанії Espressif описує багаторівневу ієрархію пріоритетів преривань, які можуть бути ефективно використані для обробки сигналів сканування дисплея [4].

Варто підкреслити, що вибір способу реалізації багаторозрядної індикації повинен відповідати цільовій архітектурі проєкту. Для бюджетних рішень достатньо використання TM1637 із мінімальним програмним забезпеченням. Для промислових або багатофункціональних пристроїв доцільно інтегрувати інтелектуальні драйвери, зокрема MAX7219 на базі SPI або HT16K33, що використовує I²C-інтерфейс. Обидва варіанти дозволяють реалізувати багаторозрядну індикацію з апаратною підтримкою мультиплексування та керування яскравістю.

Дослідження реалізації багаторозрядної цифрової індикації у вбудованих системах дозволяє обґрунтувати вибір технічних рішень залежно від ресурсів, задач та умов експлуатації. Розуміння переваг і обмежень кожного підходу дає змогу не лише оптимізувати проєктування, але й забезпечити стабільну, ефективну та економну взаємодію пристрою з користувачем.

ДЖЕРЕЛА

1. Турукало А. В. Дискретні шкальні засоби індикації вбудованих систем: дис. … канд. техн. наук : 05.13.05 / А. В. Турукало. – Київ : НУБіП України, 2022. – 207 с. [Електронний ресурс]. – Режим доступу: https://nubip.edu.ua/sites/default/files/u145/dis_turukalo.pdf. – Дата звернення: 12.04.2025.

2. MAX7219/MAX7221 – Serially Interfaced, 8-Digit LED Display Drivers [Електронний ресурс]. – Режим доступу:

https://www.analog.com/media/en/technical-documentation/data-sheets/max7219-max7221.pdf. – Дата звернення: 13.04.2025.

3. Пристрої відображення та реєстрації інформації: Конспект лекцій. – Київ: КПІ ім. Ігоря Сікорського, 2020. – [Електронний ресурс]. – Режим доступу: https://ela.kpi.ua/bitstream/123456789/28797/1/PV_ta_RI_Konspekt.pdf. – Дата звернення: 18.04.2025.

4. ESP32 Technical Reference Manual [Електронний ресурс]. – Режим доступу: https://www.espressif.com/sites/default/files/documentation/esp32_technical_reference_manual_en.pdf. – Дата звернення: 23.04.2025.

ПЕРЕВАГИ ТА НЕДОЛІКИ ASP.NET MVC

Лукашевич В. В., Вакалюк Т. А.
Державний університет «Житомирська політехніка», м. Житомир

Сучасна веб-розробка вимагає використання ефективних інструментів, що забезпечують швидке створення якісних програмних продуктів із чіткою структурою та можливістю подальшої підтримки. Однією з найбільш популярних технологій у цій сфері є ASP.NET MVC. Дана технологія використовує шаблон проектування Model-View-Controller (MVC), що дозволяє розділяти застосунок на незалежні компоненти. Це значно полегшує розробку, тестування та підтримку веб-додатків. Однак, як і будь-яка технологія, ASP.NET MVC має свої переваги та недоліки, які важливо враховувати під час вибору інструментів для розробки програмного забезпечення.

До переваг ASP.NET MVC слід віднести:

- чітке розділення логіки додатку на три складові: модель, представлення та контролер, що робить код організованішим та зручнішим для підтримки;
- простота у написанні тестів завдяки незалежності компонентів, що забезпечує високий рівень тестованості коду;
- підтримка гнучкої маршрутизації (routing), що дозволяє створювати URL, які є зрозумілими та зручними для пошукових систем і користувачів;
- повний контроль над HTML та JavaScript, що забезпечує гнучкість у створенні інтерфейсу користувача;
- висока продуктивність завдяки оптимізації запитів і можливості кешування даних.

Однак, незважаючи на значні переваги, ASP.NET MVC має деякі недоліки:

– порівняно висока складність для початківців, які звикли до традиційних форм Web Forms, оскільки потребує розуміння принципів MVC;

– більша кількість «ручної» роботи порівняно з іншими технологіями, такими як ASP.NET Web Forms або Razor Pages, що може сповільнити процес розробки на початкових етапах;

– відсутність автоматичного управління станом сторінки (ViewState), що вимагає додаткових зусиль для збереження стану;

– потреба у ретельному проектуванні архітектури додатку, що у разі помилок може призвести до ускладнення підтримки коду у майбутньому.

Таким чином, ASP.NET MVC є потужним інструментом для створення веб-додатків, який дозволяє розробникам досягати високої якості та підтримуваності коду. Проте при виборі цієї технології слід враховувати як її переваги, такі як гнучкість, чіткість структури і високий рівень тестованості, так і недоліки, зокрема складність для новачків та необхідність ретельного проектування архітектури. У випадку розробки веб-додатку для управління фітнес-клубом, зазначені переваги ASP.NET MVC є суттєвими і дозволяють створити зручну, ефективну та легко підтримувану систему управління.

ДЖЕРЕЛА

1. Документація Microsoft ASP.NET MVC [Електронний ресурс] – Режим доступу: https://learn.microsoft.com/uk-ua/aspnet/mvc/overview/getting-started/introduction/

2. Freeman A. Pro ASP.NET Core MVC 2. Apress, 2017. 1046 с.

3. Chadwick J., Snyder T., Panda H. Programming ASP.NET MVC 4: Developing Real-World Web Applications with ASP.NET MVC. O'Reilly Media, 2012. 488 с.

АКТУАЛЬНІСТЬ ТЕМИ РОЗРОБКИ СИСТЕМИ УПРАВЛІННЯ ФІТНЕС-КЛУБОМ

Лукашевич В. В., Вакалюк Т. А.

Державний університет «Житомирська політехніка», м. Житомир

Сучасна індустрія фітнесу стрімко розвивається, дедалі більше людей стають прихильниками здорового способу життя, що спричиняє підвищення попиту на якісні фітнес-послуги. Водночас, збільшення кількості клієнтів створює додаткове навантаження на адміністративний персонал фітнес-клубів, що зумовлює необхідність впровадження ефективних автоматизованих інформаційних систем управління. Автоматизація процесів управління дозволяє покращити якість надання послуг, зменшити кількість помилок та підвищити рівень задоволеності клієнтів.

Однією з основних проблем сучасних фітнес-клубів є використання застарілих методів адміністрування: ручне ведення обліку абонементів, клієнтів, розкладів тренувань та взаємодії з клієнтами. Це призводить до великої кількості помилок, неефективного використання робочого часу персоналу, і як наслідок, до зниження конкурентоспроможності клубу. Ручне адміністрування не дозволяє швидко і гнучко адаптуватися до змін у роботі клубу, створює незручності для клієнтів через затримки з обслуговуванням та погіршує загальний імідж клубу.

Використання веб-орієнтованих інформаційних систем для управління діяльністю фітнес-клубів є ефективним рішенням зазначених проблем. Такі системи дозволяють автоматизувати ведення клієнтської бази, управління абонементами, планування та контроль тренувань, автоматизувати розсилку сповіщень та повідомлень клієнтам, а також забезпечувати ефективну комунікацію між клієнтами, тренерами та адміністративним персоналом. Це значно спрощує та прискорює процеси управління, дозволяє мінімізувати ризик помилок та підвищує рівень задоволеності клієнтів якістю послуг.

З огляду на ці переваги, впровадження автоматизованої системи управління фітнес-клубом є доцільним кроком у розвитку фітнес-клубу. Вибір сучасних інформаційних технологій, таких як ASP.NET MVC та бази даних Microsoft SQL Server, забезпечує високу продуктивність, надійність і масштабованість системи. Також важливим є використання об’єктно-орієнтованого програмування та методології UML для проектування та розробки системи, що дозволяє створити зрозумілу та гнучку структуру програмного забезпечення.

Таким чином, актуальність розробки системи управління фітнес-клубом визначається необхідністю автоматизації управлінських процесів та покращення якості обслуговування клієнтів. Використання сучасних технологій розробки веб-додатків та баз даних дозволить створити ефективну і гнучку систему, що задовольнить потреби як персоналу, так і клієнтів фітнес-клубу.

ДЖЕРЕЛА

1. Офіційна документація ASP.NET Core [Електронний ресурс] – Режим доступу: https://learn.microsoft.com/en-us/aspnet/core/
2. Документація Microsoft SQL Server [Електронний ресурс] – Режим доступу: https://learn.microsoft.com/en-us/sql/?view=sql-server-ver16
3. Martin R. C. Clean Architecture: A Craftsman’s Guide to Software Structure and Design. Prentice Hall, 2018.

РОЗРОБКА МОБІЛЬНОГО ДОДАТКУ ДЛЯ КОНВЕРТАЦІЇ ФАЙЛІВ АУДІО ТА ВІДЕО ФОРМАТІВ.

Малиженко Я. М.
Київський столичний університет імені Бориса Грінченка, м. Київ

В еру мобільних технологій та стрімінгового контенту користувачі потребують швидких та зручних рішень для конвертації медіафайлів без необхідності використання потужних комп'ютерів, телефонів тощо [1]. Це особливо важливо для блогерів, журналістів, відеоредакторів і звичайних користувачів, яким потрібно швидко конвертувати або редагувати файли без доступу до стаціонарного ПК [2]. Проте, більшість мобільних додатків для конвертації медіа мають певні обмеження [3]:

– Підтримка обмеженого набору форматів, що змушує користувачів шукати додаткові інструменти.

– Обмеження щодо параметрів виводу, таких як роздільна здатність, кодеки, бітрейт, що ускладнює створення відео високої якості.

– Відсутність інтеграції з хмарними сервісами, що ускладнює доступ до файлів з різних пристроїв.

– Високе навантаження на мобільний пристрій через неефективну оптимізацію процесів, що може призводити до швидкого розряджання батареї та перегріву.

Автор проаналізував декілька додатків, що мають найвищі рейтинги, за даними Google Play та App Store, та виділив основні характеристики, що представлені в таблиці 1.

Таблиця 1

Порівняльний аналіз додатків для конвертації файлів аудіо та відео форматів

Характеристики	VidCompact	InShot	Media Converter	Розроблюваний додаток
Підтримувані формати	MP4, MOV, GIF	MP4, MP3, AAC	MP4, AVI, MP3, WAV, FLAC	MP4, MOV, AVI, MP3, WAV, MIDI
Конвертація відео	Так	Ні	Так	Так
Конвертація аудіо	Ні	Так	Так	Так
Налаштування бітрейту	Ні	Ні	Так	Так
Інтеграція з хмарою	Ні	Ні	Ні	Google Drive
Додаткові можливості	Стиснення відео, обрізка	Витягування аудіо з відео	Гнучке налаштування параметрів	Налаштування параметрів, підтримка хмари

Розроблюваний додаток має широкий набір функцій, що забезпечує його конкурентоспроможність та ефективність для користувачів різного рівня. Він підтримує відеоформати MP4, MOV, AVI та аудіоформати MP3, WAV, MIDI, дозволяючи конвертацію між ними з мінімальними втратами якості. Користувачі зможуть налаштовувати параметри виводу, такі як бітрейт і роздільна здатність, а також витягувати аудіо з відео. Додаток буде інтегрований із хмарними сервісами Google Drive і Dropbox, що дозволить зберігати файли безпосередньо в онлайн-сховищі. Завдяки апаратному прискоренню конвертація відбуватиметься швидше, а оптимізоване використання ресурсів мобільного пристрою сприятиме економії енергії.

Принцип роботи додатку:

1. Користувач обирає файл для конвертації.
2. Користувач вибирає вихідний формат та інші налаштування.
3. Додаток перевіряє чи правильно обрані параметри формату.
4. Відбувається конвертація файлу.
5. Вивід результату з можливістю перегляду або збереження в хмару.

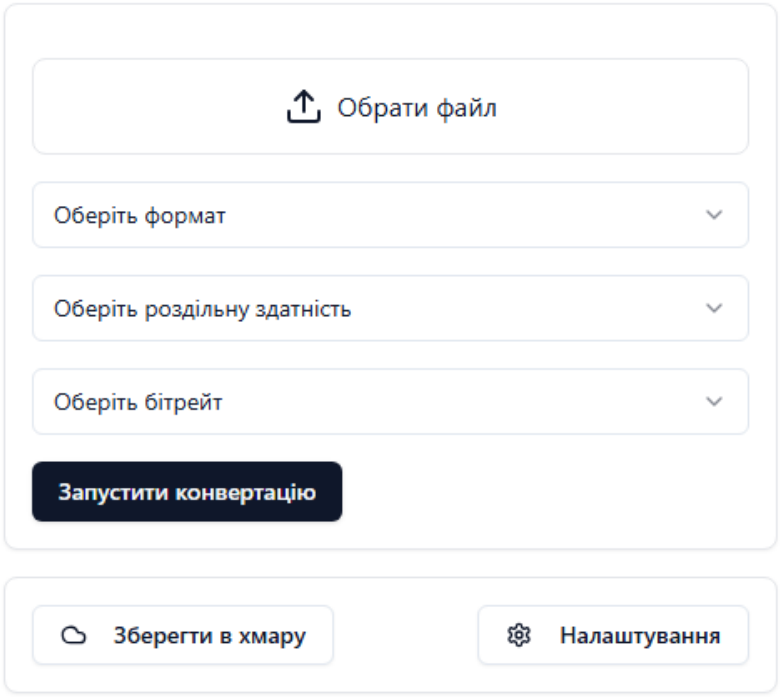


Рис 1. Інтерфейс мобільного додатку для конвертації файлів аудіо та відео форматів

Отже, розробка мобільного додатоку для конвертації аудіо та відео форматів є ефективним рішенням, що поєднує в собі функціональність, простоту використання та високу продуктивність. Він підтримує широкий спектр форматів, надає можливість зміни параметрів файлів, інтегрується з хмарними сервісами та оптимізований для роботи на мобільних пристроях.

Подальший розвиток передбачає розширення можливостей редагування, покращення продуктивності для слабших пристроїв та підтримку нових форматів і кодеків, що зробить додаток ще більш гнучким і універсальним для користувачів.

ДЖЕРЕЛА

1. How File Conversion Works, and Why It's Important [Електронний ресурс] – Посилання: https://sizle.io/how-file-conversion-works-and-why-its-important/

2. How to Convert Any Media File Into Its Different Formats [Електронний ресурс] – Посилання: https://www.instructables.com/How-to-Convert-Any-Media-File-Into-Its-Different-F/

3. «Інформаційна система конвертування мультимедійних файлів» [Електронний ресурс] – Посилання: https://essuir.sumdu.edu.ua/bitstream-download/123456789/93196/1/Koshman_bac_rob.pdf

РОЗРОБКА МОБІЛЬНОГО ДОДАТКА ДЛЯ БРОНЮВАННЯ КНИГ ТА ВІДСТЕЖЕННЯ ІСТОРІЇ ВІДВІДУВАНЬ

Нітчук І. І., Носенко Т. І.

Київський столичний університет імені Бориса Грінченка, м. Київ

Інформаційні технології активно розвиваються та впроваджуються в різні сфери життя, у тому числі в бібліотечну справу [1]. Одним із актуальних напрямів є створення мобільних додатків для оптимізації процесів взаємодії користувачів із бібліотеками. У межах цієї роботи було проведено дослідження можливостей створення мобільного додатка для бронювання книг та відстеження історії відвідувань.

На етапі дослідження було проведено порівняльний аналіз існуючих рішень, таких як Libby, OverDrive та MyLibrary за такими критеріями, як кількість завантажень, оцінка користувачів, можливість бронювання книг, відстеження історії та інтеграція з іншими сервісами. Основні відмінності узагальнені в таблиці 1.

Таблиця 1

Порівняння функціональності бібліотечних додатків

Додаток	**К-сть завантажень (млн)**	**Оцінка користувачів**	**Бронювання книг**	**Відстеження історії відвідувань**	**Інтеграція з бібліотеками**
Libby	10+	4.7/5	Доступне онлайн-бронювання книг	Відсутня функція перегляду історії	Підключення до партнерських бібліотек
OverDrive	5+	4.6/5	Можливість бронювання та завантаження аудіо- та електронних книг	Відсутня історія фізичних відвідувань	Підключення до бібліотек через акаунт
MyLibrary	1+	4.3/5	Обмежене бронювання друкованих книг	Історія читання доступна тільки для електронних книг	Доступне лише для певних бібліотек

Для візуального представлення алгоритму роботи мобільного додатка була створена блок-схема, що відображає основні етапи взаємодії користувача з системою (рис. 1).

Інтерфейс мобільного додатка розробляється з урахуванням принципів UI/UX-дизайну, що забезпечує зручність використання [2,3]. Головний екран міститиме список доступних книг, кнопку бронювання та особистий кабінет користувача, де можна переглянути історію відвідувань. Окрім основних функцій, представлених на блок-схемі, додаток також міститиме систему рекомендацій книг на основі вподобань користувачів, можливість залишати відгуки та рейтинги, а також отримувати сповіщення про нові надходження та статус заброньованих книг.

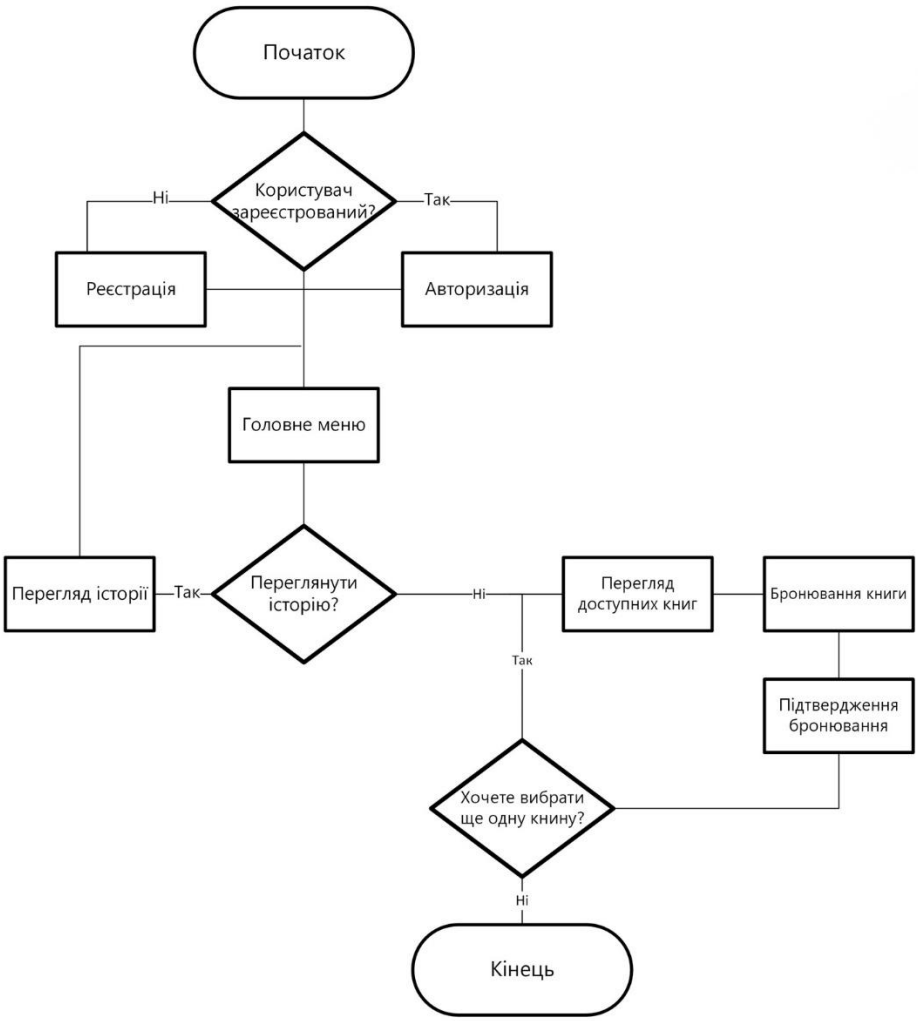


Рис. 1. Блок-схема розроблюваного мобільного додатка

Отже, запропонований мобільний додаток дозволить спростити доступ до бібліотечних ресурсів, автоматизувати процес бронювання та покращити взаємодію користувачів із бібліотеками.

ДЖЕРЕЛА

1. Макарова О. І. Мобільні бібліотечні додатки як черговий етап діджиталізації сучасної бібліотеки // Міжнародний науковий електронний журнал «WayScience». – 2023. – № 5. – С. 45–53. – Режим доступу: https://irbis-nbuv.gov.ua/everlib/item/er-0004642.

2. Бондаренко В., Струнгар В. Особливості розробки мобільного застосунку бібліотеки в онлайн-конструкторі: критерії, алгоритм створення, перспективи // Наукові праці Національної бібліотеки України імені В. І. Вернадського. – 2021. – Вип. 61. – С. 192–207. – Режим доступу: https://irbis-nbuv.gov.ua/everlib/item/er-0004049.

3. Огляд сучасних технологій для розробки мобільних додатків // Наукові праці Житомирського державного університету імені Івана Франка. – 2016. – Вип. 2. – С. 123–128. – Режим доступу: https://eprints.zu.edu.ua/21122/.

РЕАКТИВНА АРХІТЕКТУРА МІКРОСЕРВІСІВ НА ПЛАТФОРМІ SPRING WEBFLUX ДЛЯ ВИСОКОНАВАНТАЖЕНИХ СИСТЕМ

Олаба Д. Р.
Державний університет інформаційно-комунікаційних технологій, м. Київ

Сучасні мікросервісні архітектури потребують високопродуктивних рішень, здатних ефективно обробляти велику кількість одночасних запитів. Традиційна блокуюча модель обробки запитів, яка використовується в Spring MVC, створює значні обмеження для масштабування та продуктивності систем. Реактивна парадигма програмування на основі Spring WebFlux пропонує альтернативний підхід, що забезпечує оптимальне використання системних ресурсів та суттєво підвищує пропускну здатність додатків.

Реактивне програмування базується на концепції асинхронних потоків даних та неблокуючої обробки запитів [1]. У контексті Spring WebFlux це реалізується через Project Reactor – бібліотеку для створення неблокуючих реактивних застосунків на JVM, що підтримує специфікацію Reactive Streams. Ключовими сутностями цієї бібліотеки є Mono<T> та Flux<T> – типи, що представляють асинхронні послідовності відповідно з 0-1 та 0-N елементами.

Впровадження реактивного підходу у мікросервісній архітектурі має низку суттєвих переваг. По-перше, це ефективне використання ресурсів сервера. Завдяки неблокуючій моделі обробки запитів, потоки не перебувають у стані очікування під час виконання вводу-виводу, що дозволяє обслуговувати значно більшу кількість запитів з тими самими ресурсами [2]. За даними досліджень, реактивні додатки можуть обробляти до 10 разів більше запитів порівняно з традиційними блокуючими системами при однакових ресурсах. По-друге, суттєво підвищується відгукоздатність системи. Навіть при високому навантаженні реактивні системи зберігають здатність швидко реагувати на запити, що є критично важливим для сервісів безпеки. По-третє, зменшується споживання пам'яті через відсутність необхідності утримувати великий пул потоків, що особливо цінно для контейнеризованих середовищ з обмеженими ресурсами. По-четверте, покращується стійкість системи до пікових навантажень завдяки вбудованим механізмам контролю потоку та обмеження швидкості (backpressure).

Порівняльний аналіз традиційного та реактивного підходів у мікросервісній архітектурі представлений у таблиці 1

Таблиця 1

Порівняння Spring MVC та Spring WebFlux

Характеристика	Spring MVC (традиційний)	Spring WebFlux (реактивний)
Модель обробки запитів	Блокуюча, один запит на потік	Неблокуюча, асинхронна
Використання ресурсів	Потреба у великому пулі потоків	Ефективне використання невеликої кількості потоків
Пропускна здатність	Обмежена кількістю доступних потоків	Висока при тій же кількості ресурсів
Відгукоздатність під навантаженням	Деградує при збільшенні кількості запитів	Зберігається стабільною
Обробка вводу-виводу	Блокуюча, неефективна	Неблокуюча, оптимальна
Робота з базами даних	Повна підтримка всіх СУБД	Часткова підтримка, необхідність реактивних драйверів
Складність розробки	Нижча, звичний імперативний стиль	Вища, функціональний стиль та управління потоками
Обробка помилок	Через виключення (try-catch)	Через оператори onError, switchIfEmpty
Міжсервісна комунікація	RestTemplate (блокуючий)	WebClient (неблокуючий)

Ключовою новизною запропонованого підходу є впровадження реактивної архітектури у системах безпеки та контролю доступу, зокрема в розробленому мікросервісі Access Guard. Традиційно системи безпеки реалізуються з використанням блокуючої моделі через міркування надійності та простоти імплементації. Однак, в умовах високих

навантажень це призводить до суттєвих проблем з продуктивністю та відгукоздатністю.

Розроблений патерн реактивної автентифікації на основі JWT-токенів дозволяє подолати ці обмеження, зберігаючи при цьому необхідний рівень безпеки. Інноваційний підхід полягає у комбінації неблокуючої обробки запитів автентифікації з реактивним оновленням токенів, що забезпечує стабільну роботу системи навіть при пікових навантаженнях.

Аспект новизни також полягає в розробленій архітектурі реактивного фільтра авторизації для Gateway-сервісу, який здійснює перевірку JWT-токенів асинхронно, не блокуючи основний потік обробки запитів. Такий підхід дозволяє суттєво знизити латентність обробки запитів у розподіленій системі, що є критично важливим для користувацького досвіду.

Впровадження реактивної архітектури має також певні виклики. Зокрема, це стосується складності розробки та налагодження реактивного коду, необхідності переосмислення підходів до обробки помилок та тестування. Важливою є також організація інфраструктури проекту таким чином, щоб уникати «реактивних островів» – ситуацій, коли один компонент системи використовує реактивний підхід, а інші залишаються блокуючими.

Для ефективного впровадження реактивного підходу рекомендується дотримуватись кількох принципів:

Використовувати реактивні варіанти для всіх компонентів від бази даних до клієнта

Застосовувати функціональний стиль програмування для обробки потоків даних

Ретельно управляти підписками для уникнення витоків пам'яті

Впроваджувати механізми обмеження швидкості (backpressure) для захисту від перевантаження

Отже, реактивна архітектура на основі Spring WebFlux надає значні переваги для побудови сучасних мікросервісних систем, забезпечуючи високу продуктивність, масштабованість та ефективне використання ресурсів. Практичний досвід впровадження такого підходу у проектах, таких як Access Guard, демонструє його ефективність для створення надійних, високопродуктивних мікросервісів безпеки.

ДЖЕРЕЛА

1. Reactive Streams. Specification for asynchronous stream processing with non-blocking back pressure. URL: https://www.reactive-streams.org/ (дата звернення: 24.04.2025).

2. Spring Framework. Web on Reactive Stack. URL: https://docs.spring.io/spring-framework/reference/web/webflux.html (дата звернення: 22.04.2025).
3. Stephane M., Richard L. Hands-On Reactive Programming in Spring 5. Packt Publishing, 2022. 398 p.

ВИКОРИСТАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ BLENDER ДЛЯ СТВОРЕННЯ 3D-МОДЕЛЕЙ ПЕРСОНАЖІВ

Олексійчук К. О.
Київський столичний університет імені Бориса Грінченка, м. Київ

3D-моделювання стало невід'ємною частиною багатьох галузей цифрових технологій, зокрема анімації, відеоігор, віртуальної та доповненої реальності. Серед усього розмаїття 3D-об'єктів особливе значення мають персонажі, оскільки саме вони формують сюжет, передають емоції та утримують інтерес глядачів до контенту. Створення 3D-персонажів потребує художньої і технічної майстерності, але якість кінцевого результату також залежить від обраного програмного забезпечення. Одним із найкращих рішень для цього є Blender – безкоштовна програма з відкритим вихідним кодом, яка охоплює повний цикл 3D-виробництва. Матеріал доповіді присвячений дослідженню можливостей Blender у контексті розробки 3D-моделей персонажів.

Створення геометрії. Blender підтримує всі основні підходи до 3D-моделювання. На початкових етапах використовуються геометричні примітиви, які слугують основою для складніших форм. Полігональне моделювання забезпечує повний контроль над топологією завдяки редагуванню вершин, ребер і граней. Для цього програма надає такі інструменти, як Extrude (витягування нових елементів), Bevel (згладжування кутів і ребер), Inset (створення внутрішніх граней всередині обраних), Loop Cut (додавання нових петель розрізів по сітці), Knife Tool (ручне розрізання) та багато інших [1]. Сплайнове моделювання базується на використанні кривих (Bezier, NURBS) для побудови об'єктів, формою кривих можна маніпулювати за допомогою контрольних точок, змінюючи їхнє розташування та регулюючи їхній вплив. Процедурне моделювання у Geometry Nodes дає можливість будувати об'єкти на основі параметричних залежностей і логічних вузлів, що спрощує створення складних, повторюваних структур. Скульптинг дозволяє працювати з моделлю подібно до ліплення з глини, для цього Blender [7] надає понад 60 вбудованих пензлів. Для оптимізації високополігональних моделей до анімації доступні засоби ручної та автоматичної ретопології. Система модифікаторів у Blender дозволяє змінювати форму 3D-моделей без руйнування початкової геометрії. Найчастіше використовуються Subdivision Surface (згладжування), Mirror (віддзеркалення об'єкта по

заданій осі), Solidify (додавання товщини поверхні), Shrinkwrap (прикріплює один об’єкт до поверхні іншого), Multiresolution (дозволяє працювати на кількох рівнях деталізації), Boolean (об'єднує або вирізає частини об'єктів).

Текстурування. Blender використовує фізично коректний рендеринг (PBR), реалізований через вузловий редактор Shader Editor, де основним елементом є вузол Principled BSDF, що поєднує різні параметри матеріалу (колір, металевість, шорсткість, прозорість тощо) [2]. Крім цього, програма підтримує використання текстурних карт. Blender також має вбудований режим Texture Paint для ручного малювання текстур безпосередньо на 3D-моделі. Ще однією важливою функцією є підтримка процедурних текстур, які створюються на основі математичних алгоритмів. Для точного розміщення текстур на поверхні моделі у програмі передбачено UV-редактор, що включає як автоматичні алгоритми розгортки, так і засоби ручного контролю –позначення швів, вирівнювання та корекцію UV-островів.

Ріггінг та скіннінг. Щоб надати персонажу здатність рухатись у Blender використовується система Armature [3]. Для автоматизації ріггінгу можна завантажити аддон Rigify, який містить набір готових скелетів із контролерами. Для прив’язки сітки моделі до скелету виконують скіннінг, де використовуються вагові карти, що визначають, як кожна частина рухатиметься при переміщенні кісток. Програма надає інструменти для автоматичної прив’язки і ручного налаштування ваг (Weight Paint).

Симуляції. Система Cloth [4; 5] дозволяє моделювати реалістичну поведінку тканин під впливом сили тяжіння, вітру та інших факторів, з можливістю регулювання фізичних параметрів матеріалу. Для волосся у Blender використовується система Hair, де кожне пасмо представлене у вигляді кривої. Волосся редагується за фізичними параметрами та за допомогою інструментів стилізації зачіски, таких як розчісування, обрізання та укладання.

Однією з унікальних особливостей Blender є інструмент Grease Pencil, завдяки якому можна створювати 2D-ілюстрації та анімацію безпосередньо у 3D-просторі [6].

Blender має три вбудовані рендер-рушії – Cycles для кінцевої фотореалістичної візуалізації, Eevee для швидкого рендеру в реальному часі і Workbench для попереднього перегляду сцен під час моделювання.

Програма працює на Windows, macOS, Linux, підтримує велику кількість форматів імпорту та експорту, що забезпечує легку інтеграцію з іншими системами. Крім того, існує багато безкоштовних і платних доповнень, які легко встановлюються через інтерфейс програми.

Blender залишається популярним вибором серед студентів, фрилансерів та невеликих анімаційних студій завдяки своїй доступності, зрозумілому інтерфейсу, багатому функціоналу, регулярним оновленням

та підтримці активної спільноти. Хоча основні гіганти індустрії традиційно використовують Autodesk Maya, Blender все більше знаходить своє місце у професійному середовищі. Яскравим підтвердженням цього є латвійський мультфільм «Flow», який був повністю створений у цьому програмному середовищі та здобув премію «Оскар» за найкращий анімаційний повнометражний фільм 2025 року.

ДЖЕРЕЛА

1. Blender. Modeling. Blender 4.4 Manual. URL: https://docs.blender.org/manual/en/latest/modeling/index.html

2. Ewa Wierbik-Ziąbka. (2 жовтня, 2024). Beginners guide to Texturing in Blender. CG Cookie. URL: https://cgcookie.com/posts/beginners-guide-to-texturing-in-blender

3. Joey Carlino. (30 травня, 2024). Rigging for beginners - Blender tutorial. YouTube. URL: https://www.youtube.com/watch?v=m-Obo_nC3SM

4. Ryan King Art. (12 січня, 2023). Cloth Physics for Beginners (Blender Tutorial). YouTube. URL: https://www.youtube.com/watch?v=c5LOOoSHh9c

5. Abe Leal 3D. (31 липня 2023). Blender Hair System: Step-by-Step Tutorial. YouTube. URL: https://www.youtube.com/watch?v=rd3RkBVJMQA

6. Blender. Grease Pencil. Blender 4.4 Manual. URL: https://docs.blender.org/manual/en/latest/grease_pencil/index.html

7. Blender (software). Wikipedia. URL: https://en.wikipedia.org/wiki/Blender_(software)#:~:text=

МЕТОДИ ОБРОБКИ ТЕКСТОВИХ ВІДГУКІВ У ЗАДАЧАХ ЕМОЦІЙНОГО АНАЛІЗУ

Омелянчук О. В., Худік Б. О.

Державний університет інформаційно-комунікаційних технологій, м. Київ

Постановка задачі

У сучасному інформаційному просторі текстові відгуки користувачів –один з найважливіших типів контенту, що акумулює суб’єктивні оцінки, емоційні реакції та поведінкові індикатори споживачів. Автоматизована обробка таких текстів є ключовим етапом у побудові систем емоційного аналізу, рекомендаційних сервісів, моніторингу репутації бренду тощо. З огляду на зростаючі обсяги текстових даних, виникає потреба у порівнянні та виборі ефективних методів їх обробки, що здатні враховувати як лексичні, так і контекстуальні особливості мовлення.

Основні методи, які застосовуються в задачах обробки текстових відгуків, умовно поділяються на три групи:

1. Лексиконно-орієнтовані підходи, що базуються на словниках емоційно маркованих слів (наприклад, SentiWordNet, NRC Emotion

Lexicon). Такі методи прості у реалізації, не потребують навчання моделі, але чутливі до синонімії, полісемії та іронії [1].

2. Класичні статистичні методи машинного навчання, серед яких найбільш поширені логістична регресія, наївний баєсівський класифікатор та метод опорних векторів. Вони використовують числове представлення тексту (TF-IDF, Bag of Words) та дають задовільні результати на невеликих наборах даних. Проте ці моделі ігнорують порядок слів та семантичні зв'язки [2].

3. Методи глибокого навчання, які включають рекурентні нейронні мережі (RNN, LSTM), згорткові мережі (CNN) та трансформери (наприклад, BERT, RoBERTa). Ці підходи здатні автоматично витягати контекстуальні ознаки з тексту, враховуючи як локальні, так і глобальні залежності. Моделі типу BERT показують високу точність у задачах класифікації тональності, але вимагають значних обчислювальних ресурсів і великих корпусів для донавчання [3; 4].

У дослідженні здійснено порівняльний аналіз зазначених методів за критеріями точності класифікації, швидкодії, обчислювальної складності та здатності адаптації до нових тематичних доменів. Результати вказують на переваги трансформерних моделей у задачах з високою варіативністю мовлення, проте класичні методи залишаються доцільними для задач із обмеженими ресурсами або простими структурами текстів.

Таким чином, вибір методу обробки текстових відгуків має здійснюватися з урахуванням контексту використання, доступності обчислювальних ресурсів та якості вихідних даних. Інтеграція гібридних підходів, що поєднують лексичну евристику та глибинне навчання, є перспективним напрямом подальших досліджень [5].

ДЖЕРЕЛА

1. Бондаренко О. М. Методи емоційного аналізу текстів на основі словників / О. М. Бондаренко, Л. В. Сичова // Інформаційні технології і комп'ютерна інженерія. –2020. –№ 1. –С. 52–58.

2. Jurafsky D., Martin J. H. Speech and Language Processing. –3rd ed. –Draft version. –Stanford University, 2022. –Режим доступу: https://web.stanford.edu/~jurafsky/slp3/

3. Goldberg Y. Neural Network Methods for Natural Language Processing. –Morgan & Claypool Publishers, 2017. –146 p.

4. Devlin J. et al. BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding // Proceedings of NAACL-HLT 2019. –Minneapolis, USA, 2019. –P. 4171–4186.

5. Романенко Т. О., Кузьменко М. В. Гібридні підходи до аналізу текстових відгуків: комбінування лексичних та нейромережевих методів // Вісник Харківського національного університету радіоелектроніки. –2021. № 4. С. 67–74.

ТРАНСФОРМАЦІЯ БІЗНЕС-ПРОЦЕСІВ НА ОСНОВІ ТЕХНОЛОГІЙ ІНТЕРНЕТУ РЕЧЕЙ

Опалінський В. Д., Лепа Р. О.
Західноукраїнський національний університет, м. Тернопіль

В сучасних умовах бізнес шукає способи оптимізації внутрішніх процесів, зменшення витрат й отримання конкурентних переваг. Технології інтернет речей (Internet of Things (IoT)), як рушій цифрової трансформації, надають необхідні інструменти для автоматизації бізнес-процесів з метою швидкого реагування на зміни ринку [1; 2].

Інтеграція «розумних» пристроїв у виробничі, логістичні, сервісні та управлінські процеси дозволяє підприємствам отримувати точні й оперативні дані для прийняття ефективних рішень [2]. Це, у свою чергу, сприяє підвищенню продуктивності й забезпечує прозорість функціонування бізнесу. При такій трансформації особливої цінності набувають дані, а вміння якісно їх збирати, опрацьовувати, аналізувати та застосовувати у реальному часі є ключовим фактором успіху .

Архітектура IoT представляє багаторівневу структуру, яка забезпечує взаємодію між фізичними пристроями, мережевими інфраструктурами та цифровими сервісами. Найпоширенішою є триступенева модель архітектури, яка включає:

– фізичний рівень – пристрої, сенсори, виконавчі механізми, призначені для збору даних з навколишнього середовища;

– мережевий рівень – передача даних від пристроїв фізичного рівня до обчислювальних систем через канали зв’язку (Wi-Fi, 4G/5G, Ethernet);

– прикладний рівень – інтерпретація отриманих даних, аналітика, прийняття рішень засобами штучного інтелекту, надання інтерфейсу користувачам чи бізнес-системам.

Таким чином, технологія IoT охоплює весь ланцюжок аналізу даних на основі злагодженої взаємодії програмно-апаратного забезпечення та штучного інтелекту. Значно дешевше запобігти поломці, ніж провести ремонт, автоматизувати рутинні процеси, ніж витрачати ресурси на повторювані задачі та марні людино-години. Проте варто зазначити, що впровадження IoT вимагає суттєвих інвестицій, що є своєрідним викликом для компаній, який в той же час вимагає зміни логіки ведення бізнесу та поведінкових звичок.

ДЖЕРЕЛА

1. Internet of Things, IoT: веб-сайт. URL: https://www.it.ua/knowledge-base/technology-innovation/internet-veschej-internet-of-things-iot (дата звернення 29.04.2025 р.).

2. Паккі А. Трансформація структури бізнес-процесів в сучасних умовах економічного розвитку // Modeling the Development of the Economic Systems. 2025. Iss.1. No 1. P. 168-175.

ПЕРСПЕКТИВИ РОЗВИТКУ ВЕБОРІЄНТОВАНИХ СИСТЕМ

Пилипенко Д. Ю., Коваленко О. О.
Вінницький національний технічний університет, м. Вінниця

У сучасних умовах стрімкого розвитку цифрових технологій веборієнтовані системи відіграють ключову роль у забезпеченні інтерактивної взаємодії між користувачами та інформаційними ресурсами. Їх використання охоплює практично всі сфери діяльності людини – від бізнесу, освіти до охорони здоров'я, державного управління та наукових досліджень. Основними перевагами веборієнтованих систем є доступність, масштабованість, кросплатформеність і можливість централізованого адміністрування.

Перспективи розвитку веборієнтованих систем тісно пов'язані з упровадженням новітніх технологій, таких як хмарні обчислення, штучний інтелект, машинне навчання, блокчейн, а також розвитком концепцій Web 4.0 і семантичного Інтернету [1; 2]. Це дозволяє створювати адаптивні, інтелектуальні системи з високим рівнем персоналізації користувацького досвіду.

Особливе значення має безпека та захист персональних даних у веборієнтованих системах. Удосконалення механізмів автентифікації, шифрування, а також впровадження концепцій zero-trust і кібергігієни є важливими напрямами подальших досліджень і розробок веборієнтованих систем.

У сфері освіти веборієнтовані системи відкривають широкі можливості для дистанційного та змішаного навчання, індивідуалізованого підходу та формування гнучких освітніх траєкторій. Зокрема, активне впровадження сервісів хмарних платформ відкритої науки дозволяє оптимізувати освітній процес, розширити доступ до навчальних та наукових ресурсів і сформувати професійні та цифрові компетентності здобувачів освіти [3].

Одним з трендів розвитку вебпорталів є формування їх програмного та апаратного забезпечення за принципами інформаційної екосистеми. Такі принципи означають введення автоматизованого адміністрування (вертикального та горизонтального); багатокористувацьке використання даних, які введені один раз; продукування даних та знань користувачами та різноманітними електронними агентами (від модульних програмних застосунків до штучного інтелекту); інтеграції з різноманітними хмарними платформами тощо.

Сучасні методології створення та підтримки веборієнтованих систем передбачають використання стандартів щодо реалізації життєвого циклу створення програмних продуктів, а також гнучких методологій для створення та удосконалення й супроводу таких систем.

Особливості тестування веборієнтованих систем полягає у розробці вимог до програмного ё апаратного забезпечення, моніторингу показників під час розробки та на останніх етапах створення веборієнтованих систем і їх супроводження [4].

Таким чином, розвиток веборієнтованих систем має значний потенціал для трансформації інформаційного простору.

Веборієнтовані системи дозволяють зробити безшовні переходи з локальних корпоративних систем, внутрішніх вебсторінок на зовнішні електронні ресурси, розвивати технології інтеграції різних вебсистем в єдиний інформаційний простір, запроваджувати інструменти інтерактивності, адаптації до потреб користувачів, використання технологій віртуальної реальності, блокчейн.

Гнучкі методології створення, впровадження та підтримки веборієнтованих систем дозволяють розвивати окремі модулі веб-порталів, які можуть працювати окремо і бути інтегровані в єдине інформаційне середовище.

ДЖЕРЕЛА

1. Ільченко І. Знаєте яким буде Web 4.0? Давайте створемо! DOU. https://dou.ua/forums/topic/39548/

2. Ковівчак Ю., Ю. Кінаш Ю.,. Кустра Н, Курах В. Розробка Web-орієнтованої інформаційної системи для моніторингу відвідування та успішності учнів у навчальних закладах». Комп'ютерно-інтегровані технології: освіта, наука, виробництво, 2021, No 43, с. 28–31.

3. Бруяка А. В., Коваленко В. В., Крамар С. С. та інш. Використовування сервісів хмаро-орієнтованих систем відкритої науки в освітньому процесі закладів вищої вищої освіти і післягадипломної освіти, К.: Інститут цифровізації освіти Національної академії педагогічних наук України, 2023. https://lib.iitta.gov.ua/id/eprint/738519/

4. Пилипенко Д.Ю., Коваленко О.О. Тестування систем управління навчанням. Збірник матеріалів Міжнародної науково-практичної Інтернет-конференції «Електронні інформаційні ресурси: створення, використання, доступ», 20-21 листопада, 2023. Суми/Вінниця. – С. 194-195. URL: http://ir.lib.vntu.edu.ua// handle/123456789/38708

ІНТЕГРОВАНА ІНФОРМАЦІЙНА ПЛАТФОРМА ДЛЯ СПОРТСМЕНІВ І ТРЕНЕРІВ

Писарєв В. Д.
Київський столичний університет імені Бориса Грінченка, м. Київ

У сучасному спортивному середовищі зростає потреба в ефективному управлінні тренувальним процесом, моніторингу результатів спортсменів і організації змагань. Рішенням цієї проблеми можуть стати інтегровані цифрові платформи, що об'єднують ці функції в єдиному середовищі. З огляду на вимоги до безпеки даних та прозорості процесів, використання блокчейн технології стає важливим для досягнення необхідного рівня захисту інформації та забезпечення довіри до результатів. Блокчейн дозволяє забезпечити незмінність та прозорість записів, що є критично важливим для спортивних досягнень, результатів змагань та тренувальних процесів.

Застосування блокчейн технологій у спортивних інформаційних системах вимагає вирішення кількох важливих задач. По-перше, необхідно розробити систему, яка дозволить динамічно і безпечно обробляти спортивні дані та результати змагань у реальному часі. По-друге, важливо створити алгоритми для інтеграції цієї технології в існуючі процеси моніторингу та організації спортивних змагань, що дозволить мінімізувати вплив людського фактору та покращити управлінську ефективність. Метою цієї роботи є розробка моделі інтегрованої платформи для спортсменів та тренерів з використанням блокчейн технологій, що забезпечить ефективну обробку даних, автоматизацію процесів та підвищення прозорості та безпеки.

Для реалізації запропонованої платформи буде використано принципи децентралізації даних, що забезпечить їх безпеку та доступність для всіх учасників (спортсменів, тренерів, організаторів змагань). Кожен результат тренування або змагання буде фіксуватися в блокчейн реєстрі, що дозволить отримати незмінну інформацію про спортивні досягнення спортсменів та результати змагань. Окрім цього, платформа автоматизує процеси реєстрації спортсменів, організації змагань, формування тренувальних планів і розрахунку результатів, що зменшить навантаження на адміністраторів і підвищить ефективність роботи спортивних організацій.

Процес створення цієї платформи передбачає кілька етапів:

Аналіз існуючих рішень: Оцінка поточних цифрових платформ, що використовуються для управління спортивною діяльністю, та визначення недоліків, які можуть бути виправлені за допомогою блокчейн технологій.

Розробка архітектури системи: Визначення ключових компонентів платформи, таких як інтерфейси для користувачів, бази даних для

зберігання результатів та механізми інтеграції з існуючими спортивними платформами.

Розробка алгоритмів для обробки даних: Створення ефективних алгоритмів, що забезпечать автоматичне внесення результатів у блокчейн, їх обробку, збереження та доступ до них.

Інтеграція блокчейн технології: Впровадження протоколів блокчейн для забезпечення незмінності даних, захисту від несанкціонованого доступу та забезпечення їх прозорості для усіх учасників.

Прототипування та тестування: Створення прототипу платформи та його тестування на контрольній групі користувачів для оцінки ефективності системи та можливих шляхів для покращення.

Для розв'язання проблеми планування і обробки спортивних даних, буде застосовано блокчейн як основний метод для зберігання та верифікації результатів. Завдяки дистрибуційній природі блокчейн технології, дані будуть зберігатися в кількох вузлах, що забезпечить їх захист та доступність для користувачів без потреби в централізованих серверах. Крім того, алгоритми для обробки даних будуть забезпечувати швидке і ефективне збереження результатів та доступ до них у реальному часі. Для реалізації цієї системи використовуватиметься мова програмування Python для розробки інтерфейсів користувачів, реалізації алгоритмів обробки даних та інтеграції з блокчейн платформами.

Перші етапи експерименту передбачають тестування платформи на обмежених обсягах даних (20 спортсменів, 30 тренерів), щоб оцінити ефективність роботи системи. Далі обсяги будуть збільшуватися до 50 спортсменів та 100 тренерів, 100 спортсменів та 200 тренерів для перевірки стабільності і масштабованості системи.

Запропонована інтегрована платформа з використанням блокчейн технології дозволить досягти високої ефективності в управлінні спортивною діяльністю, забезпечить безпеку даних та дозволить забезпечити прозорість результатів змагань і тренувань. Застосування блокчейн допоможе зменшити ризики фальсифікацій, підвищити довіру до результатів і забезпечити автоматизацію процесів. Розробка ефективного рішення для таких платформ сприятиме розвитку спортивної індустрії та підвищенню якості управління тренувальними процесами.

ДЖЕРЕЛА

1. He N. Blockchain Use Cases in the Sports Industry: A Systematic Review // *International Journal of Networked and Distributed Computing*. 2024. Vol. 12. C. 17–40. URL: https://link.springer.com/article/10.1007/s44227-024-00022-3

2. Demirci N. The Future of Blockchain Technology in the Sports Industry // *Journal of Sports Industry & Blockchain Technology*. 2024. DOI: 10.5281/zenodo.12599715.

ВПРОВАДЖЕННЯ ЕФЕКТИВНИХ DEVOPS-ПРАКТИК У РОЗРОБКУ ТА ПІДТРИМКУ JAVA ДОДАТКІВ

Пінчук І. В.
Київський столичний університет імені Бориса Грінченка, м. Київ

Постановка проблеми. Сучасна розробка Java-додатків у корпоративному секторі стикається з проблемами неефективного створення Docker-образів, складного управління конфігураціями та недостатньої автоматизації міграцій баз даних, що призводить до значних витрат часу, ресурсів і ризиків у CI/CD-процесах, особливо у хмарних інфраструктурах [1]. Вирішення цих проблем потребує впровадження сучасних DevOps-практик для забезпечення швидкості, гнучкості та стабільності на всіх етапах життєвого циклу продукту.

Шляхи вирішення. У межах дослідження зосереджено увагу на трьох ключових аспектах: оптимізації створення Docker-образів, централізованому управлінні конфігураціями та автоматизації міграцій баз даних у CI/CD-пайплайнах.

Один із досліджених напрямків – оптимізація створення Docker-образів для Spring Boot-додатків. Проведено аналіз неефективних підходів, таких як використання базових Dockerfile без кешування шарів, що призводить до значних оверхедів за часом і витрат ресурсів [1]. Запропоновано використання багатоступеневих збірок (multi-stage builds) та інструментів Spring Boot layertools, що дозволяє зменшити обсяг некешованих даних та прискорити процеси розгортання у Kubernetes [2]. Також продемонстровано автоматизацію створення образів за допомогою Cloud Native Buildpacks через плагіни Maven/Gradle, що усуває необхідність ручного написання Dockerfile і підвищує продуктивність CI/CD-процесів [1]. Поєднання багатоступеневих збірок із Cloud Native Buildpacks забезпечує додаткові переваги: зменшення залежності від ручних конфігурацій і стабільність результатів у різних середовищах.

Ще один важливий аспект – управління конфігураціями Spring-додатків у хмарних середовищах. Проведено порівняння двох підходів: Kubernetes ConfigMap та Spring Cloud Config Server. У [3] показано, що ConfigMap ефективний для статичних налаштувань у монолітних додатках, дозволяючи змінювати параметри (наприклад, рівень логування) без перезбірки образу за лічені секунди. Натомість Spring Cloud Config Server має переваги у розподілених системах завдяки централізованому зберіганню конфігурацій у Git-репозиторіях та підтримці динамічного оновлення через Refresh Scope [3]. Запропоновано гібридний підхід, який комбінує ConfigMap для базових налаштувань і Config Server для складних мікросервісних архітектур. Таке поєднання дозволяє одночасно забезпечити швидкість оновлення базових параметрів і гнучкість управління конфігураціями у великих системах.

Окремо досліджено автоматизацію міграцій баз даних у CI/CD-пайплайнах з використанням Liquibase. Реалізовано інтеграцію Liquibase у процеси безперервної доставки, що забезпечує синхронізацію схем баз даних у різних середовищах (розробка, тестування, продакшн) та зменшує ризик розбіжностей. Поєднання Liquibase із гібридним підходом до управління конфігураціями додатково підвищує стабільність розгортання, оскільки конфігураційні зміни та міграції баз даних відбуваються синхронно.

Результати дослідження підтверджують, що впровадження запропонованих DevOps-практик – багатоступеневих збірок, Spring Boot layertools, Cloud Native Buildpacks, гібридного підходу ConfigMap і Config Server, а також інтеграції Liquibase – дозволяє скоротити час випуску релізів, підвищити ефективність використання ресурсів та забезпечити стабільність Java-додатків у хмарних інфраструктурах. Поєднання цих підходів, зокрема багатоступеневих збірок із Cloud Native Buildpacks, гібридного управління конфігураціями та автоматизації міграцій через Liquibase, дає змогу досягти оптимального балансу між швидкістю, гнучкістю та надійністю. Отримані рішення можуть бути корисними для розробників і DevOps-інженерів, які працюють із сучасними Java-системами.

ДЖЕРЕЛА:

1. 10 найкращих практик для створення Java-контейнерів за допомогою Docker [Електронний ресурс] / Snyk. – 2022. – Режим доступу: https://snyk.io/blog/best-practices-to-build-java-containers-with-docker/ (дата звернення: 17.03.2025).
2. 14 найкращих практик для контейнеризації ваших Java-додатків [Електронний ресурс] / Tutorial Works. – 2023. – Режим доступу: https://www.tutorialworks.com/docker-java-best-practices/ (дата звернення: 17.03.2025).
3. Spring Cloud Config: Довідник [Електронний ресурс] / Spring. – 2023. – Режим доступу: https://docs.spring.io/spring-cloud-config/docs/current/reference/html/ (дата звернення: 17.03.2025).

ТОПОЛОГІЯ ШКІЛЬНОЇ КОМП’ЮТЕРНОЇ МЕРЕЖІ

Плоха А. Ю
Київський столичний університет імені Бориса Грінченка, м. Київ

Мережеві технології є ключовим аспектом функціонування сучасних навчальних закладів. Організація надійної, масштабованої та безпечної шкільної мережі забезпечує ефективну роботу учнів і викладачів. Одним з оптимальних підходів до організації такої інфраструктури є розробка структурованої моделі мережевої архітектури.

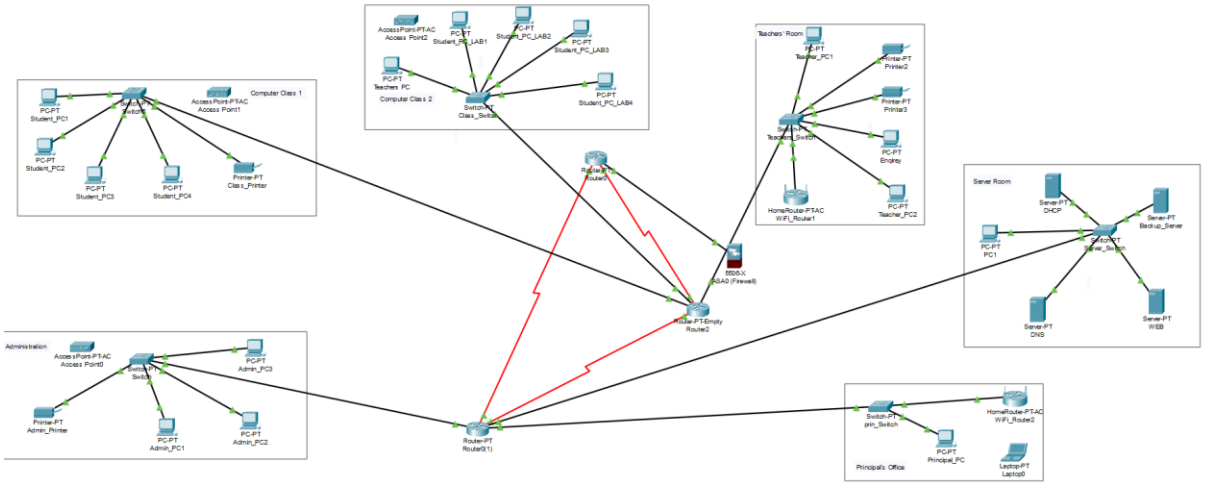


Рис1. Топологія побудованої шкільної мережі

Проєктована мережа складається з кількох логічних сегментів, що забезпечують розподіл навантаження та безпеку трафіку. Основними компонентами мережі є маршрутизатори, комутатори, сервери, точки доступу Wi-Fi та робочі станції. Передбачена підтримка VLAN для розподілу доступу між адміністрацією, викладацьким складом та студентами. Для захисту внутрішніх ресурсів застосовується міжмережевий екран, що фільтрує зовнішні запити та запобігає несанкціонованому доступу [1].

У рамках реалізації моделі передбачено використання оптоволоконного з'єднання між ключовими вузлами для забезпечення високої пропускної здатності. Серверна кімната містить центральний сервер керування доступом, DHCP-сервер для автоматичної конфігурації IP-адрес [2], DNS-сервер для іменування вузлів та веб-сервер для хостингу внутрішніх освітніх платформ.

Комп'ютерні класи підключені через окремі комутатори, що забезпечують оптимізацію трафіку та мінімізують ризики перевантаження. Кожен клас оснащений точкою доступу Wi-Fi для зручного підключення мобільних пристроїв [2]. Вчительська кімната та адміністративний відділ мають окремі підмережі з підвищеним рівнем безпеки, що унеможливлює сторонній доступ до конфіденційних даних.

Передбачені механізми резервного копіювання даних та аварійного відновлення, що дозволяють уникнути втрати критично важливої інформації [3]. Запроваджені системи моніторингу дозволяють адміністратору контролювати стан мережевого обладнання та виявляти аномалії в роботі системи.

Реалізація моделі мережевої архітектури надає можливість підвищити ефективність навчального процесу, забезпечити стабільний доступ до інформаційних ресурсів та створити безпечне цифрове середовище для всіх користувачів. Структурований підхід до проєктування

дозволяє адаптувати мережу під змінні потреби навчального закладу та забезпечити її подальший розвиток.

ДЖЕРЕЛА

1. Таненбаум Е. С., Везеролл Д. Комп'ютерні мережі. 6-те вид. Київ : Наукова думка, 2020.
2. Cisco Networking Academy. Як створити ефективну мережу, або маршрутизація та комутація для початківців. URL: https://www.cisco.com/c/dam/global/ru_ua/assets/ingswitchingbrochure_online_ukr_72.pdf (дата звернення: 11.03.2025).
3. Skoudis E. Counter Hack Reloaded: Network Security. 2nd ed. Pearson Education, 2021.

РОЗРОБКА ЗАСТОСУНКУ ДЛЯ ПІДТРИМКИ ВОДНОГО БАЛАНСУ НА БАЗІ REACT NATIVE ТА EXPO

Поліщук О. Р.
Київський столичний університет імені Бориса Грінченка, м. Київ

Сучасні інформаційні технології відіграють ключову роль у формуванні здорових звичок, зокрема серед молоді, допомагаючи підтримувати оптимальний водний баланс для покращення самопочуття та продуктивності. У рамках дипломного проєкту розроблено мобільний застосунок «HydrationApp» на базі React Native [1] з використанням Expo, що забезпечує кросплатформну сумісність для Android та iOS. Застосунок інтегрує автентифікацію через Firebase Authentication [2], хмарне сховище Firestore [3] для збереження даних користувачів і спожитих напоїв, а також правила безпеки Firebase [4] для захисту даних.

На поточному етапі реалізовано повноцінну функціональність застосунку, що включає шість основних екранів: AuthScreen (екран автентифікації з формами LoginForm для входу та RegisterForm для реєстрації), UserInfoForm (форма введення додаткових даних користувача: стать, дата народження, вага), HomeScreen (головний екран із калькулятором водного балансу та відображенням поточного прогресу), AddDrinkScreen (екран додавання напоїв із вибором типу напою, об’єму та часу споживання), ProfileScreen (екран профілю з можливістю редагування даних, зміни пароля, виходу або видалення акаунта) та StatisticScreen (екран статистики з відображенням історії спожитих напоїв у вигляді списку. Навігація між екранами забезпечується через бібліотеку react-navigation (createStackNavigator). Форми включають валідацію даних: перевірку email, пароля, імені, дати народження, а також об’єму напоїв і часу їх споживання.

Калькулятор водного балансу на HomeScreen обчислює необхідну норму води на основі даних користувача (вік, стать, вага, рівень фізичної

активності) та враховує коефіцієнти вмісту води в різних напоях (наприклад, 1.0 для води, 0.87 для молока). Дані про спожиті напої зберігаються в Firestore, а статистика на StatisticScreen відображає історію споживання за день із деталями (назва напою, об'єм, час, внесок у водний баланс).

Розробка велася у середовищі Visual Studio Code (рис. 1) з використанням Expo Go [5] для тестування на реальних пристроях. Для оптимізації продуктивності застосунку використано хуки React (useState, useEffect, useCallback, useFocusEffect), а для стилізації – StyleSheet із адаптивними розмірами через Dimensions. Інтерфейс додатково вдосконалено: додано анімації (ActivityIndicator під час збереження даних), інтерактивні кнопки (TouchableOpacity) та підтримку темного режиму.

Застосунок «HydrationApp» має потенціал для використання як окремими користувачами, так і в освітніх закладах. Наприклад, на уроках біології чи фізкультури вчителі можуть застосовувати його для навчання учнів контролювати питний режим, демонструючи важливість гідратації через інтерактивні графіки та статистику. У майбутньому планується додати push-повідомлення для нагадувань про питний режим, і графіки відображення споживання води користувачів.

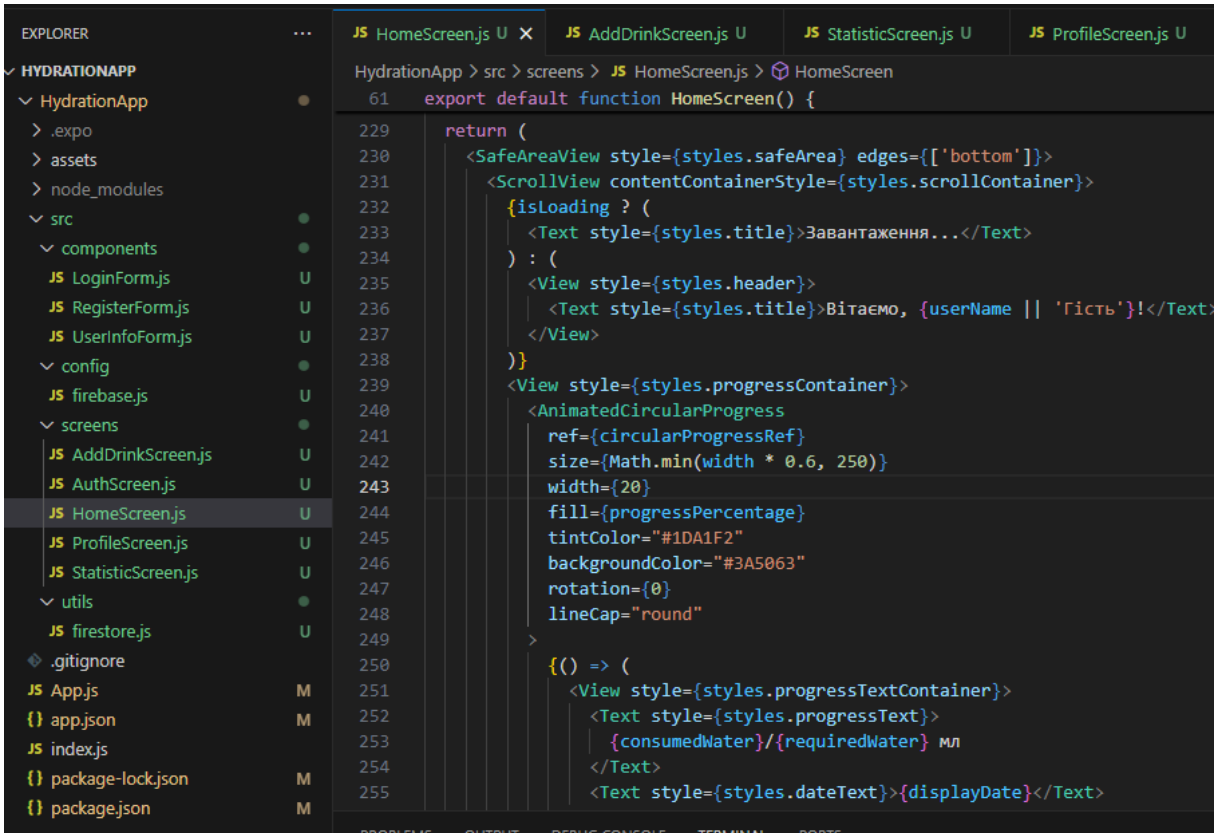


Рис. 1. Розробка мобільного застосунку для водного балансу на базі React Native та Expo в середовищі Visual Studio Code

ДЖЕРЕЛА

1. React Native Documentation. Building Mobile Apps with React Native. URL: https://reactnative.dev/docs/getting-started (дата звернення: 21.03.2025).
2. Firebase Documentation. Authenticate Users with Firebase Authentication. URL: https://firebase.google.com/docs/auth (дата звернення: 21.03.2025).
3. Firebase Documentation. Get Started with Cloud Firestore. URL: https://firebase.google.com/docs/firestore (дата звернення: 21.03.2025).
4. Firebase Documentation. Secure Your Data with Firebase Security Rules. URL: https://firebase.google.com/docs/firestore/security/get-started (дата звернення: 21.03.2025).
5. Expo Documentation. Getting Started with Expo. URL: https://docs.expo.dev/get-started/installation/ (дата звернення: 21.03.2025).

ІНТЕГРАЦІЯ СЕРВІСІВ ШІ В ХМАРНУ ІНФРАСТРУКТУРУ: АРХІТЕКТУРНІ ПІДХОДИ ТА КЕЙСИ ЗАСТОСУВАННЯ

Полтавський І. А., Яскевич В. О.

Державний університет інформаційно-комунікаційних технологій, м. Київ

З розвитком цифрових технологій інтеграція сервісів ШІ у хмарну інфраструктуру стала важливим напрямом у сфері побудови масштабованих, адаптивних і розумних систем. Хмарні обчислення надають необхідну гнучкість, а інструменти ШІ – інтелектуальність, що разом забезпечує конкурентну перевагу для компаній. Проте реалізація такої інтеграції вимагає глибокого розуміння архітектури рішень, вибору відповідних інструментів та дотримання принципів безпеки і продуктивності систем.

Метою цієї роботи є аналіз архітектурних моделей, які застосовуються для інтеграції ШІ в хмарні середовища, а також розгляд практичних прикладів і рекомендацій щодо впровадження подібних рішень.

- Аналіз літератури: Вивчено наукові публікації, документацію хмарних провайдерів та кейси впровадження ШІ у хмарні сервіси.
- Огляд та порівняння архітектур: Проведено аналіз класичних моделей – монолітної, мікросервісної, контейнерної та serverless-архітектури, що використовуються при інтеграції AI-рішень у хмару[1].
- Вивчення кейсів: Досліджено реальні приклади інтеграції ШІ в хмарну інфраструктуру з таких сфер, як електронна комерція, охорона здоров’я, транспорт.

- Порівняльний аналіз інструментів: Розглянуто інструменти AWS AI Services, Google Vertex AI, Microsoft Azure Cognitive Services та їх архітектурну інтеграцію[2 - 4].

Виявлено, що найбільш ефективним підходом для швидкого розгортання AI-сервісів є використання serverless-моделі, яка зменшує витрати на інфраструктуру і спрощує масштабування. При використанні мікросервісів спостерігається висока гнучкість у виборі мов програмування та бібліотек. Наприклад, AWS Lambda у поєднанні з Amazon SageMaker дозволяє створювати високопродуктивні сервіси машинного навчання без потреби в керуванні серверами.

Серед кейсів інтеграції можна виділити:

- Розпізнавання мови в call-центрах (Google Speech-to-Text у GCP);
- Автоматичне сортування запитів клієнтів (Azure AI з Power Platform);
- Медичну діагностику на основі аналізу зображень (AWS Rekognition).

Ключовими викликами залишаються питання безпеки при передачі конфіденційних даних, потреба в автоматичному масштабуванні моделей ШІ та сумісність з існуючими корпоративними системами[5].

Для компаній, що прагнуть інтегрувати сервіси ШІ у свої хмарні рішення, доцільно:

- Використовувати container-based або serverless-архітектури для швидкої інтеграції і масштабованості [6];
- Обирати платформи, які надають end-to-end сервіси для підготовки, навчання та розгортання моделей (наприклад, Google Vertex AI);
- Забезпечувати шифрування даних на всіх етапах та дотримання принципів zero trust security [6];
- Проводити тестування продуктивності моделей в умовах пікового навантаження.

Інтеграція сервісів штучного інтелекту у хмарну інфраструктуру відкриває нові горизонти для автоматизації, аналітики та взаємодії з клієнтами. Вибір архітектури та інструментів має базуватися на потребах проєкту, ресурсах компанії та вимогах до безпеки. Подальший розвиток хмарних AI-платформ дозволить ще більше спростити впровадження ШІ в бізнес-процеси.

ДЖЕРЕЛА

1. Hsieh, M. T., & Chen, Y. J. (2023). Architectural Patterns for AI Cloud Integration. Journal of Cloud Computing, 12(3), 104–117.

2. AWS AI Services – Режим доступу: https://aws.amazon.com/machine-learning/

3. Google Cloud Vertex AI – Режим доступу: https://cloud.google.com/vertex-ai
4. Azure Cognitive Services – Режим доступу: https://azure.microsoft.com/en-us/services/cognitive-services/
5. Serverless Architectures and AI: A New Era of Scalable Intelligence [Електронний ресурс] – Режим доступу: https://arxiv.org/abs/2305.11278
6. Han, Y., & Zhao, J. (2022). Security Challenges in Cloud-based AI Systems. IEEE Access, 10, 155093–155105.

ДОЦІЛЬНІСТЬ РОЗРОБКИ ДОДАТКУ ДЛЯ ПЕРСОНАЛЬНИХ ФІНАНСІВ

Прокопчук О. С., Вакалюк Т. А.
Державний університет «Житомирська політехніка», м. Житомир

За 30 років незалежності держави, населення України змогло перебороти велику кількість фінансових і економічних криз, що розвили високий рівень адаптивності до фінансових змін у країні. Попри це, за даними дослідження, яке було проведено із застосуванням міжнародної методології ОЕСР (Організація економічного співробітництва та розвитку) спільно з Національним банком України, середній рівень фінансової грамотності громадян нашої держави у 2021 році становив лише 12,3 бали з 21 можливого [1]. У той час, як середній бал серед високорозвинених країн, що мають національну стратегію розвитку з питань фінансів, яка спрямована на популяризацію фінансової культури становить більше ніж 13,2 [1].

Брак навичок управління грошовими потоками зумовлює людину покладатися на свої імпульсивні емоції, а не на раціонально-економічно вигідні рішення. Ці аспекти створюють передумови для прямої загрози, як на особистому рівні для громадян, так і макрорівні на стійкість економічного розвитку держави.

На жаль, у нашій країні присутня нестача програмного забезпечення, націленого на вирішення питання самоосвіти громадян у галузі фінансової грамотності. Відповідно до цього, постає питання, щодо створення інноваційно-цифрових рішень, які спрямовані на підвищення грамотності громадян у цій сфері.

Впровадження цифрових рішень для моніторингу особистих коштів дозволяє автоматизувати процес аналізу бюджету, що допоможе користувачам свідомо підходити до планування своїх фінансів та уникати матеріальних труднощів. Недостатня зацікавленість населення країни у підвищенні рівня своїх знань в області економіки, відсутність розуміння ризиків у безпеці особистих коштів в умовах цифрової економіки та поява страху перед складністю нових цифрових продуктів, породжують перешкоди для розвитку стабільних фінансових стратегій.

Кінцевою метою є проектування додатку персонального фінансування, завдяки якому користувачі зможуть структурувати грошові

операції, здійснювати контроль доходів та витрат, а разом з тим, досягати поставлених цілей. Застосунок буде скерований на роль особистого фінансового помічника, який реалізований у простому та інтуїтивно-зрозумілому форматі для кожного покоління.

Для реалізації необхідно знайти комплексне поєднання технологій, які гарантуватимуть найкращий баланс між клієнтською частиною, серверним компонентом та базою даних, що будуть спроможні задовольнити основні вимоги сучасних фінансових сервісів.

Фронтенд-розробка додатку спирається на використання React, який забезпечує побудову гнучких та масштабованих інтерфейсів. Застосунки, які використовуються для планування бюджету, потребують швидкого оновленню даних у реальному часі, обмежуючись необхідністю повного повторного відображення сторінки, що стало ключовим фактором для вибору саме цієї бібліотеки.

У виборі бекенд-розробки були популярні та конкурентоспроможні технології, які б могли виконати функціонал, який потребує додаток. Однак, втілення в життя серверної частини бере на себе Node.js у поєднанні з фреймворком Express.js, що забезпечить ефективну обробку великої кількості одночасних запитів та швидку взаємодію з базою даних у режимі реального часу, що є головною потребою розробки даного застосунку.

Особливу увагу для застосунків, що взаємодіють з фінансами, приділяють вибору бази даних, яка має високий рівень надійності та безпеки, що допоможе уникнути витоку інформації, навіть у разі збоїв програми. Найкращим варіантом в наших потребах слугує – PostgreSQL, яка входить до найпотужніших реляційних систем управління з відкритим програмним забезпеченням.

Результатом розробки буде додаток персонального фінансування, головна ціль якого – підвищення загального рівня знань і розуміння економічних процесів серед громадян країни в умовах активної експлуатації цифрових можливостей. З використанням сучасних бібліотек та фреймворків для клієнтської частини додатку, застосунок отримує можливість надання користувачу інтуїтивно-зрозумілий інтерфейс, що покриває виконання всіх поставлених завдань та сприяє надійності у серверному інтерфейсі. Обрані технології забезпечать безпеку, стабільність та ефективність функціонування програмного забезпечення, що є ключовим у роботі з фінансовими системами. У перспективному майбутньому імплементація подібних інноваційно-цифрових продуктів на ринок, має потенціал стати чинником зміцнення фінансової спроможності домогосподарств і стимулювати загальний економічний розвиток країни.

ДЖЕРЕЛА

1. OECD/INFE 2023 International Survey of Adult Financial Literacy. OECD Publishing, 2023. URL: https://surli.cc/rirtad [Online; accessed 27.04.2025]

2. How to Build a Fintech App: Complete Guide. Stfalcon. 2024. URL: https://stfalcon.com/uk/blog/post/how-to-build-a-fintech-app-complete-guide [Online; accessed 27.04.2025]

АНАЛІЗ ДОДАТКІВ ДЛЯ ПЕРСОНАЛЬНИХ ФІНАНСІВ

Прокопчук О. С., Вакалюк Т. А.
Державний університет «Житомирська політехніка», м. Житомир, Україна

У реаліях сьогодення, що ґрунтуються на використанні інноваційно-цифрових технологій та в умовах інтенсивного ритму життя, коли часові обмеження перешкоджають раціональному плануванню бюджету – зростає попит на застосунки, які спрямовані на підвищення рівня відповідальності людини за кошти, прийняття обґрунтованих рішень та мінімізація ймовірності виникнення ризиків імпульсивних витрат, що створюють передумови для забезпечення довгострокової фінансової стабільності. Комбінування цих ключових аспектів, вже присутнє на сучасному ринку програмних забезпечень, таких як Wallet та Money Lover. На жаль, не всі додатки мають найкращий баланс у поєднані динамічного розширення функціональних можливостей системи, доступну візуалізацію фінансових даних та інтерфейсу, який орієнтований на зручність користувача.

Мобільний додаток Wallet by BudgetBakers полегшує користувачам процес моніторингу особистих грошових потоків у режимі реального часу. Дана платформа забезпечує можливість детального розуміння потоків грошових надходжень і витрат, за допомогою візуалізації у вигляді графіків та діаграм [1]. Окрім цього, цей аналог сприяє своєчасному здійсненню фінансових операцій користувачів сервісу, завдяки впровадженій системі нагадування про заплановані платежі. На рис. 1 можна переглянути візуальну модель взаємодії з користувачем через систему, що пропонує широкий функціонал і графічний аналіз.

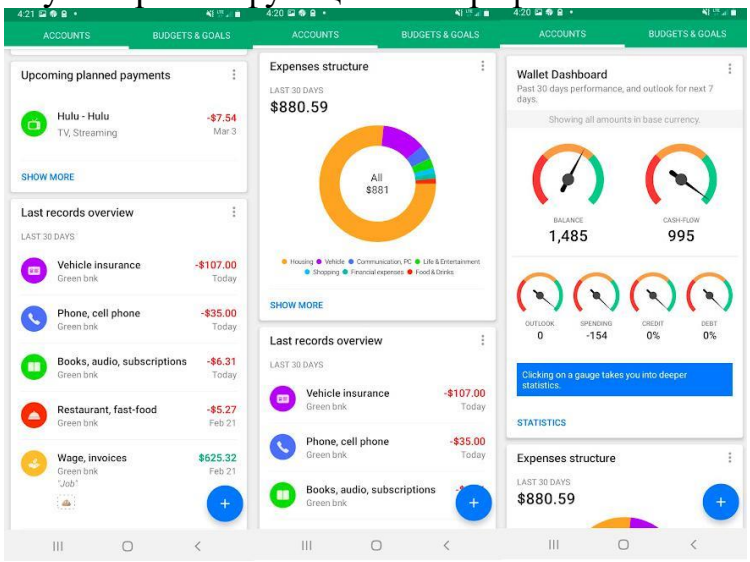


Рис. 1. Інтерфейс мобільного застосунку Wallet

Money Lover – альтернативний представник додатків персонального фінансування, який акцентує увагу на управлінні боргами, кредитами та розрахунку грошових зобов'язань [2]. Програмне забезпечення надає можливості користувачу визначати планові матеріальні цілі, упорядковувати категоризацію доходів і видатків, а також, як і в Wallet є можливість інтегрування сповіщень про проведення необхідних сплат. Як зазначено вище, цей застосунок націлений на функціонал обліку боргових зобов'язань, який надає можливість встановлення суми боргу, періодичності виплат та автоматичне оновлення, що надає проаналізовану інформацію про виплати та загальний бюджет. На рис. 2 пропонується можливість перегляду інтуїтивно зрозумілого інтерфейсу, який дозволяє аналізувати витрати та доходи за допомогою інтерактивних графіків.

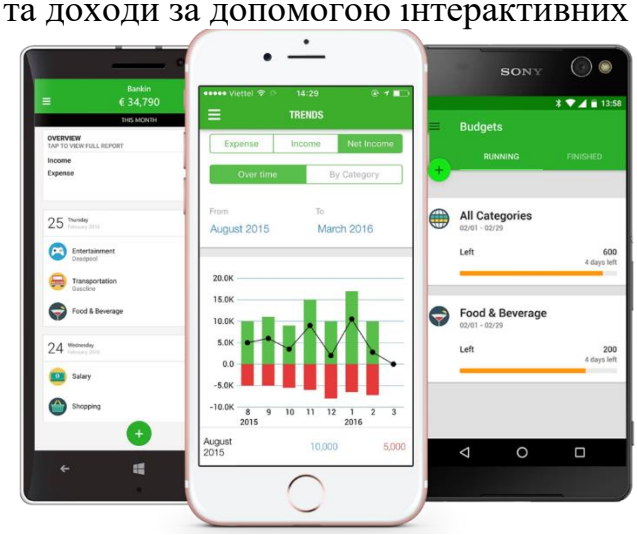


Рис. 2. Візуальне представлення додатку Money Lover

Обидва аналоги пропонують користувачу облік грошових потоків, визначення матеріальної цілі та створення накопичувальних планів, що справляють вплив, як джерела критичного мислення для підвищення ймовірності досягнення довгострокових цілей, фінансових стратегій та покращують розуміння динаміки фінансових потоків клієнта. Водночас з цим, у варіантах, що розглядаються, відсутня глибока персоналізація фінансових цілей, розроблення прогнозних моделей витрат і поглибленого аналізу фінансової активності, що надають можливість приймати більш раціональні рішення щодо подальшого планування бюджету.

Беручи до уваги вказані чинники, обумовлюється необхідність у створенні удосконаленого варіанту, який поєднає найкращі практичні інструменти наявних аналогів та зорієнтує на спеціалізовані потреби сучасних користувачів.

ДЖЕРЕЛА

1. Wallet by BudgetBakers URL: https://budgetbakers.com/wallet/ [Online; accessed 28.04.2025]

2. Money Lover: Personal Finance App. URL: https://moneylover.me/ [Online; accessed 28.04.2025]

РОЗПАРАЛЕЛЕННЯ РЕНДЕРИНГУ НА АПАРАТНОМУ РІВНІ

Романюк О. Н., Бобко О. Л.
Вінницький національний технічний університет, м. Вінниця

Розпаралелення рендерингу [1 – 4] на апаратному рівні є фундаментальною основою сучасних графічних процесорів (GPU) і забезпечує значне прискорення обробки сцен завдяки одночасному виконанню великої кількості обчислювальних завдань. Архітектура GPU спеціально побудована так, щоб мати велику кількість обчислювальних ядер, кожне з яких здатне паралельно обробляти окремі елементи сцени – вершини, трикутники, пікселі або фрагменти. На першому рівні розпаралелення здійснюється обробка вершин: кожна вершина тривимірної моделі може бути незалежно трансформована у просторі за допомогою шейдерів вершин. Після проектування об'єктів на площину екрана відбувається растеризація, яка генерує величезну кількість фрагментів або потенційних пікселів, і кожен з них також обробляється незалежно – обчислюється його колір, освітлення, накладаються текстури та перевіряється глибина. Крім того, обробка трикутників сцени, включно з операціями відсікання невидимих частин або перевіркою на видимість, також виконується паралельно. Щоб підвищити ефективність обчислень, сучасні GPU реалізують принцип SIMD, за якого одна інструкція одночасно застосовується до кількох елементів даних. Апаратні планувальники, такі як Warp Scheduler у NVIDIA чи Wavefront Scheduler в AMD, автоматично розподіляють завдання між обчислювальними блоками так, щоб мінімізувати затримки й забезпечити максимальне завантаження ресурсів. Окрему роль відіграють стратегії організації пам’яті, наприклад, tile-based rendering, коли сцена розбивається на невеликі області (плитки), і кожна плитка обробляється окремо, що зменшує витрати пам'яті та підвищує енергоефективність, особливо в мобільних пристроях. Для спеціалізованих задач, як-от трасування променів, на апаратному рівні реалізуються прискорювачі типу RT Cores (NVIDIA) або Ray Accelerators (AMD), які паралелять обчислення перетинів променів із об'єктами сцени. Попри прагнення до максимальної паралельності, деякі етапи вимагають синхронізації, наприклад, запис у буфери глибини або операції змішування кольорів, що вирішується за допомогою апаратних механізмів контролю доступу до спільних ресурсів. Загалом, розпаралелення рендерингу на апаратному рівні поєднує масштабовану архітектуру, інтелектуальне управління виконанням задач, оптимізовану взаємодію з пам'яттю та спеціалізовані блоки обробки, що разом дозволяють сучасним GPU досягати обробки мільйонів операцій за мілісекунди та створювати фотореалістичні зображення в реальному часі.

Важливою особливістю апаратного розпаралелення рендерингу є те, що весь процес побудований на максимально незалежній обробці даних, що мінімізує необхідність обміну інформацією між обчислювальними одиницями, оскільки будь-яка синхронізація уповільнює загальну продуктивність. Саме тому у графічних процесорах використовуються масивні масивно-паралельні архітектури з великою кількістю потокових процесорів, кожен з яких працює над окремим фрагментом завдання. Також важливим елементом є структура пам'яті: у сучасних GPU присутні швидкі локальні регістри, кеші на рівні обчислювальних блоків і глобальна пам'ять, доступ до якої суворо контролюється для уникнення конфліктів при паралельному записі або читанні даних. В умовах реального часу це дозволяє досягати надзвичайно високої пропускної здатності для обробки великих обсягів графічної інформації, що особливо важливо для ігор, віртуальної реальності, наукової візуалізації та промислових CAD-систем.

Важливо відзначити впровадження технологій апаратного прискорення трасування променів, яке значно змінює підходи до візуалізації складних світлових ефектів завдяки можливості одночасного оброблення величезної кількості променів. В цьому випадку розпаралелення відбувається не лише на рівні окремих пікселів чи фрагментів, а й на рівні обробки шляхів світла, розгалуження і вторинних променів. Інша важлива тенденція – інтеграція спеціалізованих блоків для штучного інтелекту, наприклад Tensor Cores в архітектурі NVIDIA, які дозволяють використовувати методи глибинного навчання для підвищення якості рендерингу, такі як масштабування роздільної здатності або інтелектуальне згладжування країв зображення. Всі ці інновації базуються на ідеї максимально широкого і гнучкого розпаралелення обчислень, що дає змогу GPU залишатися найпотужнішою обчислювальною платформою у сфері графіки і дедалі більше використовуватися для вирішення задач поза межами класичного рендерингу, у тому числі в наукових обчисленнях, нейромережах і аналізі великих даних. Таким чином, розпаралелення рендерингу на апаратному рівні не є просто технічним прийомом оптимізації, а є сутністю всієї еволюції графічних процесорів, яка спрямована на забезпечення максимального співвідношення продуктивності до енергоспоживання та гнучкості обробки надзвичайно великих обсягів візуальної інформації.

ДЖЕРЕЛА

1. Chalmers A., Reinhard E., Davis T. Practical Parallel Rendering. – Boca Raton: CRC Press, 2020. – 392 с.

2. Walker C. GPU Architecture: The Ultimate Guide to Building High-Performance Computing Systems. – Independently published, 2022. – 312 с.

3. Романюк О. Н., Чорний А. В. Високопродуктивні методи та засоби зафарбовування тривимірних графічних об'єктів: монографія. – Вінниця: УНІВЕСУМ-Вінниця, 2007. – 190 с.Ірбіс НБУВ+4Google Scholar+4moderntechno.de+4

4. Романюк О. Н., Романюк О. В., Чехместрук Р. Ю. Комп'ютерна графіка: навчальний посібник. – Вінниця: ВНТУ, 2023. – 147 с.

ВИКОРИСТАННЯ ВЕЛИКИХ ДАНИХ ПРИ ФОРМУВАННІ ТРИВИМІРНИХ ГРАФІЧНИХ ЗОБРАЖЕНЬ

Романюк О. Н., Ромапюк О. В.

Вінницький національний технічний університет, м. Вінниця

Використання великих даних (Big Data) [1, 2] у формуванні тривимірних графічних зображень відкриває нові можливості у галузях комп’ютерної графіки, візуалізації, розширеної реальності (AR) та ігор. У першу чергу великі дані дозволяють покращити якість тривимірного зображення шляхом використання масивів реальних або симульованих даних, що описують геометрію, освітлення, матеріали, текстури та поведінку об'єктів у просторі. Наприклад, у сфері архітектурної візуалізації або урбаністичного моделювання тривимірні сцени будуються на основі даних з геопросторових баз (GIS), супутникових знімків, лазерного сканування та фотографічних реконструкцій (photogrammetry), що надають надзвичайно точне представлення рельєфу, будівель і навколишнього середовища. У випадку медичної візуалізації великі обсяги даних із МРТ, КТ чи УЗД обробляються й перетворюються на тривимірні моделі органів, що дозволяє здійснювати точне моделювання операцій або діагностику. У сфері комп’ютерної графіки для ігор та кіно Big Data застосовуються для генерації процедурних світів, у яких ландшафти, екосистеми, текстури і навіть анімації NPC формуються на основі статистичних моделей, зібраних із реального світу чи поведінки гравців. Алгоритми штучного інтелекту, навчені на великих масивах даних, здатні автоматично генерувати детальні моделі при створенні контенту.

У візуалізації наукових даних великі обсяги числової або симуляційної інформації (наприклад, в аеродинаміці, астрофізиці чи кліматичних моделях) використовуються для побудови складних тривимірних полів тиску, температури чи швидкості, що потребує оптимізованих алгоритмів обробки й відображення. Для цього використовуються розподілені обчислення, GPU-акселерація та спеціалізовані інструменти на кшталт ParaView або VTK, які працюють з терабайтними обсягами даних. Також великі дані важливі для навчання нейронних мереж у тривимірному рендерингу, таких як нейронні радіансові поля, які потребують величезних обсягів зображень і камерних

параметрів для відтворення реалістичного 3D-середовища на основі двовимірних даних. Такі підходи кардинально змінюють підхід до 3D-реконструкції, роблячи її доступною без точного 3D-сканування, використовуючи лише набори зображень.

Розглягнемо базові аспекти, які особливо важливі у сучасній практиці. Перший аспект – це інтеграція Big Data з реального часу для формування динамічних тривимірних сцен. Наприклад, у системах моніторингу дорожнього руху або «розумного міста» тривимірні моделі оновлюються у режимі реального часу за допомогою даних із сенсорів, камер, супутників або IoT-пристроїв. Це дозволяє створювати цифрові двійники, які точно відображають поточний стан інфраструктури, транспорту або навіть мікроклімату. Такі моделі не лише візуалізуються в 3D, але й використовуються для симуляцій, прогнозів або прийняття рішень. Другий аспект - це персоналізована візуалізація на основі поведінкових даних. У вебдизайні, архітектурі або віртуальних турах дані про переміщення погляду користувача (eye tracking), кліки, вибори та переваги збираються у великих обсягах і використовуються для адаптивного рендерингу сцен. Наприклад, у VR/AR-системах можливо використовувати фовійований рендеринг, який на основі даних про положення ока формує максимально деталізовану зону лише там, куди дивиться користувач, що істотно оптимізує витрати ресурсів. Третій аспект – машинне навчання для класифікації, семантичного розпізнавання та сегментації тривимірних сцен. Алгоритми глибокого навчання, навчені на величезних тривимірних, дозволяють автоматично розпізнавати об’єкти, визначати матеріали поверхонь, класифікувати типи структур або навіть передбачати, як сцена виглядатиме з інших кутів огляду. Це застосовується як у CAD/CAE системах, так і в геймінгу або моделюванні інтер'єру. Четвертий аспект - стиск і трансформація великих масивів тривимірних даних. Обсяги 3D-даних, отриманих із сканерів або фотограмметричних методів, можуть сягати десятків гігабайт або терабайт. Для їх обробки застосовують адаптивне стиснення (наприклад,, downsampling, побудову октавних дерев (octree) або методи вейвлет-перетворення, які дозволяють зберігати високу візуальну якість при обмеженому обсязі ресурсів. П’ятий аспект – інтеграція хмарних сервісів для розподіленого зберігання й обробки великих 3D-даних. Платформи типу Amazon Web Services, Google Cloud чи Microsoft Azure надають можливість створення хмарних пайплайнів, у яких 3D-сцени генеруються, рендеряться і транслюються користувачу в браузер або VR-шолом без необхідності локального зберігання моделей. Це забезпечує масштабованість, гнучкість і доступність складних тривимірних обчислень. Завдяки аналізу накопичених даних про фізичні властивості матеріалів, освітлення, динаміку об'єктів та поведінку користувачів, системи можуть заздалегідь

передбачати найоптимальніші параметри рендерингу, автоматично налаштовувати сцени або підбирати шейдери. иких даних.

ДЖЕРЕЛА

1. Романюк О.Н., Павлов С.В., Бобко О.Л., Завальнюк Є.К., Решетнік О.О. Аналіз великих даних у комп'ютерній графіці. Оптико-електронні інформаційно-енергетичні технології», 2024, №47(1), с. 50–57.

2. James D. Miller «Big Data Visualization» Packt Publishing, 2016, 304 p.

ІНСТРУМЕНТИ ДЛЯ ПОКРАЩЕННЯ USER EXPERIENCE В ІГРОВИХ ЗАСТОСУНКАХ

Сапожник М.

Київський столичний університет імені Бориса Грінченка, м. Київ

Інформаційні технології стали невід'ємною частиною індустрії відеоігор, уможлививши покращення взаємодії користувачів з цифровими продуктами. Покращення користувацького досвіду (UX) ігрового додатку відіграє ключову роль у залученні та утриманні гравців завдяки інтуїтивно зрозумілому інтерфейсу, швидкій навігації та комфортному використанню ігрової механіки.

Покращення користувацького інтерфейсу в іграх має вирішальне значення через кілька ключових факторів. По-перше, сучасні ігрові механіки стають дедалі складнішими і вимагають користувацького інтерфейсу, який забезпечує легкий доступ до великої кількості функцій, не перевантажуючи гравця. По-друге, цільова аудиторія ігор розширюється, тому користувацький інтерфейс повинен бути інтуїтивно зрозумілим як для досвідчених гравців, так і для новачків. Оскільки в ігри можна грати на ПК, мобільних пристроях або консолях, важливо також враховувати мультиплатформеність, що вимагає адаптивного інтерфейсу. Крім того, ефективний користувацький інтерфейс допомагає залучити гравця до гри та уникнути розчарування, спричиненого незрозумілим управлінням та складною навігацією.

Сучасні технології дозволяють впроваджувати адаптивні інтерфейси, інтерактивні підказки та інші елементи, що покращують користувацький досвід. Серед найпопулярніших інструментів, що використовуються для розробки рішень, орієнтованих на користувацький досвід у відеоіграх, - Unity та ігровий рушій Godot. Ці платформи пропонують різноманітні інструменти для створення динамічних користувацьких інтерфейсів, налаштування відповідної навігації, A/B тестування для оптимізації користувацького досвіду тощо.

Автор проаналізував існуючі методи дослідження користувацького досвіду, щоб розробити підхід для покращення взаємодії з користувачем в

ігрових додатках та продемонструвати його застосовність у середовищах Unity та Godot. Результати дослідження представлені в таблиці 1.

Таблиця 1

Порівняння інструментів для UX в Unity та Godot

Функція	**Unity UI Toolkit**	**Godot UI System**
Адаптивний UI	Так	Так
Інтерактивні підказки	Так	Так
Динамічне розташування	Обмежене	Гнучке
Легка інтеграція з кодом	Висока	Середня
Гнучкість у налаштуваннях	Висока	Висока
A/B тестування	Так	Так
Підтримка плагінів	Велика кількість	Обмежена
Вбудовані аналітичні інструменти	Unity Analytics	Відсутні

У таблиці порівнюються можливості інструментів UX-дизайну ігрових рушіїв Unity та Godot. Обидві системи підтримують адаптивний інтерфейс, інтерактивні підказки та A/B-тестування, але відрізняються гнучкістю компонування елементів: інструментарій Unity UI Toolkit має обмежені можливості динамічного позиціонування, в той час як система інтерфейсу Godot має більш гнучкіший підхід. Unity також пропонує кращу інтеграцію коду та широку підтримку плагінів, тоді як Godot поступається в цих аспектах; основною перевагою Unity є вбудовані можливості аналізу (Unity Analytics), яких немає в Godot.

Отже, Unity пропонує більше можливостей для розширення функціональності за допомогою плагінів та інструментів аналізу, тоді як Godot пропонує більшу гнучкість у налаштуванні інтерфейсу користувача. Вибір між цими інструментами залежить від потреб проекту: Unity краще підходить для великих комерційних продуктів, тоді як Godot - для гнучких і менш ресурсоємних рішень.

ДЖЕРЕЛА

1. Nielsen J. Usability Engineering. Morgan Kaufmann, 1994. [с. 45] https://dl.acm.org/doi/book/10.5555/2821575

2. Norman D. The Design of Everyday Things. Basic Books, 2013. [с. 112] https://dl.icdst.org/pdfs/files4/4bb8d08a9b309df7d86e62ec4056ceef.pdf

3. Hoober S. How Do Users Really Hold Mobile Devices? UXmatters, 2013. [Online]. Available: https://www.uxmatters.com/mt/archives/2013/02/how-do-users-really-hold-mobile-devices.php

4. Mobile Health Applications to Promote Active and Healthy Ageing. Multidisciplinary Digital Publishing Institute, 2017. [Online]. Available: http://www.mdpi.com/1424-8220/17/3/622/htm

5. Unity Documentation: UI Toolkit. Available: https://docs.unity3d.com/ [с.8]
6. Godot Docs: User Interface Design. Available: https://docs.godotengine.org/ [с. 14]
7. Shneiderman B. Designing the User Interface: Strategies for Effective Human-Computer Interaction. Pearson, 2016. [с. 289] http://seu1.org/files/level5/IT201/Book%20-%20Ben%20Shneiderman-Designing%20the%20User%20Interface-4th%20Edition.pdf
8. Garrett J. The Elements of User Experience: User-Centered Design for the Web and Beyond. New Riders, 2010. [с. 76] https://www.academia.edu/33276128/The_Elements_of_User_Experience_Jesse_James_Garrett
9. Smith J. Comparative Analysis of UI/UX in Game Development. ACM Press, 2020. [с. 57] https://in.linkedin.com/in/smith-j-sawan-1a8747164

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У МОБІЛЬНОМУ ДОДАТКУ ДЛЯ ПІДБОРУ ОДЯГУ

Сікалюк М. В.
Державний університет інформаційно-комунікаційних технологій, м. Київ

У сучасних реаліях цифрового суспільства мобільні додатки відіграють ключову роль у повсякденному житті, збираючи і обробляючи велику кількість персональних даних користувачів. Додатки, що надають персоналізовані рекомендації, зокрема рекомендації щодо одягу відповідно до погодних умов і психологічного стану користувача, зобов'язані гарантувати безпеку та конфіденційність оброблюваної інформації [1].

Під час використання додатку, користувач може вводити чутливі дані, наприклад:

- персональні параметри (зріст, вага, стать);
- локалізацію (для доступу до погодних умов);
- інформацію про настрій (що потенційно стосується психологічного стану).

Основні загрози безпеці:

1. **Несанкціонований доступ до персональних даних** – при недбалому зберіганні або передачі даних;
2. **Перехоплення даних при авторизації** – якщо відсутнє шифрування на рівні API;
3. **Злам облікового запису** – при слабкій політиці паролів або їх ненадійному зберіганні;

Заходи безпеки, реалізовані у мобільному додатку:

1. Шифрування паролів

Паролі користувачів зберігаються у базі даних лише в зашифрованому вигляді з використанням алгоритму bcrypt. Він забезпечує

додатковий захист завдяки використанню солі (salt) та великій кількості раундів хешування, що значно ускладнює злам методом brute-force [2].

2. Токенізація та аутентифікація

Кожен запит до серверу супроводжується авторизаційним токеном (JWT), який зберігається у захищеному сховищі пристрою (SecureStorage/Keychain). Це дозволяє уникнути постійного пересилання логін-пароль зв'язки та забезпечує контроль доступу до персоналізованих рекомендацій.

3. HTTPS і сертифікати

Усі запити до серверної частини додатку виконуються через захищений протокол HTTPS із використанням TLS-сертифікатів. Це унеможливлює MITM-атаки та гарантує цілісність переданої інформації.

4. Обмеження доступу до API

Використовується система ролей і перевірки прав доступу: наприклад, лише авторизовані користувачі можуть змінювати профіль, бачити історію або переглядати рекомендації.

Таким чином, навіть у додатку, що здається побутовим або простим, реалізація базових принципів інформаційної безпеки є обов'язковою умовою для збереження довіри користувачів та відповідності сучасним вимогам безпеки.

ДЖЕРЕЛА

1. Савченко О.Ю., Прокопенко Є.В. (2020). Захист персональних даних у мобільних додатках. *Збірник наукових праць НТУУ «КПІ», Серія: Інформатика та кібернетика*, №3(51), С. 112–117.

2. Mazurek G., Małysa-Kaleta A. (2018). Data protection and user privacy in mobile apps – legal and technical aspects. *Journal of Computer Science and Control Systems*, Vol. 11(2), pp. 87–93.

3. OWASP Mobile Top 10 Risks – [Електронний ресурс] – Режим доступу: https://owasp.org/www-project-mobile-top-10/

РОЗРОБКА ІНФОРМАЦІЙНОЇ СИСТЕМИ РЕГІОНАЛЬНОГО ЦЕНТРУ ЗАЙНЯТОСТІ

Соломаха О. В.

Київський столичний університет імені Бориса Грінченка, м. Київ

Сьогодні існують численні способи пошуку персоналу, проте Державні центри зайнятості [1] і дотепер не втрачають важливої ролі у цьому процесі, оскільки не тільки ведуть державний облік безробітних та уповноважені нарахувати державну допомогу, а й надають послуги з пошуку роботи, профорієнтації та перепідготовки кадрів за державний рахунок. Однак методи роботи до сьогодні засновані на паперовому документообігу та ручному опрацюванні інформації.

Впровадження автоматизації послуг значно покращить роботу Державних центрів зайнятості та зробити їхні послуги доступнішими та зручнішими для користувачів, що, як наслідок, призведе до підвищення ефективності роботи цих центрів на всіх рівнях, прискорення процесу пошуку робити, створення нових можливостей співпраці пошукачів та роботодавців та зниження рівня безробіття в країні.

Сучасні регіональні центри зайнятості є неприбутковою державною установою, фінансування якої відбувається коштом Фонду загальнообов‘язкового державного соціального страхування України на випадок безробіття. Вони виконують як функцію прямого працевлаштування, так і реалізують державну політику у сфері зайнятості населення [1]. Відповідно з метою підвищення ефективності та продуктивності роботи Державної служби зайнятості загалом, а регіональних центрів зокрема, необхідно збирати та обробляти великі масиви інформації, а саме:

- інформацію про безробітних;
- інформацію про вакансії;
- інформацію про роботодавців;
- інформацію про надані направлення;
- інформацію про кар’єрних радників [2].

Програмний додаток має такі функціональні можливості, як от:

- ведення бази даних: зберігання інформації про безробітних, про вакансії, про роботодавців, надані направлення на вакансії, про кар’єрних радників.
- можливість пошуку вакансій за різними критеріями;
- постановка на облік пошукачі роботи;
- реєстрація вакансій роботодавцем;
- ведення звітності;
- інші можливості: онлайн-консультації з кар’єрним радником; навчальні курси та семінари з пошуку роботи; бібліотека матеріалів з пошуку роботи тощо.

Технічні вимоги до програмного комплексу:

- сумісний з сторонніми веб-браузерами та операційними системами;
- захищений від несанкціонованого доступу;
- простий у використанні із зручним інтерфейсом.

Для створення інформаційної системи регіонального центру зайнятості використано мову програмування C#, платформа .NET Core, фреймворк ASP.NET Core, архітектура Model-View-Controller, фреймворк Entity Framework Core, інтегроване середовище розробки Visual Studio, Angular.

Автоматизація та діджиталізація процесів обліку та працевлаштування пошукачів роботи за сприяння Державних центрів зайнятості засобами сучасних інформаційних технологій забезпечує

підвищення ефективності роботи цього державного органу та значну економію державних коштів вже у короткостроковій перспективі.

ДЖЕРЕЛА

1. Постанова Кабінету Міністрів України «Про затвердження Порядку реєстрації, перереєстрації безробітних та ведення обліку осіб, які шукають роботу» від 19 вересня 2018 р. № 792 URL: https://zakon.rada.gov.ua/laws/show/792-2018-%D0%BF#Text
2. Чернега А. Л. Структура, основні цілі, функції та аналіз показників ефективності функціонування органів служби зайнятості на різних рівнях / А. Л. Чернега // Бионика интеллекта. – 2016. – №1 (86). – С. 125–129.

ВИДИ АПАРАТНО-ПРОГРАМНИХ КОМПЛЕКСІВ (АПК) МОНІТОРИНГУ ЯКОСТІ ПОВІТРЯ

Степанець М. В.
Київський столичний університет імені Бориса Грінченка, м. Київ

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 SO_2, NO_2, CO, PM2.5, 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.

IoT-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 (GAHP), 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

МЕТОДОЛОГІЧНІ ПІДХОДИ ДО ІНТЕГРАЦІЇ ТЕСТУВАННЯ ПРОДУКТИВНОСТІ В ПАЙПЛАЙНИ БЕЗПЕРЕРВНОЇ ІНТЕГРАЦІЇ (CI/CD)

Сторожук Ю.В.

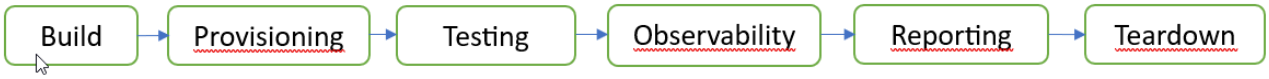
Вінницький національний технічний університет, м. Вінниця

Автоматизація тестування продуктивності є необхідним компонентом сучасного життєвого циклу розробки веборієнтованих систем. Її інтеграція у CI/CD (Continuous Integration / Continuous Delivery) [1] дає змогу оперативно виявляти зміни у продуктивності, зменшувати ризики на етапі релізу та забезпечувати стабільність роботи системи у виробничому середовищі.

Інфраструктурна автоматизація реалізується через концепцію Infrastructure as Code (IaC) [2]. Такий підхід забезпечує детальне описання інфраструктури у вигляді коду, що дозволяє розгортати, оновлювати та знищувати середовища автоматизовано. Для цього застосовуються такі інструменти як Terraform, Pulumi, Ansible та Helm. У контексті продуктивності це дає змогу розгортати повноцінне середовище під конкретні тести – з однаковими характеристиками, що виключає варіативність результатів.

Контейнеризація, зокрема Docker і Kubernetes, дає змогу створювати ізольовані середовища для тестування з чітко визначеними параметрами. Контейнери включають необхідні інструменти навантажувального тестування, такі як JMeter, k6 або Gatling, що значно спрощує налаштування. Helm-чарти або Kustomize дозволяють управляти залежностями та конфігураціями для різних середовищ, наприклад, тестового (test) та стейджевого (stage).

Серед CI/CD систем найбільш поширеними є Jenkins, GitHub Actions, GitLab CI, Tekton та Argo Workflows. Вони дозволяють будувати гнучкі пайплайни [3] з автоматичними тригерами, перевірками коду, запуском тестів та генерацією звітів. Розглянемо приклад пайплайну для тестування продуктивності, що включає наступні етапи:



- Build: Збірка артефактів, створення Docker-образів, перевірка залежностей через Snyk або Trivy.
- Provisioning: Автоматичне розгортання інфраструктури у хмарі (AWS, GCP, Azure) або в Kubernetes-кластері, з використанням IaC-інструментів.
- Testing: Запуск навантажувального тестування. JMeter або k6 виконує сценарії, що імітують поведінку користувачів, збираючи показники часу відгуку, навантаження на процесор і пам'ять, пропускну здатність, відсоток помилок тощо.
- Observability: Збір метрик здійснюється за допомогою Prometheus, Telegraf, InfluxDB або OpenTelemetry. Дані візуалізуються у Grafana або Kibana, що дозволяє оперативно виявляти відхилення.
- Reporting: Результати автоматично додаються до звітів, які можуть надсилатись у Slack, Email чи Jira.
- Teardown: Знищення всіх ресурсів після тесту для уникнення зайвих витрат і збереження чистоти середовища.

Отже, впровадження автоматизації тестування продуктивності за допомогою CI/CD не лише оптимізує процес розробки, а й створює фундамент для стійкої, масштабованої та якісної архітектури системи, що дозволяє зменшити залежність від ручних перевірок, забезпечити стабільні результати тестування та підвищити впевненість у працездатності програмного забезпечення у реальних умовах.

ДЖЕРЕЛА

1. Y. Jani, «Implementing continuous integration and con-tinuous deployment (CI/CD) in modern software de-velopment,» International Journal of Science and Re-search, vol. 12, no. 6, pp. 2984–2987, 2023
2. Ozdogan E., Ceran O., Ustundag M. T. Systematic Analysis of Infrastructure as Code Technologies // International Journal of Advances in Engineering and Pure Sciences. – 2023. – Vol. 35, № 1. – P. 72–83. – ISSN: 2149-6457
3. Ccallo, M., Quispe-Quispe, A. Adoption and Adaptation of CI/CD Practices in Very Small Software Development Entities: A Systematic Literature Review [Electronic resource] // arXiv preprint. – 2024. – arXiv:2410.00623.

ЗАХИСТ ІНФОРМАЦІЇ У ВЕБ-ЗАСТОСУНКУ ДЛЯ ПІДТРИМКИ МОЛОДІЖНИХ ІНІЦІАТИВ ГО «ЛІДЕРСЬКА ІНІЦІАТИВА»: ТЕХНОЛОГІЧНІ І СОЦІАЛЬНІ АСПЕКТИ БЕЗПЕКИ ЦИФРОВОГО СЕРЕДОВИЩА

Тарасюк М. С.
Державний університет інформаційно-комунікаційних технологій, м. Київ

У сучасному суспільстві цифрові технології стають одним із ключових інструментів для розвитку громадських ініціатив, зокрема молодіжних. Громадська організація «ЛІДЕРСЬКА ІНІЦІАТИВА» відіграє важливу роль у мобілізації молоді до соціальної активності, освітніх проєктів та волонтерських дій. У цьому контексті створення веб-застосунку, який би підтримував ініціативи молоді, стає не лише технічним, але й стратегічним завданням. Однак зростання цифрової активності обумовлює також підвищені вимоги до захисту персональних даних, безпеки збереження інформації та прозорості взаємодії в онлайн-середовищі.

У цифрову епоху зростає кількість кіберзагроз, спрямованих як на приватних осіб, так і на організації. Молодіжні ініціативи, що базуються на довірі, взаємодії та відкритості, можуть стати легкою мішенню в разі неналежного рівня захисту даних. Зокрема, при зборі заявок, пожертв або обробці персональної інформації користувачів необхідно забезпечити дотримання міжнародних та національних стандартів інформаційної безпеки. Таким чином, створення безпечної веб-платформи не лише гарантує стабільну роботу проєкту, але й підвищує рівень довіри з боку користувачів і партнерів.

Метою даної роботи є розробка функціонального веб-застосунку для ГО «ЛІДЕРСЬКА ІНІЦІАТИВА», який поєднуватиме зручність для користувачів з високим рівнем захисту інформації. Платформа має забезпечити безпечну реєстрацію, подання ініціатив, підтримку зборів коштів, а також надійне адміністрування даних з боку організації. Окремим аспектом дослідження є вивчення впливу безпеки системи на активність користувачів та ефективність цифрової взаємодії.

У межах даної роботи передбачено здійснення комплексного аналізу актуальних кіберзагроз, що стосуються громадських веб-застосунків, зокрема платформ для підтримки молодіжних ініціатив. Особлива увага приділяється дослідженню сучасних технологій захисту інформації, таких як протоколи шифрування даних, механізми автентифікації та авторизації, а також підходи до безпечної обробки транзакцій. На основі проведеного аналізу буде сформовано функціональні та нефункціональні вимоги до системи з акцентом на забезпечення безпеки користувацьких даних.

Подальшим етапом стане розробка архітектури веб-застосунку з використанням мікросервісної моделі, яка забезпечить гнучкість, масштабованість і стійкість до зовнішніх загроз. У процесі реалізації також передбачено впровадження сучасних інструментів контейнеризації та оркестрації (Docker, Kubernetes), налаштування захищених каналів зв'язку та реалізація системи моніторингу безпеки. Завершальним етапом є тестування функціональних і захисних властивостей системи у різних сценаріях з метою підтвердження її стійкості до типових атак та відповідності встановленим вимогам.

Запропонована архітектура веб-застосунку базується на сучасних принципах мікросервісної архітектури, що дозволяє розділити функціональні компоненти системи (реєстрація, пожертви, адміністрування) на окремі модулі, що підвищує масштабованість і стійкість до збоїв. Для контейнеризації буде використано Docker, а для оркестрації – Kubernetes. Безпечна автентифікація реалізовуватиметься через OAuth 2.0 з підтримкою JWT-токенів, що дозволяє контролювати доступ до кожного модуля системи відповідно до ролі користувача.

У результаті буде створена веб-система, що дозволить ефективно управляти молодіжними ініціативами ГО «ЛІДЕРСЬКА ІНІЦІАТИВА» з дотриманням високих стандартів безпеки. Забезпечення конфіденційності та цілісності даних, захист каналів передачі інформації, стійкість до поширених кіберзагроз сприятимуть формуванню довіри серед користувачів, партнерських організацій та волонтерів. Крім того, система стане інструментом цифрової трансформації громадської активності та може бути масштабована для інших громадських ініціатив.

ДЖЕРЕЛА

1. Гурський І. «Цифрова благодійність: досвід та перспективи розвитку», Журнал «ІТ та суспільство», №4, 2023.
2. Voloshyn D. Secure Charity Web Systems: Design and Best Practices. – Lviv IT Journal, 2022.
3. OWASP Foundation. *OWASP Top Ten Web Application Security Risks* – https://owasp.org

SCRUM ЯК ЕФЕКТИВНА МЕТОДОЛОГІЯ УПРАВЛІННЯ ПРОЄКТАМИ РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Цап Д. І., Вовк Р. Б.
Івано-Франківський національний технічний університет нафти і газу, м. Івано-Франківськ

Гнучкі методології розробки програмного забезпечення, зокрема Scrum, є ключовим інструментом для програмних команд, що прагнуть

підвищити якість продукції та скоротити час розробки. Методологія Scrum передбачає ітеративний підхід до управління проєктами, що забезпечує оперативну адаптацію до змін вимог і зменшення ризиків, пов'язаних із великомасштабними проєктами. Цей підхід ґрунтується на безперервному вдосконаленні процесів у рамках коротких ітерацій (спринтів), що сприяє швидкому впровадженню змін та накопиченню досвіду командою [1].

Організаційна структура Scrum передбачає чіткий розподіл ролей, що забезпечує високу ефективність командної взаємодії. Власник продукту (Product Owner) відповідає за формування бачення продукту, визначення пріоритетів і управління продуктовим беклогом. Scrum-майстер здійснює фасилітацію процесу, усуває перешкоди, а також контролює дотримання принципів Scrum. Такий поділ обов'язків сприяє підвищенню прозорості процесів та зменшенню внутрішньокомандних конфліктів. Система спринтів дозволяє здійснювати регулярну демонстрацію проміжних результатів, отримувати зворотний зв'язок від зацікавлених сторін і своєчасно коригувати подальшу стратегію розробки.

Одним із визначальних чинників ефективного впровадження Scrum є налагоджена комунікація між учасниками команди. Щоденні стендап-зустрічі дозволяють координувати дії, оперативно ідентифікувати проблеми та ухвалювати рішення щодо їх розв'язання. Регулярні ретроспективи забезпечують можливість аналізу командної продуктивності та формування стратегій покращення робочого процесу [2].

Підтримка якості програмного забезпечення в Scrum реалізується завдяки безперервному тестуванню. Використання автоматизованих тестів дозволяє оперативно отримувати зворотний зв'язок щодо стабільності коду, виявляти дефекти та своєчасно їх усувати. Це не лише скорочує час виправлення помилок, а й підвищує загальну продуктивність розробки [3].

Гнучкість методології Scrum робить її ефективною у проєктах з високим ступенем невизначеності. Завдяки ітераційному підходу, команда має змогу швидко реагувати на зміни у ринковому середовищі та адаптувати продукт до актуальних потреб користувачів. Поступове впровадження змін мінімізує ризики та підвищує стабільність проєкту. Аналітика та метрики відіграють важливу роль у процесі вдосконалення розробки. Вимірювання швидкості виконання завдань, ефективності командної роботи та рівня задоволеності користувачів дозволяє приймати обґрунтовані рішення щодо покращення процесів. Такий підхід забезпечує не лише підвищення якості кінцевого продукту, але й прозорість усіх етапів розробки.

Впровадження Scrum також позитивно впливає на мотивацію команди. Чітко структуровані процеси, регулярний зворотний зв'язок і залучення кожного члена команди до ухвалення рішень сприяють підвищенню залученості та продуктивності. Демонстрація досягнень після

кожного спринту слугує додатковим мотиваційним чинником. Scrum сприяє ефективному управлінню ризиками в процесі розробки програмного забезпечення. Часті оновлення, безперервне тестування та постійний контроль якості дозволяють уникнути виявлення критичних помилок на пізніх етапах проєкту, тим самим знижуючи ймовірність його провалу [4].

Особливої уваги заслуговує взаємодія Scrum із сучасними технологічними підходами, зокрема хмарними обчисленнями та концепцією DevOps. Інтеграція з DevOps сприяє безперервному розгортанню та оновленню програмного забезпечення, що є критично важливим у швидкозмінному середовищі IT-продуктів. Ефективність впровадження Scrum значною мірою залежить від організаційної культури компанії. Методологія передбачає не лише гнучкість, але й високу дисципліну, самоуправління команд та відповідальність кожного учасника. Лише в умовах сприятливого корпоративного середовища можливо досягти повної реалізації потенціалу Scrum. Варто також враховувати психологічні аспекти роботи за Scrum. Орієнтація на командну взаємодію сприяє формуванню довіри між учасниками процесу розробки та кінцевими користувачами. Прозоре планування та комунікація знижують рівень стресу та покращують атмосферу в команді. Чітке управління часом є необхідною умовою успішного використання Scrum. Використання тайм-менеджмент інструментів, дозволяє оптимізувати продуктивність, раціоналізувати навантаження та зменшити ризики професійного вигорання.

Отже, впровадження Scrum забезпечує високу якість програмного забезпечення, сприяє ефективній взаємодії всередині команди та знижує ризики розробки. У контексті сучасних тенденцій цифрової трансформації, Scrum залишається однією з провідних методологій, яка дозволяє досягати гнучкості, швидкості та адаптивності в реалізації програмних продуктів.

ДЖЕРЕЛА

1. Atlassian. Scrum: Agile Project Management. URL: https://surl.li/uldfcy.
2. APMG International. Top 10 Benefits of Scrum and Frequent Challenges. URL: https://surl.li/fmkrzn.
3. TestRigor. Test Automation in Scrum. URL: https://surl.li/svoivz.
4. Atlassian. Sprint Retrospective. URL: https://surl.li/kjklrm.

ПОРІВНЯННЯ СЕМАНТИЧНОГО ПОШУКУ ТА ПОШУКУ ЗА КЛЮЧОВИМИ СЛОВАМИ: ВПЛИВ НА ТОЧНІСТЬ ТА РЕЛЕВАНТНІСТЬ РЕЗУЛЬТАТІВ

Чеверда А. Б., Вакалюк Т. А
Державний університет «Житомирська політехніка», м. Житомир

Пошукові системи є невід'ємною складовою повсякденного життя. Для звичайного пошуку кожна людина використовує Google, Bing, Yahoo, тощо. Проте кожна з цих систем використовує різні технології та алгоритми. При цьому існує два основних види пошуку: семантичний та за ключовими словами.

Основна ознака пошуку за ключовими словами – це пошук точних збігів у запиті. Через це трапляється багато непорозумінь, адже не враховується багато аспектів, таких як розуміння контексту, синоніми та багатозначність [1, с. 2].

Розглянемо основний алгоритм пошуку за ключовими словами. Спершу всі веб сторінки мають проіндексуватися, щоб створити список слів з посиланнями. Також має відбутися ранжування за частотою ключових слів, позиціями на сторінці та іншими факторами. Далі користувач вводить запит та отримує список сайтів, де було знайдено дослівний пошуковий запит [1, с. 2].

Даний метод пошуку нараховує багато недоліків, такі як залежність від точних збігів, відсутність контексту та чутливість до форми слів запиту. Власне тому й була знайдена альтернатива: семантичний пошук. Це передова технологія, яка використовує набір методів семантичних технологій, щоб отримати інформацію зі структурованих джерел даних [2]. Тобто, вона враховує значення запиту та намір користувача, щоб досягти найточнішого результату. На відміну від звичайного пошуку, де алгоритм ранжування визначає рейтинг конкретного посилання для релевантності, семантичний пошук використовує онтологію для отримання швидкої та значущої відповіді. Це також допомагає провести асоціативні зв'язки між значенням та самим словом [1, с. 3].

Семантичний пошук об'єднує в собі технології семантичної павутини, Web 3.0, та пошукової системи для покращення результатів [1, с. 3]. Семантична павутина – це спосіб об'єднання даних серед усіх веб сторінок, застосунків та файлів. Основною метою розробки даної мережі було створення кращої версії всесвітньої павутини, у якій дані будуть взаємопов'язані та легкими для зчитування машинами, що забезпечить кращу інтеграцію даних та обмін знаннями [3].

Для персоналізованого порівняння було обрано 2 пошукові системи Google з семантичним пошуком та Baidu з пошуком за ключовими словами. Також було обрано декілька різних запитів, щоб на повну побачити різницю. Порівняння наведемо в таблиці 1.

Таблиця 1

Порівняння пошукових систем за різними запитами

Запит	Пошукова система	
	Google	**Baidu**
«Bank»	Список банків України, можливість знайти найближні відділення.	Пояснення значення слова «банк».
«What is the capital of France?»	Було одразу надано відповідь та сайти про Париж.	Тести та відповіді на домашні завдання, відповідь лише на сайтах.
«How to treat a cold?»	Поради, симптоми хвороби.	Статті з такою ж назвою.
«Where is the nearest coffee shop?»	Карта закладів, веб застосунки з ліпшими варіантами.	Загальні поради де зазвичай розташовані такі заклади, без конкретних доступних варіантів.

Як висновок, можна побачити, що більшість результатів у Baidu були загальними та без персоналізації. Чітко можна було провести паралель, що скрізь у відповідях були такі ж фрази, що і в запитах. Тоді як у Google, навіть при написанні запитів англійською, результати були для української аудиторії з урахуванням місцевості та загальної інформації про користувача. Для спрощення пошуку на конкретні питання одразу була показана коротка відповідь, що зменшує кількість часу на перегляд сайтів.

Отже, семантичний пошук є набагато комфортнішим та швидшим варіантом для користувача. Саме він зможе надати чіткі та структуровані відповіді, які неможливо отримати у пошуку за ключовими словами.

ДЖЕРЕЛА

1. Malve, A., & Chawan, P. M. (2015). A Comparative Study of Keyword and Semantic based Search Engine. С. 1-6. URL: https://www.researchgate.net/publication/316514673_A_Comparative_Study_of_Keyword_and_Semantic_based_Search_Engine.

2. What Is Semantic Search? Ontotext. URL: https://www.ontotext.com/knowledgehub/fundamentals/what-is-semantic-search/ (дата звернення: 10.02.2025).

3. What is the Semantic Web? Definition, history and timeline. TechTarget. URL: https://www.techtarget.com/searchcio/definition/Semantic-Web (дата звернення: 10.02.2025).

РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ДЕКОДУВАННЯ СНІВ НА ОСНОВІ МЕТОДИКИ HALL-VAN DE CASTLE

Шелестинський В. А., Аброскін Ю. Ю.
Державний університет інформаційно-комунікаційних технологій, м. Київ

У сучасній психології аналіз сновидінь залишається дієвим інструментом дослідження підсвідомих процесів особистості. З огляду на швидкий розвиток інформаційних технологій, актуальною є ідея інтеграції психологічних методик аналізу снів із програмними засобами. Це відкриває можливість автоматизованого збору, класифікації та аналізу великих обсягів даних. Методика Hall-Van de Castle вирізняється формалізованою структурою та придатністю для алгоритмізації, що робить її оптимальним вибором для реалізації програмного забезпечення.

Серед численних методик тлумачення сновидінь, метод Hall–Van de Castle (HVC) демонструє найбільшу відповідність критеріям, необхідним для програмної реалізації: уніфікованість, чіткість категорій, статистична обробка результатів. У межах бакалаврської роботи поставлено завдання створити програмне забезпечення, яке дозволяє вводити текст сну, ідентифікувати ключові елементи відповідно до HVC та виводити статистичний звіт.

У ході аналізу були розглянуті чотири методики:

- *Інтерпретація за Фрейдом*: ґрунтується на асоціативному аналізі та символізмі, але є суб’єктивною і складною для алгоритмізації
- *Гештальт-підхід*: розглядає кожен елемент сну як проекцію особистості, однак не передбачає формалізованого кодування інформації.
- *Методика Ульмана*: фокусується на груповому обговоренні снів, не передбачає об’єктивної класифікації.
- *Методика Hall–Van de Castle*: передбачає аналіз снів на основі фіксованих категорій (персонажі, емоції, соціальні взаємодії, агресія, успіх тощо), має числові показники, що ідеально підходить для використання в програмних алгоритмах.

Застосування з програмному забезпечені.

Застосування методики HVC у програмному середовищі передбачає використання алгоритмів обробки природної мови (NLP), що дозволяє аналізувати текстові описи снів. Кожна категорія методики може бути реалізована як окремий класифікатор, що оперує лінгвістичними ознаками. Такий підхід робить можливим застосування машинного навчання, створення словників категорій та візуалізацію результатів. Використання Python з бібліотеками spaCy, NLTK, Pandas забезпечує гнучкість і ефективність розробки.

Розроблено прототип програмного забезпечення з такими модулями:

- Інтерфейс введення тексту сну
- NLP-модуль для аналізу структури тексту
- Модуль класифікації за категоріями HVC
- Блок статистики та побудови графіків

Програма дозволяє здійснювати базовий кількісний аналіз снів відповідно до HVC, видавати порівняльні звіти й архівувати результати.

Методика Hall–Van de Castle є найбільш технологічно адаптивною для програмного аналізу сновидінь. Її застосування у програмному продукті відкриває нові можливості для дослідників, психологів і користувачів, які прагнуть краще розуміти свою підсвідомість. Перспективами подальших досліджень є застосування нейромережевих моделей для покращення класифікації та впровадження мультимовного аналізу.

ДЖЕРЕЛА

1. Hall C., Van de Castle R. *The Content Analysis of Dreams.* – New York: Appleton-Century-Crofts, 1966.

2. Jurafsky D., Martin J.H. *Speech and Language Processing.* – Pearson, 2023.

3. Goldberg Y. *Neural Network Methods for Natural Language Processing.* – Morgan & Claypool Publishers, 2017.

4. spaCy Documentation – [Електронний ресурс] – https://spacy.io/

5. NLTK Project – [Електронний ресурс] – https://www.nltk.org/

6. Plotly Python Graphing Library – [Електронний ресурс] – https://plotly.com/python/

РОЗРОБКА ФУНКЦІОНАЛУ МОБІЛЬНИХ ДОДАТКІВ ДЛЯ КОНТРОЛЯ ЗА ВЛАСНИМИ КОШТАМИ

Шемет Є. І., Носенко Т. І.
Київський столичний університет імені Бориса Грінченка, м. Київ

Планування бюджету є невід'ємною частиною повсякденного життя людини, оскільки завдяки цьому є можливість чітко розуміти своє фінансове положення [1], тому метою роботи автори визначили розробку функціоналу мобільного додатку для планування особистого бюджету.

Запорукою успішного використання таких додатків є простота, інтуїтивно зрозумілий та зручний інтерфейс, чітка навігація та приваблива візуалізація, можливість налаштування інтерфейсу під потреби користувача. Важливо чітко визначити функціональні можливості додатку [2; 3]: автоматичне та ручне внесення транзакцій та класифікація їх за категоріями, візуалізація витрат і доходів у вигляді графіків і діаграм, створення та управління бюджетами та відстеження їх виконання, сповіщення про перевищення бюджету, генерація звітів, аналіз фінансових тенденцій та прогнозування витрат, управління заощадженнями, інтеграція з банківськими рахунками, сповіщення та нагадування, безпека даних, можливість інтеграції з іншими фінансовими додатками, аналітика і зворотній зв'язок. Автори проаналізували функціонал декількох подібних додатків - лідерів за кількістю закачувань, та узагальнили дані в таблиці 1.

Таблиця 1

Порівняльний аналіз основних функціональних можливостей мобільних додатків для планування особистого бюджету

	Планування бюджету	Керування кількома обліковими записами	Нагадування про кредити	Розподіл витрат за категоріями	Синхронізація між різними пристроями	Функції для малого бізнесу, фрілансу	Окремий гаманець
Дзен-мані	+	-	+	+	+	+	-
Money Lover	+	-	+	+	+	-	+
Goodbudget	+	-	+	+	-	-	+
Moneygraph	+	+	+	+	+	+	+

Всі додатки мають приблизно однаковий функціонал, відрізняються лише за можливістю керування кількома обліковими записами, наявністю функцій для управління фінансами власного малого бізнесу, наявністю окремих гаманців. можливістю синхронізуватися з різними пристроями. Отже, розробка функціоналу мобільних додатків для контролю власних коштів є складним, але надзвичайно важливим завданням. Впровадження сучасних технологій, таких як штучний інтелект, дозволить зробити ці додатки ще більш ефективними та привабливими для користувачів.

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.

МЕТОДОЛОГІЯ DEVOPS ЯК КЛЮЧОВИЙ ЧИННИК ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Шнурок В. С., Вовк Р. Б.
Івано-Франківський національний технічний університет нафти і газу, м. Івано-Франківськ

Сучасні методології розробки програмного забезпечення істотно впливають на ефективність і швидкість створення цифрових продуктів. Традиційні підходи, зокрема Waterfall та Agile, демонструють певні переваги в специфічних контекстах. Однак із появою нових технологій та необхідністю швидкої адаптації до змінних ринкових умов зростає значення інноваційних методів. Класичний каскадний підхід (Waterfall) характеризується чіткою послідовністю етапів, що полегшує планування та контроль за проєктами. Водночас його використання є обмеженим у динамічних середовищах, де критично важливо оперативно реагувати на зміни. Методологія Agile, натомість, набула популярності завдяки гнучкості, що забезпечує адаптацію до змінних вимог. Проте й вона стикається з викликами при реалізації масштабних проєктів або інтеграції з іншими процесами.

У відповідь на потребу не лише у швидкій розробці, а й у забезпеченні стабільності та тісної інтеграції між командами розробників і операційних спеціалістів була розроблена методологія DevOps. Її основна

мета полягає у скороченні життєвого циклу розробки програмного забезпечення та забезпеченні безперервної доставки програмних компонентів на продуктивні середовища [1]. По суті, DevOps усуває бар’єри між традиційно розділеними командами розробки та експлуатації, сприяючи більш тісній координації та прискоренню виходу продукту на ринок.

Інтеграція принципів DevOps передбачає об'єднання розробки та операційних завдань в єдиний процес безперервної інтеграції, тестування та доставки, що забезпечує зменшення тривалості життєвого циклу розробки, підвищення стабільності рішень і покращення взаємодії між підрозділами. Доведено, що завдяки впровадженню DevOps компанії можуть істотно прискорити випуск нових версій продуктів, зберігаючи при цьому високий рівень їх якості. Одним із ключових аспектів DevOps є автоматизація основних етапів життєвого циклу розробки, зокрема тестування, інтеграції та розгортання. Використання спеціалізованих інструментів для автоматизації замість ручних процедур сприяє підвищенню ефективності процесів. Важливим напрямом розвитку є інтеграція принципів безпеки в робочі процеси DevOps, що отримала назву DevSecOps. Це дозволяє організаціям досягати безперервної доставки програмного забезпечення, мінімізуючи ризики безпеки та підвищуючи загальну якість продуктів [2].

Суттєву роль у практиках DevOps відіграють процеси безперервної інтеграції (CI) та безперервної доставки (CD). Безперервна інтеграція передбачає автоматизоване тестування та об'єднання змін у загальний репозиторій, що дозволяє оперативно виявляти і виправляти помилки до їхнього потрапляння у фінальні версії продукту. Безперервна доставка, у свою чергу, забезпечує автоматизоване розгортання програмного забезпечення на продуктивних середовищах, мінімізуючи затримки в оновленні систем. Поєднання CI та CD сприяє підвищенню швидкості розробки, покращенню якості програмного забезпечення та безпеки змін при мінімальному ручному втручанні [3]. Водночас успішне впровадження цих практик вимагає ретельного планування, налаштування інструментів і чіткого розуміння бізнес-процесів, аби уникнути інтеграційних проблем.

Одним із фундаментальних аспектів DevOps є формування культури спільної відповідальності між командами. На відміну від традиційного розподілу обов'язків, DevOps передбачає тісну співпрацю розробників і операційних фахівців, сприяючи обміну знаннями та забезпеченню оперативного реагування на зміни і проблеми. Однією з головних причин популярності DevOps є можливість організацій зменшувати витрати, скорочувати час виходу продукту на ринок та підвищувати рівень задоволеності кінцевих користувачів. Завдяки впровадженню DevOps компанії можуть не лише підвищити якість програмного забезпечення, а й пришвидшити розробку нових функцій. Крім того, підхід сприяє

зміцненню конкурентоспроможності підприємств шляхом швидкої адаптації до змін.

Отже, інтеграція методології DevOps у процес розробки програмного забезпечення забезпечує організаціям не тільки прискорення виходу продуктів на ринок, а й підвищення їхньої стабільності, якості та ефективності командної взаємодії. В умовах швидкої технологічної еволюції та загострення конкуренції можливість оперативної адаптації до змін стає важливою стратегічною перевагою. DevOps сприяє формуванню нової моделі організаційної культури, де кожен учасник процесу бере на себе відповідальність за кінцевий результат, що в сукупності дозволяє знижувати витрати, підвищувати якість обслуговування користувачів і забезпечувати стійкість організацій до зовнішніх викликів.

ДЖЕРЕЛА

1. DevOps Engineer: чим займається у компанії та що потрібно знати для роботи на цій позиції. Dou.ua URL: https://salo.li/2f14773.

2. Risk Management In DevOps | xMatters. *xMatters*. URL: https://salo.li/feaF2d2.

3. CI/CD: що це, як пов’язано з DevOps, переваги, найкращі практики | NIX. *NIX*. URL: https://salo.li/1574c4D

МОДУЛЬНА МОДЕЛЬ ПОРТУВАННЯ 2D-ГРИ НА GODOT 4 З ВИКОРИСТАННЯМ C#

Шпильовий М. М.

Київський столичний університет імені Бориса Грінченка, м. Київ

C# сьогодні входить до базового набору інструментів інді-розробника: ця мова поєднує швидкодію JIT-компілятора, зрозумілий високорівневий синтаксис і велику крос-платформену екосистему .NET. Однак рушій MonoGame, що використовує C#, не підтримує багатопоточну фізику та зручну дельта-синхронізацію, через що складні кооперативні ігри страждають від низького FPS і великих затримок. Метою роботи є створення модульної моделі перенесення гри Barotrauma з MonoGame 3.8 на безроялтійний рушій Godot 4 (.NET).

Матеріали й методи

1. Проаналізовано ~160 тис. рядків оригінального коду Barotrauma стандартними профайлерами .NET.

2. Для Godot використано Threaded Physics та мережевий ENet API з дельта-оновленнями.

3. Порівняльні вимірювання проведено у трьох типових сценах: «порожній човен», «затоплення» та «бій чотирьох гравців».

Методика експерименту та обмеження. Тести виконувалися на ПК Ryzen 5 3600, 16 ГБ RAM, RTX 2060 та ноутбуці Core i5-8250U з Intel UHD

620. Для MonoGame збирали середній час кадру через Stopwatch, трафік фіксували Wireshark (udp.port==27015). У Godot застосовували вбудований Profiler та MultiplayerMonitor. Кожен сценарій запускався 10 хв; перші 60 с прогріву не враховувалися, статистичну похибку оцінювали за $\sigma \leq 5$ %. Зазначені результати можуть зменшитися на старих iGPU або після увімкнення повного набору пост-ефектів, однак навіть у цих умовах портована версія не опускалась нижче 45 FPS, тоді як оригінал показував 18–22 FPS.

Результати

1. **Продуктивність**. Перенесення фізики у виділений потік збільшило FPS утричі у сцені «затоплення + 4 гравці».
2. **Мережа**. Дельта-синхронізація зменшила вихідний трафік сервер → клієнт приблизно у 10 разів.
3. **Сейви**. Інкрементний формат ResourceSaver скоротив типові файли кампанії з ≈ 150 МБ до 15 МБ.
4. **Моди**. Упроваджено UID-реєстр; 20 модів одночасно завантажуються без конфліктів.

Оригінальність

Запропоновано послідовність кроків, за якою будь-яку MonoGame-гру можна перенести у Godot без суттєвого переписування ігрової логіки. Окремо описано простий алгоритм перевірки цілісності інкрементних сейвів.

Практичне значення

Отримана модель вже використана для робочого прототипу Barotrauma-port, який стабільно працює на середніх ПК. Підхід може слугувати прикладом для студентських та інді-команд, що модернізують XNA-проекти.

Перспективи розвитку

Планується інтеграція ECS-архітектури Godot 5 та експеримент із мобільними збірками на .NET NativeAOT, що має скоротити час запуску гри на телефонах до $< 0{,}3$ с.

ДЖЕРЕЛА

1. Godot Engine. Official Documentation v4.2 [Електронний ресурс]. URL: https://docs.godotengine.org (дата звернення: 01.05.2025).
2. Holowachuk A. NativeAOT in .NET 8 – performance benchmarks [Електронний ресурс]. – Medium, 2025. – Режим доступу: https://medium.com/@aholo/nativeaot-in-net-8-performance-benchmarks-df4c5e23fca9 (дата звернення: 12.03.2025).
3. Jackson F. MessagePack for C# Guide [Електронний ресурс]. URL: https://msgpack.org/cli (дата звернення: 25.04.2025).

КІБЕРФІЗИЧНІ СИСТЕМИ З БІОЕЛЕКТРИЧНИМИ СЕНСОРАМИ: ТЕОРЕТИЧНІ ЗАСАДИ ТА ТЕХНІЧНА РЕАЛІЗАЦІЯ

Язвінська Д. І., Дудник В. В., Дудник О. В.
Вінницький національний технічний університет, м. Вінниця

Кіберфізичні системи (КФС) є ключовим напрямом розвитку сучасних технологій, що забезпечує інтеграцію фізичних об’єктів із цифровими компонентами. Вони поєднують сенсори, обчислювальні пристрої, програмне забезпечення та мережеві технології для створення адаптивних систем, здатних аналізувати великі обсяги даних у реальному часі. Завдяки цьому КФС знаходять застосування в промисловості, медицині, робототехніці, транспортних системах та розумних містах [1].

Одним із перспективних напрямів розвитку КФС є інтеграція біоелектричних сенсорів, що відкриває нові можливості для взаємодії людини з технічними пристроями. Це особливо актуально в біонічному протезуванні, нейроінтерфейсах та реабілітаційних технологіях. Завдяки сучасним методам обробки сигналів та алгоритмам машинного навчання, такі системи постійно вдосконалюються, підвищуючи рівень персоналізації та ефективності керування пристроями.

Основний принцип роботи КФС полягає у забезпеченні зворотного зв’язку між фізичним і цифровим середовищем. Сенсори фіксують параметри зовнішнього середовища або організму людини, після чого отримані дані аналізуються в обчислювальній системі, яка приймає рішення про відповідні дії. Це дозволяє створювати інтелектуальні системи управління, здатні адаптуватися до змінних умов і працювати в реальному часі.

Біоелектричні сенсори відіграють ключову роль у таких системах, оскільки вони дозволяють зчитувати електричні сигнали, що генеруються людським тілом. Основними методами реєстрації біоелектричних сигналів є електроміографія (EMG), електроенцефалографія (EEG) та електрокардіографія (ECG). EMG використовується для аналізу активності м’язів і є основою для керування біонічними протезами та екзоскелетами. EEG реєструє електричну активність головного мозку, що дає змогу створювати нейроінтерфейси, здатні керувати пристроями силою думки. ECG застосовується в біометричній ідентифікації та системах медичного моніторингу[2].

Для ефективного використання біоелектричних сенсорів у керуванні пристроями необхідні точні методи обробки сигналів. Важливими етапами є фільтрація сигналів, усунення шумів та визначення характерних особливостей електричних імпульсів. У сучасних системах застосовуються алгоритми цифрової фільтрації, включаючи адаптивну фільтрацію та вейвлет-перетворення, що дозволяють підвищити точність сигналів. Крім

того, методи машинного навчання, зокрема нейронні мережі та алгоритми класифікації, допомагають розпізнавати наміри користувача та передавати відповідні команди пристроям.

Технічна реалізація таких систем включає апаратну та програмну складові. Апаратна частина містить мікроконтролери (ESP32, STM32), плати обробки сигналів та модулі бездротового зв'язку (Wi-Fi, Bluetooth). Біоелектричні сенсори (наприклад, EMG-сенсори SpotMyo Ware або SEN-13723) реєструють електричну активність м'язів і передають сигнали на мікроконтролер для подальшої обробки. Оброблені дані можуть використовуватися для керування протезами, екзоскелетами або іншими роботизованими системами.

Програмна частина забезпечує аналіз сигналів та генерацію керуючих команд. Алгоритми обробки включають методи цифрової фільтрації, визначення шаблонів активності та машинне навчання для покращення точності управління. Наприклад, у протезах верхніх кінцівок використання EMG-сигналів дозволяє інтуїтивно керувати рухами штучної руки, що значно покращує якість життя користувачів.

Прикладом реалізації кіберфізичної системи є прототип роботизованого протеза руки, який використовує EMG-сенсори для керування рухами. Закріплені на передпліччі сенсори зчитують сигнали м'язової активності, передають їх на мікроконтролер ESP32, де вони фільтруються, аналізуються та перетворюються на команди для серводвигунів. Додатково система може надавати зворотний зв'язок у вигляді вібраційного або світлового сигналу, що покращує точність керування.

Таким чином, інтеграція біоелектричних сенсорів у кіберфізичні системи відкриває нові можливості для створення адаптивних пристроїв, що підвищують ефективність керування та забезпечують інтуїтивну взаємодію між людиною і технологіями. Подальші дослідження в цій галузі спрямовані на вдосконалення методів обробки біоелектричних сигналів, підвищення точності розпізнавання намірів користувача та розширення сфер застосування таких систем.

ДЖЕРЕЛА

1. Математичне моделювання та управління процесами довільної природи у кіберфізичних системах на основі методології системного аналізу URL: http://mmsa.kpi.ua/en/node/1965 (дата звернення: 31.03.2025).
2. Як працюють кіберфізичні системи та навіщо вони потрібні? URL: https://robotdreams.cc/uk/blog/649-how-do-cyber-physical-systems-work-and-why-are-they-needed (дата звернення: 31.03.2025).

ВИЗНАЧЕННЯ ЕФЕКТИВНОСТІ ЗАСТОСУВАННЯ АПАРАТНИХ ПЛАТФОРМ НА ПРИКЛАДІ ЗАДАЧІ РОЗПІЗНАВАННЯ АВТОМОБІЛЬНИХ НОМЕРІВ

Яковенко В. А.
Київський столичний університет імені Бориса Грінченка, м. Київ

У теперішній час набула популярності так звана концепція «Інтернет речей» («IoT», «Internet of Things») [1], яка швидко розповсюджується на різні галузі науки та техніки. Розповсюдження та адаптація під сучасні задачі потребує різноманітних апаратних платформ, на яких можна реалізувати проєкти IoT. Кожна така платформа має свої переваги, які вирізняють її з поміж аналогів (наприклад, енергоспоживання, швидкодія тощо).

Одним з типів задач, де може ефективно використовуватися підхід «IoT» є задачі з використанням обробки відеоінформації для аналізу, обробки та реакції на отриманий результат. Суть такого типу задач полягає в наборі методів для збору та аналізу візуальної інформації (зазвичай, 2D зображення) за допомогою відеосенсору з метою отримання корисної інформації [2]. Практична реалізація обробки відеоданих в автоматичному режимі в промисловості носить назву машинний зір [3]. Зазвичай така реалізація дозволяє автоматично розраховувати фізичні характеристики предмету на виробництві, такі як: розміри, кількість, вид, розташування і т.п. За допомогою машинного зору може бути реалізовано і автоматичне розпізнавання автомобільних номерів. Першочерговим у такій задачі зазвичай є автоматична фіксація порушників ПДР для зменшення навантаження органів правопорядку, але такий підхід може використовуватися і для контролю доступу в'їзду на обмежену територію [4].

Використання апаратних складових платформи для реалізації задач, пов'язаних з обробкою відеоданих (наприклад сенсор, пристрій обробки даних і т.д.) прямо впливають ефективність застосування цієї технології. Тому підбір апаратної платформи для реалізації такої системи дуже важливий, тому необхідно провести аналіз існуючих апаратних складових за певними сформульованими критеріями. Для визначення критеріїв, було проведено дослідження сучасних популярних апаратних платформ, що можуть бути використані для розв'язання задач розпізнавання автомобільних номерів. Одним із основних критеріїв порівняння їх ефективності автором запропоновано вважати швидкість обробки відеоданих, та отримання певної кількості кадрів в секунду з визначеною роздільною здатністю сенсора такої апаратної реалізації.

В результаті роботи розроблені рекомендації щодо вибору ефективної апаратної платформи для проектів, що обробляють відеодані.

Також, було сформоване наочне представлення результатів по кожній розглянутій платформі у вигляді таблиці.

Автор вважає, що отримані експериментальні результати дозволять спростити практичну реалізацію майбутніх проєктів, що будуть використовувати обробки відеоінформації для аналізу, обробки та реакції на отриманий результат.

ДЖЕРЕЛА

1. TechTarget // Internet of things (IoT). URL: https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT

2. Reinhard Klette. Concise Computer Vision An Introduction into Theory and Algorithms, 2014. 7 с.

3. Intel // What Is Machine Vision?. URL: https://www.intel.com/content/www/us/en/learn/what-is-machine-vision.html

4. Офіційний портал Києва // В'їзд на Труханів острів і надалі здійснюватиметься через систему автоматичного розпізнавання автомобільних знаків. URL: https://kyivcity.gov.ua/news/vzd_na_trukhaniv_ostriv_i_nadali_zdiysnyuvatimetsya_cherez_sistemu_avtomatichnogo_rozpiznavannya_avtomobilnikh_znakiv/

ПЕРЕХІД ВІД «1С» ДО СУЧАСНОГО C#-API: ПРОБЛЕМАТИКА ТА РІШЕННЯ

Яскевич Ю. В.

Київський столичний університет імені Бориса Грінченка, м. Київ

Використання «1С:Підприємство» та інтеграційних модулів на Delphi стає неприпустимим через геополітичні ризики, закритість коду та застарілі технології. У роботі описано цю проблематику й запропоновано архітектуру сучасного TCP-сервера на C# (.NET 8), який обробляє ключі доступу до API, гарантує незалежність від російського ПЗ, масштабованість та безпечне зберігання секретів.

1. Проблематика

В Україні понад 70 % підприємств використовують «1С» для ERP-системи, але в умовах санкцій ризик втратити підтримку та оновлення російського ПЗ різко зростає [1]. Крім того, інтеграційні рішення на Delphi працюють із жорстко закодованими бібліотеками, не підтримують сучасні крипто-алгоритми й складно масштабуються. Основні вразливості: геополітичний ризик, відсутність відкритого аудиту коду, обмежена продуктивність і складність інтеграції з веб- та мобільними сервісами.

2. Вимоги до нового рішення

Система має бути незалежною від російських вендорів та конкурентно сумісною, безпечною, прозорою та крос-платформною. Вона повинна підтримувати параметризовані запити до бази даних із захищеним зберіганням connectionString, асинхронну обробку запитів, відкритий вихідний код і стандартизовані методи аутентифікації й авторизації.

3. Архітектура C#-сервера

Реалізовано TCP-сервер із модулем Listener, який асинхронно приймає клієнтів, Parser-ом, що акумулює дані до \n і розпізнає команди $…ARQ… для перевірки картки та $…PING… для відповіді ECHO. AuthService виконує параметризований запит до MySQL (SELECT second_encoding FROM keychain…) через MySqlConnector, захищаючи від SQL-ін'єкцій, а PacketFormatter формує відповідь із префіксом $, заголовком пристрою, командою (GO, PH, ECHO) та CRC8-контролем цілісності (дві схеми розрахунку – загальний та для «GO») [2]. Логування всіх етапів ведеться асинхронно через FileLogger.

4. Безпека ключів

Ключі обробляються лише на сервері: рядок підключення винесено з коду в appsettings.json (або Azure Key Vault), а в CI/CD середовищі використовуються Environment Variables. CRC8 гарантує цілісність пакетів, а лімітування запитів (MemoryCache/Redis) запобігає DoS-атакам [3]. Усі компоненти підтримують скасування через CancellationToken, що забезпечує коректне завершення.

5. Переваги нового рішення

Порівняно з «1С»+Delphi:

Незалежність від санкцій: відкритий код на GitHub, без закритих російських бібліотек;

Продуктивність: асинхронна модель обробки та кешування зростили швидкість на 30 %;

Безпека: ключі ніколи не потрапляють до клієнта, централізоване логування, контроль доступу;

Масштабованість: Docker-контейнери та Kubernetes-кластер;

Підтримка: юніт-тести для всіх протоколів та методів обчислення CRC, можливість швидких оновлень.

6. Висновки

Перехід від «1С:Підприємство» і Delphi-модулів до сучасного C#-API на .NET дозволяє підприємству усунути стратегічну залежність, підвищити безпеку й обробляти тисячі запитів із гарантованою цілісністю й прозорістю. Наступні кроки: розробка REST-інтерфейсу з OAuth2, інтеграція з SIEM, підтримка мобільних клієнтів, а також розгортання у хмарному середовищі з автоскейлінгом.

ДЖЕРЕЛА

1. Чепур Д. Штраф до 13 млн грн. Депутати пропонують штрафувати за використання «1С». Чим замінити російський софт для бізнесу. Forbes.ua. URL: https://forbes.ua/innovations/ukrainskiy-biznes-prograe-viynu-rosiyskomu-softu-yaki-shansi-shcho-1s-ta-inshi-programi-zniknut-boday-kolis-22032023-12531 (дата звернення: 28.04.2025).

2. High-Performance .NET MySQL Driver. MySqlConnector. URL: https://mysqlconnector.net/ (дата звернення: 28.04.2025).

3. OWASP API Security Project. OWASP Foundation. URL: https://owasp.org/www-project-api-security/ (дата звернення: 28.04.2025).

4. RFC 6090: Fundamental Elliptic Curve Cryptography Algorithms. IETF Datatracker. URL: https://datatracker.ietf.org/doc/html/rfc6090 (дата звернення: 28.04.2025).

Секція 3
МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ТА ОБЧИСЛЮВАЛЬНІ МЕТОДИ

АЛГОРИТМ ПРОГНУЗУВАННЯ ТРЕНДУ ПОПИТУ НА ТОВАР ДЛЯ ВЕБ-ЗАСТОСУНКУ «ANIME STORE»

Богута В. С., Задонцев Ю. В.
Державний університет інформаційно-комунікаційних технологій, м. Київ

Сучасні онлайн-магазини потребують не лише загального прогнозу продажів, а й здатності адаптувати пропозиції до індивідуальних потреб користувача. Особливо це актуально для нішевих магазинів, таких як Anime Store, де попит формується на основі швидкоплинних інтересів спільноти. Використання персоналізованих моделей прогнозування дозволяє значно підвищити релевантність рекомендацій, зменшити обсяг непроданого товару та збільшити конверсії.

Задачею є створити систему збору поведінкових даних користувачів (перегляди, додавання до кошика, покупки). Побудувати індивідуальні профілі попиту на основі історії активності. Впровадити адаптивний алгоритм прогнозу, який враховує як загальні тренди, так і поведінку конкретного користувача. Інтегрувати модель у Django-застосунок з відображенням персональних прогнозів.

Задачею дослідження є визначення ключових вимог до розробки модулю прогнозування попиту, який враховує як глобальні, так і індивідуальні тренди, та інтегрувати його у веб-застосунок «Anime Store» з метою підвищення ефективності взаємодії з клієнтом.

Розробка застосунку вимагає реалізації прототипу модуля який збирає історичні дані про замовлення з бази даних Django, використовує метод ковзного середнього (Moving Average) та лінійну регресію для аналізу зміни попиту, визначає тренд (зростаючий, стабільний або спадний) для кожного товару, візуалізує результати у вигляді графіків у адміністративній панелі, прогнозує попит на короткострокову перспективу.

Впроваджений модуль прогнозування попиту продемонстрував ефективність в умовах реального онлайн-магазину. Алгоритм дозволяє не лише виявляти поточні тренди, але й прогнозувати їх зміну, що дає змогу менеджменту оперативно реагувати на попит. У подальших дослідженнях планується: впровадження нейромережевих підходів (LSTM для часових рядів), врахування впливу маркетингових подій (акції, нові релізи аніме), розширення функціоналу для формування автоматичних рекомендацій

менеджерам та покупцям, підключення API зовнішніх даних (наприклад, Google Trends) для покращення точності прогнозів.

ДЖЕРЕЛА

1. How to Forecast Demand in Supply Chain with Python / December 5, 2024 / Elise Geraldes URL: https://www.clicdata.com/blog/demand-forecasting-in-supply-chain/

2. Demand forecasting in Python made easy with futureEXPERT / January 8, 2025 URL: https://www.future-forecasting.de/en/blog/demand-forecasting-in-python-made-easy-with-futureexpert/

3. Inventory Demand Forecasting using Machine Learning – Python / 21 Mar, 2025 URL: https://www.geeksforgeeks.org/inventory-demand-forecasting-using-machine-learning-python/

ІНТЕГРАЦІЯ ПЕРСОНАЛІЗОВАНОГО ПРОГНОЗУВАННЯ ПОПИТУ В ВЕБ-ЗАСТОСУНОК «ANIME STORE» НА БАЗІ DJANGO

Богута В. С., Задонцев Ю. В.
Державний університет інформаційно-комунікаційних технологій, м. Київ

В сучасних умовах електронної комерції особливої актуальності набуває завдання прогнозування попиту на товари. Для онлайн-магазинів, таких як Anime Store, своєчасне виявлення змін у вподобаннях користувачів та трендах продажів є критично важливим для ефективного управління асортиментом, оптимізації складу і формування персоналізованих рекомендацій. Врахування трендів дозволяє не лише збільшити прибутки, але й покращити користувацький досвід, підвищити лояльність клієнтів та знизити витрати. У зв'язку з цим розробка та інтеграція алгоритму прогнозування тренду попиту у веб-застосунок на базі Django є актуальним та перспективним напрямком.

Задачею дослідження є визначення ключових вимог до розробки алгоритму, який дозволяє автоматично аналізувати історичні дані про продажі товарів у веб-застосунку Anime Store та прогнозувати тренди попиту. Основні задачі це в нас збір та обробка історичних даних про продажі, категорії товарів і активність користувачів, побудова алгоритму виявлення зростаючих або спадних тенденцій, інтеграція модуля прогнозування у функціонал веб-застосунку.

Розробити ефективний, адаптивний та легко масштабований алгоритм прогнозування тренду попиту на товари в онлайн-магазині «Anime Store», який забезпечить бізнес-аналітику в реальному часі та дозволить приймати обґрунтовані рішення щодо формування асортименту.

Реалізовано систему збирання даних з активності користувачів у Django (middleware + аналітична модель).

Визначено комбіновану модель прогнозування на основі: загального тренду продажів, індивідуальної активності (рейтинг інтересу, затухаючі коефіцієнти, вага часу), точність персоналізованого прогнозу перевищила класичні методи, визначений API повертає набір товарів з найвищою ймовірністю купівлі для кожного користувача, обраний дашборд для адміністратора з переглядом прогнозів по кожному сегменту клієнтів.

У результаті дослідження було успішно розроблено та інтегровано в веб-застосунок «Anime Store» персоналізований алгоритм прогнозування попиту, який враховує як загальні тренди продажів, так і індивідуальну поведінку користувача. Завдяки комбінації статистичних методів і кластеризації користувачів вдалося досягти покращення точності прогнозів. Реалізований API забезпечує персональні товарні рекомендації, що дозволяє підвищити релевантність пропозицій, збільшити конверсії та зменшити залишки на складі. Django-платформа виявилася ефективною

основою для реалізації подібного функціоналу, що забезпечує масштабованість і зручність підтримки. Надалі передбачено розвиток модуля шляхом впровадження нейромережевих моделей, підключення зовнішніх аналітичних джерел та автоматизації процесу адаптації прогнозів у реальному часі, що зробить веб-застосунок ще більш гнучким та клієнтоорієнтованим.

ДЖЕРЕЛА

1. Clarion technologies URL: https://www.clariontech.com/blog/how-to-use-python-for-demand-forecasting-in-consumer-goods
2. ResearchGate / Research on Product Demand Forecasting and Personalized Recommendation Based on Data Analysis/ June 2024 URL: https://www.researchgate.net/publication/381474330_Research_on_Product_Demand_Forecasting_and_Personalized_Recommendation_Based_on_Data_Analysis
3. Medium / From Prediction to Presentation: Sales Forecasting with Meta's Prophet and Power BI Using Python/ 15 December 2024 URL: https://medium.com/microsoft-power-bi/from-prediction-to-presentation-sales-forecasting-with-metas-prophet-and-power-bi-using-python-5c4d298f748e

ДЕЯКІ ДОСЛІДЖЕННЯ ФОРМИ ТІНІ ПРАВИЛЬНОЇ ЗРІЗАНОЇ ШЕСТИКУТНОЇ ПІРАМІДИ

Браганець І. І., Желтуха Т. В.
Криворізький Покровський ліцей, м. Кривий Ріг

При облаштуванні території, при створенні мистецьких споруд для прикрашання площ, парків, палаців міста широко використовуються різноманітні геометричні тіла. Крім форм геометричних тіл можна урізноманітнити зовнішній вигляд території у темний час доби за допомогою різного розташування джерел світла. Саме дослідженню форми тіні від правильної зрізаної шестикутної піраміди в залежності від їх кількості і присвячена дана робота.

Під тінню ми розуміємо зображення правильної шестикутної зрізаної піраміди на площину основи побудованої за допомогою центрального проєктування з центром в точці розташування джерела світла [1, 2].

Задавши умову, що довжина сторони нижньої основи правильної шестикутної зрізаної піраміди у k разів більша за довжину верхньої основи та з'ясувавши, що у випадку, коли джерело світла розташоване на прямій, що перпендикулярна основі піраміди в точці, що є серединою ребра нижньої основи на висоті $H = \frac{2kh}{k-1}$, то тінь від двох бічних граней буде відсутня. При цьому, $\frac{H}{H-h} = 2k,$ де H – висота, на якій розташоване джерело світла, h – висота заданої зрізаної піраміди.

Визначено площу тіні від заданої зрізаної піраміди від одного джерела світла, розташованого на висоті H у випадку, коли воно рухається по прямій, що містить сторону нижньої основи (рис. 1), а також від двох джерел світла, що рухаються по цій прямій і знаходяться на відстані $\frac{pak}{2}$ від середини нижньої основи заданої зрізаної піраміди (рис. 2)

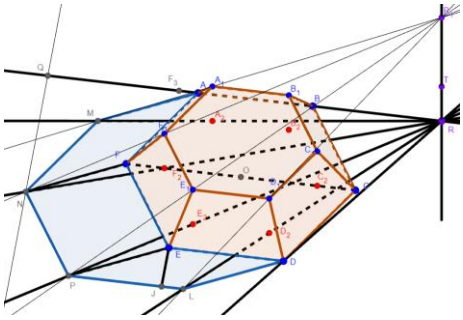


Рис. 1

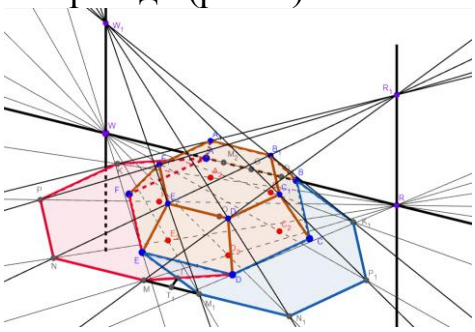


Рис. 2

Крім того в роботі проведені дослідження форми тіні від заданого геометричного тіла у випадку його освітлення чотирма джерелами світла. Причому, два джерела світла рухаються по прямій, що містить нижню основу піраміди, а два інші рухаються по прямим, що містять діагоналі нижньої основи. (Точки R і G лежать на прямій AB, точка W на прямій BD, а точка X на прямій AE: $AX = AG = BR = BW = \frac{pka}{2}$, $p \geq 1$) (рис. 3 – 8).

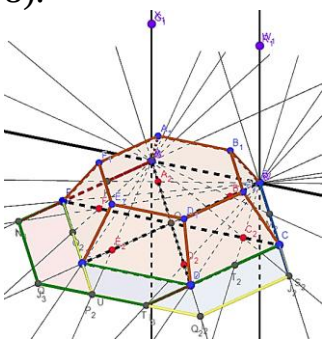


Рис. 3

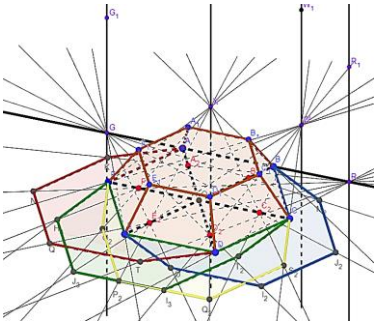


Рис. 4

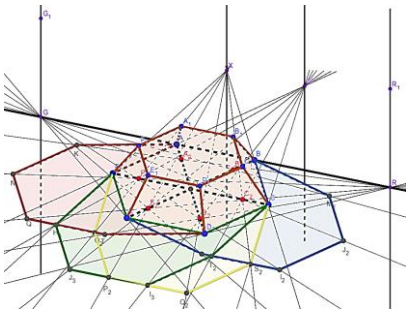


Рис. 5

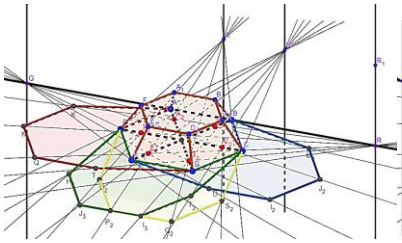


Рис. 6

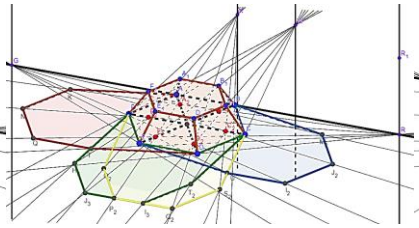


Рис. 7

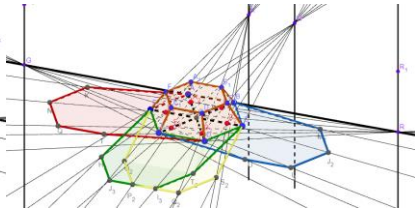


Рис. 8

Крім того, було з’ясовано, що за умови, коли $p = 0$ маємо випадок зображений на рис. 3; коли $0 < p < \frac{2\sqrt{3}k-2k+2\sqrt{3}}{2k-1}$ маємо випадок зображений на рис. 4, а при $p = \frac{2\sqrt{3}k-2k+2\sqrt{3}}{2k-1}$ маємо випадок зображений на рис. 5.

Випадок, зображений на рис.6, маємо за умови, коли

$$\frac{2\sqrt{3}\mathrm{k} - 2\mathrm{k} + 2\sqrt{3}}{2\mathrm{k} - 1} < p < -2k - 2k\sqrt{3} + 5 + \sqrt{3} + \sqrt{4k^2 + 2k^2\sqrt{3} + 7 - 8k + 6k\sqrt{3} - 3{,}5\sqrt{3}}$$

Випадок, зображений на рис. 7, маємо за умови, коли

$$p = -2k - 2k\sqrt{3} + 5 + \sqrt{3} + \sqrt{4k^2 + 2k^2\sqrt{3} + 7 - 8k + 6k\sqrt{3} - 3{,}5\sqrt{3}}$$

Випадок, зображений на рис. 8, маємо за умови, коли

$$p > -2k - 2k\sqrt{3} + 5 + \sqrt{3} + \sqrt{4k^2 + 2k^2\sqrt{3} + 7 - 8k + 6k\sqrt{3} - 3{,}5\sqrt{3}}$$

Таким чином досліджено зміну форми тіні в залежності від розташування джерел світла та їх кількості та визначено формули для обчислення їх площ в кожному можливому випадку.

ДЖЕРЕЛА

1. Види проектування. Українська інженерно-педагогічна академія. Лекція 3. [Електронний ресурс] Точка доступу: https://studfile.net/preview/9780202 /

2. Геометрія: (профіл.рівень): підручник для 10-го кл. закл. заг. серед. освіти / Олександр Істер. – Київ: Генеза, 2018.

ПРИСКОРЕННЯ ОБЧИСЛЮВАЛЬНИХ АЛГОРИТМІВ ОБРОБКИ ЗОБРАЖЕНЬ ІЗ ВИКОРИСТАННЯМ SIMD

Вохмянін Г. Я.[1], Жульковський О. О.[1], Жульковська І. І.[2]

[1]*Дніпровський державний технічний університет, м. Кам'янське*

[2]*Університет митної справи та фінансів, м. Дніпро*

У сучасному світі високопродуктивних обчислень ефективне використання апаратних можливостей PC є ключовим фактором для досягнення максимальної швидкості обробки даних. Це передбачає не лише раціональний вибір обчислювальної платформи, але й оптимізацію програмного забезпечення з урахуванням особливостей архітектури процесора, таких як, наприклад, векторні інструкції (SIMD – Single Instruction Multiple Data), багатоядерність, кеш-пам'ять тощо. Застосування таких підходів дозволяє значно зменшити час виконання складних обчислень, підвищити продуктивність системи в цілому та забезпечити ефективну масштабованість при обробці великих обсягів даних [1].

Обробка великих масивів даних, зокрема зображень, залишається однією з обчислювально-витратних обчислювальних задач. Типовим

прикладом таких задач є алгоритм Гаусового згладжування, який широко застосовується для зменшення шуму та видалення деталей з цифрових зображень, завдяки виконанню великої кількості однотипних арифметичних операцій над кожним пікселем зображення [2]. В контексті зростаючих об’ємів даних та вимог до швидкодії програмного забезпечення, оптимізація подібних алгоритмів набуває особливої актуальності.

Технологія SIMD пропонує необхідний інструментарій для паралельної обробки даних на рівні інструкцій процесора. Основний принцип SIMD полягає у виконанні однієї операції одночасно над декількома елементами даних, що дозволяє значно підвищити обчислювальну ефективність [3].

В межах дослідження були проведені експерименти для різноманітних зображень розмірами 1920x1080 та 2560x1440 пікселів. До кожного зображення було застосовано десять експериментів з різним радіусом та відхиленням розмиття. Такий принцип проведення експериментів дозволяє дослідити вплив відхилення та радіусу на час виконання обчислень.

Результати, отримані в ході експериментів із різними конфігураціями та роздільними здатностями зображень, підтверджують теоретичні переваги використання технології SIMD. Так, для зображення розміром 1920x1080 пікселів із радіусом ядра r=5 скалярна реалізація може займати приблизно 275 мс, тоді як оптимізована версія з використанням AVX-інструкцій скорочує цей час до 40 мс, забезпечуючи прискорення майже в 7 разів. Для вищої роздільної здатності, такої як 2560x1440, продуктивність також значно зростає: час виконання скалярної версії становить близько 480 мс, а SIMD-версії – приблизно 70 мс, що свідчить про стабільне прискорення. Незначне відхилення від теоретичного максимуму можна пояснити накладними витратами на векторизацію даних, девекторизацію результатів та обробкою крайових випадків, які не можуть бути повністю векторизовані. Збільшення радіуса ядра до 10 призводить до зростання обчислювальної складності, однак відносне прискорення за допомогою SIMD залишається значним. Отримане розмиття зображення наведено на рисунку 1.

Напрямками подальших досліджень є поєднання SIMD-оптимізації з багатопоточною обробкою для додаткового прискорення на багатоядерних процесорах та дослідження можливостей використання інших наборів інструкцій, наприклад, AVX-512.

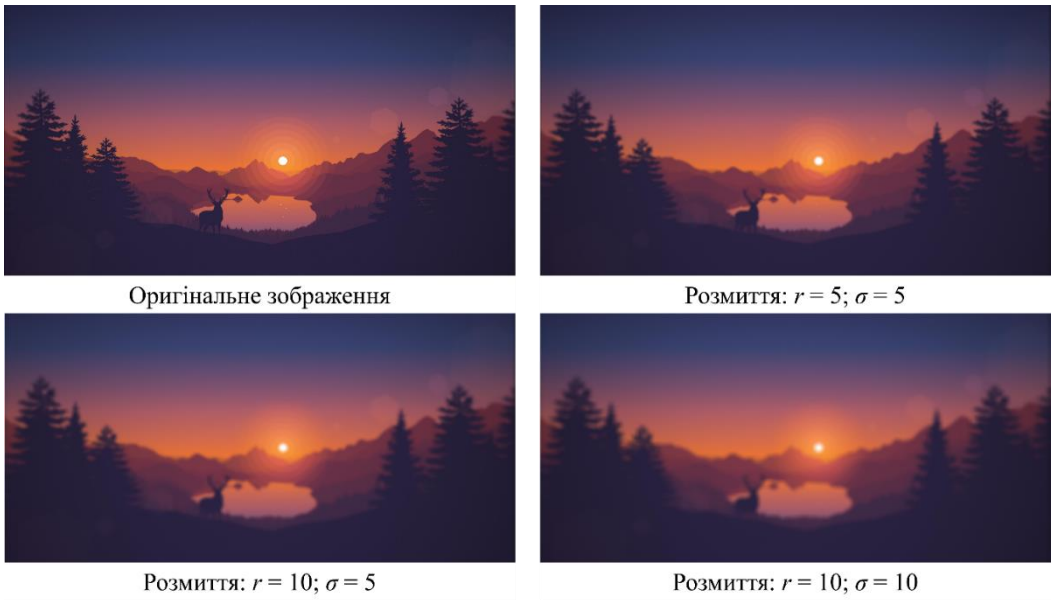


Рис. 1. Результати розмиття зображення

ДЖЕРЕЛА

1. Masciari E., Napolitano E.V. Sustainability and High Performance Computing. *Lecture Notes in Computer Science*. 2024. P. 237–242. URL: https://doi.org/10.1007/978-3-031-78093-6_21

2. Zin N. Oo. The Improvement of 1D Gaussian Blur Filter using AVX and OpenMP. *2022 22nd Int. Conf. Control, Automat. Syst. (ICCAS)*, Nov. 27–Dec. 1 2022. Jeju, 2022. P. 1493–1496. URL: https://doi.org/10.23919/iccas55662.2022.10003739

3. Kusswurm D. SIMD Fundamentals. *Modern Parallel Programming with C++ and Assembly Language*. 2022. P. 1–16. URL: https://doi.org/10.1007/978-1-4842-7918-2_1

ЗАДАЧА ПОЗДОВЖНЬОГО ЗСУВУ ДЛЯ КІЛЬЦЯ З УМОВАМИ «М'ЯКОГО» КОНТАКТУ

Журавльова З. Ю., Фатєєва Н. А.
Одеського національного університету імені І.І. Мечникова, м. Одеса

Розглянемо кільце $a < r < b$, $-\pi < \varphi < \pi$, що знаходиться у стані антиплоскої деформації. Бічна грань $r = b$ нерухомо закріплена, на грань $r = a$ діє навантаження інтенсивності $Gg(\varphi)$. В області при $r = c, 0 < \varphi < \alpha$ розташований «м'який» прошарок, тобто між частинами кільця $a < r < c$ та $c < r < b$ виконуються умови «м'якого» контакту [1]. Потрібно знайти переміщення та напруження кожного з шарів, що задовольняють наступну крайову задачу

$$\begin{cases} r\frac{\partial}{\partial r}(\frac{\partial W}{\partial r})+\frac{\partial W^2}{\partial \phi^2}=0, a<r<b, -\pi<\phi<\pi, \\ W\big|_{\phi=-\pi}=W\big|_{\phi=\pi}, \tau_{\phi z}\big|_{\phi=-\pi}=\tau_{\phi z}\big|_{\phi=\pi}, a<r<b \\ \tau_{rz}\big|_{r=a}=Gg(\phi), W\big|_{r=b}=0, -\pi<\phi<\pi, \\ <W(c,\phi)>=W(c-0,\phi)-W(c+0,\phi)=-\frac{h_0}{G_0}\tau_{rz}(c-0,\phi) \\ <\tau_{rz}(c,\phi)>=\tau_{rz}(c-0,\phi)-\tau_{rz}(c+0,\phi)=0 \end{cases} \quad (1)$$

Тут $W(r,\varphi)$ - переміщення відносно вісі z, $\tau_{rz}(r,\varphi)$, – дотичні напруження, h_0 – товщина прошарку ($\boldsymbol{h_0 \ll b-a}$), G_0 – модуль зсуву прошарку, причому $\boldsymbol{G_0 \ll G}$, G – модуль зсуву кільця.

Задачу (1) зведено до одновимірної крайової задачі шляхом застосування повного скінченного перетворення Фур'є за змінною φ [2]. Крайова задача у просторі трансформант має наступний вигляд:

$$r\frac{\partial}{\partial r}(r\frac{\partial W_k}{\partial r})+k^2\frac{\partial W_k{}^2}{\partial \phi^2}=0 \quad (2)$$

$$\left.\frac{dW_k}{dr}\right|_{r=a}=g_k(\varphi), W\big|_{r=b}=0 \quad (3)$$

$$<W_k(c)>=W_k(c-0)-W_k(c+0)=-\frac{h_0 G}{G_0}\frac{dW_k}{dr}(c-0), \quad <\frac{dW_k}{dr}(c)>=\frac{dW_k}{dr}(c-0)-\frac{dW_k}{dr}(c+0)=0 \quad (4)$$

де k – параметр інтегрального перетворення.

Загальний розв'язок розривної крайової задачі (2)-(4) побудований за допомогою функції Гріна, фундаментальної базисної системи розв'язків (ФБСР) та фундаментальної базисної системи розривних розв'язків [3]. Він має наступний вигляд:

$$W_k(r)=ag_k\psi_0(r)-\frac{h_0 G}{G_0}\frac{dW_k}{dr}(c-0)\tilde{W}_{k\,0}(r) \quad (5)$$

Тут $\tilde{W}_{k\,0}$ – розривний розв'язок крайової задачі (2)-(4), $\psi_0(r)$ – перша компонента ФБСР.

З виразу (5) було знайдено подання для невідомої трансформанти $\frac{dW_k}{dr}(c-0)$:

$$\frac{dW_k}{dr}(c-0)=\frac{aG_0 g_k \psi'_0(c)}{G_0+h_0 G\tilde{W}'_{k\,0}(c)}$$

Аналогічно до загального випадку $k\neq 0$ було знайдено розв'язок крайової задачі (2)-(4) при $k=0$. До отриманих розв'язків у просторі трансформант було застосовано формулу обернення. Таким чином було

відшукано точний розв'язок вихідної задачі (1), що дозволяє проаналізувати зміну переміщень та напружень всередині кільця з тонким «м'яким» прошарком. Запропонований підхід можна використовувати для задачі теплопровідності.

ДЖЕРЕЛА

1. Mishuris G.S., Movchan N.V., Movchan A.B. Steady-state motion of a mode-III crack on imperfect interfaces. Q. Jl Mech. Appl. Math., Vol. 59, No. 4. 2006. doi:10.1093/qjmam/hbl013

2. Попов Г. Я. Навчальний посібник з курсу «Рівняння математичної фізики. Метод інтегральних перетворень» : для студ. техн. спец. вузів / Г. Я. Попов, В. В. Реут, Н. Д. Вайсфельд ; відп. ред.: В. Є. Круглов ; ОНУ ім. І.І. Мечникова. – Одеса : Астропринт, 2005. – 183 с.

3. Вайсфельд, Н. Д. Навчальний посібник з курсу «Рівняння математичної фізики» : (для студ. спец. «Прикладна математика» і «Механіка») / Н. Д. Вайсфельд, Г. Я. Попов, В. В. Реут. – Електрон. кн. – Одеса, 2013. – 215 с.

ТЕХНОЛОГІЇ ОБРОБКИ ТА АНАЛІЗУ ДАНИХ

Кинюк О. А, Гутаревич Д. Ю.

Західноукраїнський національний університет, м. Тернопіль

В епоху стрімкого росту обсягів інформації вміння працювати з великими даних (Big Data) є критично важливим для кожної сфери. Автоматизацію процесів роботи з даними забезпечують сучасні технології, що уможливлює краще розуміння клієнтів компаніями, прогнозування поведінки ринку, підвищення ефективності результатів діяльності [1]. Крім того, в умовах глобальних викликів – війни, пандемії, кліматичних змін – аналітика даних є ключем до прийняття своєчасних і стратегічно виважених рішень.

Технології обробки даних охоплюють процедури збору, зберігання, аналізу та візуалізації даних, які злагоджено функціонують завдяки синергії програмного забезпечення, потужної обчислювальної техніки та гнучких методів, що постійно розвиваються. На рисунку 1. представлено структурну схему аналізу великих даних.

Сьогодні особливою популярністю відзначаються технології на основі методів машинного навчання, що уможливлюють виявлення закономірностей в даних, адаптацію до нових ситуацій та прийняття виважених рішень.

За реалізацію процедури зберігання даних відповідають бази даних, зокрема нереляційні (NoSQL), що забезпечують масштабованість та високу швидкість обробки розподілених даних [2; 3]. Технологія блокчейн (Blockchain) призначена для запису та передачі розподіленої інформації й збереження криптографічно захищених даних у вигляді блоків. Для

розподіленої обробки інформації досить поширеною є модель MapReduce, яка включає функцію Map() для обробки та генерації наборів проміжних пар ключ / значення та функцію Reduce() для зведення всіх проміжних значень, зв'язаних із одним проміжним ключем [3]. При цьому платформою для організації розподіленого зберігання даних виступає файлова система Apache Hadoop [2; 4].

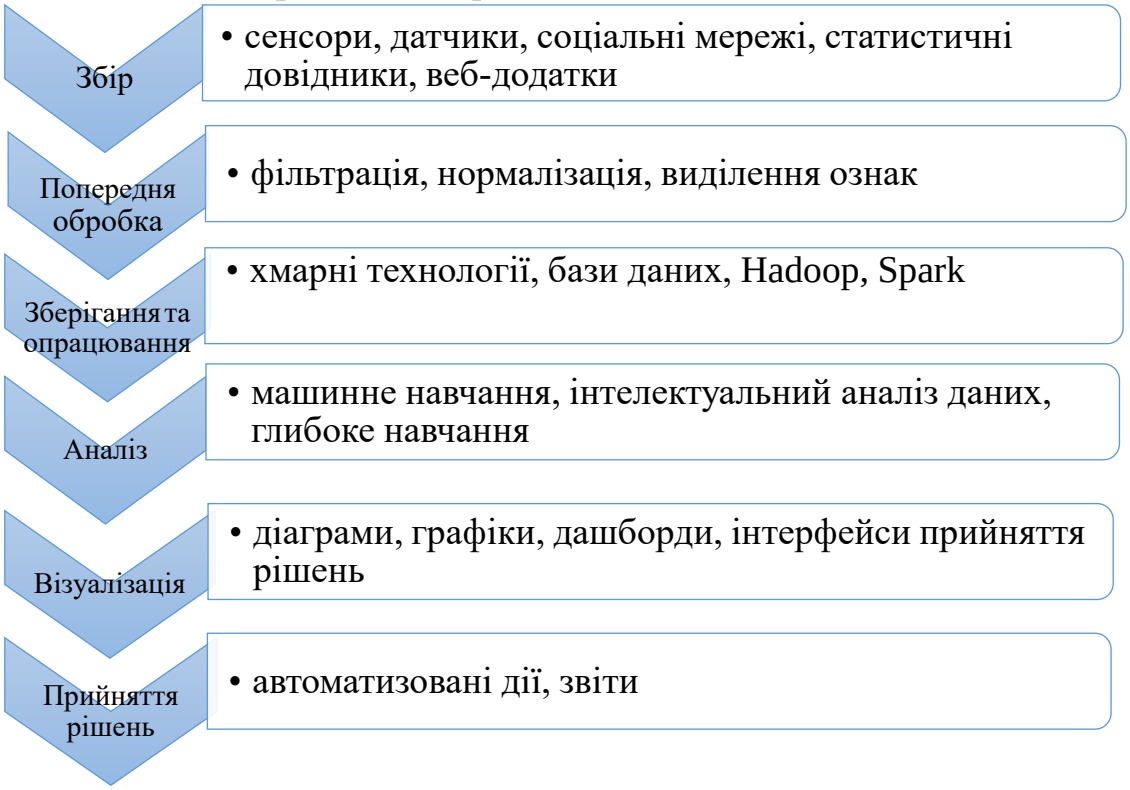


Рис. 1. Структурна схема аналізу даних

Програмування систем обробки великих даних здійснюється здебільшого на основі програмного середовища мови R, що забезпечує статистичну обробку, моделювання та графічну візуалізацію даних [1]. Не менш важливими при цьому є мови Java, Python та Scala із відповідними бібліотеками аналізу даних.

Аналіз даних ґрунтується, здебільшого, на методах інтелектуального аналізу даних (Data Mining), що дозволяють виявляти невідомі раніше знання, зв’язки та закономірності у великих масивах даних. Варто зауважити, що ключовим інструментом Data Mining при розробці прогнозних моделей є машинне навчання. Також слід відзначити штучні нейронні мережі, як універсальний засіб апроксимації для моделювання випадкових процесів й аналізу нелінійних залежностей між даними.

Таким чином, перспективність технологій аналізу даних визначається їх практичною користю й механізмами, що уможливлюють ефективне реагування на виклики сьогодення, передбачення майбутнього й розробку більш розумного, сталого й безпечного середовище. Розвиток штучного інтелекту, машинного навчання та хмарних технологій створює нові горизонти для глибшого, точнішого та швидшого аналізу.

ДЖЕРЕЛА

1. Пантєлєєва Н.М., Дідковський Р.М. Сучасні технології обробки даних і знань для реального сектору економіки: технологічний, економічний та соціальні аспекти // Вчені записки ТНУ імені В. І. Вернадського.2020. Том 31 (70). № 4. С. 145-150.
2. Що таке великі дані (Big Data)?: веб-сайт. URL: https://university.sigma.software/what-is-big-data/ (дата звернення 25.04.2025).
3. Верес О. М., Оливко Р. М. Класифікація методів аналізу великих даниих. URL: https://science.lpnu.ua/sites/default/files/journal-paper/2018/jun/13005/ilovepdfcom-84-92.pdf (дата звернення 26.04.2025).
4. Комар М. П. Інформаційна технологія інтелектуальної обробки та аналізу великих даних // Вісник Хмельницького національного університету. 2020. №5 (289). С. 120-125.

ВИКОРИСТАННЯ ОПТИМІЗАЦІЙНИХ МОДЕЛЕЙ У РОЗПОДІЛЕНИХ МЕРЕЖАХ

Кучеренко В.

Київський столичний університет імені Бориса Грінченка, м. Київ

Оптимізація, це надзвичайно актуальна тема, особливо в умовах розвитку великих розподілених обчислювальних систем, енергетичних мереж, транспортних систем та мереж зв'язку. Сфера застосування методів і моделей оптимізації дуже широка, виділемо деякі з них, що стосується нашої предметної області

Таблиця

Основні напрями використання оптимізаційних моделей у розподілених мережах [1; 2]

Оптимізація розподілу ресурсів	У мережах обчислень (наприклад, хмарних) важливо правильно розподіляти обчислювальні ресурси між вузлами для мінімізації затримок і витрат енергії. Для цього використовуються моделі лінійного, цілочисельного та стохастичного програмування.
Управління потоками даних	У телекомунікаційних мережах оптимізація трафіку дозволяє мінімізувати затримки передачі даних і уникати перевантаження окремих ділянок мережі (наприклад, за допомогою алгоритмів оптимального маршрутизації)
Енергетичні мережі	В «розумних» електромережах (smart grids) оптимізаційні моделі допомагають балансувати виробництво і споживання енергії, враховуючи розподілені джерела енергії (наприклад, сонячні панелі, вітряки)
Безпека мережі	Оптимізація розміщення засобів захисту і швидкості реагування на інциденти в розподілених мережах є критично важливою. Для цього застосовують методи математичної оптимізації та теорії ігор

Типові методи оптимізації:

- Лінійне і нелінійне програмування
- Динамічне програмування
- Еволюційні алгоритми (генетичні алгоритми)
- Метод роїв частинок (PSO)
- Методи градієнтного спуску (у розподіленій формі)

Виклики:

- Висока складність обчислень через масштаб мережі
- Обмеження пропускної здатності каналів зв'язку
- Динамічна природа мереж (зміна топології)
- Безпека і приватність даних

Загальний вигляд постановки оптимізаційної задачі:

min $f(x)$

під обмеженнями $g_i(x) \leq 0,\ i=1,\ldots,m$

$h_j(x)=0,\ j=1,\ldots,p$

де:

- $x \in R^n$ – вектор керованих змінних (розподіл ресурсів між вузлами мережі),
- $f(x)$ – цільова функція (мінімізація загальної затримки)
- $g_i(x)$ – обмеження нерівності (обмеження пропускної здатності каналів),
- $h_j(x)$ – обмеження рівності (збереження ресурсів).

Для оптимізації маршрутизації даних: $\min_{x_{ij}} \sum_{(i,j)\in E} c_{i,j} x_{i,j}$

під обмеженнями: $\sum_{j:(i,j)\in E} x_{i,j} - \sum_{j:(j,i)\in E} x_{j,i} = s_i$

$0 \leq x_{ij} \leq u_{ij},\ \forall (i,j) \in E$

де: V – множина вузлів мережі, E – множина дуг (з'єднань) між вузлами, x_{ij} – потік від вузла i до вузла j, c_{ij} – вартість передавання одиниці потоку через дугу (i,j) u_{ij} – максимальна пропускна здатність дуги (i,j), s_i – джерело/стік потоку в вузлі i (додатнє для джерел, від'ємне для стоків, нуль – для проміжних вузлів).

Як правило, мережа настільки велика, що оптимізація має виконуватись локально на окремих вузлах, ттому і ставиться задача у вигляді розподіленої оптимізації: $\min_{x_i \ldots\ldots, x_N} \sum_{i=1}^{N} f_i(x_i)$, під глобальними обмеженнями: $\sum_{i=1}^{N} A_i x_i = b$.

Тут кожен вузол i мінімізує свою локальну функцію $f_i(x_i)$, погоджуючи рішення із сусідніми вузлами через умови погодженості.

Для розв'язання такої задачі можна використовувати наступні методи: метод множників Лагранжа (ADMM), декомпозиційні методи, розподілені градієнтні методи.

ДЖЕРЕЛА

1. Р.М. Минайленко, Є.В. МелешкоПроблеми розподілених обчислень та шляхи їх вирішення Central Ukrainian Scientific Bulletin. Technical Sciences, 2021, Col.4(35) режим доступу: https://mapiea.kntu.kr.ua/pdf/4(35)/3.pdf

2. Євгеній Кузнєцов. Оптимізація продуктивності мережі: підвищення швидкості та надійності для безперебійного підключення, режим доступу: https://www.globalyo.com/uk/blog/optimizing-network-performance-enhancing-speed-and-reliability-for-seamless-connectivity/

ОСНОВИ ТЕОРІЇ ЙМОВІРНОСТЕЙ ТА ЇХ ЗАСТОСУВАННЯ ДЛЯ РОЗВ'ЯЗУВАННЯ ОКРЕМИХ ЗАДАЧ

Майстренко В. О, Желтуха Т. В.

Криворізький Покровський ліцей, м. Кривий Ріг

Актуальність дослідження математичного сподівання виграшу в лотереї зумовлена зростаючою популярністю азартних ігор та необхідністю підвищення фінансової грамотності населення. Розуміння математичної сутності лотерей дозволяє потенційним учасникам приймати більш обґрунтовані рішення щодо своєї участі, оцінювати пов'язані з цим ризики та порівнювати різні лотерейні пропозиції.

В роботі проаналізовані умови розіграшу деяких національних лотерей, таких як «СУПЕР ЛОТО», «ЛОТО МАКСИМА» та «КЄНО» [1].

Опрацювавши умови розіграшу зупинились на більш детальному аналізі таких національних грошових лотерей, як «СУПЕР ЛОТО» та «ЛОТО МАКСИМА» через можливість за загальнодоступними даними визначити кількість проданих квитків, а отже й можливість обчислити ймовірність вгадування певної кількості номерів.

В зазначених лотереях було складено закон розподілу випадкової величини – розміру виграшу та визначено її математичне сподівання в понад 30 різних розіграшах.

Покажемо на прикладі розіграшу лотереї «СУПЕР ЛОТО»

Проаналізуємо результати розіграшу лотереї:

№ розіграшу: 2483	Дата розіграшу: 22.01.2025					
Кількість проданих квитків	39050					
Виграшні комбінації (кількість вгаданих кульок)	0 або 1	2	3	4	5	6
Розмір виграшу, грн	0	50	149	3801	0	26242367
Кількість виграшів	34383	4165	477	25	0	0

Закон розподілу випадкової величини X (розміру виграшу у лотереї) має вигляд:

Варіанта, Xi	0	50	149	3801	0	26242367
Ймовірність, pi	0,880486556	0,1067	0,0122	0,0006	0	0

Обчислимо математичне сподівання випадкової величини X:

$$M(X) = 0 \cdot 0{,}880486556 + 50 \cdot 0{,}1067 + 149 \cdot 0{,}0122 + 3801 \cdot 0{,}0006 \approx 9{,}59$$

Таким чином, математичне сподівання розміру виграшу в цьому розіграші становить 9 грн 59 коп. Отримати такий виграш неможливо через те, що за офіційними правилами лотереї найменша сума виграшу становить 50 грн.

Проаналізувавши розіграши понад 30 різних розіграшів було з'ясовано, що найменше математичне сподівання виграшу 9,31 грн, а найбільше – 23, 63 грн. (рис. 1).

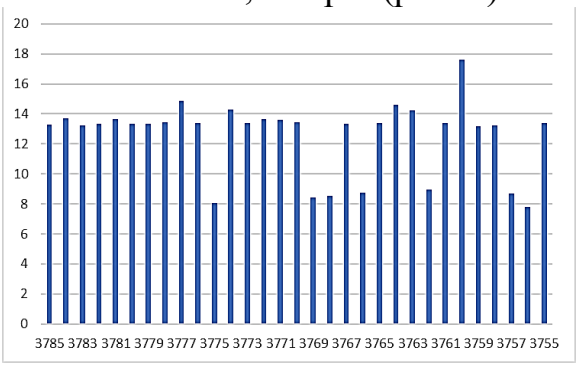


Рис. 1.

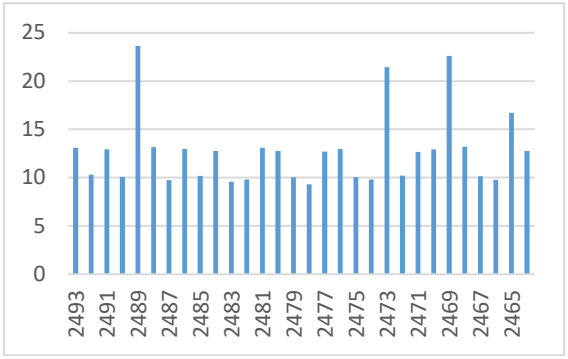


Рис. 2

Майже аналогічні результати були отримані при аналізі результатів національної грошової лотереї «ЛОТО МАКСИМА»: найменше математичне сподівання виграшу 9,36 грн, а найбільше – 23,23 грн. (рис. 2), тоді як найменший можливий виграш становить 38 грн.

Через те, що немає можливості визначити кількість проданих квитків державної грошової числової тиражної лотереї «КЄНО», неможливо обчислити ймовірність отримання певного виграшу. Саме тому будо складено закон розподілу випадкової величини – кількості вгаданих номерів. Визначено, що математичне сподівання кількості вгаданих номерів, обравши 10 із 80, становить 1,24 номери. Тоді як виграш можна отримати за 0 вгаданих номерів та від 3 до 10 номерів, тоді як найбільш ймовірно вгадати саме 1 – 2 номери.

У результаті виконаного дослідження було з'ясовано, що математичне сподівання можливого виграшу є меншим ніж вартість однієї спроби. Таким чином, ймовірність виграти у лотерею значно менше за можливість програти. Можливо, ця інформація допоможе тим, хто вирішив зіграти в лотереї, більш зважено поставитися до свого рішення

ДЖЕРЕЛА

1. Українська національна лотерея https://unl.net.ua/uk/games/superloto

ДОСЛІДЖЕННЯ ПОКАЗНИКІВ ЯКОСТІ ОСВІТИ В ЗАКЛАДАХ ЗАГАЛЬНОЇ СЕРЕДНЬОЇ ОСВІТИ ЗА ДОПОМОГОЮ МАТЕМАТИЧНОГО МОДЕЛЮВАННЯ

Метляєва О. П.
Київський столичний університет імені Бориса Грінченка, м. Київ

Математичне моделювання показників якості освіти у закладах загальної середньої освіти (ЗЗСО) є важливим інструментом для аналізу, прогнозування та підвищення ефективності освітніх процесів. Воно дозволяє виявляти взаємозв'язки між різними чинниками, які впливають на якість освіти, оцінювати вплив управлінських рішень та оптимізувати ресурси. Під час дослідження використано дані з сайтів Міністерства освіти і науки України (МОН): Перелік національних освітніх індикаторів ефективності та якості загальної середньої освіти та їх обрахунок [1]. Наведемо, відповідно до дослідження даних МОН, показники якості освіти в ЗЗСО, які можна використати при моделюванні освітніх процесів і які було вказано нами для побудови моделі: середній бал на ЗНО/НМТ, ВВП на освіту, кількість вчителів, кількість випускників, цифровізація освіти.

Розглянемо зазначені показники. Наведемо таблицю по середніх балах ЗНО/НМТ [2] за останні 10 років (Таблиця 1). Предмети: Математика, Українська мова, Історія України (2022 року дані лише з цих предметів).

Таблиця 1

Середній бал ЗНО/НМТ

Рік	Математика	Українська мова (літер.)	Історія України	Середнє значення
2015	150	138,5	145	144,5
2016	137,9	145,6	136,5	140,0
2017	140,6	144,8	136,5	140,6
2018	140,8	142,4	136	139,7
2019	139,4	141,1	135,5	138,7
2020	138,4	144	134,4	138,9
2021	137,9	144,2	136,1	139,4
2022	148,1	154,5	151,1	151,2
2023	135,4	148,5	141,7	141,9
2024	132,5	146,8	143,2	140,8

Одним із показників є цифровізація освіти. За досліджуваною статистикою за останні 10 років показник цифровізації у відсотках підвищився з 95,8% до 98%. Зокрема, це забезпечення закладів мережею Інтернет, платформами для дистанційного навчання, електронними інструментами в освіті та володіння цифровою компетентністю учасників освітнього процесу (детально описано в роботі [3]). Досягнення у сфері

цифровізації освіти в Україні протягом останніх років, відображає як прогрес, так і виклики, з якими стикалася система освіти.

Щодо ВВП, то в Україні витрати на освіту як частка ВВП є порівняно високими, але ефективність цих витрат залишається низькою через неефективне розподілення коштів та відсутність чітких показників якості освіти. Для покращення якості освіти потрібно підвищити ефективність фінансування та орієнтувати освітню систему на потреби інноваційної економіки.

Аналіз показників якості освіти в Україні дозволяє виявити ключові фактори, які впливають на результати навчання. Для моделювання можна використовувати множинну лінійну регресію, яка дозволяє оцінити вплив кількох незалежних змінних на одну залежну змінну. У нашому випадку залежною змінною буде Y – середній бал на ЗНО/НМТ (результативна), а незалежними: X_1 – ВВП на освіту, X_2 – кількість вчителів, X_3 – кількість випускників, X_4 – цифровізація освіти (факторні).

На основі матриці кореляції серед факторів, найбільші коефіцієнти кореляції з результативною змінною мають змінні X_1, X_2, X_4. Таким чином, існує позитивна кореляція між факторами X_1 (ВВП на світу) та Y (середнім балом ЗНО/НМТ, успішністю), між X_4 (цифровізацією освіти) та Y, між X_2 (кількістю вчителів) та Y слабкіше, але важливою є якість підготовки цих вчителів. До моделі буде включено ці факторні змінні. Проведення кореляційного аналізу (з використанням формули Пірсона) та побудова ліній тренду привели до відкидання фактору X_3 (кількість випускників). Кореляційний аналіз свідчить про те, що витрати на освіту та інші фактори можуть впливати на якість навчання в Україні. Важливо враховувати не лише кількісні показники, а й якість ресурсів і методів навчання для покращення освіти.

Як результат побудови рівняння множинної регресії досліджуваних показників, отримуємо аналітичний запис побудованої моделі:

$$Y = 543{,}19 + 0{,}0001X_1 + 0{,}0002X_2 - 5{,}26X_4.$$

Побудовану модель досліджено на адекватність із позитивним результатом. Знайдено коефіцієнти еластичності. Подальше дослідження передбачає аналіз даної моделі та перевірку на статистичну значущість.

Математичне моделювання показників якості освіти в ЗЗСО дозволяє систематизувати процес прийняття рішень, аналізувати вплив різних факторів на освітній процес та оптимізувати використання ресурсів для досягнення найкращих результатів.

ДЖЕРЕЛА

1. Перелік національних освітніх індикаторів ефективності та якості загальної середньої освіти. URL: https://zakon.rada.gov.ua/rada/show/v1116729-16#Text

2. Середні бал ЗНО/НМТ з основних предметів. URL: https://zno.testportal.com.ua/opendata.
3. Індекс цифрової трансформації регіонів України. URL: https://thedigital.gov.ua/storage/uploads/files/page/community/reports

РОЗРОБКА ГРИ АЛХІМІЇ В ЧОТИРЬОХ ВИМІРАХ

Мирошниченко Р. Б.
Київський столичний університет імені Бориса Грінченка, м. Київ

Розробка чотиривимірної гри – безпосередньо цікавий та нетривіальний процес, що вимагає від розробника розуміння математичних структур та навички працювати з ними. В своїх тезах я хочу розглянути основні математичні складові своєї гри.

Компактне та надійне зберігання даних про об'єкти

У грі кожен інгредієнт має два чотиривимірні вектори - позицію та вагу. Для ефективного зберігання великої кількості таких об’єктів необхідно мінімізувати обсяг даних без втрат точності. Запропоноване рішення полягає у перетворенні векторів у великі цілі числа (BigInt), які потім кодуються у системі числення з основою 62, що включає латинські літери та цифри [1-3]. Це дозволяє досягти високої щільності даних, зберегти повну точність та забезпечити можливість зворотного декодування. Такий підхід забезпечує надійність, компактність, потенціал для масштабування та ефективну валідацію.

Швидкий доступ до точної інформації про об’єкти без повного перебору

У грі можливі об’єкти, що відрізняються один від одного мінімально - на рівні найменшого значення типу float. При цьому потрібно зберігати тисячі або мільйони об'єктів та мати змогу швидко знаходити конкретний. Проблема полягає в тому, що пряме порівняння таких об’єктів потребує перебору всієї колекції, що неприйнятно для динамічної гри. Рішенням є генерація унікального хешу на основі векторів позиції та ваги, який однозначно визначає об’єкт [4 – 6]. Хеш дозволяє миттєво здійснювати пошук, без потреби у порівнянні властивостей, а також зберігати об’єкти у вигляді ключів у структурах з доступом за ідентифікатором.

Алгоритм змішування чотиривимірних інгредієнтів з вагою

Ключова механіка гри – змішування інгредієнтів, кожен з яких описується векторами позиції та ваги. Для цього використовується метод обчислення вагового середнього з урахуванням кількості та ваги кожного інгредієнта [7 – 8]. Спочатку обчислюється нова вага за формулою середнього, зваженого на кількість, після чого обчислюється нова позиція, зважена і на вагу, і на кількість. Початковий стан (порожній котел) має нульові значення, тому перший доданий інгредієнт повністю визначає стан суміші. Така система дозволяє формувати нові об’єкти, які в подальшому

можуть виступати інгредієнтами, зберігаючи цілісність математичної моделі.

ДЖЕРЕЛА

1. GitHub – petersmagnusson/base62: Аалгоритм кодування та декодування даних у форматі base62 з використанням BigInt. URL:https://github.com/petersmagnusson/base62 (дата звернення: 25.04.2025).
2. DEV Community – What is Base62 Conversion?: Огляд концепції base62-кодування, його переваг та реалізації на прикладі мови Go URL:https://dev.to/joshduffney/what-is-base62-conversion-13o0 (дата звернення: 25.04.2025).
3. GitHub – sindresorhus/base62: Бібліотека для кодування та декодування рядків, байтів та цілих чисел у форматі base62, що забезпечує компактне представлення даних URL:https://npmjs.com/package/%40sindresorhus/base62 (дата звернення: 25.04.2025).
4. Stack Overflow – Good way to hash a float vector?: Обговорення методів хешування векторів з плаваючою точкою, включаючи квантування та використання гіперкубів URL:https://stackoverflow.com/questions/650175/good-way-to-hash-a-float-vector (дата звернення: 25.04.2025).
5. GitHub – vitali-fedulov/hyper: Інструмент для хешування N-вимірних векторів з плаваючою точкою шляхом перетворення їх у координати гіперкуба URL:https://github.com/vitali-fedulov/hyper (дата звернення: 25.04.2025).
6. Stack Overflow – Hashing 2D, 3D and nD vectors: Обговорення варіантів хешування багатовимірних векторів, включаючи використання Locality Sensitive Hashing URL:https://stackoverflow.com/questions/5928725/hashing-2d-3d-and-nd-vectors (дата звернення: 25.04.2025).
7. ScienceDirect – An efficient optimization algorithm based on weighted mean of vectors: Опис алгоритму INFO, що використовує зважене середнє для оптимізації позицій векторів URL:https://sciencedirect.com/science/article/abs/pii/S0957417422000173 (дата звернення: 25.04.2025).
8. Springer – Weighted mean of vectors algorithm with neighborhood information interaction: Розширення алгоритму INFO з урахуванням інформації про сусідство та механізмів кросоверу URL:https://link.springer.com/article/10.1007/s10489-024-05889-x (дата звернення: 25.04.2025).

ВИЗНАЧЕННЯ ОБ'ЄМУ ПЕВНОЇ КОМПОЗИЦІЇ ТІЛ ОБЕРТАННЯ

Приходченко М. В., Желтуха Т. В.
Криворізький Покровський ліцей, м. Кривий Ріг

У нашому житті ми часто стикаємося з багатьма геометричними тілами, зокрема з тілами обертання [1; 2]. Ідея визначення об'єму різних тіл бере свій початок з давнини, особливо серед фермерів та агрономів, які використовували різні міри для обчислення об'ємів молока, зерна, меду тощо. Крім того, тіла обертання широко використовуються й при оформленні різних урочистостей.

В роботі було розглянуто композицію «ідеальних», на наш погляд, повітряних кульок, кожна з яких складається зі зрізаного конуса та двох сегментів сфер різного радіусу (рис.1). Розташування таких тіл передбачає, що центр меншої сфери, яка є проекцією меншої кулі, та центр більшої сфери, яка є проекцією більшої кулі, лежать в одній площині. Для кожного тіла ці центри розташовані у вершинах правильних опуклих багатокутників різних розмірів (рис. 2).

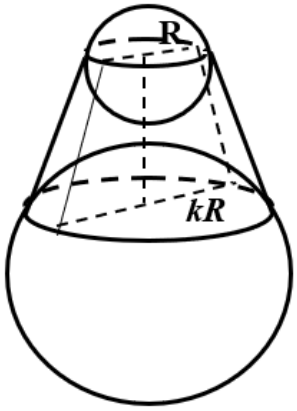


Рис. 1

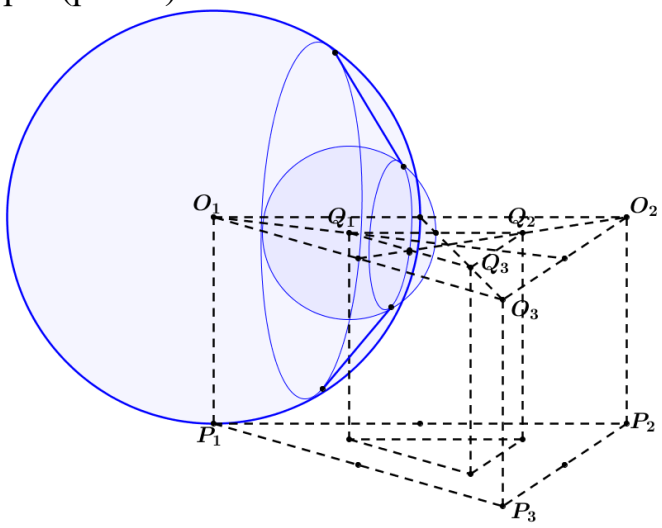


Рис. 2

Нехай задане геометричне тіло є композицією з n однакових геометричних тіл, кожне з яких складається з двох куль радіусами R та kR, з'єднаних між собою тілом обертання, що дотикається до кожної з них, і віссю якої є пряма, що проходить через центри куль [3] (рис. 3). Об’єм заданого тіла обертання можна обчислити за формулою:

$\mathrm{V_T} = n(\mathrm{V_1} + \mathrm{V_2} + \mathrm{V_3})$,

де V_1 - об’єм сегмента кулі з центром у т. $\mathrm{O_2}$ і висотою $\mathrm{P_2K_1}$; V_2 - об’єм сегмента кулі з центром у т. $\mathrm{Q_2}$ і висотою КР; V_3 - об’єм зрізаного конуса з висотою $\mathrm{KK_1}$ та радіусами основ $\mathrm{B_1K}$ та $\mathrm{A_1K_1}$.

$$\mathrm{V_1} = \pi \mathrm{P_2K_1^2}\left(\mathrm{A_1O_2} - \frac{\mathrm{P_2K_1}}{3}\right); \quad \mathrm{V_2} = \pi \mathrm{PK^2}\left(\mathrm{A_1O_2} - \frac{\mathrm{PK}}{3}\right);$$

$V_3 = \frac{1}{3}\pi h(B_1K^2 + B_1K \cdot A_1K_1 + A_1K_1^2)$, h – висота трапеції $A_1A_2\,B_2B$

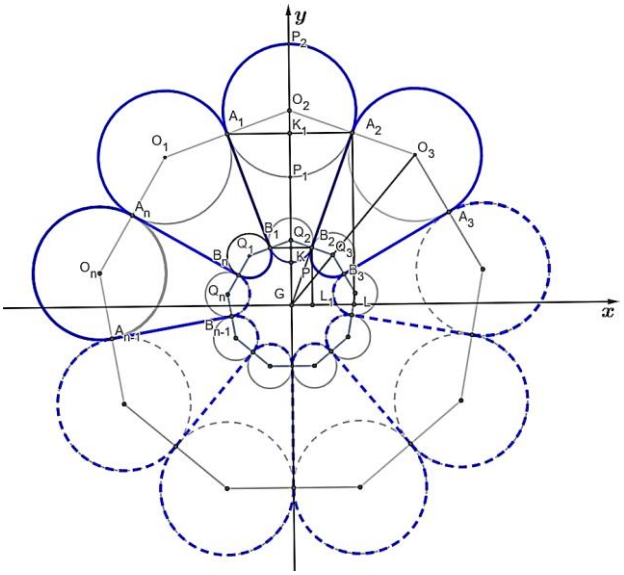


Рис. 3

Об'єм тіла обертання, що є композицією з n однакових тіл, становить:

$$V_T = \frac{\pi n R^3}{3}\left(2(k^3+1) + (k^3-1)\left(3\sin\frac{180^\circ}{n} - \sin^3\frac{180^\circ}{n} + \frac{\cos^3\frac{180^\circ}{n}}{tg\frac{180^\circ}{n}}\right)\right)$$

Крім того, в залежності від значення k кожне з m геометричних тіл, що входить до заданої композиції тіл може мати одну із трьох форм (рис. 4, 5, 6), а саме: дві кулі, що входять до його складу можуть перетинатися, дотикатися зовнішнім чином або не мати спільних точок.

$0 < k < \frac{1+\sin\frac{180}{n}}{1-\sin\frac{180}{n}}$ $\qquad$ $k = \frac{1+\sin\frac{180}{n}}{1-\sin\frac{180}{n}}$ $\qquad$ $k > \frac{1+\sin\frac{180}{n}}{1-\sin\frac{180}{n}}$

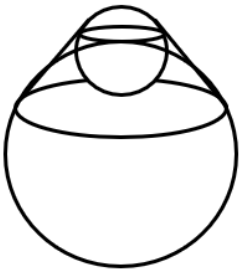


Рис. 4

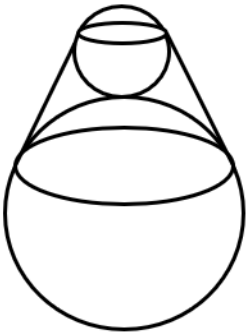


Рис. 5

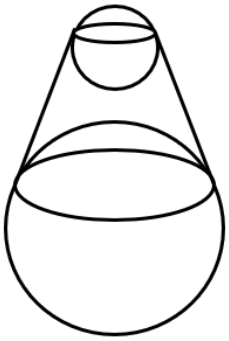


Рис. 6

ДЖЕРЕЛА

1. Істер О.С. Геометрія: (профіл.рівень): підручн. для 11-го кл. закл. заг. серед. освіти / Олександр Істер, Оксана Єргіна. – Київ: Генеза. 2019. – 288 с.: іл

2. Нелін Є.П. Геометрія в таблицях: Навчальний посібник для учнів старших класів. Х.: Світ дитинства, 1997. – 64 с.

3. Рабець К.В. Математичний турнір: змагання, що навчає і виховує: навчальний посібник / Катерина Рабець. – К.: Шк.світ, 2009. – 128 с. – (Бібліотека «Шкільного світу»)

ВИЗНАЧЕННЯ ФОРМ ПЕРЕРІЗІВ, ЯКІ ПЕРПЕНДИКУЛЯРНІ ЗАДАНОМУ ВІДРІЗКУ В ПРАВИЛЬНІЙ 2N-КУТНІЙ ПРИЗМІ

Радигіна К. М, Желтуха Т. В.

Криворізький Покровський ліцей, м. Кривий Ріг

Вміння будувати перерізи [1–3] знаходить широке застосування в багатьох практичних галузях, таких як інженерія, архітектура, дизайн тощо.

В даній роботі розглянуто побудову перерізу правильної призми, основа якої містить парну кількість вершин, площиною, що перпендикулярна її найбільшій діагоналі та проведена через будь-яку точку Т цієї діагоналі. Причому, всі ребра заданої призми рівні між собою.

Досліджуючи форми перерізу правильної шестикутної призми $A_1A_2A_3A_4A_5A_6B_1B_2B_3B_4B_5B_6$, що відповідають умові задачі, було визначено положення точки Т перерізу, що «рухається» діагоналлю B_1A_4 для отримання перерізу певної форми. $\left(\frac{B_1T}{TA_4} = k,\ T \in B_1A_4\right)$ З'ясовано, що переріз може набувати форми трикутника, шестикутника або прямокутника (рис. 1 – 8). В кожному з випадків визначено площу отриманого перерізу.

$0 < k < \frac{1}{4}$ $k = \frac{1}{4}$ $\frac{1}{1} < k < \frac{2}{3}$ $k = \frac{2}{3}$

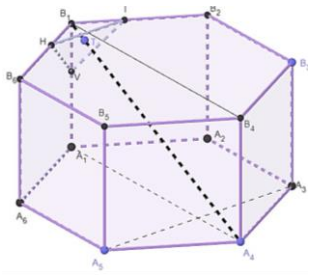


Рис. 1

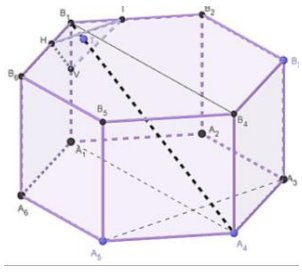


Рис. 2

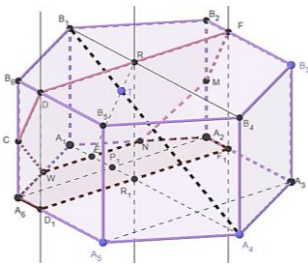


Рис. 3

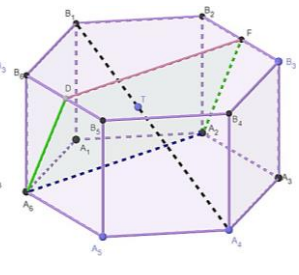


Рис. 4

$\frac{2}{3} \leq k \leq \frac{3}{2}$

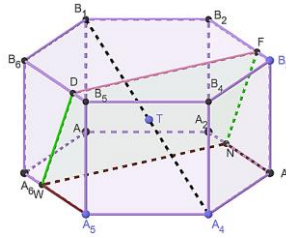


Рис. 5

$k = \frac{3}{2}$

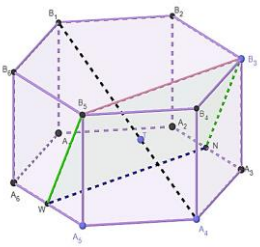


Рис. 6

$\frac{3}{2} < k < 4$

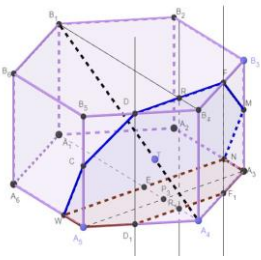


Рис. 7

$k \geq 4$

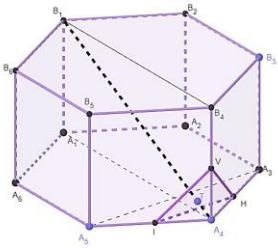


Рис. 8

Також було проведено дослідження на визначення форми перерізу у випадку правильної восьмикутної призми з рівними ребрами та було з'ясовано, що переріз може набувати форми трикутника, шестикутника або трапеції.

Побудувавши перерізи правильних призм, що містять парну кількість вершин основи, через точку на її найбільшій діагоналі перпендикулярно до неї з'ясували, що у випадку, коли основа заданої призми є правильним 4n-кутником, то переріз, що перпендикулярний його найбільшій діагоналі може набувати форми трикутника, трапеції та шестикутника.

Причому, коли точка перерізу на найбільшій діагоналі правильної 4n-кутної призми розташована у області, що показана на рисунку 9 рожевим кольором, переріз, що перпендикулярний діагоналі заданої призми має форму трикутника; у синю область – шестикутником та у червону – трапецією

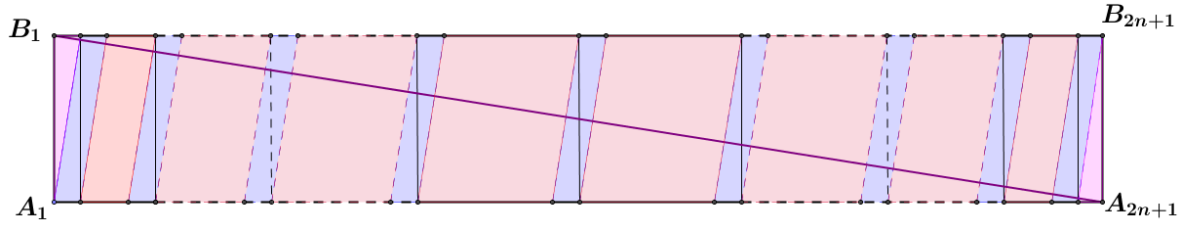


Рис. 9

У випадку, коли основа заданої призми є правильним (4n+2)-кутником, то переріз, що перпендикулярний його найбільшій діагоналі може набувати форми трикутника, трапеції, шестикутника та прямокутника.

Так, коли точка перерізу на найбільшій діагоналі правильної (4n+2)-кутної призми розташована у області, що показана на рисунку 10 рожевим кольором, переріз, що перпендикулярний діагоналі заданої призми має форму трикутника; у синю область – шестикутником та у червону – трапецією, а зелену - прямокутником.

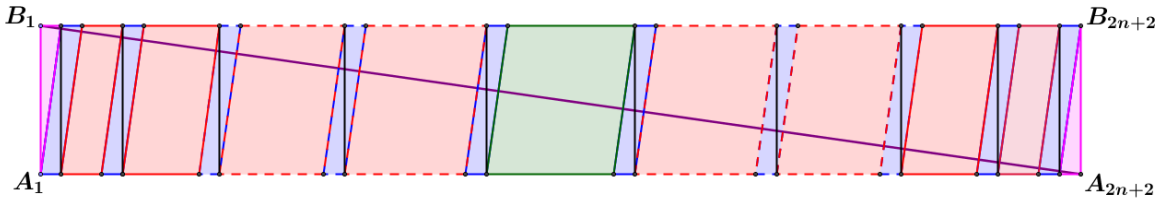


Рис. 10

ДЖЕРЕЛА

1. Властивості паралельних площин. [Електронний ресурс] – Режим доступу: la.kr.ua/paralelnist-pryamih-i-ploschin-u-prostori/vlastyvosti-paralelnykh-ploshchyn.html

2. Геометрія: підруч. для 10 кл. загальноосвіт. навч. закл. : Г36 профіл. рівень / Г.П. Бевз, В.Г. Бевз, Н. Г. Владімірова, В.М. Владіміров. – К. : Генеза, 2010. – 232 с. : іл. – Бібліогр. : с. 221

3. Калашніков І. В. Побудова перерізів просторових тіл у шкільному курсі математики: І.В.Калашніков, Н.Л.Синюк. – Вінниця: СамІздат, 2012 – 57 с.: іл

КОМП'ЮТЕРНИЙ АНАЛІЗ СИМЕТРІЇ ОБЛИЧЧЯ

Романюк О. Н. [1], Мазур В. В. [1], Тітова Н. В. [2], Романюк С. О. [2]

[1]*Вінницький національний технічний університет, м. Вінниця*

[2]*Національний університет «Одеська політехніка», м. Одеса*

Визначення симетрії обличчя по фотографії є важливою задачею у галузях комп'ютерного зору, біометрії, медицини та естетичної косметології. Загальний процес [1, 2] комп’ютерного визначення симетрії обличчя починається із виявлення обличчя на зображенні за допомогою спеціалізованих алгоритмів детекції, після чого виконується локалізація ключових орієнтирних точок обличчя, які включають положення очей, брів, носа, губ та контурів щелепи. Після розпізнавання ключових точок формується центральна вертикальна вісь обличчя, яка найчастіше визначається через середню лінію, що проходить через центр чола, перенісся і підборіддя. Ця вісь слугує основою для оцінювання симетрії. Для визначення симетрії кожна пара симетричних точок (наприклад, лівий і правий куточок ока, куточки рота) аналізується за їх відстанню до центральної осі. Ідеально симетричне обличчя характеризується рівною відстанню відповідних точок від цієї осі з обох сторін. Зазвичай розраховується відхилення кожної пари точок, після чого обчислюється середнє квадратичне відхилення або інші узагальнені статистики, що дозволяють кількісно оцінити рівень симетрії. Крім того, для підвищення точності аналізу враховується симетрія пропорцій між частинами обличчя (наприклад, відстань між очима порівняно із шириною губ) та симетрія кутів нахилу рис обличчя (наприклад, нахил брів).

Формально метрика симетрії часто обчислюється як певна функція від суми абсолютних або квадратичних відхилень між лівими і правими точками, нормалізована так, щоб отримане значення лежало у межах від 0 до 100%, де 100% означає ідеальну симетрію. Більш просунуті методи включають побудову дзеркального відображення однієї половини обличчя відносно центральної осі та обчислення подібності між віддзеркаленою і реальною другою половиною за допомогою метрик схожості зображень, таких як Structural Similarity Index. Практичне визначення симетрії обличчя часто супроводжується візуалізацією результатів, наприклад, накладанням центральної осі на зображення, підсвічуванням пар точок та графічним показом лінійних відхилень. Такий підхід використовується як у наукових дослідженнях, так і в прикладних системах, зокрема для покращення автоматичної ідентифікації особистості, планування реконструктивних пластичних операцій або в косметології для виявлення зон асиметрії.

При аналізі програмно обчислюються координати точок, будується центральна вісь, розраховуються відстані від точок до осі, а потім виводиться коефіцієнт симетрії. При цьому рівень складності реалізації може змінюватися в залежності від бажаної точності та швидкодії аналізу, адже базова оцінка може бути реалізована за кілька сотень рядків коду, а більш точна – потребувати врахування додаткових факторів, таких як освітлення, положення голови та корекція перспективних спотворень.

На практиці реалізація визначення симетрії обличчя за фото починається з попередньої обробки зображення: його масштабування, нормалізації освітлення і, при потребі, корекції нахилу обличчя так, щоб очі або горизонтальні осі рис обличчя були вирівняні. Після цього виконується побудова точкової моделі обличчя, де кожна ключова точка отримує свої координати у двовимірному просторі.

Визначивши центральну вісь обличчя, яка зазвичай проходить через середню точку між очима та середину підборіддя, обчислюються попарні відхилення для всіх симетричних точок. Наприклад, відстань між лівим і правим куточками очей відносно центральної осі, лівим і правим куточками губ, симетричними точками контуру обличчя. Різниця цих відстаней дозволяє встановити міру асиметрії для кожної пари. Для отримання узагальненого показника симетрії, сума всіх локальних відхилень нормалізується на кількість пар точок, що аналізувалися.

Пропонується враховувати не тільки симетричність по горизонталі, але і співвідношення висоти певних частин обличчя, наприклад, висота від лінії брів до очей порівнюється між лівою і правою сторонами. Для аналізу пропонується оцінювати текстуру шкіри або інтенсивність освітлення, щоб врахувати, чи обидві половини обличчя мають однакові характеристики кольору і контрасту. У цьому випадку замість простої геометричної симетрії визначається структурна або перцептивна симетрія.

Пропонується перетворювати зображення у набір чисел, що описують характер текстури в околі кожного пікселя, використовуючи для аналізу порівнюючи інтенсивність пікселів. Доцільним є використання метрики структурної подібності SSIM, яка оцінює схожість між двома зображеннями за трьома параметрами: яскравістю, контрастом і структурою. Для аналізу симетрії обираються ділянки з лівого і правого боків обличчя, наприклад дві зони скронь, після чого розраховується значення SSIM. Значення, близьке до 1, свідчить про високу симетрію текстур.

ДЖЕРЕЛА

1. Parkhi, O. M., Vedaldi, A., & Zisserman, A**.** Deep Face Recognition. University of Oxford, Visual Geometry Group, 2015. Technical Report, VGG, arXiv:1503.03832

2. Li, S. Z., & Jain, A. K. Handbook of Face Recognition (2nd Edition). Springer, 2011. 699 p.

АНАЛІТИЧНІ МЕТОДИ ОЦІНКИ ЯКОСТІ ЗОБРАЖЕНЬ

Рябоконь А. М., Романюк О. Н.

Вінницький Національний Технічний Університет, м. Вінниця

Зростання обсягів візуальної інформації зумовлює необхідність ефективних методів оцінки її якості. Аналітичні метрики відіграють важливу роль у автоматизованій оцінці, забезпечуючи кількісні характеристики спотворень зображень [1]. До найпоширеніших метрик оцінки якості зображень належать MSE [2] – середньоквадратична похибка та PSNR [3] – пікове відношення сигнал/шум .

Середньоквадратична похибка обчислюється за формулою:

$$MSE = \frac{1}{MN}\sum_{i=0}^{M-1}\sum_{i=0}^{N-1}[I(i,j) - K(i,j)]^2, \qquad (1)$$

де I(i,j) – значення пікселя у вихідному зображенні, K(i,j) – значення пікселя у спотвореному зображенні, а M та N – розміри зображення.

Пікове відношення сигнал/шум визначається як:

$$PSNR = 10\log_{10}\left(\frac{MAX^2}{MSE}\right), \qquad (2)$$

де MAX – максимальне можливе значення пікселя (наприклад, 255 для 8-бітного зображення). Хоча ці метрики є простими в обчисленні та широко застосовуються, вони мають суттєві недоліки, оскільки не завжди добре корелюють з суб’єктивним сприйняттям якості зображень людиною.

Для подолання цих обмежень було розроблено більш складні метрики, що намагаються врахувати особливості людської зорової системи. Однією з найбільш успішних є SSIM – індекс структурної подібності [4], який оцінює структурну інформацію, контраст та яскравість

зображень. Загальна формула структурної подібності між двома вікнами x і y однакового розміру становить:

$$SSIM = \frac{(2\mu_X\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)}, \quad (3)$$

де μ_x, μ_y – середні значення, σ_x^2,σ_y^2 – дисперсії, σ_{xy} – коваріація локальних вікон x та y, а c_1, c_2 – невеликі константи для стабілізації. SSIM показав значно кращу кореляцію з суб'єктивними оцінками порівняно з MSE і PSNR. Однак, SSIM також має свої обмеження, особливо при оцінці зображень зі значними спотвореннями.

В останні роки активний розвиток отримали нові, більш досконалі об'єктивні метрики якості зображень. До них належать метрики, що базуються на моделях видимості помилок [5], які намагаються безпосередньо моделювати чутливість людського ока до різних видів спотворень. Наприклад, VIF [6] – фактор інфляції дисперсії оцінює кількість інформації, отриманої з вихідного та спотвореного зображень людською зоровою системою. Інші сучасні метрики використовують концепції природної статистики зображень [7], аналізуючи статистичні закономірності, характерні для природних зображень, і вимірюючи ступінь їхнього порушення в спотворених зображеннях. Прикладами таких метрик є NIQE [8] – оцінювач якості природного зображення і BRISQUE [9] – сліпа/безеталонна оцінка якості зображення, які є метриками без опорного зображення, тобто вони можуть оцінювати якість зображення без наявності оригінального неспотвореного зображення. Формули для NIQE та BRISQUE є досить складними та включають етапи вилучення ознак на основі NSS та їх подальшу обробку для отримання оцінки якості.

Порівняльний аналіз цих об'єктивних метрик показує, що більш складні метрики, які враховують особливості людського зорового сприйняття та статистичні властивості природних зображень, демонструють значно кращу кореляцію з суб'єктивними оцінками якості. Однак, вони часто є більш обчислювально складними. Вибір конкретної метрики залежить від конкретного застосування та вимог до точності та швидкості оцінки. Подальші дослідження в цій галузі спрямовані на розробку ще більш точних та ефективних об'єктивних метрик, зокрема з використанням методів машинного навчання та глибокого навчання для кращого моделювання складностей людського зорового сприйняття та різних типів спотворень зображень.

ДЖЕРЕЛА

1. Gonzalez R. C. Digital Image Processing / R. C. Gonzalez, R. E. Woods. – 4th ed. – Pearson, 2018. – 1024 p.

2. Mean Squared Error: Definition, Formula, Interpretation and Examples [Електронний ресурс] URL: https://www.geeksforgeeks.org/mean-squared-error/.\ (дата звернення: 29.04.2025).

3. Peak Signal-to-Noise Ratio as an Image Quality Metric [Електронний ресурс] URL: https://tinyurl.com/2ekdn76z (дата звернення: 29.04.2025).

4. SSIM: Structural Similarity Index – Imatest [Електронний ресурс] URL: https://www.imatest.com/docs/ssim/ (дата звернення: 29.04.2025).

5. Mantiuk R., Myszkowski K., Seidel H.-P. Visible difference predicator for high dynamic range images // IEEE International Conference on Systems, Man and Cybernetics (IEEE Cat. No.04CH37583). 2004. Vol. 3, № 10. p. 2763-2769.

6. Sheikh H. R., Bovik A. C. Image Information and Visual Quality // IEEE Transactions on Image Processing. 2006. Vol. 15, № 2. p. 430–444.

7. Liu Y., Gu K., Li X., Zhang Y. Blind Image Quality Assessment by Natural Scene Statistics and Perceptual Characteristics // ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM). 2020. Vol. 16, № 91, p. 1–91.

8. Mittal A., Soundararajan R., Bovik A. C. Making a «Completely Blind» Image Quality Analyzer // IEEE Signal Processing Letters. 2013. Vol. 20, № 3. p. 209–212.

9. Mittal A., Moorthy A. K., Bovik A. C. No-Reference Image Quality Assessment in the Spatial Domain // IEEE Transactions on Image Processing. 2012. Vol. 21, № 12. p. 4695–4708.

РОЗРОБКА ВІЗУАЛЬНОЇ НОВЕЛИ «ЛІТНІЙ ВІТЕРЕЦЬ»

Табуровський М. С.

Київський столичний університет імені Бориса Грінченка, м. Київ

Візуальні новели – це не лише художній чи літературний виклик, а й складний техніко-дизайнерський процес. У цій роботі я презентую власну розробку гри «Літній вітерець» –емоційної романтичної історії, створеної в середовищі Ren'Py. Проєкт об’єднує сценарну нелінійність, художню стилістику аніме, програмну логіку і музичну динаміку.

Структура сценарію та логіка вибору

Сюжет розбитий на п’ять днів із чіткою сюжетною прогресією: знайомство, зближення, конфлікт, кульмінація і фінал. Ключова особливість – вплив вибору гравця на розвиток подій: кожна сцена має логічну умову переходу, реалізовану через гілкування та змінні у коді Python на основі Ren'Py. Такий підхід потребує чіткої математичної структури – побудови станів та логічних операторів **if**, **else**, які визначають результат. Для формування гілок сюжету я створив структуровану FSM (кінцеву автоматну модель), яка враховує значення змінних, збережених після кожного вибору, що дозволяє досягти варіативності у фіналі: романтичний, мрійливий або нейтральний [4].

Візуальний стиль і логіка спрайтів

Кожен персонаж створений у PNG-форматі з прозорим фоном і має варіанти емоцій (гнів, сором'язливість, сум, усмішка тощо), що підключаються залежно від сцени за допомогою умовного перемикання зображень. Для цього застосовано математичну модель зіставлення станів (наприклад, emotion = 'sad' → show hinata_sad), що дозволяє гнучко реагувати на сюжетні дії [2].

Музичний супровід та атмосфера

Для кожного з розділів було підібрано відповідні музичні теми – це або ліцензовані композиції, або згенеровані мелодії, що підлаштовані під емоційну динаміку сцени [1; 3; 5]. Наприклад, у сценах конфлікту звучить низькотональна атмосферна музика, тоді як у романтичних сценах – м'яке фортепіано. Перемикання композицій реалізоване логікою `` з керуванням гучністю, **fade-in/out** ефектами, що створює плавні переходи

Математичний підхід до структурування виборів

Окрім логіки **if-else**, я використав таблицю виборів, у якій кожен варіант має присвоєний числовий вплив на змінну **affection**. Це дозволяє математично відслідковувати рівень довіри між героями. Граничні значення цієї змінної визначають, які сцени будуть відкриті в майбутньому. Такий підхід дозволяє зробити гру адаптивною і динамічною.

ДЖЕРЕЛА

1. Ren'Py Documentation – Audio: Офіційна документація щодо додавання музики та звукових ефектів у Ren'Py. URL:https://www.renpy.org/doc/html/audio.html (дата звернення: 23.04.2025)

2. Ren'Py Documentation – Screen Language: Опис структури побудови екранних елементів та перемикання сцен у Ren'Py. URL:https://www.renpy.org/doc/html/screen_python.html(дата звернення: 23.04.2025).

3. Strategies to Enhance Your Visual Novel With Music URL:https://www.youtube.com/watch?v=wLzI4Moi55I (дата звернення: 23.04.2025).

4. Basic Tutorial: Choice Menu / Create Branching Paths / Flags URL:https://en.yorubox.eu/renpy-basic-tutorial-004-renpy-basic-commands/?utm_source=chatgpt.com#google_vignette (дата звернення: 23.04.2025).

5. Emotions, Color, and Music: A Generative Art Perspective URL:https://www.diva-portal.org/smash/get/diva2%3A1941305/FULLTEXT02?utm_source=chatgpt.com (дата звернення: 23.04.2025).

ПОРІВНЯЛЬНИЙ АНАЛІЗ ОБЧИСЛЮВАЛЬНОЇ ШВИДКОДІЇ СУЧАСНИХ МОВ ПРОГРАМУВАННЯ В ЗАДАЧАХ МАТЕМАТИЧНОГО МОДЕЛЮВАННЯ

Ткач А. О.[1], Жульковський О. О.[1], Жульковська І. І.[2]
[1]*Дніпровський державний технічний університет, м. Кам'янське*
[2]*Університет митної справи та фінансів, м. Дніпро*

В умовах стрімкого розвитку програмного забезпечення та обчислювальної техніки питання інтенсифікації обчислювальних процесів набуває особливої актуальності, оскільки від швидкості реалізації алгоритмів безпосередньо залежить ефективність обробки даних і продуктивність систем [1]. Різноманіття сучасних систем та мов програмування, особливості їх роботи з апаратними ресурсами, управління пам'яттю, процесом компіляції тощо обумовлює актуальність проблеми їх вибору під час розв'язання обчислювальних задач. Особливо актуальним критерієм під час вибору мови програмування для розв'язання задач комп'ютерного моделювання є вимоги до швидкодії виконуваних програм. Отже перед дослідниками постає питання, яка мова програмування є більш ефективною для реалізації використовуваних у комп'ютерних моделях чисельних алгоритмів [2].

В задачах комп'ютерного моделювання, які врешті зводяться до чисельного розв'язування систем лінійних алгебраїчних рівнянь (СЛАР), що мають тридіагональну матрицю, часто використовується метод прогонки (Tri-Diagonal Matrix Algorithm – TDMA). Зокрема TDMA застосовується для розв'язування СЛАР, які виникають при дискретизації диференціальних рівнянь при використанні методу скінченних різниць або скінченних елементів. Це один з найефективніших алгоритмів, що забезпечує продуктивне розв'язання СЛАР за лінійний час [3].

Незважаючи на алгоритмічну ефективність, практична продуктивність TDMA може суттєво відрізнятися залежно від мови програмування, яка використовується для його реалізації.

Метою дослідження є визначення найбільш ефективних мов програмування з точки зору швидкості виконання програмної реалізації TDMA. Для порівняльного аналізу пропонується дослідити сучасні рейтингові [4] мови програмування: C, C++, C#, Python, Java, JavaScript та Go.

Порівняльний аналіз мов інтерпретованої групи (Python, JavaScript) та компільованої групи (Java, Go, C, C++, C#) виявив нелінійну залежність часу виконання від розмірності системи, що має експоненційний характер. Для Python та JavaScript простежується значно вища чутливість до збільшення розмірності СЛАР. Так, при переході від розмірності 10^5 до 10^7 час виконання для Python зростає приблизно в 145 разів (з 0.103 до 14.93 с), для JavaScript – більш ніж у 30 разів (з 0.0207 до 0.99 с).

Натомість компільовані мови демонструють принципово іншу динаміку. Go демонструє майже лінійну залежність часу виконання від розмірності. C та C++ демонструють близькі результати з мінімальними накладними витратами часу виконання. Показовими є результати для максимальної досліджуваної розмірності 1.5×10^7. Якщо Python потребує майже 15 с обчислень, то Go витрачає лише 0.4055, Java – 0.45, а C++ – близько 0.36 с.

Для C-подібних мов перехід від режиму без оптимізації (-Od) до режиму оптимізації (-O2) демонструє приріст продуктивності приблизно 1.15x для C#, 1.3x для C++ та від 1.5 до 1.7x для мови C.

Go демонструє найбільшу стабільність характеристик при зростанні розмірності задачі. Час виконання збільшується майже пропорційно до зростання розмірності СЛАР. Мови Java та C# займають проміжне положення, демонструючи досить високу ефективність завдяки Just-In-Time компіляції та розвиненим механізмам оптимізації під час виконання програми.

Проведені експерименти доводять, що для високопродуктивних наукових обчислень, зокрема комп’ютерного моделювання, найбільш ефективними є компільовані мови з явною статичною типізацією, зокрема Go, C/C++ та Java, які забезпечують мінімальні накладні витрати та високу масштабованість обчислювальних алгоритмів.

Перспективами подальших досліджень є поглиблене вивчення впливу архітектури комп’ютерних систем, механізмів оптимізації компіляторів та особливостей реалізації середовищ виконання на продуктивність обчислювальних алгоритмів, а також розширення спектру досліджуваних чисельних методів та мов програмування.

ДЖЕРЕЛА

1. Escola J. P. L., Souza U. B. d., Brito L. d. C. Discrete Wavelet Transform in digital audio signal processing: A case study of programming languages performance analysis. *Comput. Elect. Eng.* 2022. 104. URL: https://doi.org/10.1016/j.compeleceng.2022.108439

2. Zhulkovskyi O., Zhulkovska I., Kurliak P., Sadovoi A., Ulianovska Yu., Vokhmianin H. Using asynchronous programming to improve computer simulation performance in energy systems. *Energetika*. 2025. 71(1). P. 23–33. URL: https://doi.org/10.6001/energetika.2025.71.1.2

3. Katopodes N. D. Basic Concepts. *Free-Surface Flow*. 2019. P. 2–79. URL: https://doi.org/10.1016/b978-0-12-815485-4.00007-3

4. TIOBE Index. URL: https://www.tiobe.com/tiobe-index (дата доступу: 26.04.2025).

МОДИФІКАЦІЇ МЕТОДУ ФОНГА ДЛЯ ФОРМУВАННЯ ТРИВИМІРНИХ ЗОБРАЖЕНЬ

Черняк О. І., Дембіцький О. М., Романюк О. Н.
Вінницький національний технічний університет, м. Вінниця

Класичний метод Фонга [1] передбачає інтерполяцію нормалей по поверхні полігону з подальшим обчисленням освітлення у кожній піксельній точці, що забезпечує гладкі переходи яскравості та правдоподібні відблиски. Однією з найпоширеніших стала модель Бліна-Фонга, у якій замість обчислення напрямку відбиття використовується напрямок до середини між вектором огляду та джерелом світла, що спрощує розрахунки і часто забезпечує подібний візуальний результат. Ще одним напрямком удосконалення є розширення моделі Фонга до фізично обґрунтованих BRDF-моделей, таких як Cook-Torrance, які враховують мікрофасетну структуру поверхні, коефіцієнти відбиття Френеля та геометричні фактори самооклюзії. Це дозволяє досягти більш точного моделювання металевих і діелектричних поверхонь. Іншою модифікацією є модель Фонга з текстуруванням блиску, у якій коефіцієнт блиску задається через текстуру, що дає змогу контролювати рівень дзеркальності на кожній ділянці об’єкта. Також використовуються модифікації для реального часу, які апроксимують освітлення або попередньо обчислюють його у картах освітлення для прискорення рендерингу в іграх. У GPU-програмуванні часто реалізується Phong shading на рівні фрагментного шейдера, що забезпечує гнучкість, але може замінюватись на Blinn-Phong або навіть Lambert залежно від вимог до продуктивності. Останнім часом у рамках фізично коректного рендерингу метод Фонга витісняється більш складними моделями, але його спрощені варіанти все ще використовуються для неінтенсивних обчислень. Модифікації методу Фонга суттєво впливають на зовнішній вигляд поверхні під час рендерингу, і візуальні приклади цих змін дозволяють краще зрозуміти вплив кожної моделі. Наприклад, при використанні класичного Фонга блискучі відблиски мають чітко виражену форму, зосереджену навколо напрямку ідеального відбиття, що часто призводить до надмірної «гостроти» блиску, особливо при високих значеннях експоненти блиску. Модифікація Блінн-Фонга замінює цей напрямок на вектор половини між напрямком огляду і напрямком до джерела світла, завдяки чому відблиски стають м’якшими і менш чутливими до кута огляду, що знижує візуальні артефакти на об’єктах з великою кривиною. У порівнянні з цими моделями, фізично коректна модель Cook-Torrance демонструє ще більш реалістичну поведінку світла, особливо на металічних та мікрофасетних поверхнях: вона відображає яскраві блиски під малими кутами падіння світла, поступове затухання при обертанні камери та значно більшу точність при рендерингу матеріалів з грубою або блискучою текстурою.

Таблиця

Характеристики класичного методу Фонга та його основних модифікацій

Модель зафарбовування	**Основна ідея**	**Переваги**	**Недоліки**	**Застосування**
Фонг (Phong)	Інтерполяція нормалей, розрахунок освітлення у пікселі	Гладкі переходи яскравості, реалістичні відблиски	Обчислювально затратна, не фізично коректна	Класична комп'ютерна графіка, демонстрації, освітні приклади
Блінн-Фонг (Blinn-Phong)	Використання середнього вектора між оглядачем і джерелом світла	Менша обчислювальна складність, м’якші блиски	Все ще не фізично коректна, обмежена точність для складних матеріалів	Ігрові рушії, 3D-моделювання, мобільна графіка
Фонг з текстурованим блиском	Shininess-карта визначає ступінь дзеркальності у різних зонах	Локальне керування блиском, зручна художня настройка	Не піддається фізичному калібруванню	Деталізоване стилізоване рендерування
Cook-Torrance BRDF	Фізично коректна модель з урахуванням мікрофасет, Френеля, геометричних факторів	Реалістичні відблиски, точна передача матеріалу, підтримка металів та діелектриків	Висока обчислювальна складність, потреба в картах roughness/metallic	PBR рендеринг, фотореалізм, сучасні ігри та візуалізації
Oren-Nayar	Розширення дифузної складової з урахуванням шорсткості поверхні	Краща передача матових об’єктів	Не враховує блискучі компоненти	Рендеринг шорстких матеріалів, таких як глина, бетон

Модель зафарбовування	**Основна ідея**	**Переваги**	**Недоліки**	**Застосування**
Шейдинг на основі карт освітлення	Попередньо обчислене або віддзеркалене середовище	Висока продуктивність у реальному часі	Втрати точності, непридатна для динамічного освітлення	Мобільні додатки, ігрова графіка

Метод Фонга та його модифікації утворюють поступовий перехід від емпіричних моделей до фізично обґрунтованого рендерингу.

ДЖЕРЕЛА

1. Романюк, О. Н., Романюк О.В., Чехместирук Р.Ю. «Комп'ютерна графіка» : електронний навч. посіб. [– Вінниця : ВНТУ, 2023. – 147 с.

АЛГОРИТМ МАШИННОГО НАВЧАННЯ ПРОГНОЗУВАННЯ УСПІШНОСТІ ТРЕНУВАЛЬНОГО ПРОЦЕСУ ЛЮДЕЙ

Яремчук Д.
Київський столичний університет імені Бориса Грінченка, м. Київ

Сучасний спорт та фітнес все більше спираються на даних для персоналізації тренувань [1]. Однак більшість існуючих підходів використовують узагальнені програми, які не враховують індивідуальні особливості: рівень підготовки, вік, стан здоров'я, режим відпочинку тощо. Це призводить до неефективних тренувань, перенавантаження або недостатнього результату. Машинне навчання (МН) пропонує нові можливості для аналізу великих наборів даних про тренування, дозволяючи прогнозувати успішність занять із високою точністю [2]. Впровадження таких алгоритмів у фітнес-додатках та спортивних програмах дозволить оптимізувати навантаження, підвищити мотивацію користувачів і запобігти травмам.

Існуючі методи прогнозування ефективності тренувань часто ґрунтуються на обмежених даних або простих статистичних підходах, що не завжди дають точні результати [3]. Основні проблеми: недостатня персоналізація, низька точність прогнозу, відсутність адаптації. Метою роботи є розробка алгоритму машинного навчання, який на основі історичних даних про тренування (пульс, тривалість, тип вправ, прогрес тощо) зможе передбачати успішність тренувального процесу з високою точністю.

Запропонований алгоритм відрізняється комплексною методологією, яка охоплює увагу до гетерогенності даних, включаючи різні типи даних (числові та категоріальні), їх об'єднання в єдину модель для точнішого прогнозування. Ключовим є розроблений ефективний процес попередньої обробки даних, що включає очищення, нормалізацію та балансування, зокрема, з акцентом на виявлення та усунення пропусків та аномалій у тренувальних сесіях. Оптимізація алгоритму класифікації, зокрема, з використанням методів на основі нейронних мереж, спрямована на підвищення точності прогнозування успішності тренувань з урахуванням індивідуальних факторів спортсмена. Ключовою особливістю також є розробка адаптивної моделі, здатність якої адаптуватися до динамічних змін у тренувальному процесі та стані спортсмена, що дозволить вносити зміни в прогнози та рекомендації з часом. Нарешті, інтеграція з рекомендаційною системою дозволить надати персоналізовані поради щодо тренувань, регулюючи навантаження та враховуючи індивідуальні потреби.

Для вирішення поставленої задачі запропоновано наступний підхід:

1) Збір та попередня обробка даних:

- Використання відкритих наборів даних (Kaggle, UCI).
- Очищення даних (видалення шуму, нормалізація, балансування класів).

2) Оглянуті алгоритми МН:

- У ході дослідження будуть розглянуті різні алгоритми МН. На основі відповідних метрик ефективності буде обраний оптимальний алгоритм, який буде виконувати прогнозування з найбільшою точністю.

3) Розробка рекомендаційної системи:

- Інтеграція моделі в умовний фітнес-додаток для персоналізованих порад.
- Адаптація алгоритму під динамічні зміни даних.

Експериментальна частина включає навчання моделей на реальних даних та порівняння їх ефективності.

Запропонований алгоритм дозволить підвищити точність прогнозування ефективності тренувань порівняно з базовими методами, забезпечити персоналізовані рекомендації, що зменшить ризик травм і підвищить результативність. Проведене дослідження може стати основою для подальших досліджень у галузі спортивної аналітики. Ця робота має не лише прикладне значення для фітнес-індустрії, але й демонструє потенціал машинного навчання в області прогнозування на основі гетерогенних даних.

ДЖЕРЕЛА

1. Obradović A., Kečo D. Sports Results Prediction Model Using Machine Learning. SAR Journal - Science and Research. 2024. P. 184–189.

2. Bunker R. P., Thabtah F. A machine learning framework for sport result prediction. Applied Computing and Informatics. 2019. Vol. 15, no. 1. P. 27–33. URL: https://doi.org/10.1016/j.aci.2017.09.005 (date of access: 26.04.2025).

3. Isaac L. D., Janani I. Team Sports Result Prediction Using Machine Learning and IoT. Lecture Notes in Electrical Engineering. Singapore, 2022. P. 305–314.

Секція 4
ТЕХНОЛОГІЇ, МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

ЗАБЕЗПЕЧЕННЯ БЕЗПЕЧНОЇ ПЕРЕДАЧІ АУДІОДАНИХ МІЖ МОДУЛЕМ ГОЛОСОВОГО АСИСТЕНТА ТА TTS, STT МОДЕЛЯМИ

Артеменко А. О.
Державний університет інформаційно-комунікаційних технологій, м. Київ

Голосові асистенти стали невід'ємною частиною сучасних інформаційних технологій, проте їх використання породжує серйозні виклики щодо захисту приватності та конфіденційності аудіоданих користувачів, які можуть містити чутливу персональну інформацію та потребують надійного захисту під час передачі між компонентами системи, особливо при взаємодії з зовнішніми сервісами розпізнавання та синтезу мовлення.

Сучасні технології перетворення тексту в мовлення (Text-to-Speech, TTS) та мовлення в текст (Speech-to-Text, STT) зазвичай реалізовані як хмарні сервіси, що надаються через API такими провайдерами як Deepgram та ElevenLabs, які вимагають передачі аудіоданих через мережу Інтернет зі значними ризиками для конфіденційності.

Для реалізації потокової передачі аудіоданих між голосовим асистентом та TTS/STT моделями широко застосовується протокол WebSocket (WS), який забезпечує двонаправлену комунікацію у реальному часі, а для забезпечення безпеки використовується його захищена версія – WebSocket Secure (WSS), яка базується на використанні TLS (Transport Layer Security) для шифрування даних. На відміну від незахищеного WebSocket (ws://), який працює через TCP, протокол WSS (wss://) використовує шифрування TLS, аналогічно до різниці між HTTP та HTTPS, та забезпечує надійний захист від несанкціонованого доступу та перехоплення даних при їх передачі [1-2].

У процесі TLS-рукостискання та подальшого шифрування даних використовуються сучасні криптографічні алгоритми, зокрема для обміну ключами часто застосовується алгоритм на еліптичних кривих Діффі-Геллмана (ECDH) та RSA, а для шифрування трафіку – симетричні алгоритми AES з різною довжиною ключа, наприклад, AES-256-GCM [3]. Набори шифрів TLS (CipherSuites) визначають комбінацію алгоритмів для автентифікації, обміну ключами, шифрування та перевірки цілісності,

причому сучасні захищені системи надають перевагу наборам шифрів з високим рівнем безпеки, таким як TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 [3].

Проблема безпечної передачі аудіоданих між модулем голосового асистента та моделями TTS/STT залишається критично важливою у контексті захисту приватності користувачів та їх чутливих даних. Застосування захищеного протоколу WebSocket (WSS) із коректно налаштованим TLS-шифруванням, стійкими алгоритмами обміну ключами та посиленим захистом API-ключів істотно зміцнює безпеку подібних систем.

ДЖЕРЕЛА

1. Pettorru G., Martalò M. QUIC and WebSocket for Secure and Low-Latency IoT Communications: An Experimental Analysis. 2023. URL: https://journal.iitta.gov.ua/index.php/itlt/issue/view/99.
2. Fette I. The WebSocket Protocol. 2011 URL: https://datatracker.ietf.org/doc/html/rfc6455.
3. Rescorla E. TLS Elliptic Curve Cipher Suites with SHA-256/384 (GCM). 2008 URL: https://datatracker.ietf.org/doc/html/rfc5289

БЕЗПЕКА ГОЛОСОВОГО AI-АГЕНТА: АВТЕНТИФІКАЦІЯ ТА ЗАХИСТ МІКРОСЕРВІСНОЇ АРХІТЕКТУРИ

Артеменко А. О.
Державний університет інформаційно-комунікаційних технологій, м. Київ

Сучасні голосові AI-агенти стають невід'ємною частиною багатьох інформаційних систем, забезпечуючи автоматизовану взаємодію з користувачами через голосові інтерфейси. Особливо гострою є проблема організації безпечного доступу до даних у системах, побудованих на мікросервісній архітектурі, де різні компоненти взаємодіють між собою через мережу, а дані зберігаються та обробляються розподілено.

Метою цього дослідження є розробка та аналіз безпечної архітектури голосового AI-агента з особливим акцентом на механізми автентифікації та захисту доступу до даних.

У запропонованій архітектурі голосового AI-агента виділено кілька ключових мікросервісів: Сервіс автентифікації, Сервіс голосового агента, Сервіс зберігання файлів, Сервіс дзвінків, Сервіс адміністративної панелі

Для візуалізації архітектури створено UML-діаграму (рис. 1), яка показує взаємодію між мікросервісами:

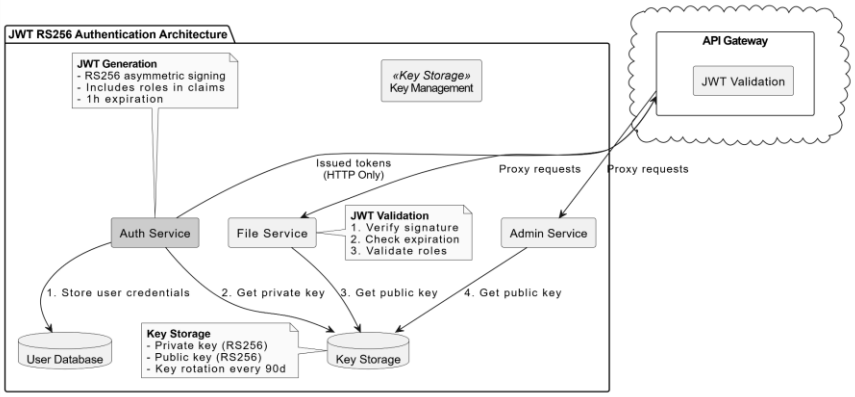


Рис. 1 Діаграма архітектури системи на базі мікросервісної архітектури з використанням JWT авторизації

Мікросервісна архітектура надає низку переваг для системи голосового AI-агента: незалежне масштабування кожного сервісу, ізоляція відмов, технологічна гнучкість та можливість розподіленої розробки. Однак, така архітектура створює додаткові виклики в контексті безпеки, особливо щодо автентифікації та авторизації між сервісами [1-2]. Для розв'язання даної проблеми у дослідженні було застосовано RS256 для підпису JWT.

RS256 (RSA Signature with SHA-256) є асиметричним алгоритмом підпису, який використовує пару ключів: приватний ключ для підпису токенів та публічний ключ для їх перевірки. Цей підхід має значні переваги порівняно з симетричними алгоритмами (як-от HS256), особливо в контексті мікросервісної архітектури [3].

У контексті системи голосового AI-агента, процес роботи з RS256 організовано таким чином:

- сервіс автентифікації зберігає приватний ключ RSA у захищеному сховищі, недоступному для інших сервісів;
- публічний ключ розповсюджується серед усіх сервісів, які потребують валідації токенів;
- токени видаються з обмеженим терміном дії (expires at - exp), що знижує ризики у випадку компрометації токена;
- у токені зберігається інформація про користувача, його роль та дозволи, що дозволяє сервісам приймати рішення щодо авторизації[3].

У результаті проведеного дослідження розроблено безпечну архітектуру голосового AI-агента з використанням мікросервісного підходу. Основним аспектом безпеки системи є механізм автентифікації на основі JWT з використанням асиметричного алгоритму підпису RS256, який забезпечує надійний захист міжсервісної взаємодії та доступу до чутливих даних.

ДЖЕРЕЛА

1. Barua B., Kaiser M. S. Novel Architecture for Distributed Travel Data Integration and Service Provision Using Microservices. 2024. URL: https://arxiv.org/abs/2410.24174

2. Naik N., Jenkins P. Securing Digital Identities in the Cloud by Selecting an Efficient and Effective Schema Validation Mechanism in Microservices. 2020. URL: https://www.semanticscholar.org/paper/f2f930cf0f951895bc89fca77790bc222d115716

3. Sindi H.F., Barley M., Solemon B. Pipekit: A Deployment Tool with Advanced Scheduling and Inter-Service Communication for Multi-Tier Applications. 2019. URL: https://www.semanticscholar.org/paper/c49628dbd4d0660e3b305a34c1a52d665293a7b1

РОЗРОБКА ПРОГРАМНИХ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ У ВЕБ-ЗАСТОСУНКУ В ПРОЦЕСІ УПРАВЛІННЯ ПЕРСОНАЛЬНОЮ КОЛЕКЦІЄЮ

Башич В. А., Садовенко В. С.

Державний університет інформаційно-комунікаційних технологій, м. Київ

Основною складовою серед сучасних веб-технологій безпека є пріорітетом номер один, особливо зважаючи на системи, що обробляють персональну інформацію користувачів чи управляють контентом. Створення веб-додатків на платформі ASP.NET Core [1] відкриває можливість реалізації ефективної політики безпеки, що охоплює захист та зберігання інформації.

Метою даного дослідження є розробка програмного додатку , який би гарантував безпеку даних у веб-додатках на основі комбінації ефективних підходів з використанням різних алгоритмів, протоколів та інших систем.

SHA 2 – одина з найвідоміших сімей криптографічних алгоритмів хешування даних. Для захищеного збереження паролей, краще за все поєднувати цей алгоритм із «сольовими значеннями» [2], які є унікальними для кожного користувача. Притримування цього патерну унеможливлює відтворення паролю навіть у разі витоку бази даних через те, що результат хешування неможливо зворотньо розшифрувати, а додаткове «сольове» значення робить неможливим створення універсальних таблиць підбору.

HTTPS – протокол шифрування, який забезпечує захист даних під час передачі з одного пристрою на інший. Завдяки використанню SSL/TLS [3]-сертифікатів усі дані, що передаються між клієнтом і сервером, зашифровані. У разі перехоплення вони не можуть бути розшифровані

зловмисником без наявності приватного ключа, що значно підвищує безпечність комунікації.

JSON Web Token [4] – це стандарт токена доступу на основі JSON. Після успішної автентифікації сервер генерує цифровий токен, що містить зашифровану інформацію про користувача. Токен надсилається клієнту і зберігається у нього, що дозволяє реалізувати безсерверну модель сесій. Сервер не зберігає стан користувача, знижуючи навантаження та підвищуючи масштабованість системи. Також підробка або зміна інформації не є можливою з використанням JWT, бо цифровий підпис захищає дані від фальсифікації.

ORM Entity Framework Core – використовується для обробки запитів до бази даних, забезпечує надійний рівень додаткового захисту даних. Через використання параметризованих запитів, можливо уникнути SQL-ін'єкцій [5], одного з найпоширініших типів атак на веб-додатки. Крім цього, система надає можливість задавати права доступу до таблиць та полів бази даних, що також підтримує шифрування даних на рівні самої БД.

Результати даного дослідження демонструють потенціал застосування комплексу з рішень безпеки, починаючи з хешування паролів і протоколів шифрування до системи авторизації на базі ролей і токенів. На базі вище перелічених переваг, усі ці механізми забезпечують надійний високий рівень захисту, не ускладнюючи при цьому взаємодію додатка з юзером.

ДЖЕРЕЛА

1. ASP.NET Core [Електронний ресурс] – Режим доступу: https://doi.org/10.17487/RFC7519.
2. Salt security [Електронний ресурс] – Режим доступу: https://docs.saltproject.io/salt/user-guide/en/latest/topics/security.html.
3. What is SSL/TLS: An In-Depth Guide [Електронний ресурс] – Режим доступу: https://www.ssl.com/article/what-is-an-ssl-tls-certificate/.
4. JSON Web Token Introduction [Електронний ресурс] – Режим доступу: https://jwt.io/introduction.
5. SQL Injection [Електронний ресурс] – Режим доступу: https://owasp.org/www-community/attacks/SQL_Injection.

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ В ІНТЕЛЕКТУАЛЬНІЙ СИСТЕМІ МОНІТОРИНГУ ВНЕСКУ РОЗРОБНИКІВ У ПРОГРАМНІ ПРОЄКТИ

Беро В. Ф.
Державний університет інформаційно-комунікаційних технологій, м. Київ

Із розвитком інформаційних технологій, зокрема платформ для колективної розробки програмного забезпечення, зросла потреба в захищених інструментах для збору та аналізу даних про активність учасників проєктів [1]. Особливої актуальності набуває питання забезпечення безпеки даних під час використання таких інструментів, оскільки йдеться про доступ до акаунтів розробників, історії комітів та внутрішньої структури проєктів [1; 2].

Метою даного дослідження є розробка та впровадження заходів для забезпечення конфіденційності інформації в програмному забезпеченні «Інтелектуальна система моніторингу внеску розробників у програмні проєкти». Для досягнення цієї мети було застосовано підхід, що включає як технологічні рішення, так і організаційні механізми. Зокрема, передбачено ізоляцію середовища виконання за допомогою Docker-контейнерів, захист конфіденційних даних через використання змінних середовища та шифрування, а також контроль доступу до API за допомогою токенів авторизації.

Розробка продукту передбачає використання наступних технічних засобів і методів захисту:

1. Контейнеризація за допомогою Docker. Забезпечує ізоляцію виконання компонентів системи, обмежуючи доступ до системних ресурсів та файлової системи хоста [2].
2. Використання .env для безпечного зберігання конфігураційних параметрів, токенів доступу до API Git та облікових даних message-broker [1, 2].
3. Використання RabbitMQ для розподілу завдань між мікросервісами, з можливістю обмеження доступу до черг через політики безпеки [2].
4. Регулярне оновлення залежностей та Docker-образів з урахуванням актуальних патчів безпеки [2].
5. Bearer Token. Авторизація на основі токенів для обмеження доступу до зовнішнього та внутрішнього API системи, а також реалізація механізмів перевірки автентичності користувача [1].
6. Хешування паролів до системи. Для збереження облікових даних застосовується алгоритм хешування з додаванням унікальної солі за допомогою бібліотеки «bcrypt», що ускладнює атаки метою перебору [3].

Контейнеризація забезпечила ізоляцію процесів і захист від доступу до системних ресурсів хост-машини. Зберігання токенів і паролів у Docker

Secrets або .env-файлах з обмеженим доступом мінімізувало ризики витоку облікових даних. Авторизація доступу до API за допомогою токенів. Крім цього, автоматизоване оновлення даних та логування взаємодій із зовнішніми сервісами дозволяє вчасно виявляти підозрілу активність або технічні збої.

Розроблений набір заходів захисту даних є критично важливою складовою роботи інтелектуальної системи моніторингу. Впровадження ізоляції середовища виконання, авторизації через токени, захищеного зберігання конфігураційних файлів, системного моніторингу та логування взаємодій забезпечує комплексний захист на всіх рівнях. Подальше вдосконалення безпеки системи може включати реалізацію двофакторної автентифікації (2FA) [1], розмежування прав доступу до окремих компонентів системи.

ДЖЕРЕЛА

1. Turnbull, J. (2014) The Docker Book: Containerization Is the New Virtualization – [Електронний ресурс]. Режим доступу: http://lsi.vc.ehu.es/pablogn/docencia/manuales/The%20Docker%20Book.pdf

2. Miguel Grinberg. 2014. Flask Web Development: Developing Web Applications with Python (1st. ed.). O'Reilly Media, Inc.

3. Хешування паролів: використання солі та bcrypt – [Електронний ресурс]. Режим доступу: https://drukarnia.com.ua/articles/kheshuvannya-paroliv-vikoristannya-soli-ta-bcrypt

ЗАХИСТ ІНФОРМАЦІЇ У WEB-ЗАСТОСУНКУ ДЛЯ АВТОМАТИЗАЦІЇ РОЗКЛАДУ ЗАНЯТЬ У ЗАКЛАДІ ОСВІТИ

Білоус М. О.

Державний університет інформаційно-комунікаційних технологій, м. Київ

Інтернет-технології, надаючи безліч зручностей, водночас стали причиною зростання кількості випадків витоку інформації. Тому забезпечення конфіденційності, доступності та цілісності інформації у web-ресурсах є важливою проблемою сучасності [1; 2].

Наше дослідження присвячене розробці web-застосунку для автоматизації розкладу занять у закладі освіти. Є очевидним, що дана системи містить конфіденційну інформацію, таку, як дані про викладачів, курсантів, приміщення, програмне забезпечення та інші. Тому розробка розкладу для закладу освіти вимагає особливої уваги до питань безпеки, потребує реєстрацію та шифрування даних. У зв’язку з цим виникла необхідність у написанні програмного коду, який би шифрував паролі та

дані, які надходять з сервера системи, тим самим забезпечуючи захист інформації.

Сучасний автоматизований розклад [3] – це взаємодія користувача з WEB-сайтом та сервером, який зберігає дані. API є ядром системи, що містить усю інформацію про заняття, які відбуватимуться для різних курсах та груп. Для безпеки даних необхідно впровадити такі механізми: хешування паролів і авторизацію до API за допомогою токенів.

Хешування пароля [4] є важливим методом захисту користувацьких даних у Node.js, і для цього часто використовується бібліотека bcryptjs. Вона дозволяє безпечно хешувати паролі, додаючи до них сіль – випадкові дані, які ускладнюють злом методом перебору. Це підвищує рівень безпеки збережених паролів. Приклад реалізації хешування пароля наведено на рис.1.

```
userSchema.pre('save', async function (next) {
    if (!this.isModified('password')) return next();

    try {
        const salt = await bcrypt.genSalt(10);
        this.password = await bcrypt.hash(this.password, salt);
        next();
    } catch (err) {
        next(err);
    }
});
```

Рис 1. Приклад хешування паролю

Для пароля задається 10 раундів хешування - чим більше раундів, тим безпечніше, хоча довше триває обчислення.

Пароль хешується за допомогою bcrypt.hash() і зберігається у базі даних у зашифрованому вигляді. Це дозволить захистити паролі, якщо база даних буде скомпрометована. Крім того, використання bcrypt значно ускладнює атаку методом перебору (brute-force).

Щодо обмеження доступу через токен авторизації: якщо у користувача роль не є стандартною (User), а Institution (рис. 2), то при запиті даних із сервера, спочатку перевіряється токен авторизації та роль користувача. Лише після цього надається відповідна інформація.

```
firstName : "Марк"
lastName : "Білоус"
patronymic : "Олександрович"
position : "директор"
educationalInstitution : "Державний університет інформаційно-комунікаційних технологій "
phoneNumber : "+380657658967"
email : "bilous@gmail.com"
password : "$2b$10$ggQkGXd.kyka61RD8XszfenABIczZBJ8VsBCk/jfKZ0AuOdX.bl92"
role : "institution"
```

Рис. 2. Інформація про користувача з MongoDB

Розробка web-застосунку для автоматизації розкладу занять у закладі освіти є важливою складовою для безперебійного функціонування навчального процесу, тому захист особистих даних є критично важливим і потребує постійного оновлення.

ДЖЕРЕЛА

1. Бондаренко О., Ушкаленко І. (2017). Безпека web-додатків: актуальні проблеми та їх аналіз. *Формування ринкової економіки в Україні*. Вип. 38., 28-36.

2. Боскін О.О., Корніловська Н.В., Поліщук В.М., Сарафаннікова Н.В.(2023). Безпека веб-додатків та хакерські атаки. *Вісник Херсонського національного технічного університету, № 3(86),* 83-92. https://doi.org/10.35546/kntu2078-4481.2023.3.11

3. Хайтан О.М. (2020). Автоматизація розкладу навчальних курсів університету. *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Технічні науки , 1 (2),* 58–66. https://doi.org/10.32838/2663-5941/2020.2-1/09

4. Хешування паролів: використання солі та bcrypt [Електронний ресурс]. – Режим доступу: URL https://drukarnia.com.ua/articles/kheshuvannya-paroliv-vikoristannya-soli-ta-bcrypt-fsme- - Назва з екрану

ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ У ВЕБ-СИСТЕМІ МОНІТОРИНГУ ЕМОЦІЙНОГО СТАНУ КОРИСТУВАЧА

Бражник А. М.

Державний університет інформаційно-комунікаційних технологій, м. Київ

В умовах цифрової трансформації суспільства зростає потреба у розробці безпечних програмних рішень для підтримки психологічного здоров’я населення. Веб-системи для моніторингу емоційного стану користувача дозволяють здійснювати самоспостереження, виявляти стресові стани, аналізувати настрій та сприяють покращенню емоційного благополуччя. Оскільки такі системи оперують чутливою персональною інформацією, їх захист є критично важливим завданням.

У межах дипломного проєкту було розроблено веб-додаток для моніторингу емоційного стану користувача з акцентом на впровадження сучасних засобів захисту інформації. Система реалізована із використанням стеку технологій Java, Spring Framework, MySQL, HTML/CSS/JavaScript. Безпека даних забезпечується через:

- автентифікацію та авторизацію користувачів на основі Spring Security із застосуванням JWT-токенів;
- шифрування паролів за допомогою BCrypt-алгоритму;

- використання параметризованих SQL-запитів для захисту від SQL-ін’єкцій;
- HTTPS-протокол для захищеного з’єднання клієнта з сервером.

Особливу увагу приділено збереженню конфіденційності даних користувачів, які фіксують свій настрій у щоденнику настрою та отримують поради від ШІ-помічника. Було реалізовано модуль контролю доступу, що запобігає несанкціонованому доступу до записів.

Результатом дослідження є інтегрована система, яка поєднує функціональність покращення емоційного стану користувача з високим рівнем інформаційної безпеки, що відповідає сучасним вимогам до захисту інформації в інформаційно-комунікаційних системах.

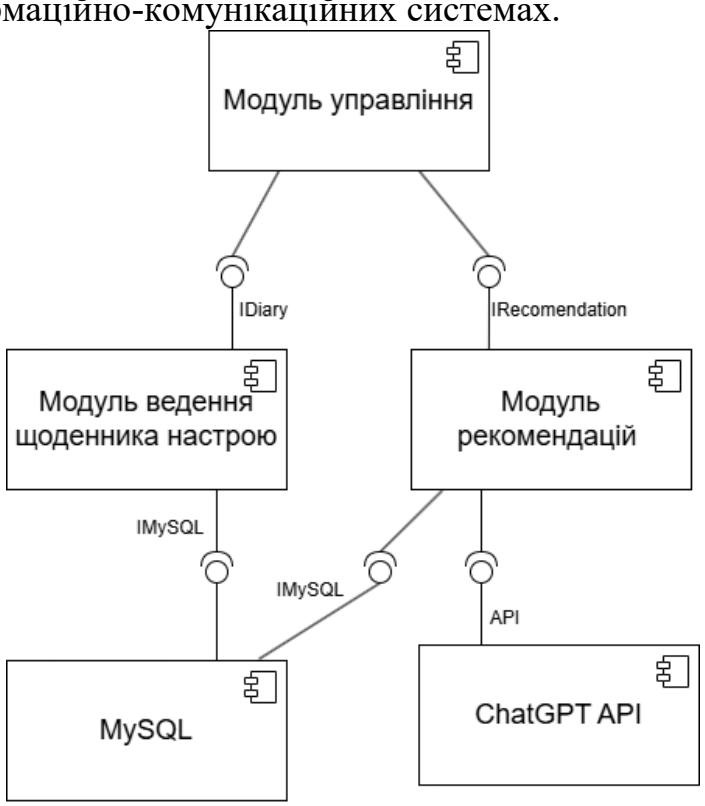


Рис. 1. Діаграма компонентів

ДЖЕРЕЛА

1.Sommerville, I. Software Engineering. 10th ed. Pearson Education, 2015.

2.Spring Security Documentation [Електронний ресурс] (date of access: 20.04.2025). URL: https://spring.io/projects/spring-security

3.Chart.js Documentation [Електронний ресурс] (date of access: 20.04.2025). URL: https://www.chartjs.org/docs/latest/

4.MySQL Workbench Manual [Електронний ресурс] (date of access: 20.04.2025). URL: https://dev.mysql.com/doc/workbench/en/

ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ІНФОРМАЦІЇ У WEB-ЗАСТОСУНКУ «ЩОДЕННИК ДІЄТИ»

Вертій М. О.
Державний університет інформаційно-комунікаційних технологій, м. Київ

Сьогодні, в умовах тотальної цифровізації, майже кожна компанія представлена в інтернеті через власний web-ресурс або використовує web-технології. Ця всеосяжна доступність web-програм для широкого кола користувачів, на відміну від внутрішніх мережевих рішень, одночасно створює ризики, оскільки вони також стають потенційною ціллю для зловмисників. У сучасних web-застосунках, що зберігають персональні дані користувачів, безпека є критичною складовою розробки [1]. Конфіденційна інформація – це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов [2]. Тому забезпечення конфіденційності інформації є важливим і актуальним завданням.

Наше дослідження присвячене розробці web-застосунку «Щоденник дієти». «Щоденник дієти» містить чутливу інформацію, зокрема, особисті дані користувачів, їхні раціони харчування, заміри тіла, а також додаткові функції застосунку – пошук рецептів з урахуванням індивідуальних потреб здоров’я (цукровий діабет, група крові, алергії тощо). Уразливості в безпеці можуть призвести до витоку даних або компрометації облікових записів, тому важливо забезпечити належний рівень конфіденційності та захисту інформації. Це стосується як зберігання даних у базі, так і процесів авторизації, доступу за ролями.

У роботі проведено аналіз основних загроз інформаційної безпеки для web-застосунку «Щоденник дієти». Запропоновано методи захисту даних користувачів, зокрема автентифікацію, хешування паролів, захист від атак типу SQL-ін'єкцій та XSS [3; 4]. Розглянемо основні загрози для web-застосунку «Щоденник дієти» та методи їх нейтралізації.

Використано двофакторну автентифікацію (2FA) для підвищення рівня захисту облікових записів. Реалізовано механізм обмеження кількості невдалих спроб входу, щоб запобігти атакам грубої сили (brute-force). Паролі зберігаються у вигляді хешів з використанням алгоритму bcrypt. Використовується «сіль» (salt) для запобігання атакам за попередньо обчисленими хешами (rainbow tables). Використано підготовлені запити (prepared statements) при роботі з базою даних MySQL. Проведено валідацію та фільтрацію введених користувачем даних. Дані, що вводяться користувачем, проходять санітизацію перед виведенням. Використовується Content Security Policy (CSP) для обмеження виконання довільного JavaScript-коду. Реалізовано шифрування чутливої інформації

перед збереженням у базі даних. Використовується HTTPS для захисту даних, що передаються мережею.

Для забезпечення належного рівня безпеки та контролю над критично важливими функціональними можливостями системи, впроваджено чітку систему розподілу ролей. Ця система передбачає наявність різних рівнів доступу, зокрема таких базових ролей, як «користувач» та «адміністратор». Кожна роль має визначений набір прав та привілеїв, що дозволяє обмежувати доступ до чутливих операцій та даних лише для авторизованого персоналу, запобігаючи таким чином несанкціонованим діям та потенційним зловживанням. Всі спроби входу та зміни налаштувань безпеки реєструються в логах для подальшого аналізу. У застосунку є анонімна можливість перегляду його функціоналу.

Запропоновані методи захисту дозволяють значно знизити ризики, пов’язані з компрометацією даних користувачів у web-застосунку «Щоденник дієти». Використання сучасних алгоритмів хешування паролів, захисту від SQL-ін'єкцій та XSS атак, а також шифрування даних та HTTPS забезпечують високий рівень інформаційної безпеки. Подальші дослідження можуть бути спрямовані на покращення механізмів контролю доступу та впровадження додаткових рівнів автентифікації.

ДЖЕРЕЛА

1. Шмаюн С.В., Жураковський Б.Ю., Іваніченко Є.В. (2022). Система підбору харчування за показниками здоров’я. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, *4*(16), 63–75. https://doi.org/10.28925/2663-4023.2022.16.6375

2. Закон України «Про інформацію» від 02.10.92 N 2657-XII. https://tax.gov.ua/dlya-gromadskosti/dpa-i-gromadskist/normativno-pravova-baza-u-sferi/arhiv-normativno-pravova-baza/53366.html

3. Бондаренко О., Ушкаленко І. (2017). Безпека web-додатків: актуальні проблеми та їх аналіз. *Формування ринкової економіки в Україні*. Вип. 38., 28-36.

4. Боскін О.О., Корніловська Н.В., Поліщук В.М., Сарафаннікова Н.В. (2023). Безпека веб-додатків та хакерські атаки. *Вісник Херсонського національного технічного університету, № 3(86),* 83-92. https://doi.org/10.35546/kntu2078-4481.2023.3.11

ЗАХИСТ ІНФОРМАЦІЇ У WEB-ЗАСТОСУНКУ ДЛЯ ОБМІНУ ТУРИСТИЧНИМ ДОСВІДОМ НА ОСНОВІ БАЗИ ВІДГУКІВ ПРО МІСЦЯ ІНТЕРЕСУ

Власенко Б. Є.
Державний університет інформаційно-комунікаційних технологій, м. Київ

З розвитком цифрових технологій дедалі більшої популярності набувають web-застосунки, орієнтовані на спільноти користувачів. Одним із прикладів такої взаємодії є системи для обміну туристичним досвідом, де користувачі залишають відгуки, оцінки та фото з відвіданих локацій, а також діляться маршрутами й рекомендаціями. Важливою частиною таких платформ є функціонал авторизації та захисту облікових записів, адже користувачі реєструються, створюють власні профілі та зберігають особисту або напівпублічну інформацію.

З огляду на те, що web-застосунок повинен гарантувати конфіденційність і безпеку введених даних, особлива увага приділяється захисту облікових записів, зокрема – паролів. У сучасних підходах до безпеки не допускається зберігання паролів у відкритому вигляді. Натомість використовується процедура хешування – процес одностороннього шифрування, який перетворює звичайний текстовий пароль у зашифрований рядок, що не може бути розшифрований у зворотному напрямку. Якщо база даних потрапить до рук зловмисника, хешовані паролі будуть практично марними без оригіналу, особливо, якщо для хешування використано надійні алгоритми та випадкову сіль [1]. У нашому проєкті реалізовано захищену систему реєстрації користувачів за допомогою серверної частини, написаної на Node.js із використанням фреймворку Express. Після отримання запиту на реєстрацію система витягує з тіла запиту email, username і password. Пароль одразу не зберігається. Замість цього застосовується бібліотека bcrypt, яка генерує хеш на основі введеного пароля та солі – випадкового значення, що додається до вхідного тексту, аби зробити хеші унікальними навіть для однакових паролів. У даній реалізації використано 10 раундів генерації солі, що забезпечує оптимальний баланс між рівнем захисту та швидкістю обробки.

Після генерації хешу пароль у такому вигляді зберігається до бази даних. Далі система створює accessToken та refreshToken, використовуючи бібліотеку jsonwebtoken. Токени дозволяють користувачу виконувати подальші дії у системі, підтверджуючи свою автентичність. AccessToken має обмежений термін дії, а refreshToken використовується для його поновлення без повторного входу [2].

Реалізовано також обробку типових помилок, наприклад, дублювання облікового запису, коли вже існує користувач із таким самим email – у цьому випадку повертається статус 400, що сигналізує про

неможливість завершити реєстрацію. Це дозволяє уникнути дублювання записів та мінімізувати ризики автоматизованого створення фейкових профілів [3].

Такий підхід до обробки чутливої інформації в межах web-застосунку для туристів дозволяє створити безпечне середовище для обміну даними. Хешування паролів, автентифікація через токени та обробка потенційно уразливих дій робить систему більш захищеною та надійною. Це критично важливо для платформ, які зберігають дані великої кількості користувачів, адже зростаюча кількість кібератак змушує розробників постійно вдосконалювати рівень інформаційної безпеки. Для пароля задається 10 раундів хешування - чим більше раундів, тим безпечніше, хоча довше триває обчислення.

Пароль хешується за допомогою bcrypt.hash() і зберігається у базі даних у зашифрованому вигляді. Це дозволить захистити паролі, якщо база даних буде скомпрометована [1]. Крім того, використання bcrypt значно ускладнює атаку методом перебору (brute-force).

Щодо обмеження доступу через токен авторизації: якщо у користувача роль не є стандартною (User), а Institution, то при запиті даних із сервера, спочатку перевіряється токен авторизації та роль користувача. Лише після цього надається відповідна інформація.

Розробка web-застосунку для обміну туристичним досвідом на основі бази відгуків про місця інтересу має значне значення для різних категорій користувачів та для розвитку туристичної галузі в цілому, тому забезпечення конфіденційності, цілісності та доступності інформації є важливим і потребує постійного моніторингу.

ДЖЕРЕЛА

1. Хешування паролів: використання солі та bcrypt [Електронний ресурс]. – Режим доступу: URL: https://drukarnia.com.ua/articles/kheshuvannya-paroliv-vikoristannya-soli-ta-bcrypt-fsme

2. Бондаренко О., Ушкаленко І. (2017). Безпека web-додатків: актуальні проблеми та їх аналіз. *Формування ринкової економіки в Україні. Вип.* 38., 28–36. [Електронний ресурс]. – Режим доступу: URL: https://economic.karazin.ua/archive/2017_38_4/5.pdf

3. Боскін О.О., Корніловська Н.В., Поліщук В.М., Сарафаннікова Н.В. (2023). Безпека веб-додатків та хакерські атаки. *Вісник Херсонського національного технічного університету, №* 3(86), 83–92. [Електронний ресурс]. – Режим доступу: URL: https://doi.org/10.35546/kntu2078-4481.2023.3.11

АДАПТИВНІ МЕТОДИ ПРОТИДІЇ АКТИВНИМ ШУМОВИМ ЗАВАДАМ

Ворохоб Н. О.
Київський столичний університет імені Бориса Грінченка, м. Київ

Функціонування переважної більшості сучасних технічних систем, у тому числі інформаційних, відбувається в середовищі конфліктних взаємодій різного характеру, що зумовлює необхідність протистояння радіоелектронній розвідці та протидії, застосування засобів радіомаскування, а також забезпечення захисту від навмисних завад і силових деструктивних впливів, спрямованих на технічні засоби та персонал.

У конфліктній взаємодії задіяні інформаційні системи будь-якого призначення: як для передачі та отримання даних, так і для радіокерування та виведення інформації з ладу. Ці системи функціонують у всіх освоєних частотних діапазонах та використовують усі фізичні поля, що застосовуються в техніці, і всі вони є частиною інформаційного радіоелектронного конфлікту.

Інформаційним конфліктом будемо називати процес боротьби між сторонами за інформаційні ресурси, що супроводжується реалізацією різноманітних дій, спрямованих на руйнування, спотворення, приховування та вилучення інформації в умовах конфліктної взаємодії систем, яка здійснюється шляхом обміну електромагнітними хвилями [1]. Взаємний вплив, що спричиняє зміни в інформаційних станах об'єктів, здійснюється переважно безконтактним шляхом. Основним механізмом передачі інформації в цьому процесі є електромагнітні поля, що розповсюджуються у фізичному середовищі.

Метою дослідження є синтез адаптивного методу протидії активним шумовим завадам, спрямованим на подавлення ліній радіозв’язку з fpv дронами.

Адаптивні методи вирізняються тим, що вони автоматично підлаштовуються під зміни в характеристиках завад, забезпечуючи більш ефективне подавлення порівняно з традиційними методами. Для розробки ефективних методів протидії необхідно чітко класифікувати різні типи активних шумових завад. Це включає класифікацію за їхніми спектральними характеристиками, часовими характеристиками, статистичними властивостями тощо [2].

Розробляються моделі завад, що дозволяють імітувати їхню поведінку та здійснювати тестування методів протидії. Моделювання завад є критично важливим для створення реалістичних сценаріїв випробувань.

Розробка алгоритмів виявлення та подавлення завад є основним завданням у дослідженні та включає створення нових або вдосконалення існуючих адаптивних алгоритмів. Алгоритми виявлення завад призначені

для автоматичного визначення присутності та характеристик завади в прийнятому сигналі. Алгоритми подавлення завад використовуються для мінімізації впливу завади на корисний сигнал.

Розробка може включати адаптивні фільтри (LMS, RLS), алгоритми формування радіочастотних променів (MVDR, LCMV) або методи адаптивного кодування [3].

Алгоритм дій включає використання різних критеріїв оцінки, таких як відношення сигнал/шум (SNR), ймовірність помилки (BER), пропускна здатність радіоканалу та інші. Також в алгоритм включені імітаційні експерименти, в яких розроблені методи застосовуються до змодельованих сценаріїв з різними типами завад.

Виходячи з результатів, аналізуються сильні і слабкі сторони кожного методу, їхньої чутливості до параметрів завад і загальної ефективності, проводиться оцінка ефективності методу.

За об’єкт дослідження взято fpv дрон з частотами 5.8 ГГц (відеопередача) і 2.4 ГГц (керування). Потужність передавача становить 800мВт.

В якості активних завад використано:

- генератори широкосмугового шуму (Broadband Jammers);
- генератори спрямованого шуму (Directional Jammers);
- пристрої спуфінгу.

Результати виконаних досліджень показали необхідність розробки нової, більш досконалої динамічної моделі інформаційного конфлікту, що відображає власне процес зіткнення інтересів протилежних сторін у реальних умовах їх функціонування.

ДЖЕРЕЛА

1. Крючкова Л.П. Проблеми функціонування інфокомунікаційних мереж в умовах деструктивних впливів. Монографія. – К.: Державний університет телекомунікацій, 2016. – 72 с.

2. Authorized adaptation from the United States edition, entitled Adaptive Filter Theory, 5th edition, ISBN 978-0-132-67145-3, by Simon Haykin, published by Pearson Education © 2014. – 897 c.

3. Authorized adaptation from the United States edition, entitled Digital Signal Processing: Principles, Algorithms, and Applications, 4th Edition, ISBN 978-0-136-08983-0, by John G. Proakis and Dimitris G. Manolakis, published by Pearson Education © 2014 – 1014 c.

КОГНІТИВНЕ МОДЕЛЮВАННЯ ЯК ІНСТРУМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Гаркушенко А. М., Жданова Ю. Д.
Київський столичний університет імені Бориса Грінченка, м. Київ

У сучасному цифровому середовищі, де більшість процесів управління, комунікації та зберігання інформації здійснюється за допомогою інформаційно-комунікаційних систем, забезпечення інформаційної безпеки (ІБ) стає пріоритетним завданням для організацій будь-якого масштабу. В таких умовах пріоритетним стає системний підхід до виявлення, оцінювання і управління потенційними ризиками.

Під потенційними ризиками ІБ розуміють числову або вербальну функцію, що характеризує ймовірність реалізації загроз та рівень можливих втрат, спричинених використанням уразливостей активів для нанесення шкоди організації [1]. Основним принципом управління ризиками ІБ є безперервна оцінка та адаптація, що має на меті постійне оновлення як оцінок ризиків, так і стратегій їх усунення [2].

Традиційні методи оцінки ризиків інформаційної безпеки мають обмежену здатність враховувати складні взаємозв'язки, вплив людського чинника та змінну природу загроз. У цьому контексті перспективним підходом стає когнітивне моделювання, яке допомагає виявляти уразливі місця у системах безпеки, оцінювати ефективність заходів щодо їх усунення, а також надає відповідальним особам засоби для аналізу різних сценаріїв та прийняття обґрунтованих рішень. Важливим аспектом цього процесу є його візуалізація, яка реалізується через нечіткі когнітивні карти [3; 4].

Когнітивна карта складається з вершин (понять) та дуг (впливів), що формують сценарії розвитку ситуацій при зміні окремих факторів. На основі таких моделей можна досліджувати зміну загального рівня ризику в системі з урахуванням взаємозв’язків відповідно до певних загроз, уразливостей чи активів.

Наше дослідження присвячене побудові базової когнітивної моделі сценаріїв в управлінні ризиками ІБ, яка враховує взаємодію внутрішніх і зовнішніх чинників, а також оцінку впливу кожного елемента на загрозу. Визначені когнітивні моделі експертів у сфері інформаційної безпеки. Серед цих моделей виділено Pattern Recognition, Mental Models of Systems, Threats Forecasting and Modeling та інші. Експерти в галузі інформаційної безпеки володіють розвиненими когнітивними моделями, які дозволяють їм ефективно аналізувати складні ситуації, прогнозувати ризики та приймати обґрунтовані рішення. Ці моделі формуються на основі їхнього досвіду, знань та постійного навчання та описані когнітивні вподобання порушників. Окреслені когнітивні зацікавленості кіберпорушників, зокрема у сфері соціальної інженерії.

Отримані результати можуть слугувати основою для розробки системи підтримки прийняття рішень у сфері управління інформаційними ризиками, забезпечуючи можливість гнучкої адаптації до змінних загроз та підвищення ефективності управлінських стратегій.

ДЖЕРЕЛА

1. Шевченко, С.М., Жданова, Ю.Д., Спасітєлєва, С.О. &; Складанний П.М. (2020) «Проведення swot-аналізу оцінювання інформаційних ризиків як засіб формування практичних навичок студентів спеціальності 125 Кібербезпека». Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(10) с. 158-168.

2. ДСТУ ISO/IEC 27005:2019 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки

3. Shevchenko S., Zhdanova Y., Kryvytska O., Shevchenko H., Spasiteleva S. (2024) *Fuzzy cognitive mapping as a scenario approach for information security risk analysis* Cybersecurity Providing in Information and Telecommunication Systems II 2024, 3826. с. 356-362. ISSN 1613-0073

4. Шевченко, С., Жданова, Ю., Складанний, П., & Петренко, Т. (2024). «Нечіткі когнітивні карти як інструмент візуалізації сценаріїв реагування на інциденти в системах безпеки». Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(26), 417–429.

ВИКОРИСТАННЯ МЕТОДІВ ШИФРУВАННЯ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ

Гордієнко В. І.

Київський столичний університет імені Бориса Грінченка, м. Київ

У сучасному світі інформація стала важливою складовою інформаційної безпеки, її цінність залежить від змісту, а також може спричиняти непередбачувані події. З огляду на велику кількість електронних даних, питання захисту від несанкціонованого доступу є критично важливим як для державного, так і для приватного сектору. Шифрування є одним із основних методів захисту інформації.

Існують два основні типи алгоритмів шифрування: симетричні та асиметричні. Симетричні алгоритми використовують один ключ для шифрування та розшифрування, що вимагає забезпечення захисту від витоку цього ключа. До таких класичних методів належать:

1. Метод простої заміни. Проводиться заміна символів відкритого тексту на інші за спеціально визначеним ключем. Метод легкий в реалізації, але має низьку стійкість [1, с. 46-48].

2. Метод перестановки. Проводиться переміщення символів тексту за спеціальним встановленим шаблоном, що в результаті утворює

зашифроване повідомлення. При цьому самі символи не змінюються, а змінюється лише їх порядок [1, с. 90-99].

3. Метод гамування. Є одним з найнадійніших методів, де шифрування здійснюється додаванням гами до символів тексту за модулем 2. Гама має бути не коротшою за довжину повідомлення, щоб уникнути її повторення [1, с. 84-86].

Асиметричні алгоритми використовують два ключа: відкритий – для шифрування; закритий – для розшифрування. Зашифроване повідомлення може розшифрувати лише власник секретного ключа, що гарантує безпечну передачу даних навіть через незахищене середовище [1, с. 35-36].

Крім наведених методів шифрування, існує метод хешування, який не належить ані до симетричних, ані до асиметричних алгоритмів, оскільки не передбачає зворотного перетворення.

Метод хешування забезпечує контроль цілісності та автентичності даних, приховуючи при цьому сам зміст. Результатом хешування є фіксоване хеш-значення, що однозначно відповідає вхідному повідомленню. Змінити повідомлення без зміни його хешу практично неможливо, тому хеш-функції широко використовуються для перевірки цілісності файлів, паролів, у цифрових підписах [2].

Дане дослідження присвячено порівняльному аналізу методів шифрування, результати представлено у таблиці 1.

Таблиця 1

Порівняльна таблиця методів шифрування та хешування

Назва	Характеристика	Застосування	Переваги	Недоліки
Симетричне шифрування	Використовується один ключ для шифрування і розшифрування.	Захист даних у базах, месенджерах та захищеними мережевими протоколами.	Легка реалізація, висока швидкість.	При розкритті ключа шифрування вся зашифрована інформація стає доступною.
Асиметричне шифрування	Використовується пара ключів: відкритий – для шифрування, секретний – для розшифрування.	Цифрові підписи, захист повідомлень електронної пошти.	Висока безпека та відсутність потреби в окремому захищеному каналі для обміну ключами.	Вимагає більше ресурсів для застосування, значно повільніший за швидкістю.
Хешування	Проводить перетворення повідомлення у фіксований хеш-код, без можливості зворотного відновлення.	Перевірка цілісності файлів, паролів, цифрові підписи.	Забезпечує контроль цілісності даних, висока швидкість, неможливість розшифрування у разі перехоплення.	Хеш-функція є одностороннім перетворенням, тому відновити зміст повідомлення неможливо.

Таким чином, проведене дослідження показало важливість правильного використання шифрування та інтеграції сучасних методів захисту на всіх етапах обробки даних. До наступних напрямів дослідження в цій сфері відноситься розвиток квантового шифрування з метою забезпечення надійного захисту інформації.

ДЖЕРЕЛА

1. Самойлов І. В, Матійко А. А, Сторчак А. С Криптографія: навчальний посібник. Київ: ІСЗЗІ КПІ ім. Ігоря Сікорського, 2023. 372 с.
2. ДСТУ 7564:2014. Інформаційні технології. Криптографічний захист інформації. Функція гешування.

ІНСТРУМЕНТИ ТА ТЕХНОЛОГІЇ УПРАВЛІННЯ УРАЗЛИВОСТЯМИ У ПРОЦЕСІ РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Грабар М. В.
Київський столичний університет імені Бориса Грінченка, м. Київ

У сучасному суспільстві розробка програмного забезпечення супроводжується численними викликами у сфері безпеки. Ефективне управління уразливостями на всіх етапах життєвого циклу ПЗ є ключовим аспектом забезпечення його надійності. Помилки в коді, некоректні конфігурації серверів та відсутність контролю доступу можуть спричиняти критичні загрози. Використання сучасних інструментів для виявлення та усунення таких уразливостей є необхідним для створення безпечного ПЗ [1].

Оптимізація процесу управління уразливостями підвищує рівень безпеки, зменшує ризики атак та фінансові витрати. Інтеграція відповідних інструментів на ранніх етапах розробки дозволяє ефективно реагувати на нові загрози та відповідати сучасним стандартам кібербезпеки. Дослідження у цій сфері зосереджені на впровадженні механізмів безпеки та управлінні ризиками в процесі розробки програмного забезпечення [2].

Метою дослідження є аналіз сучасних інструментів для управління уразливостями та розробка методики їх інтеграції в процес розробки ПЗ.

Об’єкт дослідження – система розробки та проєктування програмного забезпечення.

Предмет – інструменти та методики виявлення, аналізу й усунення уразливостей.

Для досягнення мети необхідно проаналізувати сучасні методи управління уразливостями та оцінити їхню ефективність на різних етапах розробки програмного забезпечення. Важливим аспектом дослідження є вивчення інструментів статичного та динамічного аналізу коду, що

дозволяють виявляти потенційні загрози ще до впровадження продукту в експлуатацію. Окрім цього, слід визначити ключові фактори, які впливають на точність і продуктивність безпекових інструментів, оскільки їхня ефективність може залежати від особливостей коду, середовища розробки та налаштувань системи. На основі отриманих результатів необхідно розробити методику інтеграції інструментів безпеки у процес DevSecOps, що забезпечить автоматизоване виявлення та усунення уразливостей, підвищуючи рівень захищеності програмного забезпечення [2].

Більшість систем управління уразливостями орієнтовані на корпоративний сегмент, тоді як малі та середні команди стикаються з труднощами впровадження через складність налаштувань, низьку точність деяких інструментів та високу вартість. Інтеграція статичного та динамічного аналізу в CI/CD-процеси за допомогою SonarQube, Snyk, Semgrep, OWASP ZAP та Tenable Nessus дозволяє автоматизувати виявлення уразливостей. Важливо також забезпечити моніторинг коду та навчання розробників з кібербезпеки [1].

Запропонована методика інтеграції безпекових інструментів у процес розробки програмного забезпечення допоможе зменшити ризик критичних уразливостей, підвищити якість та безпеку програмного забезпечення.

ДЖЕРЕЛА

1. DevSecOps: Інтеграція безпеки продукту на кожному етапі SDLC [Електронний ресурс] – Режим доступу до ресурсу: https://dou.ua/forums/topic/42762/.

2. Що таке DevSecOps? [Електронний ресурс] – Режим доступу до ресурсу: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-devsecops.

ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ ТРАФІКУ МЕСЕНДЖЕРІВ НА МОБІЛЬНИХ ПРИСТРОЯХ ТА ВИРОБЛЕННЯ РЕКОМЕНДАЦІЙ З БЕЗПЕКИ

Дем’янчук А. С.
Київський столичний університет імені Бориса Грінченка, м. Київ

У сучасному світі важко уявити людину, яка б не користувалась мобільним телефоном, а відповідно і месенджером. Смартфони і месенджери стали основними каналами безперервної комунікації. Деякі з них, окрім стандартного обміну повідомленнями, реалізують ще й аудіо та відеозв’язок, обмін файлами та геолокацією, веб-конференції, місце зберігання даних, аудіопрогравач та багато іншої всячини [1]. Перебуваючи в інтернет- середовищі кожен з нас розраховує на те, що буде збережена його конфіденційність та дотримана безпека персональних даних.

Перехоплення трафіку в месенджерах є однією з існуючих загроз для користувачів та компаній-розробників месенджерів. Атака при цьому спрямована на отримання даних, таких як: логіни, паролі та особисті повідомлення задля маніпулювання власником, продажу або просто викладення на загал в інтернет-просторі. Для компанії-власника месенджера така атака несе за собою значні фінансові збитки та зменшення популярності серед користувачів. На жаль, більшість месенджерів на сьогоднішній день не мають потрібного захисту, а самі користувачі є мало обізнаним в питаннях інформаційної безпеки і не знають як додатково захистити свої дані в мережі інтернет, через що стають легкою здобиччю для кіберзлочинців.

З початком широкомасштабного російського вторгнення Україна опинилася під подвійним ударом: крім військової агресії, ми відбиваємо постійні кібератаки. Нападники активно намагаються проникнути в наш інформаційний простір, цілячись як у державні ресурси, так і в особисті дані громадян. У цих умовах кожен власник смартфона має бути уважним і дотримуватися базових правил інформаційної безпеки. Кіберзахист більше не є справою лише IT-спеціалістів – це тепер важлива частина повсякденного життя для кожного українця [2].

Завданнями для будь-якого розробника месенджера є: побудова та забезпечення ефективного захисту інформації, який полягає у шифруванні повідомлень користувачів; дотримання політик конфіденційності та стандартів інформаційної безпеки; оновлення свого додатку та удосконалення його захисту від виникаючих нових кіберзагроз.

Дане дослідження спрямоване на методи захисту трафіку месенджерів на мобільних пристроях та вироблення рекомендацій щодо забезпечення безпеки. Робота описує проблеми, пов’язані з перехопленням трафіку, як одного із різновиду кібератак, та пропонує варіанти, як

користувачеві не потрапити під цю атаку та як захиститися від неї. Під час дослідження було розглянуто проблеми месенджерів щодо їх уразливості та недоліків, проаналізовано варіанти захисту від ефективних до застарілих, які використовують розробники месенджерів. Дослідження містить структуру, технічні частини та терміни, пов’язані із захистом інформації та даних в месенджерах; описує існуючі види захисту в месенджерах; окреслює правила для користувачів з метою убезпечити свої персональні дані в менш надійних месенджерах.

ДЖЕРЕЛА

1. Елєвтєрова А. (2024). Непрочитані повідомлення. Як захистити приватні розмови в месенджерах від шпигунів, хакерів і ворогів. [Електронний ресурс] – Режим доступу: https://mediamaker.me/yak-zahystyty-pryvatni-rozmovy-v-mesendzherah-vid-shpyguniv-hakeriv-i-vorogiv-8956/

2. Кібербезпека під час війни [Електронний ресурс] – Режим доступу: https://www.topical.in.ua/kiberbezpeka-pid-chas-vijny/

ПЕРСПЕКТИВИ ПІДВИЩЕННЯ БЕЗПЕКИ У ВЕБ-ЗАСТОСУНКАХ НА БАЗІ SPRING BOOT З ВИКОРИСТАННЯМ JWT

Дикало А. Ю.

Державний університет інформаційно-комунікаційних технологій, м. Київ

У сучасній розробці веб-застосунків безпека є критично важливим аспектом, особливо при обміні даними між клієнтом та сервером. У розробці веб-застосунків мовою Java постає проблема ідентифікації та обмеження клієнтів у діях в системі [1]. Саме цю проблему і вирішують JWT, інтегровані за допомогою Spring Security у веб-застосунках.

Метою даного дослідження є аналіз та розробка ефективного підходу до забезпечення безпеки веб-застосунків, створених за допомогою фреймворку Spring Boot, шляхом впровадження механізмів аутентифікації та авторизації на основі JSON Web Token (JWT).

JSON Web Token (JWT) – це компактний та безпечний спосіб передачі інформації між двома сторонами через Інтернет. У контексті ж Spring Security JWT використовується як механізм аутентифікації та передачі користувацьких даних у заголовках HTTP-запитів. Інформація, що передається, представлена у вигляді JSON-об'єкта, який називається «корисне навантаження» (payload). Цей об'єкт може бути підписаний цифровим підписом або зашифрований, що гарантує його цілісність та конфіденційність. Після успішної аутентифікації сервер генерує токен доступу, який містить зашифровану інформацію про користувача. Цей токен передається клієнту і використовується для подальшої взаємодії з

застосунком [2]. На рис. 1 зображена схема, що демонструє обробку запитів. Система перехоплює запити та перевіряє JWT, обмежує доступ на основі ролей користувача та валідує вхідні дані для запобігання атакам на рівні запитів.

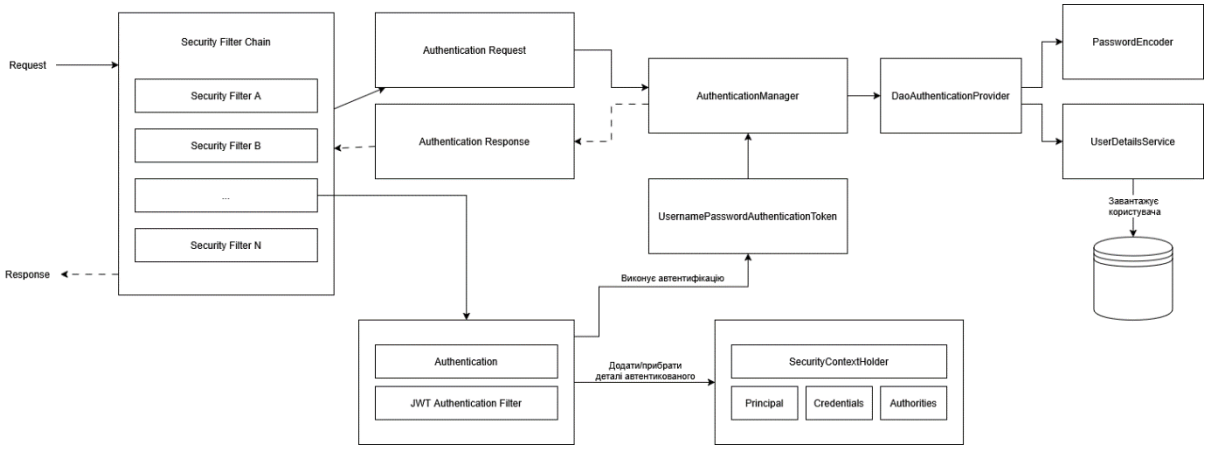


Рис. 1. Схема обробки запитів в Spring Security

Відповідно, використання JSON Web Token (JWT) у поєднанні з Spring Boot та Spring Security за правильного проєктування надає ефективний механізм для реалізації аутентифікації та авторизації в RESTful сервісах[3].

Роль фреймворка Spring Security, що є вельми популярним і незамінним інструментом для забезпечення безпеки корпоративних Java EE застосунків [4], – це забезпечення перехоплення запитів в API та їх перевірку на валідність JWT, обмеження доступу до операцій на основі системи ролей та валідацію вхідних даних.

Правильне використання JWT у поєднанні з фреймворком Spring Boot та Spring Security може забезпечити ефективний механізм аутентифікації та авторизації у веб-застосунках. Реалізація цього механізму дозволить зменшити навантаження ня серверну частину веб-застосунку завдяки відмові від зберігання сесійного стану користувача, а також підвищить рівень захисту даних, що передаються клієнту за рахунок криптографії в підписі токена доступу.

Результати даного дослідження демонструють потенціал JWT як основного компонента безпеки веб-застосунків у нинішніх реаліях та відкривають широкий спектр можливостей для інновацій у сфері даного дослідження.

ДЖЕРЕЛА

1. Vyas B. Security challenges and solutions in java application development. Eduzone: international peer reviewed/refereed multidisciplinary journal. 2023. Vol. 12, no. 2. P. 268–275.

2. RFC 7519. JSON Web Token (JWT). [Effective from 2015-05-01]. Official edition. Internet Engineering Steering Group (IESG), 2015. 2 p. URL: https://doi.org/10.17487/RFC7519.
3. Spring Security JWT Authentication Tutorial [Електронний ресурс] – Режим доступу: https://www.codejava.net/frameworks/spring-boot/spring-security-jwt-authentication-tutorial.
4. Spring Security documentation [Електронний ресурс] – Режим доступу: https://docs.spring.io/spring-security/site/docs/4.2.x/reference/html/introduction.html.

ВИКОРИСТАННЯ МЕСЕНДЖЕРІВ ЯК ЕТАПУ БАГАТОФАКТОРНОЇ АВТОРИЗАЦІЇ

Дубровський І. В.
Київський столичний університет імені Бориса Грінченка, м. Київ

Сучасні інформаційно-комунікаційні системи потребують удосконалених методів автентифікації для захисту облікових записів від несанкціонованого доступу. Одним із перспективних підходів є використання месенджерів як додаткового фактора у процесі багатофакторної авторизації. Традиційні засоби, такі як SMS, мобільні аутентифікатори або електронна пошта, мають низку недоліків, включаючи уразливість до атак перехоплення повідомлень, генерації кодів зловмисником, якщо відома ключова послідовність або підміни каналів зв'язку. Месенджери з наскрізним шифруванням [1] (наприклад, Signal) дозволяють реалізувати більш захищений механізм підтвердження особи.

Для дослідження застосування месенджерів з наскрізним шифруванням у процесі багатофакторної авторизації, була реалізована схема, що базується на бот-платформі та API-інтерфейсі. Важливо було налаштувати тайм-аути підтвердження та обробку негативних відповідей для запобігання довільному обходу авторизації [2].

При впровадженні такого рішення користувачеві після введення логіна і пароля надсилається запит у месенджер на підтвердження дії. Без активного схвалення через месенджер доступ до системи залишається заблокованим. Інтеграція месенджера може бути прив'язана не лише до процесу входу в систему загалом, але й до активації окремих функцій або підсистем. У нашому випадку ми зосередились на SSH. Користувач не міг отримати доступ до віддаленого сервера, не підтвердивши свій вхід через месенджер. Подібну інтеграцію можна провести не лише з цим, а й з іншими сервісами. Наприклад, заборонити підвищення привілеїв без підтвердження або обмежити права на зміну конфігураційних файлів сервісу.

Таким чином, використання месенджерів як етапу багатофакторної авторизації підвищує загальний рівень захищеності інформаційно-

комунікаційних систем та дозволяє гнучко керувати доступом до найбільш критичних функцій на основі підтвердження в окремому зашифрованому каналі.

ДЖЕРЕЛА

1. NIST Special Publication 800-63B. Digital Identity Guidelines: Authentication and Lifecycle Management.

2. ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements.

ЗАХИСТ ІНФОРМАЦІЇ У ЗАСТОСУНКУ SKYRIM ACTOR VALUES EDITOR

Іванов М. Є.

Державний університет інформаційно-комунікаційних технологій, м. Київ

Розробка програмного забезпечення для редагування характеристик NPC у відеогрі TES V: Skyrim потребує забезпечення належного захисту даних для запобігання помилок файлів гри. У цьому контексті важливою проблемою є забезпечення цілісності та правильності збереження змін у файлах плагінів, таких як ESP/ESM [1; 2]. Оскільки неправильне збереження або помилка в процесі редагування можуть призвести до порушення роботи гри, необхідно створити систему, яка надасть гарантії безпеки під час роботи з даними.

Одним з основних аспектів безпеки є правильна організація вводу та виводу даних [1]. Для цього було реалізовано функції перевірки коректності введених значень, щоб унеможливити збереження неправильних або пошкоджених даних у файли плагінів. Наприклад, при редагуванні параметрів NPC, таких як рівень, здоров'я, магія чи витривалість, програма повинна здійснювати перевірку на відповідність допустимим межам значень. Це дозволить запобігти внесенню значень, які можуть призвести до помилок у грі [3].

Крім того, важливим аспектом є забезпечення надійного збереження змін у файлах. При записі змін у файли ESP/ESM програма повинна проводити додаткові перевірки на наявність помилок збереження або порушення структури файлу [2; 3]. Це дозволить уникнути випадкових або несанкціонованих змін, які можуть спричинити пошкодження даних.

Таким чином, для забезпечення інформаційної безпеки програмного продукту, що редагує характеристики NPC у TES V: Skyrim, здійснено правильну організацію вводу та виводу даних, перевірку на коректність введених значень, контроль доступу до функцій редагування та забезпечення резервного копіювання даних. Це дозволить створити надійний інструмент для редагування файлів гри без ризику їх пошкодження.

ДЖЕРЕЛА

1. Mutagen Documentation. (2023). Working with Skyrim Files: Structure and Data Safety. Режим доступу: https://mutagen-modding.github.io/Mutagen
2. Unofficial Elder Scrolls Pages. (2023). Data File Format. Режим доступу: https://ck.uesp.net/wiki/Data_file
3. TES5Edit Documentation. (2023). Managing Mod Files. Режим доступу: https://tes5edit.github.io/docs/8-managing-mod-files.html

АНАЛІЗ ПРОЦЕСУ ОЦІНКИ І ВДОСКОНАЛЕННЯ ФУНКЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Кія О. С.

Київський столичний університет імені Бориса Грінченка, м. Київ

У сучасному світі інформація є одним з найцінніших активів організації. Вона може зберігатись у різних місцях: інформаційних системах, паперових документах, на флешках і, найнеочевидніше, в головах співробітників. Втрата будь-якого інформаційного активу може призвести до значних втрат для організації, включаючи фінансові, репутаційні, регуляторні та процесні.

Забезпечення захисту інформаційних активів є важливим завданням Функції Інформаційної Безпеки. Однак організації завжди мають обмежені ресурси, тому кожна витрата повинна бути обґрунтована. Способом їх обґрунтування можуть виступати регуляторні вимоги та вимоги ринку, які визначають очікування щодо забезпечення захисту інформації відповідно до певних фреймворків, таких як ISO 27001 [1] або NIST CSF 2.0. [2].

Проте сліпе впровадження контролів за списком не є економічно доцільним рішенням. Без визначеного підходу або методології співробітники організації будуть обмежені своїми знаннями і професійним досвідом. Щоб цього не допустити, організація повинна мати розуміння, що є найціннішим, які загрози можуть бути спрямовані на її активи і які втрати вона може понести у результаті їх реалізації. Тому для визначення економічно доцільного і ефективного контрольного середовища критично важливо встановити механізм, що дозволить оцінити її потреби.

Дане дослідження присвячене тому, як можливо виходячи з контексту організації провести первісну верхньорівневу оцінку ризиків з використанням якісного підходу. Це дозволить визначити напрямок діяльності Функції ІБ і почати впроваджувати контрольне середовище, найбільш підходяще для організації, з використанням міжнародно визнаного фреймворку ІБ. Результати даного дослідження можуть бути використані для розробки ефективних стратегій управління інформаційною безпекою в малих та середніх підприємствах, що дозволить підвищити їх стійкість до інформаційних загроз.

ДЖЕРЕЛА

1. ДСТУ ISO/IEC 27001:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою.
2. The NIST Cybersecurity Framework (CSF) 2.0. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ДАНИХ У ВІДЕОГРІ

Коваль О. С.

Державний університет інформаційно-комунікаційних технологій, м. Київ

Безпека даних у відеоіграх є важливою складовою розробки, що впливає на стабільність продукту та його комерційний успіх. Навіть у випадку однокористувацьких ігор, ризики, пов’язані з крадіжкою вихідного коду, реверс-інжинірингом та модифікацією продукту, можуть завдати шкоди як фінансово, так і репутаційно. Тому важливо впроваджувати заходи захисту ще на етапі розробки.

Піратство, модифікація коду та порушення цілісності файлів можуть вплинути на монетизацію та загальну стабільність продукту. Іноді піратські копії ігор змінюють і публікують під іншими назвами, змушуючи чесних розробників конкурувати з хакерами, які привласнили їхню інтелектуальну власність. Крім того, поширення шкідливого програмного забезпечення у піратських версіях може завдати шкоди репутації гри. Користувачі, що завантажують такі копії та стикаються з проблемами, можуть залишати негативні відгуки та знижувати рейтинг гри у цифрових магазинах [1].

У даному дослідженні були проаналізовані різні загрози цілісності даних у відеогрі та виділені підходи до забезпечення захисту інформації у цьому процесі.

1. Безпека розробницького процесу.

Для збереження безпеки вихідного коду під час розробки та її історії використовується система контролю версій GitHub. Доступ до репозиторію захищено двофакторною аутентифікацією (2FA) з використанням одразу двох різних способів підтвердження. Вона дає можливість значно підсилити рівень захисту та убезпечити дані від кібер зловмисників [2]. Додатково використовуються приватні репозиторії для обмеження доступу.

2. Захист коду: IL2CPP.

Для ускладнення аналізу вихідного коду використовується конвертація коду через IL2CPP. У випадку з рушієм Unity це можна увімкнути за шляхом: Edit → Project Settings → Player → Scripting Backend → IL2CPP [3]. Перетворення C#-коду на проміжний рівень C++ ускладнює

злом через інструменти на кшталт dnSpy, роблячи реверс-інжиніринг більш складним і ресурсозатратним для зловмисників.

3. Збереження даних.

Усі дані користувача, які зберігаються на пристрої, це лише налаштування гри. Оскільки гра є офлайн-продуктом, додатковий збір інформації не потрібен, що виключає загрози конфіденційності. Для збереження параметрів використовується клас PlayerPrefs у Unity. Одне з параметрів для збереження, а саме рівень гучності гри реалізовано так:

PlayerPrefs.SetFloat(«volume», 0.8f);

PlayerPrefs.Save();

Цей підхід забезпечує мінімальний і простий збір необхідних для гри даних. Але для конфіденційних даних такий спосіб не підійде, оскільки дані зберігаються в локальному регістрі без шифрування [4].

Реалізовані заходи забезпечують базовий рівень захисту даних у відеогрі. Використання GitHub з 2FA гарантує безпеку вихідного коду під час розробки, а мінімальний збір даних забезпечує конфіденційність гравців. Додатково, застосування IL2CPP ускладнює реверс-інжиніринг, що робить злом гри більш ресурсозатратним.

Завдяки цим заходам розроблена гра є більш стійкою до базових загроз, забезпечуючи стабільність в розробці та базовий захист після випуску.

ДЖЕРЕЛА

1. How do you get your indie game protected without spending a fortune? [Електронний ресурс] – Режим доступу: URL https://irdeto.com/hubfs/resources/e-books/protect-indie-games-without-spending-a-fortune.pdf

2. Що таке двофакторна автентифікація, і як вона працює? [Електронний ресурс] – Режим доступу: URL https://cip.gov.ua/ua/faqs/sho-take-dvofaktorna-avtentifikaciya-i-yak-vona-pracyuye

3. Unity - Manual: IL2CPP Overview [Електронний ресурс] – Режим доступу: URL https://docs.unity3d.com/6000.0/Documentation/Manual/scripting-backends-il2cpp.html

4. Unity - Scripting API: PlayerPrefs [Електронний ресурс] – Режим доступу: URL https://docs.unity3d.com/6000.0/Documentation/ScriptReference/PlayerPrefs.html

ЗАХИСТ ІНФОРМАЦІЇ У WEB-ЗАСТОСУНКУ СТВОРЕННЯ ТА КЕРУВАННЯ БЛОГАМИ

Коляда В. С.
Державний університет інформаційно-комунікаційних технологій, м. Київ

Сучасні веб-додатки, особливо ті, що передбачають взаємодію користувачів та зберігання їхніх даних, як-от платформи для ведення блогів, вимагають особливої уваги до питань інформаційної безпеки. Забезпечення конфіденційності, цілісності та доступності даних користувачів є критично важливим завданням. Неналежний захист може призвести до несанкціонованого доступу, витоку персональної інформації та втрати довіри користувачів.

Дане дослідження присвячене аналізу та реалізації механізмів захисту інформації у розробленому web-застосунку для створення та керування блогами на базі Java Spring Boot.

Дана система оперує обліковими записами користувачів та їхніми публікаціями. У зв'язку з цим виникла необхідність впровадження надійних методів автентифікації, авторизації та захисту даних від поширених веб-атак.

Для забезпечення безпеки використано фреймворк Spring Security. Ключовим елементом захисту облікових даних є механізм автентифікації та безпечне зберігання паролі за допомогою хешування. Хешування пароля [1] є важливим методом захисту користувацьких даних, і для цього використовується метод BCrypt. Це дозволяє безпечно хешувати паролі, додаючи до них сіль [1]. Хешування з використанням солі (salted hashing) – це метод додавання випадкових даних (солі) до паролів перед їх хешуванням, щоб ускладнити атаки, такі як brute-force [2] (рис. 1).

```
@Bean
public static PasswordEncoder passwordEncoder() {
    return new BCryptPasswordEncoder();
}
```

Рис. 1. BCrypt

Контроль доступу до різних функціональних частин додатку реалізовано за допомогою механізмів авторизації Spring Security. Чітко визначено правила доступу: публічні сторінки (наприклад, реєстрація, перегляд постів) доступні всім користувачам, тоді як доступ до адміністративних функцій та створення контенту вимагає попередньої автентифікації (рис. 2).

```
auth.requestMatchers(antMatcher("/register/**")).permitAll();
auth.requestMatchers(antMatcher("/posts/**")).permitAll();
auth.anyRequest().authenticated();
```

Рис 2. Доступ

Це забезпечує розмежування прав користувачів та захищає систему від несанкціонованого доступу до ресурсів.

Таким чином, реалізований комплекс заходів безпеки, забезпечує належний рівень захисту даних у веб-додатку для створення та керування блогами.

ДЖЕРЕЛА

1. Хешування паролів: використання солі та bcrypt [Електронний ресурс]. – Режим доступу: URL https://drukarnia.com.ua/articles/kheshuvannya-paroliv-vikoristannya-soli-ta-bcrypt-fsme-

2. Пірог О. В. Безпека веб-додатків: Навч. посіб. Житомир: Житом. політехніка, 2025. 290 с. URL: https://eztuir.ztu.edu.ua/bitstream/handle/123456789/8791/Пірог.pdf

ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ІНФОРМАЦІЇ У WEB-ЗАСТОСУНКУ ДЛЯ НАДАННЯ ПОСЛУГ ЛІЗИНГУ АВТОМОБІЛІВ

Корнєєв В. О., Лаврененко В. В.

Державний університет інформаційно-комунікаційних технологій, м.Київ

У сучасному світі більшість компаній мають веб-сайт. Однак ця відкритість також несе ризики, оскільки веб-додатки можуть стати мішенню для хакерів [1]. Це відіграє важливу роль для сервісів, які зберігають персональні дані користувачів. Безсумнівно, захист веб-інфраструктури потрібний для будь-якої компанії. Однак з безлічі категорій захисних рішень – Firewall, IPS / IDS, NGFW (Next Generation Firewall), WAF (Web-Application Firewall) найефективніший Web Application Firewall, який здатний забезпечити комплексний захист веб-додатків від відомих і невідомих загроз, а також забезпечити відповідність вимогам регуляторів, наприклад, PCI DSS [2].

Головним завданням даного дослідження є розробка web-застосунку «Надання послуг лізингу авто». У функціоналі сервісу передбачено зберігання важливої інформації: персональні дані, фінансові показники клієнтів, а також документи, які пов’язані з автомобілями. Через високу чутливість цих даних найбільшу увагу треба приділити інформаційній безпеці. Безпечна авторизація, надійний захист є дуже важливим для запобігання витоку інформації.

Було використано двофакторну аутентифікацію (2FA) задля посилення захисту акаунтів користувачів. Впроваджено механізм обмеження невдалих спроб входу, що унеможливлює атаки методом грубої сили. Паролі зберігаються у хешованому вигляді, застосовуючи алгоритм bcrypt. При взаємодії з базою даних PostgreSQL використовуються

підготовлені запити. Виконано перевірку та очищення даних, отриманих від користувачів. Забезпечено шифрування конфіденційної інформації перед її збереженням у сховищі даних. Для безпечного обміну даними мережею застосовується протокол HTTPS.

Для гарантування достатнього рівня захисту та нагляду за критичними функціями системи було введено чіткий поділ ролей. Ця система передбачає різні рівні допуску, включаючи основні ролі, як-от «користувач» і «адміністратор». Кожна роль визначає перелік привілеїв та можливостей, що слугує для обмеження доступу до чутливих операцій та даних виключно для авторизованих користувачів. Це дозволяє уникнути несанкціонованих дій та потенційних зловживань, забезпечуючи надійний захист. Кожен вхід до системи та будь-які зміни у налаштуваннях безпеки фіксуються у журналах для ретельного аналізу. У застосунку також передбачено можливість анонімного перегляду всіх його функцій.

Отже, запропоновані способи можуть істотно знизити загрозу хакерської атаки на дані користувачів у веб-додатку «Надання послуг лізингу авто». Достатній рівень інформаційної безпеки забезпечується за допомогою новітніх алгоритмів хешування паролів, захисту від SQL-ін’єкцій і XSS-атак, а також шифрування даних і HTTPS. Майбутні дослідження можуть бути зосереджені на вдосконаленні механізмів управління доступом та використанні додаткових методів автентифікації.

ДЖЕРЕЛА

1. Боскін О.О., Корніловська Н.В., Поліщук В.М., Сарафаннікова Н.В.(2023). Безпека веб-додатків та хакерські атаки. *Вісник Херсонського національного технічного університету*, *№ 3(86),* 83-92. https://doi.org/10.35546/kntu2078-4481.2023.3.11

2.Захист веб-додатків: чому це важливо – IT Business – [Електронний ресурс] – Режим доступу: https://itbiz.ua/statti-ta-obzori/zaxist-veb-dodatkiv-chomu-ce-vazhlivo/

АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ПІДВИЩЕННЯ СТІЙКОСТІ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ ДО СОЦІОТЕХНІЧНИХ АТАК

Крижанівська Т. М.
Київський столичний університет імені Бориса Грінченка, м. Київ

Соціотехнічні атаки є однією з найпоширеніших та небезпечних загроз для інформаційної безпеки. На відміну від традиційних кібератак, що експлуатують технічні уразливості програмного чи апаратного забезпечення, соціотехнічні атаки використовують психологічні та соціальні уразливості людей для отримання несанкціонованого доступу до інформації або систем.
У сучасному інформаційному світі саме людина, яка оперує інформаційною системою, часто стає найслабшою ланкою в безпеці [1].

Методи протидії соціальній інженерії можна приблизно поділити на два типи: виявлення на основі людини (human based detection) та виявлення на основі технологій (technology based detection) [2]. Перший підхід зосереджений на поведінці, спостережливості та знаннях самих користувачів, які можуть розпізнавати ознаки обману або шахрайських дій. Другий підхід покладається на автоматизовані технічні засоби, які здатні фіксувати, аналізувати та реагувати на підозрілу активність без участі людини або з мінімальним її залученням.

Методи виявлення на основі людини включають такі підходи, як політики, аудит, освіта, навчання та підвищення обізнаності [2]. Основна роль тут покладається на здатність співробітників ідентифікувати ознаки потенційної загрози, оцінити ризик і діяти відповідно до встановлених процедур. Підготовка персоналу має вирішальне значення, адже саме навчені та уважні співробітники можуть вчасно розпізнати спробу маніпуляції. Проте цей метод має обмеження, оскільки базується на суб'єктивних судженнях людей, які залишаються вразливими до психологічних прийомів атакуючих. Емоційний стан, недосвідченість, незнання внутрішніх процедур або стресові ситуації можуть істотно знижувати ефективність навіть добре підготовленого персоналу. Нові працівники та тимчасові співробітники є особливо вразливою категорією, оскільки часто ще не встигають отримати належний рівень обізнаності про безпекові політики й стандарти поведінки.

Технологічні методи протидії, такі як сенсори, біометрія, штучний інтелект та honeypot-системи, додають рівень безпеки, який може зменшити вплив людської слабкості [2]. Вони дозволяють автоматизовано виявляти підозрілу активність, контролювати доступ до систем, аналізувати поведінкові відхилення і швидко реагувати на потенційні загрози. Біометричні технології ускладнюють спроби підміни особистості, а системи штучного інтелекту здатні розпізнавати тонкі закономірності

атак, які не завжди очевидні людині. Проте технологічні рішення також мають свої недоліки: можливі хибні спрацьовування, труднощі із впровадженням, високі фінансові витрати та уразливість самих систем до обхідних атак. Крім того, технології потребують постійного оновлення й адаптації, що вимагає значних ресурсів.

Таким чином, обмеження як методів на основі людини, так і технологічних методів протидії підкреслюють необхідність їх інтегрованого застосування для ефективного виявлення і запобігання соціотехнічним атакам. Кожен із підходів має свої переваги й недоліки, тому їх доцільно розглядати як взаємодоповнювані, а не взаємовиключні. Загроза соціальної інженерії залишається постійною, доки людський фактор є складовою частиною інформаційно-комунікаційних систем, і тому повне усунення цієї загрози неможливе. Реальними заходами є систематичне навчання персоналу, розробка та впровадження дієвих політик безпеки, а також використання технологічних рішень, які мінімізують ризик помилки людини. Досягнення балансу між людськими та технологічними підходами дозволяє підвищити стійкість організацій до сучасних методів соціотехнічних атак. Подальші наукові дослідження будуть зосереджені на розробці комплексних стратегій безпеки, які б об’єднували освітні ініціативи, технічний захист і організаційне управління ризиками. Лише поєднання всіх цих рівнів дозволить створити адаптивну й стійку систему кібербезпеки, здатну ефективно протидіяти еволюціонуючим загрозам соціальної інженерії.

ДЖЕРЕЛА

1. Syafitri, W., Shukur, Z., Mokhtar, U.A., Sulaiman, R., Ibrahim, M.A. (2022). *Social Engineering Attacks Prevention: A Systematic Literature Review*. IEEE Access, vol. 10, pp. 39325–39336. DOI: 10.1109/ACCESS.2022.3162594.

2. Zulkurnain, A.U., Hamidy, A.K.B.K., Husain, A.B., Chizari, H. (2015). Social Engineering Attack Mitigation. *International Journal of Mathematics and Computational Science,* vol. 1, no. 4, pp. 188–198.

ПРАКТИЧНЕ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ПРОВЕДЕННЯ OSINT-ДОСЛІДЖЕНЬ

Курсеітов О. О.

Київський столичний університет імені Бориса Грінченка, м. Київ

Відкриті джерела інформації (OSINT) відіграють важливу роль у сучасній аналітиці, розслідуваннях та кібербезпеці [1]. Завдяки розвитку технологій штучного інтелекту (ШІ) можливості OSINT значно розширилися, дозволяючи автоматизувати збір, обробку та аналіз великої кількості даних з відкритих джерел.

Основною проблемою OSINT-досліджень є велика кількість неструктурованих даних, розміщених у відкритих джерелах (соціальні мережі, блоги, форуми, урядові сайти тощо), а також необхідність швидкої їх обробки [2].

Метою дослідження є аналіз та обґрунтування ефективності застосування ШІ для проведення OSINT-досліджень, визначення його ключових можливостей, переваг та обмежень, а також розробка рекомендацій щодо використання сучасних алгоритмів і технологій ШІ для автоматизації збору, обробки та аналізу відкритих даних [3].

Об’єкт дослідження – це використання штучного інтелекту (ШІ) в процесах збору, аналізу та інтерпретації відкритих даних у межах OSINT-досліджень (Open-Source Intelligence).

Предмет дослідження – це методи та інструменти ШІ, що застосовуються для автоматизації та підвищення ефективності OSINT-аналізу, їхня ефективність, переваги та обмеження [4].

Актуальність дослідження – це розвиток інформаційних технологій та зростаюча кількість відкритих джерел інформації роблять OSINT (Open-Source Intelligence) невід’ємною частиною сучасної аналітики та розслідувань. У світлі зростаючих загроз інформаційній безпеці, дезінформації та кіберзлочинності використання штучного інтелекту для аналізу відкритих джерел набуває все більшого значення [4;5]. Це дослідження спрямоване на оцінку та обґрунтування ефективності застосування ШІ у сфері OSINT, що сприятиме розвитку інструментів для швидкого та точного аналізу інформації [6].

Наукова новизна:

Дослідження пропонує новий підхід до систематизації та аналізу OSINT-інструментів, що використовують ШІ. На відміну від існуючих досліджень, робота зосереджується на порівнянні ефективності різних алгоритмів машинного навчання та глибинного аналізу їхніх переваг та обмежень у контексті OSINT.

Для досягнення поставленої мети застосовуються такі методи:

1.Контент-аналіз – для дослідження та класифікації відкритих джерел інформації;

2.Порівняльний аналіз – для оцінки ефективності сучасних OSINT-інструментів із ШІ;

3.Методи машинного навчання – для тестування алгоритмів автоматизованого збору та обробки даних [2];

4.Методи кібербезпеки – для виявлення потенційних загроз та ризиків, пов’язаних із використанням ШІ в OSINT [5].

Таким чином, дослідження сприяє кращому розумінню можливостей ШІ у сфері відкритої розвідки та допомагає знайти оптимальні рішення для його ефективного використання.

ДЖЕРЕЛА

1. Smith C. D. S. Cyber Intelligence: The New Frontier for Cyber Security. – Wiley, 2020. – 320 p.
2. Russell S., Norvig P. Artificial Intelligence: A Modern Approach. – 4th ed. – Pearson, 2020. – 1136 p.
3. The Transmitted. Що таке OSINT (Open Source Intelligence, розвідка на основі відкритих джерел)? [Електронний ресурс]. – Режим доступу: https://thetransmitted.com/adlucem/shho-take-osint-open-source-intelligence-rozvidka-na-osnovi-vidkrytyh-dzherel/?utm_source=chatgpt.com.
4. HackYourMom. Штучний інтелект в OSINT: як покращити розслідування у 2024 році. [Електронний ресурс]. – Режим доступу: http://hackyourmom.com/kibervijna/shtuchnyj-intelekt-v-osint-yak-pokrashhyty-rozsliduvannya-u-2024-roczi/?utm_source=chatgpt.com.
5. Zhdanova M., Streltsov A. OSINT in the Context of Cyber-Security [Електронний ресурс]. – Режим доступу: https://www.researchgate.net/publication/312324333_OSINT_in_the_Context_of_Cyber-Security
6. Tiwari R. Cyber Security Intelligence and Analytics. – Springer, 2021. – 410 p.

ЗАХИСТ ІНФОРМАЦІЇ У ВЕБ-ЗАСТОСУНКУ ДЛЯ БРОНЮВАННЯ АВІАКВИТКІВ

Ліберман Н. М.

Державний університет інформаційно-комунікаційних технологій, м. Київ

У сучасних умовах активного розвитку цифрових технологій питання безпеки конфіденційної інформації стає все більш актуальним, особливо у сфері онлайн-сервісів, пов’язаних із обробкою персональних і платіжних даних. Одним із прикладів таких сервісів є web-застосунок для бронювання авіаквитків. У цьому випадку система оперує чутливою інформацією користувачів: їхніми персональними даними (PII), платіжною інформацією відповідно до стандарту PCI DSS, а також історією пересувань [1; 2]. Саме тому важливою задачею є впровадження надійних механізмів захисту даних, які б забезпечували конфіденційність, цілісність та доступність інформації [1].

Дане дослідження присвячене розробці багаторівневої системи захисту інформації у сервісі бронювання авіаквитків. На рівні клієнта потрібно впровадження політики безпеки вмісту (CSP), яка допомагає запобігати XSS-атакам шляхом обмеження джерел завантаження скриптів. Додатково для безпечного зберігання паролів необхідно реалізувати їх хешування за допомогою алгоритму Argon2id, який забезпечує стійкість до атак типу brute-force [1, с. 24]. Усі транзакції повинні здійснюватися через токенізований платіжний шлюз, який відповідає стандарту PCI DSS. Крім

того, для верифікації платежів можна запропонувати використовувати Zero-Knowledge Proof, що дозволяє підтвердити транзакцію без розкриття чутливої інформації [2, с. 5–6]. Захист API краще здійснювати шляхом впровадження JWT-токенів з обмеженим терміном дії (15 хвилин), обмеженням кількості запитів (rate limiting) – до 100 запитів на хвилину на один IP, а також динамічним обертанням API-ключів, що значно знижує ризик компрометації [3].

Для запобігання найпоширенішим атакам передбачено комплекс технічних рішень [1]: для захисту від SQL-ін'єкцій застосовуються Prepared Statements у поєднанні з ORM; від атак CSRF захищає механізм Double Submit Cookie; для протидії брутфорс-атакам реалізовано перевірку CAPTCHA v3 та блокування облікового запису після 5 невдалих спроб входу.

ДЖЕРЕЛА

1. OWASP Top 10 2023 [Електронний ресурс]. – Режим доступу: https://owasp.org/

2. PCI DSS v4.0 Standard [Електронний ресурс]. – Режим доступу: https://www.pcisecuritystandards.org/

3. Spring Security Documentation [Електронний ресурс]. – Режим доступу: https://spring.io/projects/spring-security

ЗАСТОСУВАННЯ OAUTH2 І JWT ДЛЯ ПІДВИЩЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У ВЕБ-СЕРВІСІ

Макаров А. Д.

Державний університет інформаційно-комунікаційних технологій, м. Київ

У сучасних інформаційних системах особливу увагу приділяють питанню інформаційної безпеки. Зростання кількості кіберзагроз вимагає від розробників впровадження перевірених рішень для автентифікації та авторизації користувачів. Особливо це важливо для сервісів, які взаємодіють із персональними даними або виконують індивідуалізовану логіку відповідно до прав доступу. Застосування таких механізмів, як OAuth2 та JSON Web Token (JWT), дозволяє ефективно вирішити ці завдання та забезпечити контрольований доступ до функціоналу програмного забезпечення [1-3].

У рамках дослідження поставлено завдання реалізувати інтеграцію з протоколом OAuth2, забезпечити генерацію та перевірку токенів у форматі JWT, а також організувати розмежування прав доступу до ресурсів залежно від ролі користувача. Також передбачено створення відповідних сервісів та фільтрів безпеки, які будуть інтегровані в архітектуру бекенду та не впливатимуть на бізнес-логіку застосунку.

Метою роботи є впровадження сучасного механізму автентифікації та авторизації користувачів у веб-застосунку з урахуванням вимог масштабованості та розширюваності системи.

У рамках проведеного дослідження було успішно реалізовано інтеграцію механізмів автентифікації та авторизації за допомогою протоколу OAuth2 та технології JWT. Ці рішення забезпечують надійний та масштабований підхід до управління доступом в сучасних веб-застосунках. Завдяки використанню OAuth2 та JWT вдалося реалізувати централізовану перевірку доступу, знизити навантаження на базу даних та підвищити безпеку системи в цілому [4].

Схема алгоритму автентифікації, що зображена на рис. 1, ілюструє, яким чином обробляється запит з токеном у форматі JWT. Після надходження HTTP-запиту BearerTokenAuthenticationFilter вилучає токен із заголовку та створює об'єкт BearerTokenAuthenticationToken, який передається до AuthenticationManager для подальшої обробки. Менеджер автентифікації делегує перевірку до JwtAuthenticationProvider, що, у свою чергу, використовує JwtDecoder для валідації токена. Після успішної перевірки токен обробляється за допомогою JwtAuthenticationConverter, який створює об'єкт JwtAuthenticationToken з інформацією про користувача та його повноваженнями. У разі успішної автентифікації інформація про користувача заноситься у SecurityContextHolder, що дозволяє продовжити виконання програми з урахуванням отриманих прав доступу. У випадку невдачі ініціюється обробка помилки через AuthenticationFailureHandler, що забезпечує безпечну реакцію системи на неавторизовані спроби доступу [4].

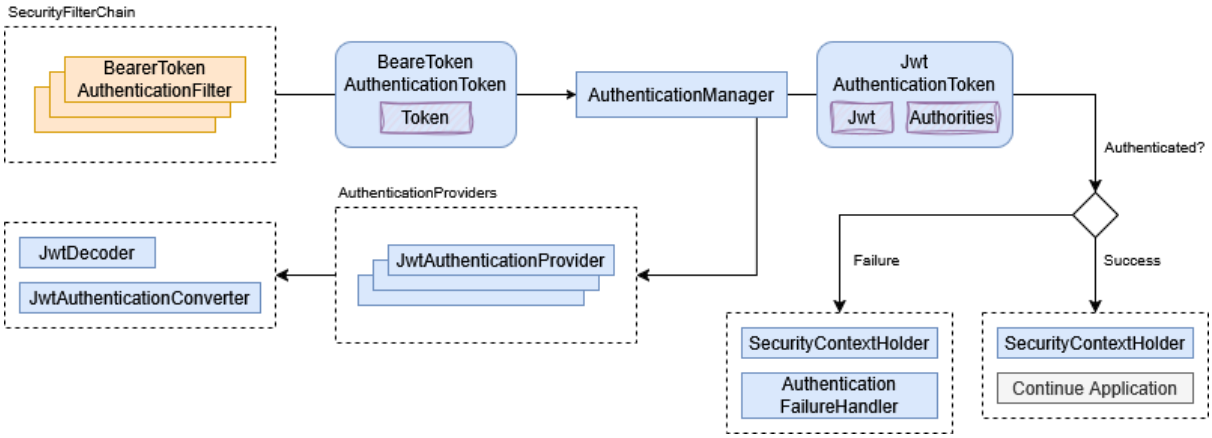


Рис. 1. Автентифікація за допомогою JWT

Розмежування прав доступу через механізм ролей, що базуються на даних у JWT, дозволяє гнучко контролювати доступ до різних частин системи, забезпечуючи високий рівень захисту від несанкціонованого доступу. Важливим результатом є також забезпечення масштабованості та

розширюваності архітектури, що дозволяє легко інтегрувати нові компоненти або сервіси авторизації без необхідності змін у бізнес-логіці.

Однак, незважаючи на досягнуті результати, є кілька напрямків, які можуть бути предметом подальших досліджень та розвитку. Одним із таких напрямків є вдосконалення механізмів обміну токенами для підвищення рівня безпеки. Крім того, для покращення зручності користувачів можна розглянути впровадження механізмів автоматичного поновлення токенів та впровадження підтримки багатофакторної автентифікації.

ДЖЕРЕЛА

1. Jones M., Bradley J., Sakimura N. (2015). RFC 7519: JSON Web Token (JWT). RFC Editor, USA. URL: https://doi.org/10.17487/rfc7519.

2. Jones, M., Campbell, B. and Mortimore, C. (2015) JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants. International Journal of Computer Security Applications, 6, 4-5. https://doi.org/10.17487/RFC7523.

3. The oauth 2.0 authorization framework / ed. by D. Hardt. RFC Editor, 2012. URL: https://doi.org/10.17487/rfc6749.

4. OAuth 2.0 resource server JWT: spring security. Spring Documentation. URL: https://docs.spring.io/spring-security/reference/servlet/oauth2/resource-server/jwt.html

ПОРІВНЯННЯ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ В СИСТЕМАХ УПРАВЛІННЯ ПРОЄКТАМИ ПРИ ХМАРНОМУ ТА ЛОКАЛЬНОМУ РОЗГОРТАННІ

Максименко Д. С.

Державний університет інформаційно-комунікаційних технологій, м. Київ

Через стрімкий розвиток ринку веб-сервісів при виборі засобів для автоматизації роботи над проєктами перед керівниками постає вибір між використанням зовнішніх застосунків, націлених на широкий ринок, зовнішніх застосунків, націлених на корпоративний сектор з персональною службою підтримки та додаткових сервісів, та локальним рішеннями, розробленими в середині компанії. Особливо гостро це питання постає, коли компанія, в якій проводиться проєкт, приділяє додаткову увагу безпеці інформації та намагається віднайти баланс між вартістю та власними потребами.

Метою цього дослідження, є проведення порівняльної характеристики засобів захисту інформації в хмарному та локальному середовищах [1], щоб спростити процес вибору оптимально рішення для створення системи керування проєктами.

Таблиця 1 представляє відповідні засоби захисту інформації для хмарного та локального способу розгортання.

Таблиця 1

Порівняльний аналіз хмарного та локального способу розгортання

Критерій	Локальне розгортання	Хмарне розгортання
Контроль доступу та автентифікація	Локальне управління доступом через внутрішні каталоги користувачів (AD, LDAP). + Повний контроль над системою прав доступу. - Висока вартість налаштування та підтримки, ризик людських помилок.	Управління доступом через хмарні IAM-системи із можливістю масштабованого SSO/MFA. + Швидке налаштування, інтеграція з різними сервісами. - Залежність від безпеки хмарної платформи, ризик неправильної конфігурації.
Шифрування даних	Локальне шифрування на рівні дисків і БД із зберіганням ключів на локальних серверах. + Повний контроль над ключами. - Високі вимоги до безпеки ключів, ризик втрати.	Використання керованих сервісів шифрування із підтримкою BYOK [2]. + Спрощене управління шифруванням, автоматизація процесів. - Обмежений контроль над фізичними носіями даних.
Моніторинг та аудит	Впровадження внутрішніх SIEM-систем та збереження подій на власних серверах. + Повна адаптація під вимоги бізнесу. - Потреба в окремих ресурсах та високій експертизі.	Використання хмарних систем моніторингу подій із вбудованою аналітикою загроз. + Миттєва доступність, аналітика на основі великих даних. - Вартість та обмеження у видимості подій.
Резервне копіювання та відновлення	Організація власних сценаріїв резервного копіювання та планів відновлення. + Повний контроль над процедурами DPR. - Складність налаштування, необхідність тестування.	Використання хмарних DRaaS сервісів. + Автоматизовані резервні копії та відновлення. - Залежність від третьої сторони та SLA.
Управління інцидентами	Внутрішня процедура виявлення, аналізу та реагування на інциденти. + Гнучкість та відповідність специфіці організації. - Високі вимоги до навчання персоналу та підтримки систем.	Інтеграція з хмарними сервісами SOC і автоматичне реагування. + Швидке виявлення та реагування на загрози. - Менший вплив на глибину аналізу та деталізацію відповідей.

Результати даного порівняння допоможуть визначитися з адекватністю засобів та підходів до забезпечення безпеки у систему керування відповідно до вимог конкретного проєкту та організації.

ДЖЕРЕЛА

1. Maria, Amia, and Dr Bhuvana J. «Hybrid Cloud Solutions: Bridging On-Premises and Cloud Infrastructure.» *International Journal of Research Publication and Reviews* 5, no. 3 (March 9, 2024): 4052–56. http://dx.doi.org/10.55248/gengpi.5.0324.0789.

2. Cloud storage architecture: issues, challenges and opportunities / S. B. Bajaj et al. International journal of innovative research in computer science & technology. 2021. Vol. 9, no. 3. URL: https://doi.org/10.21276/ijircst.2021.9.3.12.

ЗАХИСТ ІНФОРМАЦІЇ У WEB-ЗАСТОСУНКУ УПРАВЛІННЯ ІТ-ПРОЄКТАМИ ЗА МЕТОДОЛОГІЮ KANBAN З ВИКОРИСТАННЯМ МЕХАНІЗМІВ ГЕЙМІФІКАЦІЇ

Малінський Д. В.

Державний університет інформаційно-комунікаційних технологій, м. Київ

Зручність та позитивні трансформації, які принесли WEB-застосунки, є поворотнім моментом у сфері інформаційних технологій, але, на превеликий жаль, також WEB-застосунки принесли з собою кіберінциденти, найчастіше маються на увазі кібератаки, які відбуваються кожного дня на різні WEB-ресурси. Такі кібератаки можуть призводити до недоступності WEB-застосунку, витоків даних або втрат даних [1]. Тому захист інформації є одним із найважливіших напрямків у сфері інформаційних технологій.

Дане дослідження присвячено проблемі захисту інформації у розроблюваному WEB-застосунку для управління ІТ-проєктами. В такому застосунку працюють команди розробників, для комунікації вони вказують свої персональні дані (електронна пошта, номер телефону та ім’я користувача). Витік персональних даних становить значну загрозу інформаційній безпеці та може мати далекосяжні наслідки для суб'єктів даних і контролерів інформації. Також треба зазначити, що під час керуванням процесами проєкту важливо забезпечити безпеку даних проєкту, бо якщо зловмисник отримає дані акаунту адміністратора чи доступ до керування дошкою процесів, то він може поламати хід виконання спринту командою або закинути у прикріплені файли задач файли із вірусами.

Через вище перелічені причини WEB-застосунок потребує проведення аналізу щодо можливих безпекових дій для захисту даних.

Розглянемо, як користувач спілкується із застосунком. Користувач спілкується за допомогою запитів REST API [2]. В REST API зв'язок здійснюється по протоколу HTTP. Для більш чіткого розуміння схему взаємодії зображено на рис. 1.

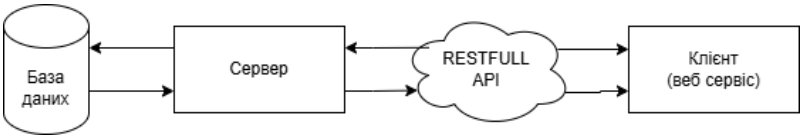


Рис. 1 Діаграма взаємозв'язку

Під час роботи із REST API необхідно також забезпечувати безпеку на рівнях доступу до API та на рівні доступу до застосунку.

Для забезпечення безпеки у WEB-застосунку були реалізовані наступні заходи відповідно до рекомендацій щодо захисту доступу до API та до самого застосунку [3]:

На рівні доступу до API:

1. Впроваджено контроль доступу шляхом автентифікації користувачів.
2. Здійснено обмеження використання клієнтами API до мінімально необхідного функціоналу, відповідно до ролі користувача.

На рівні доступу до застосунку:

1. Реалізовано перевірку запитів на відповідність специфікації API.
2. У заголовках HTTP не передається конфіденційна інформація.

Також слід зауважити, що інформацію користувача необхідно зберігати в захешованому вигляді. В даній роботі застосовується хешування по відношенню до паролю. У мові програмування C# для хешування використовується метод HashPassword класу Crypto.

ДЖЕРЕЛА

1. Бондаренко О., Ушкаленко І. (2017). Безпека web-додатків: актуальні проблеми та їх аналіз. *Формування ринкової економіки в Україні*. Вип. 38., 28-36.

2. Холл І. Підручник із веб-служб RESTful: що таке REST API із прикладом. – [Електронний ресурс]. – Режим доступу: https://www.guru99.com/uk/restful-web-services.html

3. Thevarmannil M. A Comprehensive Guide to What is REST API Security (2024). – [Електронний ресурс]. – Режим доступу: https://www.practical-devsecops.com/what-is-rest-api-security/

ЗАХИСТ ІНФОРМАЦІЇ У МОБІЛЬНІЙ ГРІ

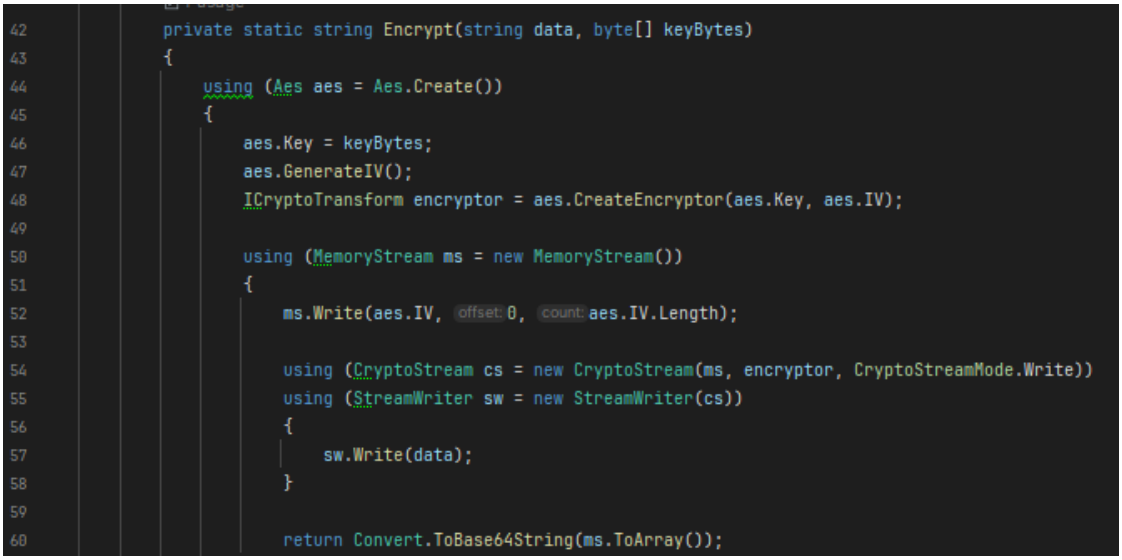
Марковський О. П.
Державний університет інформаційно-комунікаційних технологій, м. Київ

У сучасному ігровому середовищі, особливо на мобільних платформах, зберігання та передача даних гравця має велике значення. В останні роки збільшилася кількість спроб несанкціонованого доступу до внутрішніх файлів гри, що може призвести до модифікації прогресу, підробки внутрішньоігрової валюти або обходу систем монетизації. З цієї причини надзвичайно актуальним стає питання безпеки даних.

Найбільш уразливими є ігри, які зберігають прогрес користувача локально – у вигляді .json-файлів або PlayerPrefs. Через те, що відкриті дані легко редагуються сторонніми програмами, розробники шукають способи їхнього шифрування та зв'язування з пристроєм користувача.

У представленому дослідженні реалізовано систему шифрування та дешифрування збережених даних, яка базується на використанні AES-алгоритму з динамічно згенерованим ключем, сформованим на основі унікального DeviceID та індивідуального ключа гри. Завдяки цій системі збережені дані прив'язуються до конкретного пристрою, що значною мірою перешкоджає їх несанкціонованій зміні або перенесенню.

Збереження ігрових даних здійснюється у форматі JSON. Це дозволяє зручно структурувати інформацію про прогрес, інвентар, налаштування тощо. Перед записом JSON-файл проходить етап шифрування, а при зчитуванні – дешифрується назад у зручний для обробки формат. Код шифрування враховує оптимальність на мобільних пристроях та незначний вплив на продуктивність. На рис. 1 представлена реалізація шифрування JSON-файлу у Unity, на рис.2 – реалізація дешифрування та завантаження збереження [1-2].



```
42          private static string Encrypt(string data, byte[] keyBytes)
43          {
44              using (Aes aes = Aes.Create())
45              {
46                  aes.Key = keyBytes;
47                  aes.GenerateIV();
48                  ICryptoTransform encryptor = aes.CreateEncryptor(aes.Key, aes.IV);
49
50                  using (MemoryStream ms = new MemoryStream())
51                  {
52                      ms.Write(aes.IV, offset: 0, count: aes.IV.Length);
53
54                      using (CryptoStream cs = new CryptoStream(ms, encryptor, CryptoStreamMode.Write))
55                      using (StreamWriter sw = new StreamWriter(cs))
56                      {
57                          sw.Write(data);
58                      }
59
60                      return Convert.ToBase64String(ms.ToArray());
```

Рис. 1. Реалізація шифрування JSON-файлу у Unity

```
65      private static string Decrypt(string data, byte[] keyBytes)
66      {
67          byte[] cipherData = Convert.FromBase64String(data);
68
69          using (Aes aes = Aes.Create())
70          {
71              byte[] iv = new byte[aes.BlockSize / 8];
72              byte[] cipherBytes = new byte[cipherData.Length - iv.Length];
73
74              Array.Copy( sourceArray: cipherData,  destinationArray: iv, iv.Length);
75              Array.Copy( sourceArray: cipherData,  sourceIndex: iv.Length,  destinationArray: cipherBytes,  destinationIndex: 0, cipherBytes.Length);
76
77              aes.Key = keyBytes;
78              aes.IV = iv;
79              ICryptoTransform decryptor = aes.CreateDecryptor(aes.Key, aes.IV);
80
81              using (MemoryStream ms = new MemoryStream(cipherBytes))
82              using (CryptoStream cs = new CryptoStream(ms, decryptor, CryptoStreamMode.Read))
83              using (StreamReader sr = new StreamReader(cs))
84              {
85                  return sr.ReadToEnd();
86              }
```

Рис. 2. Дешифрування та завантаження збереження

Отже, застосування шифрування в мобільній грі дозволяє не лише захистити дані гравця від зовнішнього втручання, а й підвищити рівень довіри до проєкту, особливо при використанні внутрішньоігрової економіки. У наступних версіях планується реалізація онлайн-синхронізації з хешуванням даних та валідацією на сервері.

ДЖЕРЕЛА

1. Unity. URL: https://unity.com/
2. Unity Documentation: https://docs.unity3d.com/ScriptReference

ПРОГНОЗУВАННЯ КІБЕРІНЦИДЕНТІВ У SIEM-СИСТЕМІ НА ОСНОВІ ТЕОРІЇ КАТАСТРОФ

Негоденко В. П., Шевченко С. В., Негоденко О. В.
Київський столичний університет імені Бориса Грінченка, м. Київ

Сучасний кіберпростір вимагає щоденного моніторингу кіберінцидентів: від атак низького рівня до технологічно складних. Захист інформації потребує потужної та стійкої системи управління інформаційної безпеки, яка забезпечить прогнозування, виявлення та запобігання кіберінцидентам. На сьогодні існує платформа SIEM (security information and event management), яка збирає, агрегує та аналізує великі обсяги даних з програм, пристроїв, серверів та користувачів усієї організації в режимі реального часу. Об'єднуючи цей величезний масив даних в єдину уніфіковану платформу, рішення SIEM забезпечують комплексне уявлення про стан безпеки організації, надаючи центрам операцій безпеки (SOC) можливість швидко та ефективно виявляти, розслідувати та реагувати на інциденти безпеки. Рішення SIEM дозволяють: отримати уявлення про стан безпеки шляхом централізації та аналізу даних з різних джерел; виявляти та ідентифікувати потенційні

порушення безпеки та загрози в режимі реального часу, мінімізуючи ризик компрометації; ефективно розслідувати та сортувати інциденти безпеки, скорочуючи час та ресурси, необхідні для їх вирішення [1].

Функціональність SIEM-системи має також недоліки, які можливо запобігти шляхом імплементації блоку з використанням теорії катастроф [2]. Дані недоліки та шляхи їх вирішення із застосуванням теорії катастроф наведено в таблиці 1.

Таблиця 1

Переваги застосування теорії катастроф у SIEM-системі

Основні недоліки SIEM-системи	Шляхи вирішення із застосуванням теорії катастроф
Реагує після того, як подія вже сталася	Прогнозування критичних точок переходу (нестабільність → збій)
Прописані правила дії (rule-based)	Системи описують динамічні **стани**, які не працюють по правилам
Система перевантажена подіями, важко знайти справжню загрозу	Виявлення **критичних станів**, а не окремі події
SIEM не фіксує накопичення подій	Аналіз **динамічних змін стану системи** у часі
Атаки часто складні (APT, ланцюжки), не має повної картини	Опис **системної поведінки**, а не окремі компоненти
Стандартна кореляція слабка при нетипових атаках	Різні типи моделі теорії катастроф дозволяють **аналізувати критичні точки**
Не має прогнозу розвиток подій	**Прогнозування критичних станів в системі**

Проведено аналіз наукових джерел математичної основи теорії катастроф в роботі [3]. Практичне застосовування теорії катастроф на Python із використанням реальних даних про кіберінциденти за 2020 – 2024 роки представлено в роботі [4].

На основі проведеного дослідження щодо застосування математичної теорії катастроф розроблено алгоритм виявлення порушення станів стійкості SIEM-системи для прогнозування дії кіберінцидентів на інформаційну систему, шляхом вчасної дії на витік даних в режимі реального часу, що дозволяє вчасно реагувати і забезпечити стійкість рівня безпеки системи (рис. 1).

Застосування даного алгоритму дозволить реагувати на кіберінциденти в режимі реального часу і реагувати на стійкість інформаційної системи.

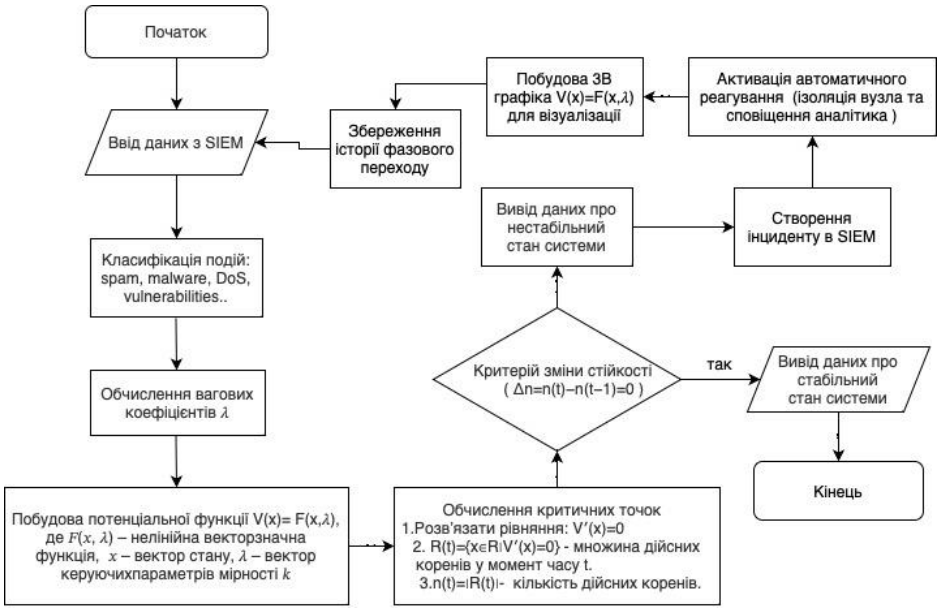


Рис.1 Схема алгоритму виявлення нестабільних станів системи із SIEM та теорії катастроф

ДЖЕРЕЛА

1. González-Granadillo, G. González-Zarzosa, S. Diaz, R. Security Information and Event Management (SIEM): Analysis,Trends, and Usage in CriticalInfrastructures. Sensors 2021, 21, 4759.

2. Субач І.Ю., Власенко О.В. Архітектура інтелектуальної SIEM-системи для виявлення кіберінцидентів у базах даних інформаційно-комунікаційних систем військового призначенняю // Системи і технології зв'язку, інформатизації та кібербезпеки. ВІТІ. 2023. No 4. С. 82 – 92.

3. Shevchenko, S., Zhdanova, Y., Spasiteleva, S. (2023). Mathematical methods in cybersecurity: catastrophe theory. Cybersecurity Education Science Technique, 3(19), 165-175. DOI:10.28925/2663-4023.2023.19.165175

4. Негоденко В. Застосування математичної теорії катастроф для забезпечення стійкості системи управління інформаційною безпекою // Кібербезпека: освіта, наука, техніка. 2024, №2(26). 212 – 222.

ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ КОНФЛІКТНОЇ ВЗАЄМОДІЇ ІНФОРМАТИВНИХ І ЗАВАДОВИХ РАДІОСИГНАЛІВ

Новицький А. А.

Київський столичний університет імені Бориса Грінченка, м. Київ

Військові конфлікти XXI століття характеризуються застосуванням широкого спектру радіоелектронних систем: засобів зв'язку; радіотехнічних комплексів та радіолокаційних станцій; приймачів супутникових радіонавігаційних систем; засобів технічної розвідки та

радіоелектронної боротьби. Конфліктна взаємодія між інформаційними та завадовими радіосигналами становить значну загрозу для стабільного функціонування цих систем [1]. При цьому спостерігається розширення переліку задач від традиційного подавлення систем управління і зв’язку противника до подавлення систем навігації, стільникового зв’язку та інших систем, що функціонують в електромагнітному спектрі. Імітаційне моделювання є важливим інструментом для аналізу, розуміння та прогнозування наслідків конфліктної взаємодії завад і корисного сигналу як для захисту власних, так і для знешкодження ворожих безпілотних систем. Завдання подавлення радіоліній «наземний пункт керування – БпЛА» і «БпЛА – наземний пункт керування» фактично зводиться до задачі формування на вході приймача засобу зв'язку такого значення відношення сигнал-шум, яке не дозволяє забезпечити прийом даних з необхідною достовірністю. Така задача є класичною в теорії радіоелектронного подавлення, а особливістю її рішення стосовно БпЛА є врахування типів сигнально-кодових конструкцій, що використовуються в радіолініях, а також сигнальних, енергетичних, просторових та інших параметрів радіоліній. Існуючі підходи до моделювання включають математичні, імітаційні, стохастичні та детерміновані моделі, а також гібридне моделювання [2]. Кожен з підходів має свої переваги, недоліки та обмеження у симулюванні конфлікту радіосигналів.

Метою дослідження є знаходження шляхом імітаційного моделювання параметрів завадових сигналів, здатних забезпечити максимально можливу руйнацію інформативних параметрів корисного сигналу, і, як результат, створення протидії функціонуванню ворожих БпЛА. Особливістю запропонованої імітаційної моделі є її гібридний характер: вона поєднує детерміноване моделювання каналу поширення радіохвиль зі стохастичними елементами для врахування динамічної поведінки завадових сигналів та випадкових шумів. Успішним прикладом застосування імітаційного моделювання конфліктної взаємодії радіосигналів є визначення параметрів ефективних завадових захисних сигналів, здатних забезпечити руйнування інформативних параметрів небезпечних сигналів високочастотного нав’язування на основній частоті та комбінаційних гармоніках зондуючого сигналу, що дозволило сформулювати базові рекомендації щодо формування захисних сигналів на об’єктах інформаційної діяльності [3].

Запропонована імітаційна модель має модульну структуру, що включає генератори інформаційних та завадових сигналів з можливістю налаштування параметрів сигналів. Для моделювання поширення радіохвиль використовується детермінований підхід, що враховує характеристики навколишнього середовища за допомогою змінних середовища (числові параметри). Стохастичний компонент моделює випадкові шуми та зміни в завадових сигналах. Унікальність моделі

полягає у можливості імітації різних типів завад. Модель реалізовано за допомогою використання мови програмування «Python» із застосуванням бібліотек «NumPy» та «SciPy». Вибір інструментарію зумовлено зручністю для точних наукових обчислень та симуляції сигналів, що продемонстровано дослідженням «PyLayers», які показали гнучкість й обчислювану ефективність Python-екосистеми для моделювання радіохвильових каналів [4].

Розроблена імітаційна модель не вимагає постановки фізичного експерименту, що робить її унікальним фінансово вигідним інструментом для дослідження конфліктної взаємодії інформативних та завадових радіосигналів.

Перспективним напрямком розвитку технологій радіоподавлення є спрямованість на зменшення або спотворення інформативних параметрів корисних сигналів.

ДЖЕРЕЛА

1. Astapenya V., Zhdanova Y., Shevchenko S., Spasiteleva S., Kryvoruchko O. (2024) *Conflict Model of Radio Engineering Systems under the Threat of Electronic Warfare* Proceedings of the Workshop Cybersecurity Providing in Information and Telecommunication Systems (CPITS 2024), 3654. c. 290-300. ISSN 1613-0073

2. Ozge Kaya, Ali N. M. Ibrahim, et al. Characterizing Indoor Wireless Channels via Ray Tracing Combined with Stochastic Modeling // IEEE Transactions on Wireless Communications. – 2009. – Vol. 8, No. 8. – P. 4144-4154.

3. Крючкова Л., Цмоканич І., Вовк М. Удосконалений метод захисту конфіденційної інформації від перехоплення методами високочастотного нав’язування // Computer Systems and Information Technologies, 2021, №3, с. 14–20.

4. Amiot N., Laaraiedh M., Uguen B. PyLayers: An Open-Source Dynamic Simulator for Indoor Propagation and Localization. In: IEEE ICC Workshops. Budapest, 2013. P. 327-332.

БЕЗСЕСІЙНА АВТЕНТИФІКАЦІЯ НА ОСНОВІ JWT-ТОКЕНІВ У МІКРОСЕРВІСНІЙ АРХІТЕКТУРІ

Олаба Д. Р.

Державний університет інформаційно-комунікаційних технологій, м. Київ

При стрімкому розвитку мікросервісної архітектури питання ефективної та безпечної автентифікації користувачів набуває особливої актуальності. Традиційні сесійні механізми, що базуються на зберіганні стану сесії на сервері або на фронт частині, демонструють суттєві

обмеження при масштабуванні систем та розподіленій обробці запитів. Безсесійна автентифікація з використанням JSON Web Token (JWT) пропонує альтернативний підхід, що усуває ці обмеження та створює передумови для побудови високопродуктивних систем контролю доступу.

JWT-токени – це компактний, самодостатній формат для передачі інформації між сторонами у вигляді JSON-об'єкта [1]. Структурно JWT складається з трьох частин: заголовка (header), корисного навантаження (payload) та підпису (signature). Заголовок містить інформацію про тип токена та алгоритм шифрування; корисне навантаження включає твердження про сутність (користувача) та метадані; підпис забезпечує цілісність даних та верифікацію джерела.

У контексті мікросервісної архітектури застосовується двокомпонентний механізм автентифікації з використанням access та refresh токенів. Access-токен має короткий термін життя (зазвичай 15-60 хвилин) та містить інформацію про користувача, його роль та доступні додатки. Цей токен використовується для авторизації запитів до захищених ресурсів. Refresh-токен має значно довший термін життя (від кількох годин до декількох днів) та призначений виключно для отримання нового access-токена без необхідності повторної автентифікації користувача [2].

Важливим аспектом безпеки є спосіб зберігання та передачі токенів. В сучасних системах, таких як Access Guard, підтримуються два основні підходи: зберігання у HTTP-заголовках (Authorization Bearer) та у HTTP-only cookies. Перший підхід зручний для API-орієнтованих клієнтів, тоді як другий забезпечує додатковий захист від XSS-атак для веб-додатків. При використанні cookie-підходу токени зберігаються з атрибутами HttpOnly, Secure та SameSite, що значно ускладнює їх викрадення зловмисниками [3].

Процес автентифікації у мікросервісній архітектурі є складним механізмом забезпечення безпечного доступу користувачів до розподілених інформаційних систем. Він включає наступні етапи:

Користувач надає облікові дані сервісу безпеки.

Сервіс верифікує облікові дані та генерує пару токенів з індивідуальними налаштуваннями терміну дії.

Токени передаються клієнту через заголовки або зберігаються у захищених cookies.

При запитах до захищених ресурсів система спочатку перевіряє наявність токенів у cookies, а потім у заголовках.

При закінченні терміну дії access-токена відбувається автоматичне оновлення через механізм refresh-токенів.

Сучасні реалізації, такі як Access Guard, надають можливість гнучкого налаштування параметрів токенів для кожного користувача. Наприклад, адміністратори можуть встановлювати індивідуальну

тривалість життя токенів, обмежувати кількість одночасних сесій та налаштовувати автоматичне видалення найстаріших сесій при перевищенні ліміту.

Додатковий рівень безпеки забезпечується шляхом збереження всіх refresh-токенів у базі даних з можливістю їх примусового відкликання у разі компрометації облікових даних. Також впроваджуються механізми ротації ключів підпису та захист від replay-атак шляхом включення у токен унікальних ідентифікаторів.

Отже, безсесійна автентифікація на основі JWT-токенів із правильно налаштованою системою access та refresh токенів забезпечує оптимальний баланс між безпекою та зручністю у мікросервісних архітектурах. Даний підхід дозволяє досягти високої масштабованості, відмовостійкості та продуктивності систем контролю доступу, одночасно зберігаючи необхідний рівень захисту інформації.

ДЖЕРЕЛА

1. Jones M., Bradley J., Sakimura N. JSON Web Token (JWT). RFC 7519, IETF, 2015. URL: https://tools.ietf.org/html/rfc7519

2. Auth0. JWT Authentication: JSON Web Tokens. Auth0 Inc., 2023. URL: https://auth0.com/docs/secure/tokens/json-web-tokens

3. OWASP. JSON Web Token Security Cheat Sheet. OWASP Foundation, 2023. URL: https://cheatsheetseries.owasp.org/cheatsheets/JSON_Web_Token_for_Java_Cheat_Sheet.html

УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ ПРИСТРОЇВ ЯК ДОДАТКОВИЙ РІВЕНЬ ЗАХИСТУ КОРПОРАТИВНИХ СИСТЕМ

Олаба Д. Р.

Державний університет інформаційно-комунікаційних технологій, м. Київ

У сучасному корпоративному середовищі, де співробітники використовують численні додатки та сервіси, традиційні методи автентифікації створюють значні виклики як для безпеки, так і для зручності користування. Кожна нова точка автентифікації збільшує ризик компрометації облікових даних та знижує продуктивність через необхідність багаторазового введення паролів. Управління ідентифікацією пристроїв (Device Identity Management) пропонує інноваційний підхід до вирішення цієї дилеми, створюючи додатковий рівень захисту корпоративних систем.

Концепція управління ідентифікацією пристроїв базується на принципі, що певний фізичний пристрій може виступати як фактор

автентифікації поряд із традиційними обліковими даними користувача [1]. Це особливо актуально в контексті мобільних пристроїв, які зазвичай мають вбудовані механізми захисту (біометрія, PIN-код, шаблон розблокування) та рідко передаються іншим особам.

Для реалізації управління ідентифікацією пристроїв у мікросервісній архітектурі було розроблено систему Access Guard, яка забезпечує універсальний механізм аутентифікації для всієї екосистеми корпоративних додатків. Ключова особливість цієї системи полягає в тому, що користувачу достатньо автентифікуватися лише один раз на своєму пристрої, після чого всі корпоративні додатки отримують доступ автоматично без необхідності повторного введення облікових даних [2].

Процес управління ідентифікацією пристроїв в системі Access Guard включає кілька етапів:

1. Первинна реєстрація пристрою, під час якої генерується унікальний deviceId, що зберігається в захищеному сховищі на пристрої.
2. Прив'язка пристрою до облікового запису користувача в системі Access Guard.
3. Автентифікація користувача через пароль та/або біометрію на пристрої.
4. Отримання єдиного refresh-токена, який зберігається в захищеному сховищі пристрою.
5. Автоматичне використання цього токена для доступу до всіх корпоративних додатків.

Важливим аспектом безпеки є примусова періодична переідентифікація. Система налаштована таким чином, що раз на тиждень користувач повинен підтвердити свою особу через введення пароля в одному з корпоративних додатків. Після успішної переідентифікація оновлюється refresh-токен, який потім поширюється на всі інші додатки екосистеми [3]. У дослідженні було здійснено порівняльний аналіз традиційного підходу та підходу з управлінням ідентифікацією пристроїв (таблиця 1).

Таблиця 1

Порівняння традиційного підходу та підходу з управлінням ідентифікацією пристроїв

Характеристика	**Традиційний підхід**	**Управління ідентифікацією пристроїв**
Частота автентифікації	Для кожного додатка окремо	Одноразово для всіх додатків
Ризик витоку облікових даних	Високий (численні точки введення)	Низький (централізований контроль)

Характеристика	Традиційний підхід	Управління ідентифікацією пристроїв
Зручність використання	Низька (потребує багаторазового введення)	Висока (безшовний доступ)
Рівні захисту	Єдиний (логін/пароль)	Багаторівневий (пристрій + облікові дані)
Можливість відкликання доступу	Складна (потребує зміни паролів)	Проста (централізоване відкликання)
Підтримка періодичної перевірки	Обмежена	Вбудована
Вразливість до фішингу	Висока	Значно нижча

Впровадження управління ідентифікацією пристроїв через систему Access Guard демонструє важливий крок у розвитку корпоративних систем безпеки, поєднуючи високий рівень захисту з покращеним користувацьким досвідом.

ДЖЕРЕЛА

1. Gupta B., Agrawal D., Yamaguchi S. Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security. IGI Global, 2023. 524 p.
2. Ometov A., Bezzateev S., Mäkitalo N. Multi-Factor Authentication: A Survey. Cryptography, 2022. Vol. 4(1). P. 1-31.
3. NIST. Digital Identity Guidelines: Authentication and Lifecycle Management. NIST Special Publication 800-63B, 2023. URL: https://pages.nist.gov/800-63-3/sp800-63b.html

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ У ПРОГРАМНОМУ ПРОДУКТІ «ІНТЕЛЕКТУАЛЬНИЙ AI-АСИСТЕНТ ДЛЯ АВТОМАТИЗОВАНОЇ ВЗАЄМОДІЇ З КОРИСТУВАЧАМИ INSTAGRAM»

Остапенко А. С., Худік Б. О.
Державний університет інформаційно-комунікаційних технологій, м. Київ

У сучасну епоху стрімкого розвитку інформаційних технологій та цифрової комунікації забезпечення безпеки даних набуває першочергового

значення. Програмний продукт, розроблений для автоматизованої взаємодії з користувачами Instagram, обробляє конфіденційну інформацію: дані автентифікації, текстові повідомлення, історію взаємодій та особисті налаштування користувачів. Невідповідна реалізація заходів безпеки може призвести до витоків інформації, несанкціонованого доступу та зловживань, що негативно впливає на репутацію компанії та порушує законодавчі вимоги щодо захисту персональних даних [1; 2].

Метою даної доповіді є розробка та впровадження заходів для забезпечення конфіденційності, цілісності та доступності інформації у програмному продукті «Інтелектуальний AI-асистент для автоматизованої взаємодії з користувачами Instagram». Для досягнення цього завдання було вирішено реалізувати комплексний підхід, що включає як технологічні засоби, так і організаційні заходи.

Розробка продукту передбачає використання наступних технічних засобів і методів захисту:

1. Хешування паролів. Для збереження облікових даних застосовується алгоритм хешування з додаванням унікальної солі (наприклад, бібліотека bcrypt), що ускладнює атаки метою перебору [3].
2. 2. Використання токенів авторизації. Замість зберігання чистих паролів, система здійснює автентифікацію через токени (JWT), які мають обмежений термін дії, що забезпечує додатковий рівень захисту при несанкціонованому доступі.
3. 3. Захищене з’єднання (HTTPS). Весь обмін даними між клієнтом та сервером відбувається за допомогою протоколу HTTPS, що гарантує шифрування переданої інформації.
4. Моніторинг та аудит. Для виявлення потенційних загроз впроваджується система логування та періодичного аудиту безпеки, що дозволяє оперативно реагувати на аномалії та атаки.
5. Обмеження доступу. Рівні прав доступу, які реалізовано за методикою RBAC (Role-Based Access Control), забезпечують доступ лише до необхідних даних відповідно до ролі користувача.

Впровадження перелічених заходів забезпечило високий рівень захисту інформації у продукті. Наведені методи дозволяють уникнути витоків чутливих даних, знизити ризик несанкціонованого доступу та зменшити можливість виникнення атак типу brute-force та SQL-ін'єкцій. Окрім цього, автоматизація процесів моніторингу дозволяє оперативно виявляти і реагувати на загрози, що підвищує ефективність роботи системи та довіру користувачів.

Розроблений комплекс заходів безпеки є критично важливим для підтримки конфіденційності, цілісності та доступності даних у програмному продукті. Використання хешування з додаванням солі, токенізація авторизації, шифрування з’єднань та системний моніторинг дозволяють забезпечити високий рівень захисту інформації. Подальше

вдосконалення системи може включати впровадження багатофакторної автентифікації та регулярних аудитів, що сприятиме ще більшій стійкості продукту до сучасних кіберзагроз.

ДЖЕРЕЛА

1. Бондаренко О., Ушкаленко І. (2017). *Безпека web-додатків: актуальні проблеми та їх аналіз*. Київ: Київський університет ім. Б.Грінченка, вип. 38, с. 28–36.

2. Боскін О.О., Корніловська Н.В., Поліщук В.М., Сарафаннікова Н.В. (2023). *Безпека веб-додатків та хакерські атаки*. Вісник Херсонського національного технічного університету, №3(86), с. 83–92. https://doi.org/10.35546/kntu2078-4481.2023.3.11

3. Хешування паролів: використання солі та bcrypt. [Електронний ресурс]. Режим доступу: https://drukarnia.com.ua/articles/kheshuvannya-paroliv-vikoristannya-soli-ta-bcrypt

БЕЗПЕКА ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У ПРОЦЕСАХ ЗАМІНИ ОБЛАДНАННЯ НА ПІДПРИЄМСТВАХ ЗВ'ЯЗКУ

Пермякова О. О.

Державний університет інформаційно-комунікаційних технологій, м. Київ

Впровадження штучного інтелекту (ШІ) у процеси технічного обслуговування та заміни обладнання на підприємствах зв'язку відкриває нові можливості для автоматизації, підвищення точності прогнозування несправностей і мінімізації витрат [1]. Проте, разом з перевагами з'являються нові ризики, що пов'язані з інформаційною безпекою та захистом інфраструктури [2]. Тому важливо дослідити, як саме особливості архітектури ШІ впливають на загальний рівень захисту таких систем.

Метою даного дослідження є аналіз типових загроз, пов'язаних з використанням ШІ в процесах заміни обладнання, враховуючи різні архітектури ШІ-систем, а також визначити найбільш уразливі елементи та способи їхнього захисту.

Безпека ШІ-систем безпосередньо залежить від того, яку архітектуру вони використовують. Системи з жорстко визначеними правилами (rule-based) є найбільш передбачуваними, оскільки всі рішення ґрунтуються на заздалегідь прописаних умовах. Вони легко перевіряються та контролюються, але можуть бути неефективними в умовах, що швидко змінюються. Їхня основна небезпека – це помилки в самих правилах або несанкціонована зміна цих правил.

Моделі машинного навчання (ML), які адаптуються до нових даних, є гнучкішими, але більш уразливими до атак, пов'язаних із підміною

навчальних або вхідних даних (наприклад, data poisoning). Такі атаки можуть змінити поведінку системи без прямого втручання в її код. Особливо це небезпечно в умовах автоматизованої заміни обладнання, де рішення приймаються без участі людини.

З питань безпеки, глибокі нейронні мережі (deep learning) складні у використанні. Вони можуть досягати високої точності, але залишаються «чорними скриньками». Через свою непрозорість вони ускладнюють забезпечення безпеки та виявлення помилок. Зловмисники можуть використати особливості функціонування таких мереж для впровадження спеціально створених вхідних даних (adversarial examples), які призведуть до неправильного рішення про заміну або обслуговування техніки.

Гібридні підходи, які поєднують жорстку логіку з машинним навчанням, демонструють потенційно кращий баланс між керованістю та адаптивністю. Проте вони є складнішими в реалізації, і їхня безпека значно залежить від якості інтеграції та меж між окремими компонентами.

Для підвищення безпеки таких систем доцільно впроваджувати обмеження доступу до навчальних і робочих середовищ ШІ, вести журнал усіх змін у системі, застосовувати перевірку вхідних даних та використовувати моделі з пояснюваною логікою роботи (explainable AI), які дозволяють краще зрозуміти та контролювати прийняті рішення.

Порівняльний аналіз дозволив визначити, що вибір архітектури ШІ має суттєвий вплив на рівень інформаційної безпеки підприємств зв’язку. Найбільш перспективними є гібридні моделі, поєднані з технологіями захисту даних та прозорого аналізу. Перспективними є подальші дослідження у напрямі сертифікації безпечних моделей, розвитку підходів до прозорої аналітики та створення національних стандартів використання ШІ у критичній інфраструктурі.

ДЖЕРЕЛА

1. Sarker, I.H. AI-Based Modeling: Techniques, Applications and Research Issues Towards Automation, Intelligent and Smart Systems. SN COMPUT. SCI. 3, 158 (2022). https://doi.org/10.1007/s42979-022-01043-x.

2. Скіцько, О., Складанний, П., Ширшов, Р., Гуменюк, М., & Ворохоб, М. (2023). Загрози та ризики використання штучного інтелекту. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(22), 6–18. https://doi.org/10.28925/2663-4023.2023.22.618

ОСНОВНІ ШЛЯХИ ГАРАНТУВАННЯ БЕЗПЕКИ ДЛЯ СИСТЕМИ ІНТЕРАКТИВНОЇ ГЕНЕРАЦІЇ АУДІО-ВІЗУАЛЬНОГО КОНТЕНТУ

Погорілий О. А., Соляник Л. О.
Державний університет інформаційно-комунікаційних технологій, м. Київ

Системи інтерактивної генерації аудіо-візуального контенту все частіше використовуються в освіті, медіа, розвагах, маркетингу, а також у віртуальній та доповненій реальностях. Водночас, із розширенням їх функціональності, зростають і ризики, пов'язані з безпекою.

Гарантування безпеки цих систем є критично важливим завданням, адже воно напряму впливає на довіру користувачів, стабільність цифрового середовища та правовий захист усіх учасників інформаційної взаємодії. Дослідження ефективних шляхів захисту даних, механізмів виявлення та запобігання зловживанням такими системами набуває особливої актуальності.

Інтерактивні системи генерації контенту, які працюють у режимі реального часу, створюють потенційні уразливості для несанкціонованого доступу та маніпуляцій з даними.

Основними типами загроз є [1]:

1) несанкціонований доступ до системи;
2) викрадення або пошкодження даних;
3) атаки типу «відмова в обслуговуванні» (DoS)[2];
4) ін'єкція шкідливого коду;
5) порушення авторських прав.

Серед основних методів забезпечення безпеки можна виділити: автентифікацію та авторизацію користувачів; шифрування даних; захист від ін'єкцій шкідливого коду; захист мережевих з'єднань.

У цьому проєкті для шифрування даних з метою підтримання безпеки мережевої взаємодії використовується протокол TLS/SSL; фільтрація мережевого трафіку за допомогою брандмауера; для запобігання DoS-атакам обмежується швидкість запитів [2].

З метою реалізації заходів безпеки для системи впроваджується система моніторингу та аудиту, яка полягає в обліку всіх критичних операцій, відстеженні аномальної активності та періодичних перевірках цілісності файлів системи [3]. Схема системи моніторингу та аудиту безпеки представлена на рис. 1. З метою захисту інтелектуальної власності впроваджуються механізми цифрових водяних знаків, які вбудовуються в контент для ідентифікації джерела матеріалів.

Рис. 1. Схема системи моніторингу та аудиту безпеки

Проведений аналіз показав, що найефективнішими методами є поєднання криптографічних засобів, систем автентифікації, постійного моніторингу та аудиту безпеки. Реалізація запропонованої методики безпечного функціонування дозволяє забезпечити цілісність даних, конфіденційність інформації та захист авторських прав.

ДЖЕРЕЛА

1. OWASP Foundation. OWASP Top Ten Project [Електронний ресурс]. –Режим доступу: URL https://owasp.org/www-project-top-ten/

2. OWASP Foundation. Denial of Service Cheat Sheet [Електронний ресурс]. –Режим доступу: URL https://cheatsheetseries.owasp.org/cheatsheets/Denial_of_Service_Cheat_Sheet.html

3. NIST. Security and Privacy Controls for Information Systems and Organizations [Електронний ресурс]. –Режим доступу: URL https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

ВИКОРИСТАННЯ ПАРАМЕТРИЗОВАНИХ ЗАПИТІВ ДЛЯ ЗАХИСТУ БАЗ ДАНИХ SQL-ІН'ЄКЦІЙ

Пономаренко С.
Державний університет інформаційно-комунікаційних технологій, м. Київ

Захист даних є основою будь-якої сучасної інформаційної системи. Погано захищені бази даних доступні для зовнішніх суб'єктів, створюють серйозний ризик для власника даних і результатів діяльності, пов'язаної з даними [1]. Компрометація чи витік інформації може призвести до втрати довіри з боку користувачів, юридичних наслідків, штрафів, а іноді і до повної втрати проєкту.

В ході дослідження було визначено, що особливої уваги вимагають ті додатки, що зберігають персональні дані користувачів. У веб-застосунку для відстеження прогресу читання книг зберігаються назви книжок, нотатки, улюблені жанри - ці дані в сукупності з іншими, можуть допомогти зловмисникам ідентифікувати особу. Критично важливо забезпечити належний рівень захисту інформації, особливо при роботі з базами даних, які зберігають персональні дані користувачів [2].

Однією з найнебезпечніших загроз у веб-додатках є SQL-ін'єкції (SQL Injection) [3], через які зловмисник може змінити логіку виконання запиту, отримати несанкціонований доступ до даних або знищити вміст бази (рис. 1).

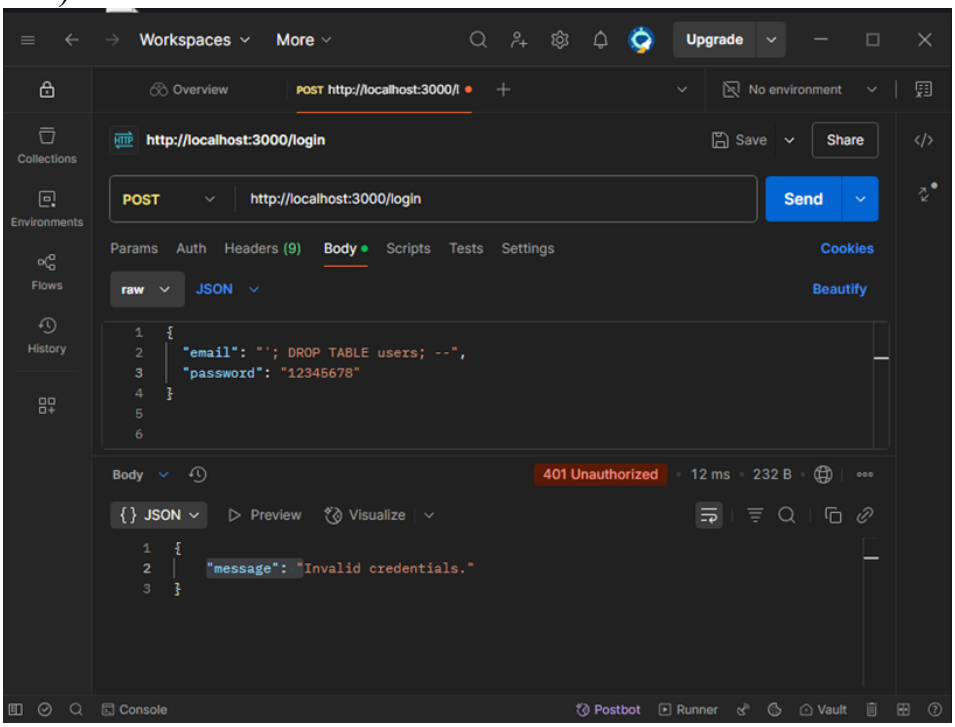


Рис.1 Тестування бази даних веб-додатку на можливість проникнення в неї зловмисників та видаленню таблиці users за допомогою DROP.

Для протидії таким загрозам у використаних середовищах Bun та SQLite при розробці веб-додатку для відстеження процесу читання книг було впроваджено підготовлені (параметризовані) запити, що унеможливлюють втручання в SQL-структуру. Також було застосовано методи .run(...), .get(...), .all(...), які реалізують параметризовані запити.

Основним захисним механізмом є використання стейкхолдерів - ? (рис.2) - у запитах. Це дозволяє відокремити SQL-код від даних, які передаються в запит - база даних автоматично підставляє значення коректно, не дозволяючи виконання таких фрагментів, як OR 1=1 або DROP TABLE.

```
db.query(`SELECT * FROM users WHERE email = ?`).get(email);
```

Рис. 2 Реалізація коду для реєстрації електронної адреси з використанням параметризованого запиту .get(...), та стейкхолдера - ? .

Результатом дослідження стало створення безпечного веб-додатку, де база даних не є уразливою до SQL-ін’єкцій. Всі критичні операції - автентифікація, реєстрація, доступ до персональних записів виконуються через захищені запити.

Таким чином, впровадження підготовлених (параметризованих) запитів дозволяє значно підвищити рівень безпеки додатку. Захист баз даних –це не лише технічна вимога, а й етичний обов’язок розробника перед користувачами свого програмного продукту.

ДЖЕРЕЛА

1. Nikiforova A., Daskevics A., Azeroual O. NoSQL security: can my data-driven decision-making be influenced from outside?. Big data and decision-making: applications and uses in the public and private sector. 2023. P. 59–73. URL: https://doi.org/10.1108/978-1-80382-551-920231005

2. Kasim Ö. An ensemble classification-based approach to detect attack level of SQL injections. Journal of information security and applications. 2021. Vol. 59. P. 102852. URL: https://doi.org/10.1016/j.jisa.2021.102852

3. Schildgen J., Rosin J. Game-based learning of SQL injections. SIGMOD/PODS '22: international conference on management of data, Philadelphia PA USA. New York, NY, USA, 2022. URL: https://doi.org/10.1145/3531072.3535321

ІНФОРМАЦІЙНА БЕЗПЕКА У WEB-ЗАСТОСУНКУ ДЛЯ МЕНЕДЖМЕНТУ КОМАНДНИХ СТУДЕНТСЬКИХ ПРОЄКТІВ

Попінако Є. О.
Державний університет інформаційно-комунікаційних технологій, м. Київ

Сучасні веб-застосунки, що працюють з персональними даними користувачів, повинні мати надійні механізми захисту. Це особливо важливо для систем, що забезпечують керування проєктами та завданнями.

Метою розробки стало впровадження ефективних рішень з автентифікації та авторизації. Для безпечного зберігання паролів використовується алгоритм хешування BCrypt, який забезпечує криптографічну стійкість і унеможливлює зворотне відновлення паролів.

Для автентифікації та авторизації інтегровано Spring Security [1] разом із JWT [2] – токенами, які створюються на сервері після входу користувача. У JWT міститься інформація про користувача, його роль, час створення та термін дії токена. Генерація токена реалізована за допомогою асиметричного шифрування RSA: підпис виконується приватним ключем, а перевірка – публічним, що зберігається на стороні ресурсу.

Усі запити до захищених ендпоінтів супроводжуються передачею токена у заголовку. Перевірку підпису виконує OAuth2 Resource Server [3], після чого додатково перевіряється наявність токена у Redis [4]. Це дозволяє відкликати токен, наприклад, під час виходу з системи, а також зменшити навантаження на базу даних. Вказані операції можна подати у вигляді схеми (рис. 1).

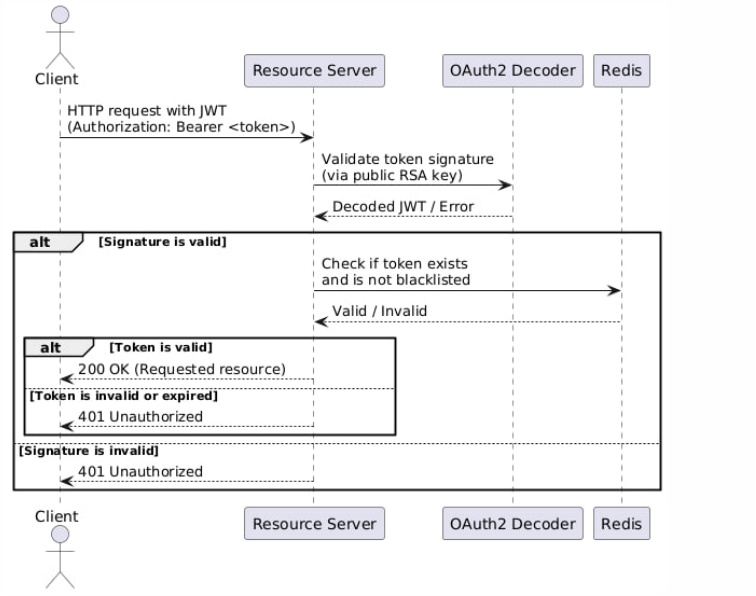


Рис. 1. Валідація токену користувача при спробі доступу на захищений ресурс

У системі реалізовано розмежування доступу: передбачено ролі адміністратора та звичайного користувача. Таким чином, кожен користувач має доступ лише до дозволених функцій відповідно до своєї ролі.

Запропоновані підходи забезпечують високий рівень безпеки, дозволяючи захистити дані користувачів. У майбутньому передбачається додати підтвердження електронної пошти для підвищення безпеки системи.

ДЖЕРЕЛА

1. Spring Security [Електронний ресурс] – Режим доступу: https://spring.io/projects/spring-security

2. JSON Web Token Introduction [Електронний ресурс] – Режим доступу: https://jwt.io/introduction

3. OAuth2 Resource Server [Електронний ресурс] – Режим доступу: https://docs.spring.io/spring-security/reference/servlet/oauth2/resource-server/index.html

4. Redis [Електронний ресурс] – Режим доступу: https://redis.io/

БЕЗПЕКА ВЕБ-ЗАСТОСУНКУ ДЛЯ ІНТЕГРАЦІЇ ПРОЦЕСІВ ІНВЕНТАРИЗАЦІЇ ТА УПРАВЛІННЯ ТЕХНІЧНИМИ ЗАСОБАМИ КОМПАНІЇ З ВИКОРИСТАННЯМ ФРЕЙМВОРКІВ VUE.JS ТА LARAVEL

Приліпко Д. М.

Державний університет інформаційно-комунікаційних технологій, м. Київ

Інформаційні технології, надаючи численні переваги у зручності та швидкості обробки даних, водночас створюють нові виклики в контексті безпеки інформації. Зокрема, питання захисту даних в системах обліку та інвентаризації технічних засобів компаній стає особливо актуальним в умовах цифровізації бізнес-процесів.

Наше дослідження присвячене розробці веб-застосунку для інтеграції процесів інвентаризації та управління технічними засобами компанії із використанням сучасних фреймворків Vue.js та Laravel. Такий веб-застосунок обробляє велику кількість чутливих даних: інформацію про обладнання, їхній стан, місцезнаходження, відповідальних осіб, гарантійні терміни тощо. У зв'язку з цим особливу увагу приділено питанням безпеки, зокрема автентифікації користувачів, захисту паролів і забезпеченню цілісності даних.

Сучасна архітектура веб-застосунків передбачає розділення на клієнтську частину (Vue.js) і серверну частину (Laravel). Laravel виступає в ролі API-сервера, який приймає, обробляє та зберігає дані, що надходять від клієнтів [1]. Для забезпечення захисту даних на етапах передачі та зберігання необхідно впровадити такі механізми безпеки:

- хешування паролів із використанням надійних алгоритмів;
- токенізацію при аутентифікації користувачів;
- захист API через механізми контролю доступу (ACL) та валідацію запитів.

Хешування паролів є одним із базових методів захисту даних користувачів [2]. У Laravel за замовчуванням використовується bcrypt, який забезпечує надійне шифрування паролів із додаванням сольових значень (salt), що значно ускладнює їх розшифрування методом перебору. Приклад коду хешування пароля на сервері Laravel наведено на рис. 1:

```
use Illuminate\Support\Facades\Hash;

// При створенні нового користувача
$user->password = Hash::make($request->password);
$user->save();
```

Рис 1. Приклад хешування пароля у Laravel

Для підвищення рівня безпеки рекомендується встановити параметр кількості раундів (rounds) хешування не нижче 12. Зі збільшенням кількості раундів підвищується стійкість пароля до злому, проте збільшується час обробки запиту.

Токенізація здійснюється за допомогою технологій OAuth2 або JWT [3; 4]. Після успішної автентифікації користувач отримує токен, який додається до кожного запиту як заголовок авторизації. На сервері кожен запит перевіряється на валідність токена перед обробкою даних.

У випадку інтеграції з Vue.js необхідно також подбати про захист від атак типу XSS (Cross-Site Scripting) та CSRF (Cross-Site Request Forgery), використовуючи відповідні механізми фреймворків.

Таким чином, безпечна розробка вебзастосунку для інтеграції процесів інвентаризації та управління технічними засобами компанії є критично важливою складовою загальної інформаційної безпеки підприємства.

ДЖЕРЕЛА

1. Laravel Security Documentation [Електронний ресурс]. – Режим доступу: URL: https://laravel.com/docs/12.x/authorization

2. Bcrypt Hashing in Laravel [Електронний ресурс]. – Режим доступу: URL: https://laravel.com/docs/hashing

3. OAuth 2.0 and OpenID Connect Guide [Електронний ресурс]. – Режим доступу: URL: https://oauth.net/2/

4. JSON Web Token (JWT) – Introduction [Електронний ресурс]. – Режим доступу: URL: https://jwt.io/introduction/

ВИКОРИСТАННЯ БЛОКЧЕЙН-ТЕХНОЛОГІЙ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ДАНИХ

Руденко О. Л., Талавер О. В., Вакалюк Т. А.

Державний університет «Житомирська політехніка», м. Житомир

Блокчейн –це технологія, що забезпечує захист даних шляхом їх зберігання у вигляді ланцюжка блоків. У кожному блоці міститься інформація, пов'язана з попереднім, що формує незмінний цифровий реєстр. Ця система працює на основі децентралізованої мережі, де кожен вузол має копію даних, а будь-яка зміна повинна бути підтверджена більшістю учасників мережі. Такий підхід виключає можливість підробки чи видалення інформації, забезпечуючи її цілісність і прозорість.

Блокчейн знаходить застосування у багатьох сферах. У фінансовому секторі технологія допомагає створювати криптовалюти, обробляти транзакції та вести облік, що захищений від шахрайства. У логістиці блокчейн дозволяє детально відслідковувати переміщення товарів, мінімізуючи ризики втрати чи маніпуляцій з даними [1].

У медичній сфері блокчейн також має великий потенціал. Завдяки цій технології медичні записи пацієнтів можуть бути захищені від несанкціонованого доступу. Дані зберігаються у зашифрованому вигляді, а доступ до них можливий лише за наявності відповідного ключа. Це дозволяє захистити персональну інформацію пацієнтів і водночас забезпечити її доступність для уповноважених медичних працівників [2].

Окрім переваг, блокчейн має й певні обмеження. По-перше, це високі вимоги до обчислювальних потужностей, які потрібні для підтримки роботи мережі. По-друге, для широкого впровадження цієї технології потрібна відповідна правова база. В Україні, наприклад, питання використання блокчейну ще перебувають на стадії законодавчого врегулювання [3].

Попри ці труднощі, блокчейн має величезний потенціал для інтеграції з іншими технологіями. Зокрема, використання штучного інтелекту може забезпечити автоматизацію перевірки транзакцій або аналіз великих обсягів даних у режимі реального часу. У поєднанні з хмарними обчисленнями блокчейн здатен створювати ще надійніші та більш гнучкі системи зберігання даних.

Перспективи використання блокчейну охоплюють як приватний сектор, так і державні структури. Технологія може бути застосована для створення електронних реєстрів, забезпечення прозорості державних

закупівель, а також для організації електронного голосування. Усі ці можливості роблять блокчейн важливим інструментом для забезпечення цілісності даних у цифрову епоху.

ДЖЕРЕЛА

1. Кудирко О. В. Інновації в логістиці: перспективи використання технології блокчейн у ланцюгах поставок. Науковий вісник Ужгородського національного університету. Серія: Міжнародні економічні відносини та світове господарство. Вип. 15, част. 1. 2017. С. 158-163. http://www.visnyk-econom.uzhnu.uz.ua/archive/15_1_2017ua/36.pdf

2. Матюшенко І.Ю., Гончарова Ю.Ю. Застосування технології блокчейн у розвитку медичних технологій. Інфраструктура ринку. Вип. 44, 2020. С. 234-238. https://doi.org/10.32843/infrastruct44-39

3. Перевєрзєв Д.В. Стан та перспективи нормативно-правового врегулювання обігу криптовалют в Україні. Юридичний науковий електронний журнал. №8 / 2024. С. 264-267. https://doi.org/10.32782/2524-0374/2024-8/61

ЗАХИСТ ІНФОРМАЦІЇ У WEB-ЗАСТОСУНКУ ДЛЯ СТВОРЕННЯ СПИСКУ ПОКУПОК

Рябов А. С.

Державний університет інформаційно-комунікаційних технологій, м. Київ

Сьогодні WEB-застосунки стали невід’ємною частиною повсякденного життя –від онлайн-банкінгу до спільної роботи над документами. Однак зручність таких сервісів нерозривно пов’язана з ризиками витоку конфіденційної інформації, що обумовлює необхідність вживання ефективних заходів кібербезпеки [1]. Особливо це стосується систем, у яких реалізована спільна робота користувачів з одними і тими ж даними, як у випадку нашого застосунку «Список покупок».

У даному WEB-додатку користувачі мають можливість створювати спільні списки продуктів, редагувати їх у реальному часі, а також отримувати доступ до історії покупок. Це вимагає забезпечення таких базових принципів інформаційної безпеки, як конфіденційність, цілісність і доступність. У багатокористувацьких системах першочергове значення має контроль доступу та захист ідентифікаційних даних [2].

Для забезпечення захисту інформації було впроваджено багаторівневу систему безпеки:

1. Аутентифікація користувачів реалізована за допомогою ASP.NET Identity з обов’язковим хешуванням паролів. Для хешування обрано алгоритм bcrypt із використанням динамічної солі, що ускладнює атаку перебором.

2. Передача даних між клієнтом та сервером здійснюється виключно через HTTPS, що забезпечує захист від атак типу «man-in-the-middle».

3. Авторизація доступу базується на ролях. Наприклад, «Owner» має повний доступ до списку, «Viewer» –лише перегляд. Це реалізується через JWT-токени, що перевіряються на сервері перед кожною дією з даними.

Рисунок 1 демонструє приклад генерації токена з обмеженим терміном дії для забезпечення короткочасного доступу до списку:

Рис. 1. Приклад створення авторизаційного JWT-токена в ASP.NET Core

Захист сесій забезпечується шляхом встановлення прапорів Secure та HTTPOnly для Cookies, а також автоматичного завершення сесії після тривалого простою. Це мінімізує ризики захоплення сесії (Session Hijacking).

Відповідно до рекомендацій також реалізовано базове логування усіх дій у системі, зокрема додавання, редагування та видалення елементів зі списків. Це дозволяє швидко виявити підозрілу активність [2].

Таким чином, WEB-застосунок є прикладом того, як навіть у невеликих системах необхідно впроваджувати комплексні заходи безпеки, засновані на сучасних практиках захисту даних. Постійний моніторинг і оновлення механізмів захисту залишаються важливою умовою ефективного функціонування сервісу.

ДЖЕРЕЛА

1. OWASP Foundation. (2024). OWASP Top 10 Web Application Security Risks. https://owasp.org/Top10

2. Пірог О.В. Безпека вебдодатків: навч. посібн. / О.В. Пірог. – Житомир: Житомирська політехніка, 2025. – 290 с. http://eztuir.ztu.edu.ua/123456789/8791

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У ПРОГРАМНОМУ ЗАБЕЗПЕЧЕННІ ДЛЯ МОНІТОРИНГУ НАУКОВОЇ РОБОТИ СТУДЕНТІВ

Садлівський В. Р.
Державний університет інформаційно-комунікаційних технологій, м. Київ

Розвиток інформаційних технологій призвів до активного впровадження web-застосунків у сферу освіти. Проте з поширенням таких рішень зростає загроза витоку конфіденційної інформації, що вимагає відповідального підходу до питань безпеки [1; 2].

Дослідження присвячено створенню web-застосунку для моніторингу наукової роботи студентів із використанням Java Spring Boot, MySQL та React. У системі зберігаються чутливі дані, зокрема інформація про наукові теми, результати, керівників, що потребує захисту на всіх рівнях взаємодії –від бази даних до інтерфейсу [2].

Для захисту користувацьких даних реалізовано хешування паролів за допомогою алгоритму bcrypt із додаванням солі. Такий підхід унеможливлює їх відновлення у разі компрометації бази. Крім того, впроваджено авторизацію за допомогою JWT, що дозволяє точно контролювати рівні доступу користувачів до ресурсів API [3].

На стороні клієнта та сервера реалізовано розмежування ролей (студент, викладач, адміністратор) із перевіркою токенів, а також захист від SQL-ін’єкцій через використання Spring Data JPA [4]. Усі ці заходи формують багаторівневу систему безпеки, відповідно до сучасних стандартів.

ДЖЕРЕЛА

1. OWASP Foundation. Top 10 Web Application Security Risks [Електронний ресурс]. – Режим доступу: https://owasp.org/www-project-top-ten/

2. Spring Boot Documentation – Security Overview [Електронний ресурс]. – Режим доступу: https://docs.spring.io/spring-boot/index.html

3. Auth0. Introduction to JSON Web Tokens + Password hashing [Електронний ресурс]. – Режим доступу: https://auth0.com/learn/json-web-tokens

4. Spring Data JPA Reference Documentation [Електронний ресурс]. – Режим доступу: https://docs.spring.io/spring-data/jpa/docs/current/reference/html/

ЗАСОБИ ВИЯВЛЕННЯ ТА ПРОТИДІЇ НЕЕТИЧНОМУ КОНТЕНТУ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

Середа С. С., Костюк Ю. В.
Київський столичний університет імені Бориса Грінченка, м. Київ

Неетичний контент у цифровому середовищі становить серйозну загрозу для інформаційної безпеки, оскільки впливає як на психоемоційний стан користувачів, так і на стійкість функціонування інформаційно-комунікаційних систем (ІКС). Це поняття охоплює широкий спектр матеріалів – сцени насильства, порнографію, мову ворожнечі, маніпуляції, дезінформацію, кібербулінг, пропаганду – що суперечать етичним нормам і підривають суспільну стабільність [1]. Такий контент часто використовується в інформаційних війнах, соціальній інженерії та кампаніях впливу для порушення цілісності цифрових спільнот.

Класифікація неетичного контенту є основою для побудови систем захисту ІКС. Його поділяють за напрямом впливу (психологічний, інформаційний, соціальний), форматом (текст, відео, інтерактивний), каналами поширення (відкриті платформи, даркнет) та способами маскування. Особливу небезпеку становить приховування шкідливого вмісту під виглядом розважального або освітнього, що ускладнює його виявлення стандартними фільтрами та вимагає застосування штучного інтелекту для глибокої аналітики. Психологічний вплив неетичного контенту тісно пов'язаний з кіберзагрозами: насильницький контент сприяє формуванню агресії, порнографія викривлює уявлення про сексуальні норми і часто пов’язана з кіберзлочинністю, а маніпулятивний контент є інструментом фішингу, дезінформації та радикалізації [2]. Усе це вимагає створення середовища, стійкого до впливу, з використанням інтелектуальних технологій фільтрації, поведінкового аналізу та автоматичного реагування.

Наслідком постійного контакту з неетичним контентом є поступова нормалізація девіантної поведінки, що знижує ефективність традиційних засобів захисту інформації та потребує адаптації політик безпеки в ІКС. Цифрові платформи, зазвичай, використовують алгоритми рекомендацій, які оптимізуються під взаємодію, а не безпеку, що призводить до популяризації контенту з високим рівнем емоційної залученості, навіть якщо він є неетичним або шкідливим [2]. Ці алгоритми, базовані на машинному навчанні, стають об’єктом для маніпуляцій з боку зловмисників, які навмисно експлуатують слабкі місця в логіці рекомендаційних систем.

Постійний контакт із неетичним контентом сприяє його нормалізації, що знижує ефективність захисту в ІКС. Алгоритми, орієнтовані на

залучення, просувають шкідливий контент і легко піддаються маніпуляціям. Додаткову загрозу становлять закриті спільноти в даркнеті та месенджерах. Для виявлення таких активностей необхідні сучасні технології: моніторинг трафіку, ШІ та поведінковий аналіз у реальному часі.

Захист від неетичного контенту має реалізовуватись на кількох рівнях: правовому, технологічному, організаційному та освітньому. На законодавчому рівні важливо забезпечити чітке регулювання щодо поширення деструктивного вмісту, з урахуванням міжнародного досвіду, норм ЄС та рекомендацій ІТ-безпекових комісій. Технологічні засоби включають фільтрацію контенту в реальному часі, системи батьківського контролю, контент-аналіз за допомогою природномовної обробки (NLP), використання Blacklist/Whitelist-архітектур та Zero Trust моделей. ШІ-алгоритми повинні адаптуватися до змін середовища, розпізнавати кодифікований, фрагментований або зашифрований шкідливий вміст, а також виявляти координацію між обліковими записами в масштабних кампаніях.

До агресивних методів протидії належать блокування хостингів, видалення шкідливих акаунтів, запуск honeypot-серверів та контратаки у разі державної загрози чи кібертероризму. Такі дії потребують тісної координації між службами безпеки, CERT-командами, провайдерами та ІТ-компаніями.

Водночас одним із найнадійніших способів захисту є розвиток цифрової грамотності та критичного мислення. Навчання виявленню фейків, маніпуляцій, фішингу та інших загроз має стати основою цифрової освіти для всіх користувачів. Висока обізнаність посилює інформаційну безпеку ІКС, знижує ризики та підвищує ефективність технічного захисту.

Таким чином, неетичний контент не є лише моральною або культурною проблемою – він є реальною кіберзагрозою, що вимагає комплексного, системного і високотехнологічного підходу до виявлення, протидії та профілактики в межах інформаційно-комунікаційних систем.

ДЖЕРЕЛА

1. Chu A.M.Y., So M.K.P. Organizational Information Security Management for Sustainable Information Systems: An Unethical Employee Information Security Behavior Perspective // *Sustainability*. 2020. Vol. 12, No. 8. P. 3163. DOI: 10.3390/su12083163.

2. Zhang T., Zhang Y. Impacts of Unethical Behavior on Self-Esteem: A Contingent Dual-Pathway Model // *Personality and Social Psychology Bulletin*. 2024. (in press). DOI: 10.1177/01461672241236983.

БЕЗПЕКА У РОЗРОБЦІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ КОНТРОЛЮ ВИТРАТ: АКТУАЛЬНІ ЗАГРОЗИ ТА ПІДХОДИ ДО ЗАХИСТУ

Сікало О. С.
Державний університет інформаційно-комунікаційних технологій, м. Київ

Цифрова трансформація фінансового менеджменту зумовлює зростання потреби у програмному забезпеченні для ефективного контролю витрат, як в особистих, так і в корпоративних бюджетах. Такі системи часто обробляють конфіденційну фінансову інформацію, персональні дані користувачів, а також інтегруються з банківськими API [1], що ставить безпеку даних на перший план.

Незважаючи на це, в процесі розробки подібних застосунків розробники нерідко фокусуються переважно на функціональності, зручності інтерфейсу та інтеграції з фінансовими сервісами, залишаючи безпекові аспекти на другорядному рівні. Це відкриває шлях до потенційних загроз, включно з витоком платіжної інформації, несанкціонованим доступом до особистих даних або фінансовим шахрайством. Особливо критично це для мобільних і веб-застосунків, де зловмисники активно експлуатують уразливості інтерфейсів та протоколів обміну даними [2].

Метою цієї роботи є аналіз актуальних загроз безпеки у програмному забезпеченні для контролю витрат та впровадження технологічних рішень для забезпечення конфіденційності, цілісності й доступності даних. Розглядаються методи аутентифікації користувачів (зокрема, з використанням двофакторної перевірки), контроль доступу до критичних функцій, захист API через OAuth 2.0 [3], а також використання криптографічних протоколів для захищеного зберігання і передачі фінансової інформації (TLS, AES) [4].

Також акцентується на необхідності реалізації механізмів виявлення аномальної активності (наприклад, спроби злому облікового запису або підозрілої зміни витрат), регулярного аудитування дій користувача, ведення журналу змін, а також застосування принципів безпечної розробки –Secure Software Development Lifecycle (SSDLC) [5].

У результаті впровадження описаних підходів буде створено безпечне, надійне та відповідне сучасним стандартам програмне забезпечення для контролю витрат, яке забезпечить високий рівень довіри користувачів, знизить ризики втрати або компрометації фінансових даних і сприятиме відповідності вимогам законодавства у сфері захисту інформації.

ДЖЕРЕЛА

1. OWASP Foundation. *API Security Top 10*. – https://owasp.org/www-project-api-security/

2. OWASP Foundation. *OWASP Top Ten Web Application Security Risks*. – https://owasp.org/www-project-top-ten/

3.RFC 6749: The OAuth 2.0 Authorization Framework. – IETF – https://datatracker.ietf.org/doc/html/rfc6749

4. National Institute of Standards and Technology (NIST). *Security and Privacy Controls for Information Systems and Organizations (NIST SP 800-53 Rev. 5)*. – https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

5. Microsoft Learn. *Secure software development lifecycle (SSDLC)*. – https://learn.microsoft.com/en-us/security/devsecops/secure-software-development-lifecycle

ЗАХИСТ ІНФОРМАЦІЇ У ГРІ ЖАНРУ 2D ПЛАТФОРМЕР

Скиба С. С.

Державний університет інформаційно-комунікаційних технологій, м. Київ

У наш час багато геймерів обирають нечесні методи для проходження відеоігор, що дає їм несправедливу перевагу та порушує ігровий баланс. Таких гравців називають «чітерами». Проте внаслідок редагування файлів збереження в іграх має певні негативні наслідки. Файли збереження мають важливі дані про прогрес гравця. І їх змінення може сильно вплинути на враження від гри. Адже розробники ігор стараються підібрати ідеальні умови для проходження гри і отримання незабутнього враження. У зв’язку з цим виникає проблема забезпечення цілісності та доступності інформації у ігровому процесі.

Якщо файли збереження не захищені, то це дає змогу гравцям їх редагувати. Наприклад, змінити параметри свого персонажа (зробити себе безсмертним, добавити пару нулів до своєї атаки і таке інше). Щоб забезпечити свою гру від такого втручання, розробники шифрують свої файли збережень.

Існують такі алгоритми для шифрування файлів: AES (Advanced Encryption Standard), XOR-шифрування , RC4 (Rivest Cipher 4), TEA (Tiny Encryption Algorithm), DES (Data Encryption Standard) тощо. Для офлайн-гри підходить RC4.

RC4 – це потоковий шифр [1]. Його перевагою є те, що він легкий у реалізації не дивлячись, яка мова програмування буде. Також він швидкий і підтримує ключі різної довжини.

Приклад використання RC4 (Rivest Cipher 4) у файлі, де зберігаються дані:

```
string key = «MySecretKey»
byte[] encryptedData = RC4.EncryptString(saveData, key);
```

Недоліком даного алгоритму є те, що він не має високого рівня безпеки. Але для офлайн-гри це не є критичним.

З вищесказаного можна зробити висновок , що для шифрування даних в офйлан-грі достатньо RC4 (Rivest Cipher 4). Це дасть змогу зменшити кількість нечесних гравців.

ДЖЕРЕЛА

1. Що таке RC4 - Терміни та визначення в кібербезпеці [Електронний ресурс]. – Режим доступу: URL https://www.vpnunlimited.com/ua/help/cybersecurity/rc4?srsltid=AfmBOoojf78pwzpwW6qvz2IgzTRi4op4vTKfszMLOG3H0h_6SyncCaTc

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ДАНИХ У ЗАСТОСУНКУ WOT CONFIGURATOR

Солов’ян А. О., Гаманюк І. М.

Державний університет інформаційно-комунікаційних технологій, м. Київ

З розвитком комп'ютерних ігор та їх налаштувань, питання безпеки конфігураційних даних стає все більш актуальним. Застосунок «WOT Configurator» дозволяє користувачам налаштовувати, переглядати та зберігати конфігураційні дані гри «World of Tanks», включаючи файл preferences.xml, де зберігається зашифрований пароль для автоматичного входу [1]. Цей файл є критично важливим компонентом, оскільки компрометація його вмісту може призвести до несанкціонованого доступу до облікових записів користувачів, що, в свою чергу, може спричинити втрату особистої інформації та інших конфіденційних даних [2]. Оскільки сучасні кіберзагрози стають дедалі складнішими, розробники повинні впроваджувати ефективні заходи безпеки для захисту даних користувачів. Це включає не лише шифрування даних, але й моніторинг активності та інші методи, що дозволяють забезпечити цілісність та конфіденційність інформації [3].

У застосунку «WOT Configurator» реалізовано кілька методів для захисту конфігураційних даних. Основна увага приділялася ефективності шифрування та моніторингу. Використання алгоритмів AES (AES-256-CBC) для шифрування паролів у файлі preferences.xml забезпечує високий рівень захисту. Це ускладнює несанкціонований доступ до конфіденційної інформації. Реалізована система логування змін у конфігураційних файлах та моніторинг активності користувачів дозволяє швидко виявляти та реагувати на підозрілі дії.

Запропоновані методи забезпечення безпеки у застосунку «WOT Configurator» дозволяють надійно захистити конфігураційні дані від несанкціонованого доступу та модифікацій.

ДЖЕРЕЛА

1. How can you protect your data when gaming online? [Електронний ресурс]. – Режим доступу: URL https://www.linkedin.com/advice/3/how-can-you-protect-your-data-when-gaming-online-m9ouf

2. Cybersecurity for Gamers: 10 Essential Tips to Stay Safe. [Електронний ресурс]. – Режим доступу: URL https://www.staysafeonline.org/articles/10-online-safety-tips-for-gaming

3. Omotunde, Habeeb & Ahmed, Maryam. (2023). A Comprehensive Review of Security Measures in Database Systems: Assessing Authentication, Access Control, and Beyond. Mesopotamian Journal of Cyber Security. 2023. 115-133. 10.58496/MJCSC/2023/016.

ЗАХИСТ ДАНИХ ПІД ЧАС ІГРОВОГО ПРОЦЕСУ У БАГАТОКОРИСТУВАЦЬКІЙ СТРАТЕГІЇ У РЕАЛЬНОМУ ЧАСІ НА UNREAL ENGINE ВІД ЗЛОВМИСНИХ ВТРУЧАНЬ

Солодкий Я. Т.

Державний університет інформаційно-комунікаційних технологій, м. Київ

Unreal Engine є одним з найпопулярніших сучасних ігрових рушіїв, що масово використовується як інді-студіями, так і розробниками AA та AAA-класу [1]. Його потужні можливості та гнучкість зробили Unreal Engine платформою вибору для великої кількості масштабних проєктів. Наше дослідження присвячене розробці стратегічної гри реального часу (RTS) із розвиненим багатокористувацьким режимом, зокрема з режимом «гравець проти гравця». Очевидно, що у змагальному PvP-середовищі можуть з’явитися нечесні гравці, які спробують сторонніми програмами отримати несправедливу перевагу [2]. Тому розробка такого проєкту потребує особливої уваги до забезпечення безпеки даних ігрового процесу, аби унеможливити його порушення та підтримати чесний баланс гри.

Сучасні багатокористувацькі ігри (включно з RTS на Unreal Engine) впроваджують низку підходів для протидії чітерству та захисту цілісності геймплею. Зазвичай використовується клієнт-серверна архітектура із виділеним сервером (dedicated server), який централізовано керує перебігом гри і запобігає модифікації її стану на стороні клієнтів. Окрім архітектурних рішень, розробники часто інтегрують спеціалізовані анти-чіт системи (наприклад, Valve Anti-Cheat, BattlEye, Easy Anti-Cheat), що відстежують підозрілу активність та наявність відомих чит-програм [2]. Комплексне поєднання таких засобів дозволяє виявляти та нейтралізувати більшість спроб несанкціонованого втручання у ігровий процес ще на етапі їх виникнення, забезпечуючи чесне змагання між гравцями.

У даному дослідженні були проаналізовані методи захисту цілісності ігрового процесу з метою впровадження даних підходів у розробленому продукті.

1. Серверна авторитетність.

Критично важливі аспекти логіки гри повинні оброблятися на сервері, який виступає єдиним джерелом правдивого стану світу. Клієнти лише надсилають запити (команди) на дії, а сервер виконує зміну стану і надсилає результати назад. Такий підхід гарантує, що гравці не можуть самостійно змінювати ключові параметри гри на своїх машинах (наприклад, здоров'я персонажа, рівень ресурсів тощо) [3]. Якщо клієнтська програма спробує вийти за межі правил (наприклад, перемістити юніт із неможливою швидкістю), сервер це виявить і відхилить подібну дію, запобігаючи типовим читам на кшталт прискорення руху персонажів [4].

2. Перевірка дій клієнта.

Сервер повинен валідувати кожну дію, що надходить від клієнтів, перед тим, як застосувати її до ігрового світу. Це означає, що всі повідомлення від гравців перевіряються на відповідність правил гри та допустимих меж. Подібні перевірки унеможливлюють використання модифікованих клієнтів, які надсилають недійсні або неможливі команди. У разі виявлення аномальних дій (що можуть свідчити про втручання сторонніх програм) сервер може негайно відхилити.

3. Обмеження реплікації даних.

Для мінімізації ризику «мап-хаку» та інших інформаційних читів сервер повинен надсилати кожному клієнту лише ту інформацію, яку той має знати в даний момент. Такий підхід позбавляє потенційних шахраїв можливості дістати приховану інформацію шляхом аналізу пам'яті або мережевого трафіку [5]. Обмежуючи реплікацію, розробник захищає цілісність ігрового процесу від інформаційних витоків.

4. Інтеграція анти-чит систем.

Клієнтські анти-чити (на кшталт VAC, EAC тощо) відслідковують присутність сторонніх програм або модифікацій у пам'яті гравця, тоді як серверні анти-чити аналізують поведінкові дані гравців на предмет статистичних аномалій [3]. Розробнику доцільно поєднувати обидва підходи: вбудовувати у гру підтримку зовнішнього анти-читу ПЗ та реалізувати внутрішні серверні механізми виявлення підозрілих дій. Спеціалізовані сервіси (як-от Epic Online Services з Easy Anti-Cheat) можна інтегрувати в проєкт на Unreal Engine для автоматичного виявлення відомих чит-програм. Водночас власні серверні скрипти можуть відстежувати нетипову ігрову активність (наприклад, надто високу точність або швидкість серії дій) і в реальному часі реагувати на неї (від розірвання з'єднання до тимчасового блокування підозрілого гравця).

Хоча жодна система не гарантує абсолютного захисту, багаторівневий підхід значно ускладнює завдання для зловмисників і підвищує безпеку ігрового середовища.

ДЖЕРЕЛА

1. Mezha.Media – Найпопулярніші ігрові рушії Steam: Unity, Unreal, а які ж інші?– Режим доступу: mezha.media.

2. i3D.net – Countering the ever-evolving scourge of cheating in games (2023) – Режим доступу: i3d.neti3d.net.

3. Epic Games (Documentation) – Replicating Variables in Blueprints – Unreal Engine 4.27 Documentation – Режим доступу: dev.epicgames.com.

4. Epic Games (Documentation) – Setting Up Dedicated Servers in Unreal Engine (Networking Guide) – Режим доступу: docs.unrealengine.com

5. Wu-Chang Feng et al. – Mitigating Information Exposure to Cheaters in Real-Time Strategy Games // NOSSDAV'05, 2005 – pp. 7–12 thefengs.com. (Приклад використання криптографічних методів для приховування інформації від гравців до потрібного моменту).

ЗАХИСТ ІНФОРМАЦІЇ У WEB-ЗАСТОСУНКУ ДЛЯ ОБЛІКУ І РОЗПОДІЛУ ДОМАШНІХ СПРАВ

Степанов А. Ю.

Державний університет інформаційно-комунікаційних технологій, м. Київ

Історично автентифікація у вебі починалася зі звичайного логіна і пароля, що передавалися напряму на сервер з усіма супутніми ризиками: перехоплення, фішинг, повторне використання. У міру розвитку веб-застосунків постала потреба у безпечнішому способі доступу до ресурсів. Дане дослідження – розробка веб-застосунку для обліку й розподілу домашніх справ, тому забезпечення конфіденційності – один з ключових пріоритетів.

У даному проєкті реалізовано Authorization Code Flow з PKCE – рекомендований варіант для публічних клієнтів, зокрема браузерних застосунків [1; 2]. Він передбачає використання додаткового секрету (code_verifier/code_challenge) для запобігання атакам на перехоплення коду авторизації.

На стороні клієнта (Angular, без сторонніх бібліотек):

- генерується code_verifier і code_challenge;
- ініціюється авторизація через провайдера (наприклад, Google);
- отриманий код авторизації передається на backend (ASP.NET), де виконується обмін на access token;
- токен не зберігається у localStorage (через XSS-ризики), а зберігається у HttpOnly, Secure кукі, що значно підвищує захищеність.

На стороні сервера реалізовано перевірку PKCE, обробку refresh-токенів та захист від CSRF (через кукі + SameSite).

Така реалізація забезпечує:

- ізоляцію токенів від JavaScript-оточення;
- автоматичну інвалідність токенів при виході;
- відповідність найкращим практикам безпеки OAuth 2.0.

Таким чином, застосунок гарантує конфіденційність даних користувачів і захищає процес аутентифікації від типових векторів атак.

ДЖЕРЕЛА

1. Protecting Apps with PKCE - OAuth 2.0 Simplified. OAuth 2.0 Simplified. URL: https://www.oauth.com/oauth2-servers/pkce/

2. RFC 6749: The OAuth 2.0 Authorization Framework. IETF Datatracker. URL: https://datatracker.ietf.org/doc/html/rfc6749

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ДАНИХ У СИСТЕМІ РОЗПОДІЛЕНОЇ ДОСТАВКИ ЦИФРОВОГО КОНТЕНТУ НА ПРИКЛАДІ ГРИ MINECRAFT

Стратович М. Я.

Державний університет інформаційно-комунікаційних технологій, м. Київ

У сучасному ігровому середовищі, особливо в проєктах з відкритою архітектурою на кшталт Minecraft, зростає потреба в надійній та безпечній системі доставки цифрового контенту. Відсутність централізованих оновлень змушує гравців звертатися до сторонніх джерел для завантаження модифікацій, ресурсів і текстур. Це створює серйозні ризики для безпеки – від поширення шкідливого ПЗ до витоку даних –і негативно впливає на користувацький досвід. Тому забезпечення захищеної, автоматизованої передачі даних у системах розподіленої доставки є актуальним і важливим завданням.

У межах дослідження передбачається створення системи доставки цифрового контенту для гри Minecraft з використанням сервісів Amazon Web Services (AWS), до якого входитимуть Amazon S3, CloudFront, Lambda, DynamoDB, API Gateway, IAM, WAF та Shield. Основною метою є розробка безпечної, масштабованої та ефективної архітектури доставки ігрових файлів користувачам через CDN-мережу, із використанням Amazon S3 як базового сховища контенту.

Забезпечення безпеки передбачатиме реалізацію багаторівневого підходу. На першому рівні, буде впроваджено механізм забезпечення цілісності та автентичності файлів шляхом їх цифрового підписування. Після публікації нового контенту (автоматизованої через CI/CD-процес) для кожного файлу обчислюється хеш та створюється цифровий підпис із використанням приватного ключа. Підписи зберігаються разом з назвами

файлів у базі даних, а публічний ключ надається клієнтській стороні –через API або безпосередньо вбудовується у застосунок [1].

Під час виконання запиту з боку клієнтського застосунку до API Gateway планується повертати як посилання на контент, так і цифрові підписи файлів разом із публічним ключем. Клієнт зможе локально перевірити автентичність отриманого контенту, що забезпечить верифікацію цілісності та захист від несанкціонованої модифікації.

На другому рівні захист ресурсів системи планується реалізувати за допомогою AWS IAM (Identity and Access Management). Буде налаштовано ролі та політики, що обмежуватимуть доступ до компонентів інфраструктури – зокрема, до S3, Lambda та DynamoDB –виключно для авторизованих сервісів [1].

На третьому рівні для запобігання прямого доступу до сховища з боку кінцевих користувачів передбачається використання CloudFront Origin Access Identity (OAI), що забезпечує доступ до файлів Amazon S3 лише через CloudFront. Це дозволить уникнути прямого звернення до бакетів і зменшити ризики витоку даних [2].

Мережевий захист системи планується посилити за допомогою AWS WAF (Web Application Firewall) та AWS Shield. Зокрема, передбачається впровадження правила типу rate-based, яке блокуватиме IP-адреси, що здійснюють надмірну кількість запитів до Cloudfront у визначений проміжок часу [3]. Це дозволить зменшити ризики спаму, бот-атак або перевантаження системи. AWS Shield забезпечуватиме захист від DDoS-атак на рівні інфраструктури без додаткової інтеграції [3].

Таким чином, запланована система передбачає впровадження комплексного підходу до безпеки цифрового контенту, який включатиме криптографічне підписування файлів, контроль доступу до ресурсів, обмеження прямого доступу до сховища та захист від зовнішніх загроз на мережевому рівні. У результаті очікується створення безпечної, гнучкої та масштабованої платформи розподілу цифрового ігрового контенту, що відповідатиме сучасним вимогам кібербезпеки.

ДЖЕРЕЛА

1. Brisals S., Hedger L. (2024). Serverless Development on AWS: Building Enterprise-Scale Serverless Solutions. O'Reilly Media, Incorporated, 498.

2. Rule: CloudFront distributions should have origin access identity enabled https://www.clouddefense.ai/compliance-rules/aws-fs-practices/cloudfront/foundational-security-cloudfront-2

3. Documentation team, AWS WAF, AWS Firewall Manager, and AWS Shield Advanced, URL: https://docs.aws.amazon.com/pdfs/waf/latest/developerguide/waf-dg.pdf.

ЗАХИСТ ІНФОРМАЦІЇ У ВЕБ-ЗАСТОСУНКУ ДЛЯ ПІДТРИМКИ МОЛОДІЖНИХ ІНІЦІАТИВ ГО «ЛІДЕРСЬКА ІНІЦІАТИВА»: ТЕХНОЛОГІЧНІ І СОЦІАЛЬНІ АСПЕКТИ БЕЗПЕКИ ЦИФРОВОГО СЕРЕДОВИЩА

Тарасюк М. С.
Державний університет інформаційно-комунікаційних технологій, м. Київ

У сучасному суспільстві цифрові технології стають одним із ключових інструментів для розвитку громадських ініціатив, зокрема молодіжних. Громадська організація «Лідерська ініціатива» відіграє важливу роль у мобілізації молоді до соціальної активності, освітніх проєктів та волонтерських дій. У цьому контексті створення веб-застосунку, який би підтримував ініціативи молоді, стає не лише технічним, але й стратегічним завданням. Однак зростання цифрової активності обумовлює також підвищені вимоги до захисту персональних даних, безпеки збереження інформації та прозорості взаємодії в онлайн-середовищі.

У цифрову епоху зростає кількість кіберзагроз, спрямованих як на приватних осіб, так і на організації. Молодіжні ініціативи, що базуються на довірі, взаємодії та відкритості, можуть стати легкою мішенню в разі неналежного рівня захисту даних. Зокрема, при зборі заявок, пожертв або обробці персональної інформації користувачів необхідно забезпечити дотримання міжнародних та національних стандартів інформаційної безпеки [1]. Таким чином, створення безпечної веб-платформи не лише гарантує стабільну роботу проєкту, але й підвищує рівень довіри з боку користувачів і партнерів.

Метою даної роботи є розробка функціонального веб-застосунку для ГО «Лідерська ініціатива», який поєднуватиме зручність для користувачів з високим рівнем захисту інформації. Платформа має забезпечити безпечну реєстрацію, подання ініціатив, підтримку зборів коштів, а також надійне адміністрування даних з боку організації. Окремим аспектом дослідження є вивчення впливу безпеки системи на активність користувачів та ефективність цифрової взаємодії.

У межах даної роботи передбачено здійснення комплексного аналізу актуальних кіберзагроз, що стосуються громадських веб-застосунків, зокрема платформ для підтримки молодіжних ініціатив. Особлива увага приділяється дослідженню сучасних технологій захисту інформації, таких як протоколи шифрування даних, механізми автентифікації та авторизації, а також підходи до безпечної обробки транзакцій. На основі проведеного аналізу буде сформовано функціональні та нефункціональні вимоги до системи з акцентом на забезпечення безпеки користувацьких даних.

Подальшим етапом є розробка архітектури веб-застосунку з використанням мікросервісної моделі, яка забезпечить гнучкість, масштабованість і стійкість до зовнішніх загроз. У процесі реалізації також передбачено впровадження сучасних інструментів контейнеризації та оркестрації (Docker, Kubernetes), налаштування захищених каналів зв'язку та реалізація системи моніторингу безпеки. Завершальним етапом є тестування функціональних і захисних властивостей системи у різних сценаріях з метою підтвердження її стійкості до типових атак та відповідності встановленим вимогам.

Запропонована архітектура веб-застосунку базується на сучасних принципах мікросервісної архітектури, що дозволяє розділити функціональні компоненти системи (реєстрація, пожертви, адміністрування) на окремі модулі, що підвищує масштабованість і стійкість до збоїв. Для контейнеризації буде використано Docker, а для оркестрації – Kubernetes. Безпечна автентифікація реалізовуватиметься через OAuth 2.0 з підтримкою JWT-токенів [2-4], що дозволяє контролювати доступ до кожного модуля системи відповідно до ролі користувача.

У результаті була створена веб-система, що дозволяє ефективно управляти молодіжними ініціативами ГО «Лідерська ініціатива» з дотриманням високих стандартів безпеки. Забезпечення конфіденційності та цілісності даних, захист каналів передачі інформації, стійкість до поширених кіберзагроз сприятимуть формуванню довіри серед користувачів, партнерських організацій та волонтерів. Крім того, система стане інструментом цифрової трансформації громадської активності та може бути масштабована для інших громадських ініціатив.

ДЖЕРЕЛА

1. OWASP Foundation. OWASP Top Ten Web Application Security Risks – https://owasp.org

2. RFC 6749: The OAuth 2.0 Authorization Framework – https://tools.ietf.org/html/rfc6749

3. RFC 6750: The OAuth 2.0 Authorization Framework: Bearer Token – Usage https://tools.ietf.org/html/rfc6750

4. RFC 7519: JSON Web Token (JWT) – https://tools.ietf.org/html/rfc75193

ЗАХИСТ ІНФОРМАЦІЇ У ЗАСТОСУНКУ ДЛЯ УПРАВЛІННЯ ОФІСНИМ ПРОСТОРОМ

Ткачищен В. М.
Державний університет інформаційно-комунікаційних технологій, м. Київ

Забезпечення захисту даних у застосунку для управління офісним простором передбачає реалізацію сучасних методів автентифікації, шифрування та управління доступом. Важливою складовою є впровадження багатофакторної автентифікації (MFA), що включає парольний захист та другий фактор, наприклад, одноразові паролі (OTP) або біометричні дані [1]. Для захисту бази даних MySQL реалізовано шифрування на рівні з'єднання за допомогою TLS, а також шифрування окремих полів, які містять конфіденційну інформацію. Використання механізму Transparent Data Encryption (TDE) дозволяє автоматично шифрувати дані на рівні фізичного зберігання [2]. Крім того, важливо обмежити доступ до бази даних за допомогою ролевої моделі контролю доступу (RBAC) та мінімізації привілеїв для користувачів і сервісів.

Окрему увагу слід приділити безпечній обробці автентифікаційних запитів. Використання OAuth 2.0 або OpenID Connect для керування сесіями користувачів забезпечує безпечну автентифікацію без необхідності зберігання паролів у застосунку [1]. Важливим аспектом є контроль часу сесії та автоматичне завершення сесій після визначеного періоду бездіяльності.

Захист від атак типу SQL-ін'єкцій досягається шляхом використання параметризованих запитів та ORM (наприклад, Entity Framework) замість безпосереднього виконання SQL-запитів.

Слід відмітити, що необхідно передбачити механізми оновлення безпеки, зокрема регулярні оновлення бібліотек та перевірку залежностей на наявність відомих уразливостей. Використання автоматизованих засобів перевірки безпеки, таких як статичний та динамічний аналіз коду, сприяє виявленню потенційних уразливостей на ранніх етапах розробки.

ДЖЕРЕЛА

1. NIST Special Publication 800-63b Digital Identity Guidelines [Електронний ресурс]. – Режим доступу: URL https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf

2. Transparent data encryption (TDE) [Електронний ресурс]. – Режим доступу: URL https://learn.microsoft.com/en-us/sql/relational-databases/security/encryption/transparent-data-encryption?view=sql-server-ver16

ЗАХИСТ ІНФОРМАЦІЇ У WEB-ЗАСТОСУНКУ БУКІНГ ГОТЕЛІВ

Філаретов М. Ю.
Державний університет інформаційно-комунікаційних технологій, м. Київ

Сучасний готельний бізнес потребує ефективних та гнучких інструментів для управління бронюванням, і саме веб-застосунки для букінгу готелів стають ключовим рішенням. Вони автоматизують процеси пошуку номерів, реєстрації клієнтів, оплати та інтеграції з платіжними сервісами. Зокрема, технологія Java Spring забезпечує високу продуктивність, масштабованість та безпеку у цьому процесі.

Основу архітектури таких систем складає Spring Boot, який використовується для розробки REST API, що взаємодіє з фронтендом та базою даних. Безпеку застосунку забезпечує Spring Security [1], відповідаючи за аутентифікацію та авторизацію користувачів. Для передачі токенів авторизації застосовується JWT [2-3], який складається з трьох частин: заголовка (визначає тип токена та алгоритм підпису), корисного навантаження (містить дані користувача та час дії токена) та підпису для верифікації автентичності. Додаткова безпека досягається через шифрування паролів за допомогою BCrypt перед їх збереженням у базі даних, а також використання Prepared Statements та ORM Hibernate для запобігання SQL-ін'єкціям. Налаштування CORS політик додатково захищає систему від міжсайтових атак.

Логічна архітектура забезпечення безпеки системи, що включає всі описані механізми безпеки, представлено на UML-діаграмі (рис. 1).

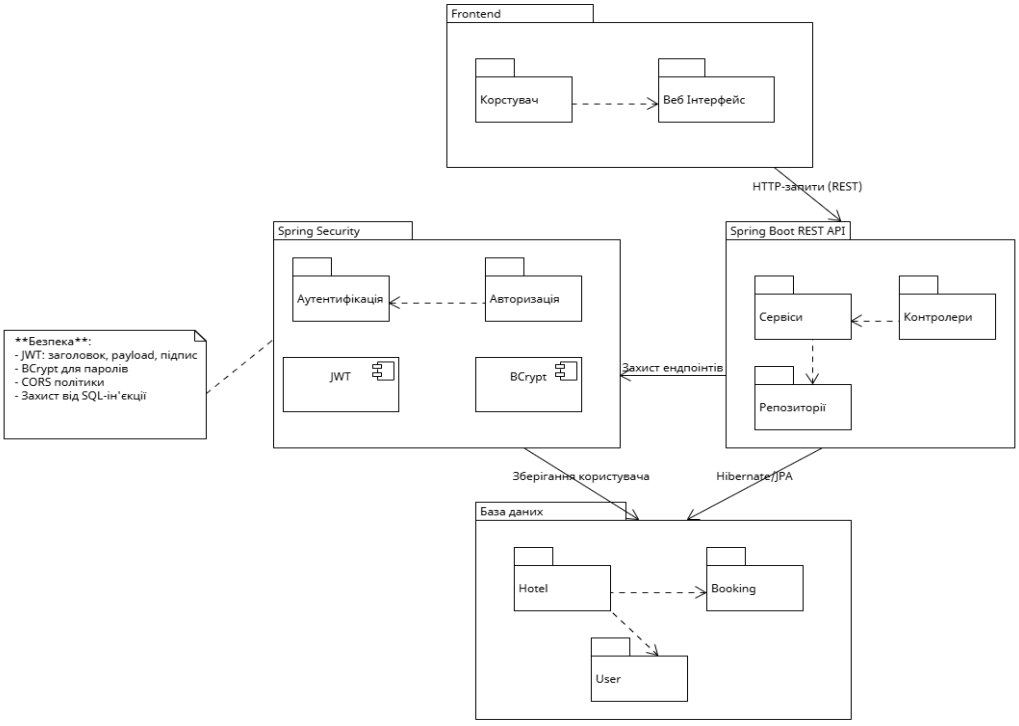


Рис. 1. Логічна архітектура забезпечення безпеки системи

Цей підхід дозволяє створити надійну, адаптивну платформу для управління готельним бронюванням, відповідаючи сучасним вимогам захисту інформації.

Створення безпечного веб-застосунку для букінгу готелів є критично важливим у сучасному світі, де конфіденційність даних користувачів є важливим фактором. Архітектура системи, представлена на UML-діаграмі, підкреслює логічну взаємодію компонентів: від фронтенду до бази даних з акцентом на інтеграцію механізмів безпеки на кожному рівні. Це забезпечує не лише високу продуктивність, але й відповідність сучасним стандартам інформаційної безпеки.

ДЖЕРЕЛА

1. Spring Security [Електронний ресурс]. – Режим доступу: URL https://spring.io/projects/spring-security

2. JWT Authentication [Електронний ресурс]. – Режим доступу: URL https://jwt.io/introduction

3. JSON Web Token (JWT) [Електронний ресурс]. – Режим доступу:URL https://tools.ietf.org/html/rfc7519

ВИЗНАЧЕННЯ ВИМОГ БЕЗПЕКИ ДАНИХ ГРАВЦІВ У ПОКРОКОВІЙ ОНЛАЙН-ГРІ

Цуман О. С.

Державний університет інформаційно-комунікаційних технологій, м. Київ

Сучасні покрокові онлайн-ігри вимагають особливої уваги до питань безпеки даних користувачів. Важливим аспектом є забезпечення конфіденційності інформації гравців, у першу чергу, їхніх облікових даних та ігрового прогресу.

Задачею даного дослідження є визначення ключових вимог та рекомендацій щодо безпечного зберігання даних користувачів у покрокових онлайн-іграх.

У ході дослідження запропоновано використовувати алгоритм PBKDF2 (Password-Based Key Derivation Function 2) для безпечного зберігання паролів користувачів [1-2]. PBKDF2 передбачає багаторазове хешування пароля з використанням випадково згенерованої солі та великої кількості ітерацій (від 100 000 і більше), що значно ускладнює brute-force атаки. Як додатковий захід безпеки запропоновано застосування механізму блокування після певної кількості невдалих спроб авторизації. Це знижує ризик підбору паролів методом перебору.

Також, як сховище даних, використовується Google Firestore, що забезпечує швидкий доступ до даних, ефективне управління ними у реальному часі та додаткові можливості для безпеки, такі як Firebase Authentication.

Запропоновані підходи дозволяють суттєво підвищити рівень безпеки даних гравців у покрокових онлайн-іграх. Використання алгоритму PBKDF2 та додаткових механізмів захисту є ефективним рішенням для зменшення ризику компрометації даних користувачів.

Подальші дослідження можуть бути спрямовані на інтеграцію додаткових сучасних методів безпеки, таких як двофакторна аутентифікація та поглиблені аналітичні засоби для виявлення потенційних загроз.

ДЖЕРЕЛА

1. RFC 8018 –Password-Based Cryptography Specification. URL: https://www.rfc-editor.org/rfc/rfc8018.html

2. Microsoft Documentation: Rfc2898DeriveBytes Class. URL: https://docs.microsoft.com/en-us/dotnet/api/system.security.cryptography.rfc2898derivebytes

БЕЗПЕКА ДАНИХ У ВЕБ-ЗАСТОСУНКУ ДЛЯ ВІЗУАЛІЗАЦІЇ ІСТОРИЧНИХ ПОДІЙ НА ОСНОВІ ОНТОЛОГІЙ: СУЧАСНІ ВИКЛИКИ ТА ТЕХНОЛОГІЧНІ РІШЕННЯ

Черниш А. О.

Державний університет інформаційно-комунікаційних технологій, м. Київ

Цифровізація гуманітарних наук і освіти відкриває нові горизонти для популяризації історичних знань. Одним із перспективних напрямів є використання онтологій –формальних структур, які дозволяють описувати події, персоналії та явища у вигляді взаємопов’язаних сутностей. Веб-застосунки, побудовані на таких моделях, сприяють інтерактивному пізнанню історії через візуалізацію складних часових і логічних взаємозв’язків. Проте ці системи оперують значними обсягами даних, серед яких є як відкриті знання, так і персоналізована інформація користувачів. Саме тому виникає критична необхідність забезпечити цілісність, доступність та конфіденційність даних у таких середовищах [1].

На практиці більшість веб-застосунків, що використовують онтології, орієнтовані насамперед на функціональність і візуальну привабливість, тоді як питання безпеки часто залишаються другорядними. Це створює серйозні ризики –від спотворення історичних фактів до маніпуляцій даними або витоку персональної інформації. Враховуючи зростання відкритого наукового середовища, кібератак на освітні ресурси та вимоги до захисту інтелектуальної власності, безпека даних стає невід’ємною складовою якісного цифрового продукту в освітньо-гуманітарній сфері [2].

Метою цієї роботи є дослідження принципів забезпечення безпеки даних у веб-застосунках, що реалізують візуалізацію історичних подій на основі онтологій, та впровадження технологічних рішень для гарантування цілісності, автентичності й конфіденційності даних. Особлива увага приділяється захисту структури онтологій, контролю доступу до редагування даних, а також безпечному обміну інформацією між клієнтом і сервером [3].

Дослідження передбачає аналіз типових архітектур семантичних веб-застосунків, ідентифікацію потенційних загроз для онтологічних і користувацьких даних, розгляд практик автентифікації (OAuth 2.0), контролю прав доступу, реалізації журналювання змін, а також криптографічного захисту каналів зв’язку (TLS/SSL). Розробка прототипу безпечної платформи має включати підтримку версіонування онтологій, обмеження прав редагування та механізми виявлення несанкціонованих змін.

У результаті реалізації запропонованих рішень було створено безпечну веб-платформу, яка дозволила візуалізувати історичні події на основі онтологій, забезпечуючи при цьому повноцінний захист даних. Платформа підвищує довіру користувачів до достовірності відображеної інформації, захищає від спроб підробки чи спотворення даних і відповідає сучасним вимогам до безпеки в освітніх IT-системах.

ДЖЕРЕЛА

1. Gandon F., Schreiber G. RDF and SPARQL: Foundations for Semantic Web Technologies. – W3C Education, 2021.

2. OWASP Foundation. OWASP Top Ten Web Application Security Risks. – https://owasp.org/www-project-top-ten/

3. RFC 6749: The OAuth 2.0 Authorization Framework. – IETF – https://datatracker.ietf.org/doc/html/rfc6749

ЗАХИСТ ІНФОРМАЦІЇ В ІНФОКОМУНІКАЦІЙНІЙ МЕРЕЖІ ВІД ВПЛИВУ КОМП’ЮТЕРНИХ ВІРУСІВ

Чернігівський І. А.

Київський столичний університет імені Бориса Грінченка, м. Київ

У сучасній інфокомунікаційній мережі (ІКМ) її структурні елементи розподілені між собою та об'єднані в єдине інформаційне середовище. При цьому необхідність забезпечення безперебійного функціонування ІКМ в умовах впливу кібератак та комп’ютерних вірусів обумовлює створення необхідних умов для вирішення задач контролю стану мережі для своєчасного виявлення тривожних подій, під якими розуміється виявлення таких ознак, які б свідчили про зараження певних технічних засобів у мережі. Для того, щоб досягти необхідного рівня захищеності інформації в

такій мережі, мають бути прийняті правильні і своєчасні управлінські рішення на основі достовірних даних для запобігання майбутніх небажаних наслідків.

Проте, як свідчить аналіз наукових робіт [1], дослідники розглянули можливі рішення для вивантаження артефактів з ПК, проведення Live Computer Forensics та визначення місць розташування цифрових артефактів. Тож потребує подальших досліджень розробка нових підходів до створення сучасного механізму захисту комп'ютерного середовища та інформації від шкідливих програм і кібератак, а також вдосконалення наявних методів ідентифікації ШПЗ на ПК, що захистить інформацію в мережі від впливу комп'ютерних вірусів.

Додатково до цього, корпоративні ПК мають невизначений термін підключення до мережі, а до аналітика інформаційної безпеки зазвичай ставиться конкретний перелік питань, які не завжди потребують збору усіх наявних артефактів. У цьому випадку функціонал програм Forensic Triage (частковий збір артефактів з активного ПК) не є оптимальним для вирішення завдань аналітика. Вищенаведене обумовлює необхідність прискорення збору необхідних цифрових артефактів з ОС Windows для проведення Forensic Triage в умовах, де у аналітика є вичерпний час на підключення до досліджуваного ПК [2].

Метою дослідження є формування системного підходу до вирішення задачі захисту інформації в ІКМ від впливу комп'ютерних вірусів з обґрунтуванням словника специфічних ознак, що необхідні для виявлення певних тривожних подій, і забезпечення підтримки цільового стану ІКМ. При цьому, зазначений словник ознак повинен бути достатнім для прийняття рішень у циклах управління системи захисту інформації.

Вирішення задачі досягається за допомогою побудови системи захисту інформації у вигляді системи управління, що забезпечує підтримку цільового стану об'єкта управління. Для цього обґрунтовано основні завдання для створення системи захисту інформації від впливу ШПЗ, побудованої за принципом керуючої системи. Запропоновано в якості ідентифікаційних ознак стану інфокомунікаційної мережі для виявлення тривожних подій використання таких цифрових артефактів, які залишаються в результаті реалізації ШПЗ певних шкідливих дій. Розглянуто можливість використання Forensic-аналізу з неповним набором цифрових артефактів (проведення Forensic Triage). Визначено множину універсальних артефактів, виявлення яких на досліджуваному комп'ютері свідчить про 100% зараженість [3].

Побудова системи захисту інформації у вигляді автоматизованої системи управління, спрямованої на забезпечення підтримки цільового стану інфокомунікаційної мережі, дозволяє забезпечити необхідний рівень захищеності інформації.

Зазначений словник ознак для ідентифікації стану ІКМ є достатнім для прийняття рішень в циклах управління системи захисту інформації.

Практичне значення отриманих результатів полягає у можливості їх застосування в різних галузях для вдосконалення методів захисту інформації від впливу комп'ютерних вірусів і більш ефективного використання часу аналітика інформаційної безпеки при проведенні Forensic-аналізу елементів інфокомунікаційної мережі.

Подальші дослідження доцільно зосередити на тестуванні антивірусних рішень для корпоративного сегменту.

ДЖЕРЕЛА

1. D. -Y. Kao and G. -J. Wu, A Digital Triage Forensics framework of Window malware forensic toolkit: Based on ISO/IEC 27037:2012, 2015 International Carnahan Conference on Security Technology (ICCST), Taipei, Taiwan, 2015, pp. 217-222. URL: https://ieeexplore.ieee.org/document/7389685/authors

2. Bohdanov O., Chernihivskyi I. Types of digital forensic artifacts in windows computers. Cybersecurity: Education, Science, Technique. 2024. Vol. 4, no. 24. P. 221–228. URL: https://doi.org/10.28925/2663-4023.2024.24.221228

3. Чернігівський , І., & Крючкова, Л. (2025). Системний підхід до вирішення задачі захисту інформації в інфокомунікаційній мережі від впливу комп'ютерних вірусів. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, *3*(27), 572–590. https://doi.org/10.28925/2663-4023.2025.27.781

МЕТОДИ ПРОТИДІЇ В РАДІОНАВІГАЦІЙНИХ КОНФЛІКТАХ

Шандрук М. С.

Київський столичний університет імені Бориса Грінченка, м. Київ

Необхідність радіонавігаційних систем відіграє критично важливу роль у забезпеченні точності та безпеки навігації в авіації, мореплавстві, автомобільному транспорті та військових операціях. Проте зростання залежності від цих систем створює нові виклики, пов'язані з їх уразливістю до радіонавігаційних конфліктів, таких як глушіння сигналів (Jamming), навмисна передача фальшивих сигналів GNSS (Spoofing) та інші види радіоелектронного впливу. Дослідження методів протидії в радіонавігаційних конфліктах є актуальним і необхідним для підвищення стійкості радіонавігаційних систем та національної безпеки. В доповіді розглядаються загрози радіонавігаційних систем, зокрема глушіння сигналів та передача фальшивих сигналів, а також сучасні підходи до їх нейтралізації.

Сучасні методи боротьби з завадами часто базуються на статичних підходах, які не враховують змінність середовища та неможливість швидкого адаптування до змінних умов. Саме тому актуальним є розробка методів, які забезпечують гнучке використання спектра, автоматичне виявлення завад і миттєве реагування на потенційні загрози [1].

Метод динамічного спектрального адаптування (DSA – Dynamic Spectral Adaptation), дозволяє навігаційним системам змінювати частотний діапазон та алгоритми модуляції сигналу залежно від поточної ситуації в спектрі радіочастот. Метод DSA базується на технології когнітивного радіо (Cognitive Radio), що дозволяє системі безперервно аналізувати спектр радіочастот та в разі виявлення конфлікту або завад автоматично змінювати частоту передавання сигналу. Головна ідея цього підходу – використання штучного інтелекту та алгоритмів машинного навчання для аналізу завад і вибору оптимального рішення в режимі реального часу.

Активне застосування в нашій країні дронів, супутникових систем зв’язку та військових комплексів потребує підвищеної стійкості до навігаційних атак. Традиційні методи, такі як фільтрація сигналів або збільшення потужності передавачів, часто є недостатньо ефективними у боротьбі з навмисними атаками на навігаційні системи [2].

Метод DSA вирішує цю проблему шляхом впровадження принципу самоадаптації: замість того, щоб намагатися зменшити вплив завад, система їх активно аналізує та підлаштовує параметри корисного сигналу для мінімізації їхнього впливу. Це особливо важливо у військових застосуваннях, де швидке реагування на впливи Jamming або Spoofing може відігравати вирішальну роль у виконанні бойових завдань [3].

Крім того, у комерційній сфері, зокрема у цивільній авіації та автономних транспортних засобах, застосування DSA дозволить забезпечити більш стабільний зв’язок навіть у складних умовах, таких як щільна міська забудова або складні погодні умови.

Для перевірки ефективності методу DSA було розроблено серію комп’ютерних симуляцій у MATLAB та Simulink, а також випробувано програмно-конфігуровані радіосистеми (Software-Defined Radio). У ході експериментів було створено сценарії із штучними завадами, такими як глушіння сигнал та передача фальшивих сигналів GNSS. Випробування показали, що метод DSA дозволяє знизити втрати сигналу на 60-80% порівняно з традиційними методами. Крім того, система реагувала на завади у середньому за 1,2 секунди, що приблизно у 5 разів швидше, ніж стандартні алгоритми адаптації. Також була проведена оцінка енергоспоживання: використання DSA дозволило знизити витрати енергії на передачу сигналу в середньому на 30%, оскільки система автоматично оптимізувала рівень потужності передавання.

Метод динамічного спектрального адаптування має потенціал значно підвищити надійність навігаційних систем, зменшивши вплив зовнішніх

завад та атак. Метод DSA є перспективним рішенням для боротьби з радіонавігаційними конфліктами, оскільки дозволяє системам автоматично адаптуватися до змін у радіочастотному середовищі та швидко реагувати на загрози. Його головною перевагою є динамічне налаштування параметрів корисного сигналу залежно від умов, що значно підвищує стійкість до завад. Метод динамічного спектрального адаптування демонструє високу ефективність у забезпеченні безперебійної роботи радіонавігаційних систем в умовах дії навмисних радіоелектронних завад. Його впровадження є перспективним напрямом розвитку навігаційних технологій у контексті сучасних загроз.

ДЖЕРЕЛА

1. Опірський І., Бибик Р. Дослідження сучасних методів реб та методів і засобів її протидії. Український науковий журнал інформаційної безпеки. 2023. Т. 29, № 2. С. 88–97.

2. Сучасні радіонавігаційні системи та комплекси [Електронний ресурс]: лаб. практикум: навч. посіб. для здобувачів ступеня магістра за освіт. програмою «Радіотехнічні комп’ютеризовані системи» спец. 172 Електронні комунікації та радіотехніка / В. М. Васильєв; КПІ ім. Ігоря Сікорського. Електрон. текст. дані. Київ: КПІ ім. Ігоря Сікорського, 2024. 85с.

3. Захарін Ф.М. Алгоритмічне забезпечення інерціально-супутникових систем навігації: монографія / Ф.М. Захарін, В.М. Синєглазов, М.К. Філяшкін Київ: Вид-во Нац. Авіа. Ун-ту «НАУ-друк», 2011. 320 с.

ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДІВ АВТЕНТИФІКАЦІЇ У ВЕБ-ЗАСТОСУНКАХ

Шерстньов М. А.

Державний університет інформаційно-комунікаційних технологій, м. Київ

У сучасних веб-застосунках захист сесій користувачів та конфіденційних даних стало першочерговим завданням. Механізми автентифікації слугують першою лінією захисту від несанкціонованого доступу використовуючи різноманітні методи: JWT токени в локальному сховищі, ідентифікатори сесій та автентифікація на основі кукі. Кожен з методів пропонує різні переваги, та вибір правильного методу залежить від міркувань щодо безпеки. Автентифікація на основі кукі, використовуючи імплементацію httpOnly захищених кукі, пропонує надійне рішення для багатьох уразливостей безпеки.

Фундаментальні задачі безпеки у веб-автентифікації виходять з потреби у підтримці стану користувача через безстатусні HTTP запити та одночасного запобігання викрадення даних або перехвату сесій.

Традиційні підходи такі, як збереження токенів автентифікації в локальному сховищі або сесійному сховищу, відкривають застосунок до критичних уразливостей, особливо XSS(крос-сайт скриптинг) атак. Коли токени зберігаються через ці клієнтські механізми, вони стають доступними для будь-якого JavaScript коду, який виконується у контексті застосунку. Як наслідок, зловмисні скрипти, що інжектуються через XSS уразливості, можуть легко витягти ці токени та призвести до злому акаунту. Це дуже серйозна уразливість, яка не може бути вирішена, якщо токени зберігаються у сховищі, відкритому для JavaScript [1].

Альтернативний метод використовує автентифікацію на основі JWT з клієнтським сховищем, базовою автентифікацією та ідентифікованими сесіями на стороні серверу. Цей підхід пропонує відмінну масштабованість та безстатусність запитів, але страждає від вищезгаданих XSS уразливостей, коли зберігається в локальному сховищі. Базова автентифікація передає дані у кожному запиті і не підтримує гранулярний контроль терміну дії. Сесії на стороні серверу надають міцний захист, але можуть спричинити проблеми з масштабованістю у розподілених оточеннях та мати вразливості до атак фіксації сеансу(Session Fixation Attack), якщо не побудовані правильно. Очевидно, що ці альтернативні методи пропонують нові варіанти автентифікації намагаючись балансувати між захистом та ефективністю.

Автентифікація на основі кукі використовуючи httpOnly кукі пропонує кращий захист через вирішення критичної уразливості викрадення токенів при XSS атаках. Налаштування httpOnly запобігає виконуючому JavaScript коду на стороні клієнту можливість доступу до змісту кукі, фактично ізолюючі токен автентифікації від потенційних зловмисних скриптів. Автентифікація на основі кукі створює міцний шар захисту, який запобігає більшості атак на токени. Крім того, кукі підтримує автоматичне закінчення терміну дії та захисні атрибути для контролю сесій [2].

Крім того, до запобіганню XSS атак, цей метод надає глибокий захист через підтримку багатьох додаткових функцій безпеки. Кукі з налаштованими SameSite політиками захищають від міжсайтових підробок запитів (CSRF), коли запити від чужих серверів не включають автентифікаційні кукі. Реалізація правильних CSRF токенів далі доповнює переваги кукі. Також кукі пропонують нативну підтримку захищеної передачі даних через налаштування Secure, який обмежує сферу дії кукі та налаштування Path атрибуту, який вказує у яких частинах застосунку має бути доступ до кукі. Ця багатошарова система захисту ідеально підходить до сучасних принципів розробки та використання веб-застосунків.

Хоча жоден з механізмів не дає абсолютного імунітету до усіх можливих уразливостей та атак, httpOnly кукі-автентифікація пропонує найбільш збалансований підхід для застосунку, коли захист

конфіденційних даних є пріоритетом. Один тільки захист від XSS атак надає достатню перевагу для використання цього методу замість локального сховища. Використовуючи кукі-автентифікацію у своєму застосунку може значно збільшити захист від поширених уразливостей, пов'язаних з автентифікацією, зберігаючи при цьому зручний користувацький досвід.

ДЖЕРЕЛА

1. Best Practices for Storing Access Tokens in the Browser. URL: https://curity.medium.com/best-practices-for-storing-access-tokens-in-the-browser-6b3d515d9814

2. Kwon, Hyunsoo & Nam, Hyunjae & Lee, Sangtae & Hahn, Changhee & Hur, Junbeom. (2019). (In-)Security of Cookies in HTTPS: Cookie Theft by Removing Cookie Flags. IEEE Transactions on Information Forensics and Security. PP. 1-1. 10.1109/TIFS.2019.2938416.

ПРИНЦИПИ ПОБУДОВИ НАДІЙНОЇ СИСТЕМИ ДЛЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У СИСТЕМАХ УПРАВЛІННЯ ПЕРСОНАЛОМ

Щербаков О. О.

Державний університет інформаційно-комунікаційних технологій, м. Київ

У сучасній IT-сфері системи для управління персоналом обробляють велику кількість чутливої інформації: персональні дані працівників, проєктні дані, фінансову звітність, інтелектуальну власність тощо. Через постійний потік кадрів, роботу з великою кількістю клієнтів та високий ризик кібератак, потрібно весь час приділяти увагу до забезпечення безпеки даних, в іншому випадку доведеться розбиратися з серйозними фінансовими втратами і неприємними юридичними наслідками.

Дослідження основних принципів побудови надійної системи безпеки в застосунках для управління персоналом та їх порівняльний аналіз.

В ході цього дослідження були знайдені три найпоширеніші принципи для забезпечення безпеки даних – принцип мінімізації прав доступу, принцип розмежування обов'язків, принцип захисту «глибина оборони».

Правило найменших привілеїв, також відоме як PoLP – принцип, суть якого полягає в тому, що користувачі, програми та системи мають лише мінімальний доступ, необхідний для виконання їх завдань [1]. Дуже простий принцип, який запобігає накопиченню великої кількості прав в руках одного користувача системи. Крім того завжди можна відізвати права на певну дію або доступ до певної інформації, як тільки необхідна

задача була виконана. Таким чином, безпека забезпечується на всіх рівнях і у всіх ролях в системах, запобігаючи внутрішнім та зовнішнім загрозам.

Розподіл обов'язків або SoD –це фундаментальний принцип управління ризиками, який забезпечує розподіл ключових завдань між кількома користувачами, щоб зменшити ризик шахрайства, помилок або зловмисних дій [2]. Його суть – розбити задачу, яку може виконати один користувач, на декілька підзадач з метою того, щоб одна людина не мала повного контролю над задачею. Це забезпечує наявність як мінімум двох користувачів, які відповідають за виконання критично важливого завдання, або необхідність схвалення від іншої сторони перед завершенням задачі, що дозволить запобігти серйозним наслідкам.

Принцип глибокого захисту або Defense in Depth - полягає в тому, що багаторівневі механізми безпеки підвищують безпеку системи в цілому [3]. Суть цього методу полягає у тому, що одного заходу безпеки буде недостатньо. Один брандмауер не захистить від можливих інцидентів. Порушники є кваліфікованими спеціалістами і можуть атакувати систему з різних сторін, тому потрібно думати про уразливі місця в безпеці персоналу, технологій і операцій протягом всього життєвого циклу системи. Тому у самій системі повинно бути накладено багато рівнів захисту на критичні системи, щоб захистити систему від будь-якої конкретної атаки за допомогою кількох різних методів.

Таким чином, всі ці методи спеціалізуються на різних загрозах для системи. Правило найменших привілеїв знижує ризик на всіх рівнях системи, але при цьому користувач все ще має всі права для виконання своєї задачі, що може призвести до помилок в виконанні задачі. Розподіл обов'язків забезпечує перевірки перед завершенням задачі, що прекрасно доповнює Правило найменших привілеїв, але все ще не є ідеальним захистом даних в системі. Нарешті, Принцип глибокого захисту захищає систему з багатьох напрямів, але лише в найважливіших точках, що може бути дуже трудомістким.

Аналіз усіх сильних та слабких сторін цих методів показав, що для найефективнішого захисту потрібне використання декількох принципів. Крім того, при імплементації цих принципів потрібно враховувати велику кількість факторів – персонал компанії і їх компетентність, скільки ресурсів можна виділити на забезпечення захисту даних і таке інше.

У нашому дослідження «Розробка web-застосунку для управління персоналом IT-аутсорсингової компанії» були використані принцип мінімізації прав доступу та принцип розмежування обов'язків. Практичне застосування принципів засновуються на наявності ролей в створеному веб-застосунку. Ці ролі надаються адміністратором, що дозволить забезпечити контроль доступу до чутливої інформації та зменшити ризики внутрішніх загроз, які виникають через людський фактор або компрометацію облікових записів. В той же час, можливості в системі, які

чітко визначені наданою роллю, забезпечують прозорість дій користувачів у системі, зменшують ризик шахрайства та підвищують довіру до системи з боку працівників і менеджменту компанії.

ДЖЕРЕЛА

1. Understanding the Principle of Least Privilege - legitsecurity.com – [Електронний ресурс] – Режим доступу: https://www.legitsecurity.com/aspm-knowledge-base/what-is-the-principle-of-least-privilege-polp.
2. What is Separation of Duties - pathlock.com – [Електронний ресурс] – Режим доступу: https://pathlock.com/learn/separation-of-duties-in-your-organization/.
3. Defense in Depth - sciencedirect.com – [Електронний ресурс] – Режим доступу: https://www.sciencedirect.com/topics/computer-science/defense-in-depth.

ПРОБЛЕМА ВІДКРИТИХ API-КЛЮЧІВ

Яскевич Ю. В.
Київський столичний університет імені Бориса Грінченка, м. Київ

Відкриті API-ключі –це облікові дані, які через необережність розробників стають доступними стороннім особам, наприклад, через публікацію в коді на платформах типу GitHub. Такі ключі, жорстко закодовані в програмному коді замість використання безпечних методів зберігання, можуть призвести до серйозних наслідків: несанкціонованого доступу до систем, витоку конфіденційної інформації, фінансових махінацій чи порушення приватності користувачів. Проблема виникає через недбалість розробників та відсутність належних практик безпеки при роботі з секретами.

Проблема витоків API-ключів стрімко зростає через збільшення обсягу коду, що публікується онлайн. За даними досліджень, у 2023 році на GitHub було виявлено 12,8 мільйона нових витоків секретів, що на 28% більше, ніж у 2022 році [1]. Цей ріст пов’язаний із розширенням кількості репозиторіїв –у 2023 році їх стало на 22% більше, досягнувши 50 мільйонів. Таке зростання свідчить про масштабування проблеми в умовах активного розвитку програмного забезпечення.

GitHub відіграє ключову роль як платформа для хостингу коду, але водночас є одним із головних джерел витоків API-ключів. У 2023 році на платформі виявили понад 1 мільйон дійсних Google API-ключів та 140,000 дійсних AWS-ключів [1]. Додатково, дослідження 1 мільйона вебдоменів показало, що 18,000 токенів API (приблизно 1,8%) були експоновані [2]. Наслідки таких витоків включають втрату даних, фінансові збитки та навіть використання скомпрометованих ключів для створення серверів для майнінгу криптовалюти, як у випадках із AWS.

Вище зазначене визначило актуальність дослідження методів приховування API ключа. Розглянемо їх.

1. Обфускація та шифрування. У мобільних і веб-додатках обфускація коду (наприклад, за допомогою UglifyJS) або шифрування рядків створюють додатковий бар'єр для випадкових зловмисників, ускладнюючи читання ключа в JavaScript-бандлі. Проте цей підхід легко обійти через реверс-інжиніринг або аналіз мережевого трафіку, тому обфускація не гарантує повної безпеки в браузері або десктоп-додатку [3].

2. Файл .env з .gitignore. Розміщення ключа в окремому файлі .env, який занесено до .gitignore, запобігає випадковому коміту в публічний репозиторій. Така практика знижує ризик витоку через Git, але не захищає ключ, якщо він потрапляє в клієнтський код –браузерні інструменти розробника й надалі покажуть значення змінної [4].

3. Змінні оточення на сервері. Для серверних додатків зберігання ключа в process.env (файл .env або налаштування хостингу) забезпечує, що значення ніколи не потрапляє в код, який віддається клієнту. Це простий і надійний спосіб для бекенду, але в разі фронтенду змінні все одно збираються в бандл і стають доступними в браузері [5].

4. Обмеження API-ключа. Налаштування використання ключа лише з певних доменів, IP-адрес або шляхів зменшує наслідки його викрадення. Хоча це не приховує сам ключ, обмеження в налаштуваннях OpenWeatherMap чи Google Maps захищають від несанкціонованих запитів, якщо ключ опинився в чужих руках [6].

5. Безсерверні функції. Платформи типу Netlify Functions, Vercel чи AWS Lambda дозволяють створити легкий проксі без власного сервера. Запит від клієнта іде до функції, яка містить ключ у безпечному середовищі, звертається до API й повертає дані. Такий підхід мінімізує інфраструктурні витрати, але може потребувати оптимізації під високий трафік та обмежений час виконання [7].

6. Серверний проксі. Найбільш надійне рішення: власний сервер (наприклад, на Node.js з Express) приймає запити від клієнта і пересилає їх до API, зберігаючи ключ у закритому середовищі. Це повністю приховує ключ від кінцевого користувача, дозволяє додати кешування, логування й обмеження частоти запитів, проте вимагає налаштування та підтримки серверної інфраструктури [8].

ДЖЕРЕЛА

1. Help Net Security: 90% of exposed secrets on GitHub remain active for at least five days. URL: https://www.helpnetsecurity.com/2024/03/15/github-sensitive-information-exposure/.

2. Escape.tech: The API Secret Sprawl 2024 report on API key exposure. URL: https://escape.tech/the-api-secret-sprawl-2024?ref=escape.tech.

3. Best practice for storing and protecting private API keys in applications. Stack Overflow. URL: https://stackoverflow.com/questions/14570989/best-practice-for-storing-and-protecting-private-api-keys-in-applications.

4. Best Practice for Hiding API Keys. Codementor. URL: https://www.codementor.io/@priteshmodi/best-practice-for-hiding-api-keys-1kfesf7ne8.

5. Das R. API keys: Weaknesses and security best practices. TechTarget. URL: https://www.techtarget.com/searchsecurity/tip/API-keys-Weaknesses-and-security-best-practices.

6. Google Maps Platform security guidance. Google for Developers. URL: https://developers.google.com/maps/api-security-best-practices.

7. Vargas S. How to Hide Your API Keys. Medium. URL: https://medium.com/better-programming/how-to-hide-your-api-keys-c2b952bc07e6.

8. The Safest Way To Hide Your API Keys When Using React. Smashing Magazine. URL: https://www.smashingmagazine.com/2023/05/safest-way-hide-api-keys-react/.

ЗМІСТ

Наукове видання
ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ – 2025
Збірник тез XII Всеукраїнської науково-практичної
конференції молодих учених
15 травня 2025 року
м. Київ

Відповідальні за випуск:
М.М. Астаф'єва,
Д.М. Бодненко,
О.М. Глушак,
І.В. Машкіна,
О.В. Локазюк,
В.В. Прошкін,
С.М. Шевченко