

Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Інститут цифровізації освіти НАПН України
Національний технічний університет України «Київський політехнічний
інститут» ім. І. Сікорського
Вінницький національний технічний університет
Житомирський військовий інститут імені С.П. Корольова
Тернопільський національний технічний університет імені Івана Пулюя
Харківський національний університет радіоелектроніки
Уманський державний педагогічний університет імені Павла Тичини
Національний університет біоресурсів і природокористування України
Державна наукова установа «Український інститут науково-технічної
експертизи та інформації»
Черкаський державний технологічний університет
Національний авіаційний університет

ТЕЗИ ДОПОВІДЕЙ

*VI Всеукраїнської науково-технічної
конференції*

**Комп'ютерні технології:
інновації, проблеми, рішення**

м. Житомир, 29-30 листопада 2023 р.

Житомир
2023

УДК 004

*Рекомендовано до друку Вченою радою Державного університету
«Житомирська політехніка» (протокол № 15 від 05.12.2023 р.)*

K63 Комп'ютерні технології: інновації, проблеми,
рішення: тези VI Всеукраїнської науково-технічної
конференції, м. Житомир, 29-30 листопада 2023 р. – Житомир:
Житомирська політехніка, 2023. – 382 с.

ISBN 978-966-683-637-6

Представлено доповіді учасників VI Всеукраїнської науково-технічної конференції. Наведено аналіз та результати досліджень сучасних проблем інформаційних технологій, математичного моделювання та розробки програмного забезпечення, інформаційних систем, комп'ютерної інженерії та кібербезпеки, цифрової обробки сигналів та зображень, комп'ютерно-інтегрованих технологій, робототехніки та приладобудування, інформаційних технологій в телекомунікаціях та біомедицині, інформаційно-комунікаційних технологій в освіті.

УДК 004

Наукове видання

Тези VI Всеукраїнської науково-технічної
конференції «Комп'ютерні технології: інновації,
проблеми, рішення»,
Житомир, 29-30 листопада 2023 р.

Відповідальний за випуск

О. Л. Коренівська

Свідоцтво про внесення до Державного реєстру суб'єктів видавничої справи ДК № 7177 ВІД 04.11.2021 р.

Адреса редакції: Державний університет «Житомирська політехніка»,
вул. Чуднівська, 103, м.Житомир, 10005

ISBN 978-966-683-637-6

© Житомирська політехніка, 2023

Секція 1 МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ТА РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

УДК 004.62

**Чухов В. В., к.т.н., доцент,
Варганова Д. О., ст. викладач,
Ващенко А. І., здобувач**

Державний університет «Житомирська політехніка»

АНАЛІЗ МЕТОДІВ СОРТУВАННЯ МАСИВІВ, ПОРІВНЯННЯ ШВИДКОДІЙ

У сучасному світі інформаційних технологій потреба в швидкому та оптимізованому пошуку та впорядкуванні інформації відіграє ключову роль. Сортування масиву, будучи процесом впорядкування всіх елементів масиву за деякими критеріями, є надійним способом прискорення роботи практично будь-якого алгоритму. Операції над масивами мають ряд переваг: ефективна адресація та пошук даних, покращення швидкодії обробки масивів, забезпечення коректного використання та організації даних. Тому задачі на сортування мають надзвичайно важливе значення.

Розглянемо на практиці деякі методи сортування, а саме: сортування вставками, метод Шелла, пірамідальне сортування. Зокрема, проаналізуємо швидкодії даних методів, виконаємо сортування та проведемо дослідження співвідношення часу виконання до кількості елементів. Виконаємо порівняння на основі медіани даних, отриманих в процесі сортування псевдовипадково згенерованого масиву, кількість елементів якого лінійно збільшується з 1000 до 100000 одиниць кроком в 1000 елементів (рис. 1, 2).

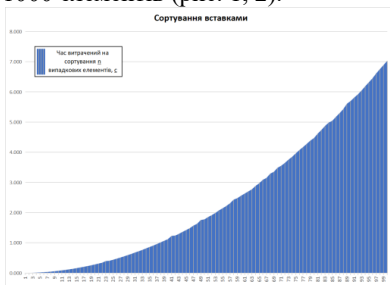


Рис. 1. Графік співвідношення швидкодії сортування масиву вставками до кількості його елементів

```
int c = 0;
for (int i = 1; i < maxlen; i++) {
    c = arr[i];
    for (int j = i - 1; j >= 0 && arr[j] > c; j--) {
        arr[j + 1] = arr[j];
        arr[j] = c;
    }
}
```

Рис. 2. Фрагмент коду на мові С. Сортування вставками

Проведемо аналогічне дослідження сортування методом Шелла і пірамідального сортування. Візуалізацію усіх результатів подамо у вигляді спільного графіка даних методів, за допомогою якого можна проаналізувати швидкодії методів сортування (рис. 3). Переваги, недоліки та показники ефективності даних методів наведено в табл. 1.

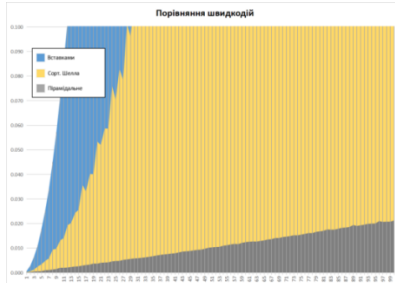


Рис. 3. Графік швидкодій методів сортування

Таблиця 1

Метод сортування	Переваги	Недоліки
Сортування вставками	Проста реалізація	Має складність $O(n^2)$
	Висока ефективність на масивах невеликого об'єму даних.	Можлива нестабільність методу при повторюваності даних
	Висока ефективність на частково відсортованих масивах	Низька ефективність для великої кількості даних
Метод Шелла	Має складність $O(n \log^2 n)$	Низька ефективність для даних, що розміщені далеко один від одного
	Адаптація для великого об'єму даних	
	Оптимізована система порівнянь елементів	Можлива нестабільність методу при повторюваності даних
Пірамідальне сортування	Проста реалізація та оптимальна швидкодія	
	Має складність $O(n \log n)$	Складна реалізація
	Висока ефективність на великих об'ємах даних	На майже відсортованих масивах працює так само довго, як і на хаотичних даних
	Універсальний метод сортування	

Список використаних джерел

1. Крєневич А.П. Алгоритми і структури даних. Підручник. – К.: ВПЦ "Київський Університет", 2021. – 200 с.

2. Мелешко Є.В., Якименко М.С., Поліщук Л.І. Алгоритми та структури даних: Навчальний посібник для студентів технічних спеціальностей денної та заочної форми навчання. – Кропивницький: Видавець – Лисенко В.Ф., 2019. – 156 с.

УДК 004.43

*Полоневич Д. В., магістрант
Вакалюк Т. А., д.пед.н., професор
Державний університет «Житомирська політехніка»*

АНАЛІЗ МОЖЛИВОСТЕЙ КРОСПЛАТФОРМОВОГО НАБОРУ ІНСТРУМЕНТІВ GTK ПРИ СТВОРЕННІ ВІДЕОРЕДАКТОРА

Відеоредактори відіграють ключову роль у сучасному цифровому світі, надаючи користувачам можливість творчо виражати свої ідеї через медійний контент. Забезпечуючи інструменти для обробки, монтажу та покращення відеоматеріалів, вони стають невід'ємною частиною виробництва відеоконтенту для платформ соціальних мереж, відеоблогів, та інших цифрових проєктів. Ці редактори допомагають не лише зробити відео естетично привабливим, а й надають можливість вираження креативності та створення вражаючого візуального вмісту.

GTK, колишній GTK+, (від The GIMP ToolKit) – є бібліотекою для створення графічних інтерфейсів користувача в програмах. Ця бібліотека широко використовується у багатьох проєктах, і вона підтримується мовами програмування, такими як C, C++, Python, і багатьма іншими. При створенні відеоредактора за допомогою бібліотеки GTK можна та варто використовувати її можливості для створення графічного інтерфейсу та інтеграції функціоналу відео редагування [1].

Основні можливості бібліотеки:

- створення GUI програми: легко створити вікна, різні кнопки, панелі інструментів, меню та інші елементи інтерфейсу для зручної взаємодії з користувачем;
- інтеграція з іншими відео-бібліотеками: найбільш популярним рішенням поєднанням є GStreamer або OpenCV, для реалізації функціоналу зчитування, обробки та відтворення відео;
- обробка подій та взаємодія з користувачем: система подій, що доступна з коробки дозволяє відстежувати дії користувача, такі як натискання кнопок, переміщення миші та інші;
- використання ресурсів та тем: налаштування зовнішнього вигляду відео редактора та його подальшої кастомізації;
- мультимовленість: підтримує різні мови програмування (C++, Fortran, Perl, Ruby, Python, Java, C#), таким чином у розробника програмного продукту є вибір стеку розробки, що найбільш відповідатиме потребам та вмінням.

Модульність GTK (GIMP Toolkit) реалізована через концепцію модулів. Модуль – це невеликий блок коду, який може бути динамічно завантажений та розширює функціональність GTK. Ця модульна структура дозволяє розробникам використовувати лише ті частини GTK, які їм потрібні для конкретного проекту. Основні модулі GTK: Glib (основна бібліотека, на якій ґрунтується GTK, вона надає основні структури даних, систему типів та роботу з пам'яттю), GObject (система об'єктів, надає можливості для об'єктно-орієнтованого програмування, включаючи спадкування, інкапсуляцію та поліморфізм), Gdk (бібліотека для роботи з низькорівневими операціями малювання та обробки подій), Gtk (модуль для створення графічного інтерфейсу, включає різні елементи GUI, такі як вікна, кнопки, меню та багато інших).

GTK є відкритою бібліотекою для створення графічних інтерфейсів користувача, і вона є частиною проекту GNU. Її відкритий вихідний код дає розробникам велику гнучкість і можливість адаптації для різноманітних проектів. GTK надає вичерпну документацію, що включає в себе описи класів, функцій та приклади коду, що значно полегшує процес вивчення та використання цієї бібліотеки у розробці програмного забезпечення з графічним інтерфейсом [2].

Найбільш вдалі та популярні відеоредактори, що створені на базі GTK, є Piviti та OpenShot. Обидва редактори, Piviti та OpenShot, є потужними та безкоштовними інструментами для редагування відео під операційною системою Linux, і вони надають користувачам широкі можливості для створення та редагування відеоматеріалів [3, 4].

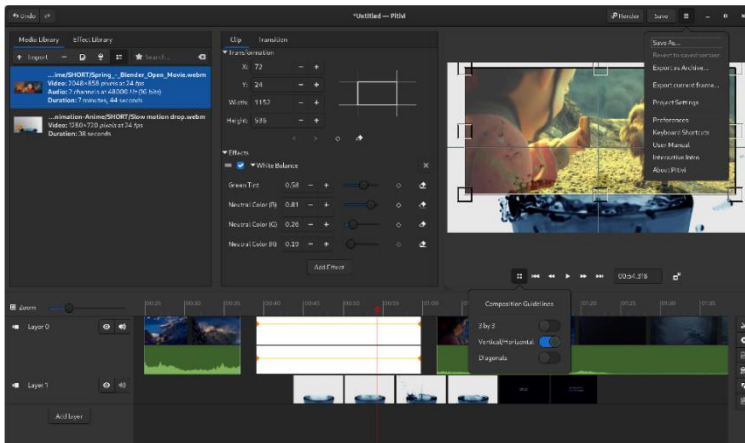


Рис. 1. Зовнішній вигляд відеоредактора PiTiVi версії 2021.01

Серед можливостей Píivi можна відзначити підтримку необмеженого числа шарів, збереження повної історії операцій з можливістю відкоту, відображення ескізів на шкалі часу, підтримку типових операцій обробки відео і звуку.

Серед можливостей OpenShot можна відзначити інтуїтивний інтерфейс, можливість обробки відео та аудіо, застосування різноманітних переходів та ефектів. OpenShot також підтримує створення анімацій та ключових кадрів для точного керування рухом та візуальними елементами. Завдяки інтеграції з Blender, редактор відкриває можливості для роботи з 3D-моделями та додавання вражаючих візуальних ефектів до проектів. Крім того, OpenShot підтримує різні формати відео, забезпечуючи гнучкість у роботі з різними типами мультимедіа.



Рис. 2. Зовнішній вигляд відеоредактора OpenShot

Аналіз бібліотеки GTK та відеоредакторів Píivi та OpenShot дало можливість визначити основні вимоги до відеоредактора, який буде розроблено. В процесі розробки було розроблено діаграму варіантів використання нелінійного відеоредактора, яку можна побачити на рисунку 3.

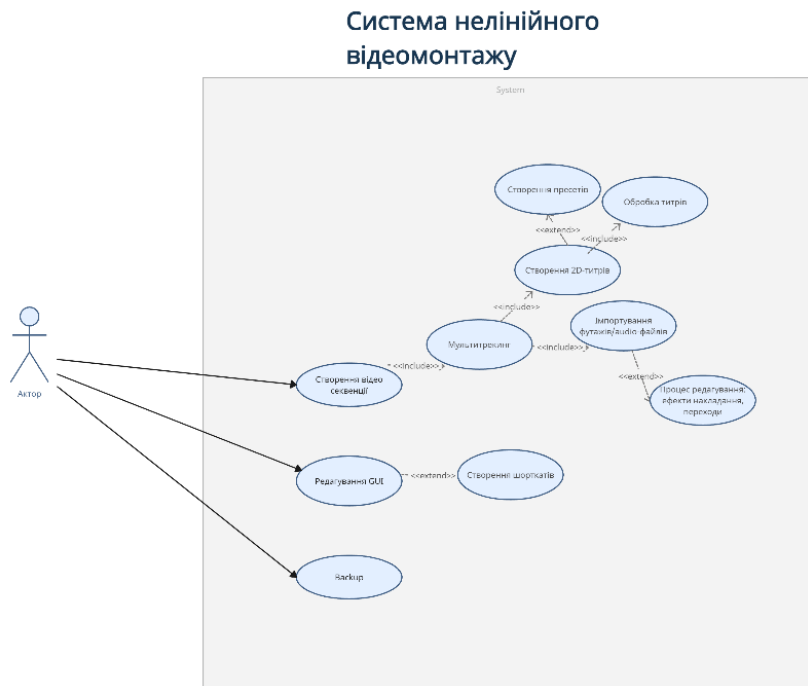


Рис. 3. Варіанти використання нелінійного відеоредактора

Список використаних джерел

1. The GTK Project [Електронний ресурс] – Режим доступу до ресурсу: <https://www.gtk.org/>.
2. GTK Documentation [Електронний ресурс] – Режим доступу до ресурсу: <https://docs.gtk.org/>.
3. Pitivi [Електронний ресурс] –Режим доступу до ресурсу: <https://www.pitivi.org/>.
4. OpenShot [Електронний ресурс] – Режим доступу до ресурсу: <https://www.openshot.org/>.

УДК 004.42

*Блоха Я. С., здобувач,
Петросян Р. В., ст. викладач
Державний університет «Житомирська політехніка»*

PWA ЯК ОДИН ІЗ СУЧАСНИХ ПІДХОДІВ ДЛЯ СТВОРЕННЯ МОБІЛЬНИХ ЗАСТОСУНКІВ

Сучасні мобільні застосунки, стикаються з проблемами, такими як обмеженість доступу до ринку через необхідність установки, знижена взаємодія з користувачем через обмежені ресурси і підтримка певних платформ. Багато бізнесів, можуть відчувати труднощі у створенні та підтримці власного мобільного застосунка через великі витрати і технічні труднощі [1]. Вирішенням є використання Progressive Web App (PWA) – технології, яка дає сайту функціональність застосунку[2].

PWA поєднує в собі переваги веб-сайту і мобільного застосунка, надаючи користувачам зручний доступ через браузер та збільшуючи взаємодію.

В основі PWA лежать 4 ключові технології, що революціонізують взаємодію веб-застосунків:

1. Service Worker. Service Worker – це JavaScript-файл, який дозволяє виконувати операції у браузері. Він може обробляти події, такі як push-повідомлення, працювати з кешем для збереження ресурсів на пристрої та виконувати завдання в офлайн-режимі. Це поліпшує швидкодію, доступність та ефективність роботи застосунка.

2. App Shell. App Shell – це архітектурний підхід, при якому основна оболонка сторінок PWA завантажується в кеш під час першого відвідування. Після цього, при подальшому використанні застосунка, лише контент завантажується з сервера. Це забезпечує швидке завантаження.

3. HTTPS. PWA працює виключно через захищений протокол HTTPS. Це забезпечує зашифровану передачу даних, що підвищує безпеку користувачів. Для забезпечення роботи через HTTPS, необхідно підключити SSL-сертифікат до налаштувань хостингу.

4. Web App Manifest. Web App Manifest – це файл, що містить дані про застосунок, такі як назва, іконка, режим вікна тощо. Він дозволяє налаштовувати вигляд і поведінку PWA на пристрої. Наприклад, режим вікна може бути мінімальним, автономним або повноекранним, що дає різноманітні варіанти відображення.

Дані технології, об'єднані в одне ціле, створюють потужну інфраструктуру для створення швидких і безпечних веб-застосунків, які можуть працювати як в онлайн, так і в офлайн-режимі, надаючи враження використання мобільного застосунка.

Розглянемо основні переваги використання даної технології:

- Легкий доступ без установки. PWA дозволяють користувачам отримувати доступ до застосунка через веб-браузер без необхідності встановлення. Це розширює аудиторію та спрощує взаємодію.

- Підтримка всіх платформ. PWA використовують стандартні веб-технології, тому підтримують всі основні платформи і пристрої, що робить їх універсальними для різних типів користувачів.

- Взаємодія в автономному режимі. PWA можуть працювати в автономному режимі, що дозволяє користувачам використовувати застосунок навіть при відсутності Інтернет - з'єднання.

- Збільшена швидкодія. PWA відзначаються високою швидкістю завдяки кешуванню ресурсів.

- Висока безпека. Використання протоколу HTTPS та інших стандартів безпеки робить цю технологію безпечною для використання. Інформація користувача та дані зашифровані, що зменшує ризик витоку конфіденційної інформації.

- Проста розробка та підтримка. Стандартні веб-технології, такі як HTML, CSS і JavaScript використовуються для створення PWA, що полегшує розробку та підтримку. Це зменшує витрати на розробку і спрощує майбутнє супровідне обслуговування.

Незважаючи на переваги PWA має обмеження та недоліки:

- Обмежені можливості на iOS. На деяких пристроях з iOS PWA не можуть повноцінно використовувати функціональність, наприклад, таку як push-повідомлення та фонові синхронізація. Однак з часом все може змінитися, оскільки Apple постійно вдосконалює підтримку PWA.

- Обмежені функції пристроїв. Деякі функції пристроїв, наприклад, такі як доступ до деяких сенсорів або розташування, можуть бути менш доступними порівняно з нативними застосунками, що може обмежити можливості застосунка.

- Не усі функції працюють в офлайн-режимі: Хоча PWA розроблені для роботи в офлайн-режимі, не всі функції можуть бути доступні без Інтернет-з'єднання. Залежно від реалізації і потреб застосунка, може бути обмежена функціональність в офлайн-режимі.

Список використаних джерел

1. Progressive Web Apps. *Google Developers*. URL: <https://developers.google.com/web/progressive-web-apps> (date of access: 12.11.2023).

2. Безуглий В.О., Петросян Р.В. Сучасні сайти як прогресивні веб-додатки. Тези XI Міжнародної науково-технічної конференції «Інформаційно-комп'ютерні технології – 2020», м. Житомир, 9-11 квітня 2020 р. Житомир: Житомирська політехніка. 2020. С. 35 – 36.

УДК 004.43

*Гаманюк І. А., здобувач,
Петросян Р. В., ст. викладач
Державний університет «Житомирська політехніка»*

ОСОБЛИВОСТІ МОВИ ПРОГРАМУВАННЯ RUST

За останні роки мова програмування Rust здобула значну популярність серед розробників програмного забезпечення. Rust була розроблена з метою боротьби з типовими та потенційно небезпечними вразливостями безпеки пам'яті [1, 2]. Розглянемо переваги використання мови Rust для підвищення надійності та безпеки програмного забезпечення.

Досить складною темою для програмістів C++ є невизначена поведінка (Undefined behavior). Навіть досвідчені розробники найчастіше неспроможні чітко сформулювати причини його виникнення. На рис.1 показано однаковий код, але результат буде різний при чому результат може змінюватися в залежності від компілятора, оптимізації тощо.

<pre>int val1 = INT_MAX; int val2 = val1 + 1; bool x = val1 > val2; cout << x << endl;</pre>		<pre>int val1 = INT_MAX; bool x = val1 > (val1 + 1); cout << x << endl;</pre>
---	--	--

Рис. 1. Порівняння коду на мові C++ з невизначеною поведінкою

Одна з найважливіших переваг Rust – це безпека пам'яті. Rust має унікальну модель безпеки, яка обіцяє безпеку пам'яті та конкурентну безпеку, забезпечуючи при цьому продуктивність рівня C/C++. На рис.2 показано код C++ (зліва) та Rust (справа) при роботі з покажчиками.

<pre>vector<int> v = { 1, 2, 3 }; int& v0 =v[0]; v.push_back(4); cout << v0 << endl;</pre>		<pre>let mut y = vec![1, 2, 3]; let v0 = &y[0]; v.push(4); println!("{}", v0);</pre>
--	--	--

Рис. 2. Порівняння кода при роботі з покажчиками

Rust забезпечує безпеку пам'яті через концепції «володіння» та «запозичення». Концепція «володіння» передбачає, що кожна частина пам'яті має одного власника, що запобігає помилкам використання після звільнення. Концепція «запозичення» дозволяє декільком фрагментам коду отримувати доступ до пам'яті одночасно, але лише

одному з доступом до зміни даних, запобігаючи «гонці» даних, коли декілька потоків або процесів одночасно намагаються змінити одні й ті ж самі дані. Rust також забороняє нульові покажчики, автоматично змінює розмір структур даних, включає перевірки переповнення для цілих чисел і багато іншого.

Однією з переваг Rust є наявність високоякісної документації та інструментів, які роблять мову доступною для вивчення та дозволяють розробникам створювати програмне забезпечення високої якості. Cargo – це інструмент управління пакетами та збіркою проектів. Він автоматизує завдання, такі як завантаження залежностей, компіляція та виконання тестів. Cargo також допомагає управляти версіями пакетів і спрощує процес створення та розповсюдження програм у Rust.

Rust широко використовується в різноманітних програмних проектах, включаючи ядра операційних систем, такі як Windows та Linux [3, 4]. Він також застосовується у безпекових рішеннях, наприклад, системах захисту від DDoS атак. Крім того, Rust використовується у сфері розробки ігор та графічних програм.

Завдяки тому, що Rust забезпечує надійність, безпеку та продуктивність, він набирає оберти у програмуванні вбудованих систем (embedded systems). Вбудовані системи – це спеціалізовані обчислювальні системи, які є частиною більших систем і виконують певні функції у режимі часу. Ці системи вбудовуються в інші пристрої, такі як мікроконтролери, і використовуються в різних сферах: автомобільні системи, пристрої Інтернету речей (IoT), промислові системи керування та інші.

Підсумовуючи можна відмітити, що Rust є відносно новою мовою програмування, але вона швидко набуває популярності. Це потужна мова програмування, яка забезпечує надійність, безпеку та продуктивність. Використовується майже у всіх напрямках програмування. Rust має потенціал, щоб стати однією з найважливіших мов програмування у майбутньому.

Список використаних джерел

1. Nichols C., Klabnik S. Rust Programming Language. No Starch Press. 2019. 560 p.
2. Learn rust. Rust Programming Language. URL: <https://www.rust-lang.org/learn> (date of access: 11.11.2023).
3. Gatlan S. New Windows 11 build ships with more Rust-based Kernel features. Bleeping Computer. URL: <https://www.bleepingcomputer.com/news/microsoft/new-windows-11-build-ships-with-more-rust-based-kernel-features/> (date of access: 11.11.2023).
4. Rust in the linux kernel. The New Stack. URL: <https://thenewstack.io/rust-in-the-linux-kernel/> (date of access: 11.11.2023).

УДК 004.43

*Болотіна В. В. ст. викладач,
Субчак Ю. Ю., здобувачка*

Державний університет «Житомирська політехніка»

ОПТИМІЗАЦІЯ ВЕБ-ДОДАТКІВ З ВИКОРИСТАННЯМ АСИНХРОННОГО ПРОГРАМУВАННЯ В JAVASCRIPT

У сучасному світі люди не уявляють свого життя без гаджетів. Щодня з'являються все нові і нові додатки та веб-ресурси, мета яких зробити життя людей простіше. Однією з основних вимог користувачів до веб-додатків є швидкість роботи, зручність інтерфейсу та зрозумілий інтерфейс. У світі технологій постійно з'являються нові засоби та методи для оновлення вже існуючих веб-додатків та створення нових. ІТ спеціалісти спрямовують свої дослідження на пошук технологій, що значно покращать продуктивність веб-додатків та зможуть урізноманітнити їх функціонал.

На даному етапі розвитку веб-технологій основними мовами програмування є JavaScript, який використовується як на клієнтській, так і на серверній стороні завдяки платформі Node.js. JavaScript є основою фронтенд-розробки і використовується для створення і відображення веб-сторінок та взаємодії з користувачами. Для розробки фронтенду існують різні фреймворки та бібліотеки, такі як React, Angular і Vue.js. React, наприклад, спеціалізується на створенні користувацьких інтерфейсів, Angular надає структурований підхід до фронтенд-розробки, а Vue.js відомий своєю легкістю вивчення та використання. На бекенді для створення серверної логіки та обробки запитів використовуються різні мови програмування. Node.js, який базується на JavaScript, дозволяє розробляти серверні додатки. Крім того, інші мови, такі як Python, Ruby, PHP і Java, також використовуються для бекенд-розробки взаємності від вимог проекту. Фронтенд відповідає за створення користувацького інтерфейсу, відображення даних та взаємодію з користувачами, в той час як бекенд забезпечує обробку серверних запитів, виконання бізнес-логіки та взаємодію з базами даних, забезпечуючи бекграунд-функціональність веб-додатка.

Створення веб-додатків на JavaScript – це складний та багатоетапний процес, що починається зі збору функціональних вимог та розробки дизайну інтерфейсу. Після цього розробники створюють структуру додатку, включаючи HTML-сторінки для відображення контенту та JavaScript-код для обробки взаємодії з користувачем. Для покращення продуктивності та реактивності веб-додатків, розробники використовують асинхронне програмування.

Однією з ключових стратегій є використання Promises для управління асинхронними операціями та їх обробки. Асинхронні функції (`async/await`) дозволяють писати код, який виглядає як синхронний, але виконується асинхронно, спрощуючи розуміння та підтримку коду.

Callbacks були популярним способом управління асинхронним кодом до появи Promises та `async/await`. Promises пропонують більш структурований спосіб керування асинхронним кодом. `Async/await` надає більше читабельності, роблячи код подібним до синхронного стилю.

Кешування даних є важливою стратегією оптимізації, оскільки дозволяє зберігати результати попередніх запитів на клієнтському боці, зменшуючи кількість необхідних запитів до сервера та покращуючи відгук додатку. Мінімізація запитів до сервера включає в себе зменшення кількості запитів та оптимізацію їх структури, щоб зменшити навантаження сервера та покращити швидкість завантаження сторінок. Паралельні асинхронні запити, такі як використання AJAX або Fetch API, дозволяють взаємодіяти з сервером одночасно, покращуючи реактивність додатку та знижуючи час очікування результатів. Керування завантаженням ресурсів на вимогу (`lazy loading`) – це важлива стратегія для зменшення часу завантаження сторінок, дозволяючи завантажувати ресурси лише при необхідності.

Ще одним важливим аспектом оптимізації є робота над швидкістю виконання JavaScript-коду. Відсутність зайвих обчислень та надмірної вкладеності може покращити продуктивність додатку. Використання інструментів профілювання дозволяє ідентифікувати та усувати вузькі місця в коді, забезпечуючи більш ефективну роботу додатку. Оптимізація також включає в себе мінімізацію використання ресурсів браузера, таких як пам'ять та процесор, що допомагає забезпечити стабільну та високошвидкісну роботу на різних пристроях та браузерах.

Загалом, оптимізація веб-додатків з використанням асинхронного програмування включає в себе комплексний підхід, спрямований на покращення продуктивності, реактивності та користувацького досвіду, що стає важливим в умовах сучасного веб-середовища.

Список використаних джерел

1. Асинхронне програмування: що це таке та його особливості. 2023. URL: <https://foxminded.ua/asyncnhronne-prohramuvannia/>

УДК 004.060

Бондаренко А. В., здобувач

Державний університет «Житомирська політехніка»

ДОСЛІДЖЕННЯ UX НА РІЗНИХ ЕТАПАХ ЦИКЛУ ПРОЕКТУВАННЯ

У сучасному світі розробка продуктів та послуг неможлива без врахування потреб та зручностей користувачів. Дослідження користувацького досвіду (UX) на різних етапах циклу проектування відіграє ключову роль у створенні продуктів, які не лише задовольняють, а й перевершують очікування користувачів.

На рис. 1 зображено головні етапи циклу проектування.

Top UX Research Methods	
Discover	<ul style="list-style-type: none">• Field study• Diary study• User interview• Stakeholder interview• Requirements & constraints gathering
Explore	<ul style="list-style-type: none">• Competitive analysis• Design review• Persona building• Task analysis• Journey mapping• Prototype feedback & testing (clickable or paper prototypes)• Write user stories• Card sorting
Test	<ul style="list-style-type: none">• Qualitative usability testing (in-person or remote)• Benchmark testing• Accessibility evaluation
Listen	<ul style="list-style-type: none">• Survey• Analytics review• Search-log analysis• Usability-bug review• Frequently-asked-questions (FAQ) review

Рис. 1. Головні етапи циклу проектування

На початковому етапі, що називається «Дізнавайся», дослідження UX визначається основним завданням – отримати поглиблені знання та визначити реальні потреби користувачів. Проведення польових досліджень, інтерв'ю з користувачами та зацікавленими сторонами.

На етапі «Дослідження» важливо вивчати інноваційні можливості. Тут увага приділяється порівнянню функціоналу з конкурентами, розгляданню можливостей дизайну та аналізу завдань користувачів. Ідеї, які виникають на цьому етапі, мають потенціал трансформувати проект.

Дослідження UX на етапі «Тестування» визначається як ключовий компонент успішної реалізації проекту. Проводяться тести для визначення ефективності та зручності продукту для користувачів, враховуючи думку різних користувачів, включаючи представників різних груп.

Основним принципом на етапі «Слухайте» є постійний аналіз користувацького досвіду та слухання відгуків. Моніторинг соціальних мереж, аналіз питань та проблем користувачів, а також стеження за трендами дозволяє оперативно реагувати на зміни та вносити вдосконалення.

На всіх етапах циклу проектування, зосередження на систематичних покращеннях грає ключову роль. Відсутність жорсткої послідовності дій дозволяє гнучко адаптувати процес дослідження UX відповідно до змін у вимогах користувачів та ринкових умов.

Дослідження UX на різних етапах циклу проектування є необхідним елементом для створення продуктів, що відповідають реальним потребам користувачів. Використовуйте різноманітні методи та підходи на кожному етапі, надаючи перевагу постійним покращенням.

Список використаних джерел

1. UX Research Cheat Sheet. URL: <https://www.nngroup.com/articles/ux-research-cheat-sheet/>

УДК 004.67

*Варганова Д. О., ст. викладач, магістрант,
Свістельник О. С., магістрант,
Локтікова Т. М., ст. викладач
Державний університет «Житомирська політехніка»*

ДОСЛІДЖЕННЯ ПРИНЦИПІВ ПОБУДОВИ ТА ПРОЄКТУВАННЯ ВЕБОРІЄНТОВАНОЇ СИСТЕМИ ТРАНСФЕРНОГО РИНКУ ФУТБОЛІСТІВ

Сьогодні дозволя для кожної людини перетворюється на певний спосіб життя, заповнення вільного часу різноманітними та насиченими подіями. Активне, змістовне дозволя вимагає певних потреб і здібностей людей, в тому числі й у сфері спорту. Найбільш зручні форми для цього вже вироблені життям – це спортивні клуби за інтересами, центри з фізичного виховання та спорту та ін.

Сучасний професіональний футбольний клуб є економічним суб'єктом, який надає розважальні послуги глядачам та телеглядачам. Професіональні футболісти виступають найманими працівниками футбольних клубів, яким надаються права на використання індивідуальних унікальних навичок в рамках організованих змагань. Зазвичай, за професіональні клуби виступають футболісти зі статусом професіонала, які мають письмовий контракт з клубом і за свою трудову діяльність отримують винагороду, яка перевищує їхні фактичні витрати. Всі інші футболісти вважаються аматорами. Всі гравці мають бути зареєстровані за свій клуб в національній асоціації та лізі, до яких належить футбольний клуб. Професіональні футболісти, як будь-які працівники, мають можливість змінювати свого роботодавця, тобто переходити з одного футбольного клубу до іншого, що називається трансфером [1].

На даний час постає проблема поінформованості широкого кола користувачів мережі Інтернет, про діяльність установ, підрозділів, центрів для сфери спорту. Тому актуальною є задача створення веборієнтованого інформаційного ресурсу для сфери спорту.

Отож, проведено дослідження принципів побудови та проєктування веборієнтованої системи для ринку трансферів футболістів та трансферної діяльності футбольних клубів, чинників формування ринкової вартості футболіста, а також аналіз їхнього впливу на конкурентоспроможність професіональних футбольних клубів та ліг у рамках існуючих впроваджених фінансових обмежень.

Нині існують декілька сайтів на дану тематику. Тож, необхідно проаналізувати можливості аналогів. Для порівняння були розглянуті такі вебдодатки: <https://www.transfermarkt.com>, <https://www.sport.ua>.

<https://www.transfermarkt.com> – це популярна та всеосяжна платформа для футбольних ентузіастів, але, як і будь-який сервіс, вона має свої переваги та недоліки [2].

Як переваги можливо відзначити: велика база даних; пропонує глибоку статистику – доступні профілі гравців зі статистикою, ринковою вартістю, історією трансферів та інформацією про кар'єру.

До недоліків належать: основною мовою застосунку є німецька, тому деяка інформація може бути недоступною іншими мовами, в тому числі українською; нагромаджений дизайн; обмежена мобільна версія застосунку, яка призводить до того, що не всі функції є доступними порівняно з сайтом.

Іншим близьким за змістом можна вважати веб-сайт **<https://www.sport.ua>** [3]. Він є популярним в Україні сервісом для отримання інформації про спорт, зокрема й про футболістів.

Перевагами можна вважати: мовою сайту є українська; до того ж статті, що публікуються на сайті, орієнтовані на внутрішнє споживання мешканцями України.

Як недоліки потрібно відзначити: відсутність інформації про ринкову вартість футбольних гравців; перенасиченість рекламою.

Після проведених огляду й аналізу були визначені вимоги, яким повинна задовольняти сучасна веборієнтована система трансферного ринку футболістів, а саме: наявність детальної інформації про кожного гравця; простий та інтуїтивно зрозумілий інтерфейс; адаптивність додатка для різноманітних пристроїв користувача; відсутність реклами.

На основі викладеного вище розроблено веборієнтовану систему трансферного ринку футболістів у середовищі PHPStorm, із використанням бази даних MySQL та вебсерверу Apache, які надаються OSPanel.

Список використаних джерел

1. Вплив світового ринку трансферів футболістів на конкурентоспроможність футбольних клубів Європи. [Електронний ресурс]. – Режим доступу: http://www.economy.in.ua/pdf/11_2017/22.pdf.

2. Football transfers, rumours, market values and news [Електронний ресурс] – Режим доступу: <https://www.transfermarkt.com>.

3. СПОРТ.UA ⇔ Свіжі новини спорту онлайн * Все про спорт України та світу * Спортивні новини на сьогодні [Електронний ресурс] – Режим доступу до ресурсу: <https://sport.ua/uk>.

УДК 621.3: 455.63

*Вакалюк Т. А., д.пед.н., професор,
Власенко О. В., ст. викладач,
Василенко М. К., магістрант*

Державний університет «Житомирська політехніка»

АНАЛІЗ МЕТОДІВ РОЗПІЗНАВАННЯ НОМЕРНИХ ЗНАКІВ

В сучасному світі транспорт є невід'ємною частиною нашого життя, але зростаючий об'єм транспортного потоку вимагає інноваційних підходів до управління безпекою та ефективністю. Одним із ключових елементів в цьому контексті є системи розпізнавання номерних знаків.

Для виявлення та розпізнавання номерних знаків використовується багато різних методів. Розглянемо деякі з них: метод Віоли-Джонса і машину опорних векторів.

Метод Віоли-Джонса, представлений у 2001 році П. Віолою та М. Джонсом, є алгоритмом виявлення об'єктів у реальному часі. В основі його функціональності лежить виявлення облич, але він також застосовується для розпізнавання різних класів зображень, не виключенням є і розпізнавання номерних знаків.

Принцип дії методу Віоли-Джонса базується на використанні каскаду класифікаторів для швидкого визначення регіонів із зображення, які можуть містити об'єкти певного типу. Це досягається завдяки використанню ознак, таких як інтенсивність пікселів та їхнє положення, що дозволяє ефективно виділяти ключові ознаки номерних знаків.

Однією з переваг використання методу Віоли-Джонса є його висока швидкодія, що робить його придатним для використання в режимі реального часу. Однак важливо враховувати обмеження методу, такі як зниження точності та ефективності при куті нахилу об'єкта понад 30 градусів.

При розпізнаванні автомобільних номерів за допомогою методу Віоли-Джонса, важливо налаштовувати параметри та оптимізувати навчені класифікатори для досягнення найкращих результатів у різних умовах освітлення та перспективи.

Розглянемо другий обраний метод – машину опорного вектора (SVM). SVM є контрольованим алгоритмом навчання, спрямованим на класифікацію та регресійний аналіз. У контексті розпізнавання державних автомобільних номерів, SVM може використовуватись для ефективної класифікації з використанням максимального розриву між класами. Техніка Тихоновської регуляризації у SVM додає до його

точності та гнучкості. Основний принцип SVM полягає в максимізації розриву між класами, що робить його ефективним для точного та достовірного розпізнавання державних автомобільних номерів в реальному часі.

Також для розпізнавання широко розповсюджене використання штучних нейронних мереж які допомагають в розпізнаванні автомобільних номерів. Цей підхід також є ефективним, що ґрунтується на принципах машинного навчання та комп'ютерного зору. Нейронні мережі можуть автоматично вивчати складні шаблони та залежності у великих наборах даних, що робить їх ефективними для розпізнавання варіативних форм та структур автомобільних номерів.

Порівняння розглянутих методів представлено у вигляді таблиці 1.

Таблиця 1

Порівняння запропонованих методів

<i>Характеристика</i>	<i>Штучні нейронні мережі</i>	<i>Машина опорного вектора</i>	<i>Метод Віолі-Джонса</i>
<i>Принцип дії</i>	Адаптивне навчання з використанням шарів нейронів та ваг.	Класифікація та регресійний аналіз з використанням розриву між класами.	Каскад класифікаторів для визначення регіонів з використанням признаков.
<i>Ефективність</i>	Гнучкий, здатний визначати складні залежності та адаптуватися до різних умов.	Точний та надійний, особливо в умовах збалансованих даних.	Швидкий та ефективний, але може втратити точність при деяких умовах, наприклад, великому куті нахилу.
<i>Використання у режимі реального часу</i>	Залежить від архітектури та оптимізації, можливе використання у реальному часі.	Здатний працювати у реальному часі, особливо для задач класифікації.	Використовується у реальному часі, але може втратити швидкість при деяких обставинах.

Продовження таблиці 1

Навчання	Вимагає великої кількості даних для навчання та налаштування параметрів.	Потребує налаштування параметрів, але може працювати з меншим обсягом даних.	Навчання каскаду класифікаторів, потребує менше даних для швидкого визначення регіонів.
Відповідність специфікаціям	Здатні адаптуватися до різноманітних форматів та умов.	Ефективний при збалансованих даних та деяких умовах.	Залежить від якості признаков та умов визначення регіонів.

Список використаних джерел

1. Віола П., Джонс М. Дж. Надійне виявлення обличчя в реальному часі / Міжнародний журнал комп'ютерного зору. – 2014. – Т. 57. – С. 137-154.
2. Нелло Крістіаніні, Джон Шоу-Тейлор. Вступ до підтримки векторних машин та інших методів навчання на основі ядра / Cambridge University Press, 2020
3. Хайкін С. Нейронні мережі: повний курс: пер. з англ. / С. Хайкін. – 2-е вид., переп. – М.: Вільямс, 2016. – 1103 с.

УДК 004.421

**Жовноватюк Р. М., к.т.н., с.н.с.,
Варшавський П. В., курсант**

Житомирський військовий інституту імені С. П. Корольова

СТВОРЕННЯ БАЗИ ВЕБ-ОРІЄНТИРІВ У СИСТЕМІ ІР-ГЕОЛОКАЦІЇ

ІР-геолокація може бути використана для виявлення аномальної активності, аутентифікації користувачів, фільтрації контенту, захисту від DDoS-атак, а також для інших заходів кібербезпеки та контролю в мережі Інтернет. Наразі відомо декілька методів ІР-геолокації. Зокрема це GeoPing, CBG, SOI, TBG та Ostant методи [1, 2]. Найбільш перспективним методом ІР-геолокації вважається дещо модифікований CBG метод. При його реалізації є необхідність знаходження веб-орієнтирів, їх координати використовуються для визначення координат цілі за ІР-адресою. У якості веб-орієнтирів обираються організації, компанії, наукові установи та урядові установи, які розміщують свої веб-служби локально. Такі орієнтири є стабільними, надійними та довготривалими.

У доповіді зазначено, що для розробки програмного забезпечення по створенню бази веб-орієнтирів використовувалась технологія WindowsForms з використанням мови програмування C# та фреймворка NET. Структура проекту складається з сукупності окремих компонентів, таких як ядро парсерів, ядро роботи з API, ядро роботи з базою даних, моделей, що описують структуру JSON-файлів та даних, що описують сутність «орієнтир». При написанні програмного коду застосовувався об'єктно-орієнтований принцип програмування.

Створення бази веб-орієнтирів розпочинається зі складання списку потенційних веб-орієнтирів, для чого використовуються каталоги з навчальними закладами і компаніями України.

Особливо важливою є інформація про фізичне розташування установи та посилання на її веб-сайт. Ця інформація може бути використана для перевірки, чи існує локальний веб-сервер конкретного закладу за вказаною адресою. Важливо враховувати, що не всі компанії мають власний локальний веб-сервер, оскільки деякі можуть орендувати віддалений веб-сервер або використовувати віртуальний хостинг. Для перевірки цього використовуються веб-додатки з власним API. В результаті обробки даних з геосервісів отримується інформація про географічне розташування ІР-адреси, а саме про країну

розміщення, область та місто. Цей етап отримав назву «грубої фільтрації».

Далі порівнюється фізична адреса та дані розташування серверу, на якому хоститься веб-сайт компанії. Оскільки на сайті адреса може бути у різному вигляді, то для обробки такої інформації реалізовано спеціальні модулі. Модулі здійснюють перевірку таких елементів: назва країни, населеного пункту, вулиці, номера будинку та поштового коду міста тощо. Якщо елемент – непотрібна інформація (номер квартири, поверху тощо), то ці дані ігноруються. В результаті роботи отримується клас даних: місто, вулиця, номер будинку, поштовий код установи.

Далі за допомогою сервісу LocationQ, для якого реалізовано окремий клас даних, визначаються координати. З метою підвищення точності ці координати перевіряються на сервісі GeoApiFu, який повертає зворотні дані про місто, вулицю та номер будинку за координатами: якщо дані співпадають, то це означає, що координати визначені правильно.

Заключним етапом є обробка всієї наявної інформації та записування в базу даних веб-орієнтирів. Дані, отримані шляхом парсингу веб-ресурсів, зберігаються в окремих таблицях. Кожен запис у таблиці обробляється за таким алгоритмом:

1. Перевірка доступності сайту.
2. Отримання даних з геосервісів (виклик окремого методу).
3. Верифікація отриманої інформації.
4. Запис у базу даних веб-орієнтирів такої інформації: IP-адреса веб-сайту, домене ім'я, повна фізична адреса, адреса з геосервісів та координати.

У результаті розроблено програмне забезпечення, що створює базу даних веб-орієнтирів системи IP-геолокації, що має функцію оновлення відомостей. Подальша робота спрямована на розробку та програмну реалізацію алгоритму визначення місцеположення об'єктів за їх IP-адресою.

Список використаних джерел

1. Wang Y., Burgener D., Flores M., Kuzmanovic A. and Huang C. (2011) Towards Street-Level Client Independent IP Geolocation. In NSDI'11. Proceedings of the 8th USENIX conference on networked systems design and implementation, pp: 27-36.
2. Eriksson B., Barford P., Sommers J. and Nowak R. (2010) A Learning-based Approach for IP Geolocation. IN PAM'10 Proceedings of the 11th international conference on Passive and active measurement, pp: 171 – 180.

УДК 004.94

Яконюк А. В., магістрант,

Сугоняк І. І., к.т.н., доцент

Державний університет «Житомирська політехніка»

АВТОМАТИЗОВАНІ СИСТЕМИ КОНТРОЛЮ ТА МОНІТОРИНГУ ГРОМАДСЬКОГО ТРАНСПОРТУ

В сучасних умовах розвитку міст невід’ємною частиною цього процесу є громадський транспорт. На думку урбаніста Девіда Сіма [1], громадський транспорт забезпечує не лише функцію логістики, а й безпосередньо впливає на майже на всі сфери міського життя. Транспортні вузли не лише забезпечують пересування людей з точки А до точки Б, а ще й сприяють виникненню нових соціокультурних просторів навколо себе, тим самим даючи поштовх зростанню економіки та покращенню соціально-культурного становища містян. Бізнес та інвестиції охочіше притягуються саме до тих місць, до яких люди можуть легко дістатися з різних куточків міста.

Громадський транспорт намагається вирішити одну з основних проблем сучасного міста – транспортні затори. Світова статистика показує, що лише за 2022 рік у світі було виготовлено 61 мільйон 600 тисяч автомобілів, що на 6 відсотків більше за попередній рік [2]. Враховуючи наростаюче збільшення кількості автомобілів, громадський транспорт виглядає не лише як альтернатива, але як і потенційне вирішення проблеми високої завантаженості міст, адже дозволяє компактно перевозити значно більшу кількість пасажирів, використовуючи при цьому вже існуючі автомобільні шляхи.

Отже, метою нашої роботи є проведення дослідження доцільності автоматизації системи контролю та моніторингу громадського транспорту.

Можна окреслити такі основні напрямки для аналізу:

1. Аналіз існуючих підходів в оптимізації маршрутів та графіків руху. Автоматизовані системи дозволяють оптимізувати маршрути та графіки руху транспортних засобів з урахуванням пасажирського попиту, трафіку та дорожніх подій. Такі системи корисні при плануванні руху при використанні автобусів, трамваїв та тролейбусів, зменшуючи час очікування для пасажирів в умовах обмеженої кількості транспортних засобів.

2. Використання аналітичних інструментів для обробки даних руху транспорту та пасажирського потоку. Використання аналітики та даних щодо пасажирського попиту дозволяє оптимізувати маршрути руху, забезпечуючи більш точне відображення потреб користувача.

Маршрути та графіки руху можна оптимізувати з урахуванням піків пасажиропотоку, щоб забезпечити достатню кількість транспортних засобів у часи найбільшого попиту.

3. Застосування систем глобального позиціонування (GPS). Використання GPS дозволяє в режимі реального часу відстежувати рух транспортних засобів і коригувати їхні маршрути в залежності від поточної ситуації на дорозі, а також надавати пасажирам актуальну інформацію про рух транспорту для підвищення якості користування транспорту.

В ході виконання роботи планується розробка комплексної автоматизованої системи контролю та моніторингу громадського транспорту з використанням аналітичних інструментів.

Отже, тема автоматизації систем громадського транспорту є важливою складовою забезпечення комфортного життя пересічної людини. Забезпечення ефективного контролю та оптимізації громадського транспорту дозволить поліпшити якість обслуговування пасажирів та раціонального використання ресурсів.

Список використаних джерел

1. Sim D. Soft City: Building Density for Everyday Life. Island Press, 2019. 256 p.
2. 2022 statistics | www.oica.net. www.oica.net. URL: <https://www.oica.net/category/production-statistics/2022-statistics/> (дата звернення: 19.11.2023).
3. Segaran T. Programming Collective Intelligence: Building Smart Web 2. 0 Applications. O'Reilly Media, Incorporated, 2007.

УДК 519.2

**Андреев С.М., к.т.н., доцент,
Шостак А.В., к.т.н., доцент**

Національний аерокосмічний університет ім. М.Є. Жуковського, «Харківський авіаційний інститут»

ОЦІНКА ОДНОРІДНОСТІ ВИБІРОК ВИПАДКОВИХ ЧИСЕЛ ПЛАТФОРМИ .NET

Оцінимо однорідність двох вибірок. Перша вибірка складається з 1000 рівномірно розподілених у діапазоні від 0 до 100 цілих випадкових чисел і згенерована з використанням класу Random із простору System платформи .Net (варіант 1). Друга вибірка має той самий розмір, вихідні дані та згенерована з використанням класу RandomNumberGenerator з простору System.Security.Cryptography (варіант 2).

У гіпотезі однорідності потрібно визначити, чи ці вибірки є однорідними, тобто отриманими з одного і того ж розподілу, або закон розподілу спостережень від вибірки до вибірки змінювався. Тобто гіпотезою однорідності є твердження $H_0 F_1(x) \equiv F_2(x)$, де $F_i(x)$ – функція розподілу i -ї вибірки.

Для оцінки однорідності двох вибірок використовувався критерій однорідності χ^2 -квадрат. Діапазон значень вибірок було розбито на 15 інтервалів. Для двох вибірок з однаковим розміром 1000 значення статистики χ^2 -квадрат дорівнювало 6,7. За рівня значимості $\alpha=0,05$ критична межа дорівнює 23,7.

Так як значення статистики χ^2 -квадрат менше критичної межі, то виконується згода гіпотези однорідності для двох даних вибірок.

На рис.1 наведено гістограму для розподілу значень χ^2 -квадрат для 1000 пар вибірок розміру 1000.

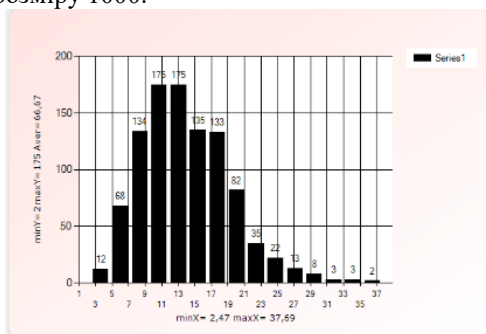


Рис. 1. Гістограма розподілу значень χ^2 -квадрат

Причому з 1000 одержаних значень χ^2 -квдрат кількість значень χ^2 -квдрат більших величини критичної межі 23,7 дорівнює 51. Тобто, з 1000 пар вибірок 51 пара не відповідає поняттю однорідності, а 949 – відповідають.

Оцінимо так само випадковість тих самих двох вибірок. Для оцінки випадковості вибірки використовувався критерій інверсій, статистикою даного критерію є число інверсій I у вибірці. Гіпотеза про випадковість не відхиляється, якщо $I_{\alpha/2} < I < I_{1-\alpha/2}$, де α – рівень значущості. Число інверсій I приймає цілі значення, безліч яких залежить від розміру вибірки n . Математичне очікування та дисперсія статистики I мають відповідно вигляд $E = n \cdot (n-1)/4$,

$D = (2 \cdot n^3 + 3 \cdot n^2 - 5 \cdot n)/72$. Нормалізована статистика має вигляд $I^* = (I-E)/D^{0.5}$ і за $n \geq 30$ досить точно описується стандартним нормальним законом.

Для двох вибірок з однаковим розміром 1000 значення нормалізованої статистики виявилось рівно відповідно 0,0474 та 0,0674. При рівні $\alpha = 0,05$ критична межа дорівнює $\pm 2,326$.

Оскільки значення нормалізованих статистик перебувають у інтервалі від $-2,326$ до $2,326$, то для двох даних вибірок виконується згода гіпотези про випадковість.

На рис. 2 наведена гістограма для розподілу значень нормалізованих статистик для 1000 вибірок розміру 1000 для варіанта 1. Причому з 1000 отриманих значень статистик I^* кількість 29 значень I^* не потрапили в інтервал $\pm 2,326$.



Рис. 2. Гістограма розподілу значень I^* для варіанта 1

Список використаних джерел

1. Огірко О. І., Галайко Н. В. Теорія ймовірностей та математична статистика: / О. І. Огірко, Н. В. Галайко. – Львів: ЛьвДУВС, 2017. – 292 с.
2. Шпігельгальтер Д. Мистецтво статистики. Прийняття аргументованих рішень на підставі даних: / Д. Шпігельгальтер. – К.: Країна мрій Київ, 2023. – 384 с.

УДК 51-7+004.4

*Огінський Є. В., аспірант,
Антонюк Д. С., к.пед.н., доцент
Державний університет «Житомирська політехніка»*

МЕТОД МОНТЕ-КАРЛО У МОДЕЛЮВАННІ ПРОЦЕСІВ УПРАВЛІННЯ ПЕРСОНАЛЬНИМИ ФІНАНСАМИ

Метод Монте-Карло представляє собою метод чисельного обчислення, який застосовується у різних галузях наукових та інженерних досліджень. В його основі лежить ідея використання випадкових чисел для моделювання ймовірнісних процесів. Даний метод використовує велику кількість випадкових значень, щоб оцінити ймовірнісну характеристику реального явища. Метод Монте-Карло застосовується для моделювання процесів і вирішення задач в різних сферах: математиці, фізиці, хімії, економіці, теорії управління.

Метод Монте-Карло також широко застосовується у фінансовій сфері для прогнозування фінансових показників, оцінки ризику інвестиційних та кредитних портфелів, тощо.

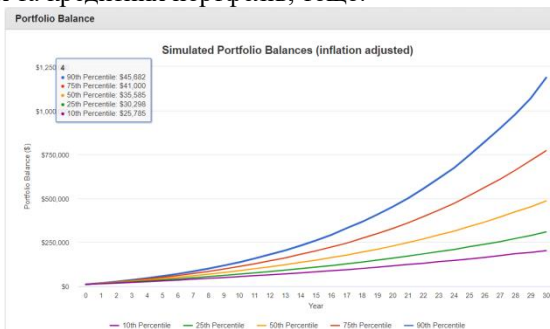


Рис. 1. Приклад використання методу Монте Карло для розрахунку прибутковості інвестиційного портфелю

Для застосування даного методу треба виконати наступні дії:

1. Визначити змінні, значення яких є джерелом невизначеності системи;
2. Визначити допустимі значення і розподіли ймовірностей для кожної змінної для генерації вхідних даних;
3. Виконати обчислення з випадковими значеннями вхідних даних;
4. Повторити обчислення багато разів та звести результати окремих обчислень для отримання кінцевого результату.

Метод Монте-Карло також може бути застосований в сфері персональних фінансів. Припустимо, визначена фінансова ціль така, як

накопичення коштів на купівлю будинку і є декілька можливих стратегій для її досягнення:

1. Накопичення виділених коштів на депозиті в гривні;
2. Конвертація коштів у валюту і накопичення на валютному депозиті;
3. Конвертація коштів у валюту і купівля акцій біржового інвестиційного фонду SP500.

Кожна зі стратегій має певний елемент невизначеності і ризику, а саме: зміна процентних ставок за депозитами, рівень інфляції, ризик пов'язаний зі зміною курсу валют, зміна ринкової ціни будинка. Зазначені невизначеності можна використати, як вхідні дані для симуляції. Необхідно задати правила розподілу, що будуть використовуватись для генерації вхідних даних, і на багатьох ітераціях виконати обчислення для суми накопичених коштів і визначення, чи достатньо цієї суми для досягнення цілі. Результати розрахунків можна використати для порівняння ефективності стратегій.

Також можливі наступні сценарії використання методу Монте-Карло в сфері персональних фінансів:

- Планування сімейного бюджету, при якому метод застосовується для оцінки ймовірності того, що бюджет буде дотриманий. Для цього генеруються випадкові вхідні значення в певному діапазоні для доходів, витрат, непередбачених витрат. На основі вхідних даних розраховується ймовірність дотримання бюджету.
- Оцінка досяжності фінансової цілі. Припустимо, що людина має певну ціль в сфері персональних фінансів, наприклад накопичення коштів на навчання. Метод можна використовувати для оцінки ймовірності досягнення цілі. Для цього можна згенерувати вхідні значення для доходів, витрат, зміна вартості навчання, а потім використовувати ці значення для розрахунків.
- Прогнозування фінансового майбутнього. Метод можна застосувати для планування персонального пенсійного фонду, в якості вхідних значень можна взяти тривалість життя, рівень доходів і розмір внесків.

Отже, метод Монте-Карло можна використовувати для дослідження процесу прийняття фінансових рішень та для визначення оптимальних стратегій управління особистими фінансами.

Список використаних джерел

1. Raychaudhuri Samik. Introduction to monte carlo simulation. quot; 2008 Winter simulation conference. IEEE, 2008.
2. McLeish Don Monte Carlo simulation and finance. Vol. 276. John Wiley & Sons, 2011.

УДК 004

*Ожго Ю. А., здобувач,
Дацюк Д. В., асистент
Державний університет «Житомирська політехніка»*

ROUNDROBINTOURNAMENT АЛГОРИТМ ДЛЯ ГЕНЕРАЦІЇ РОЗКЛАДУ СПОРТИВНОЇ ЛІГИ

Розробка програми для генерації розкладу спортивних подій є складним завданням, яке передбачає багато аспектів та вимагає уважної підготовки. Визначення формату та структури події є ключовим етапом у цьому процесі. Алгоритм для генерації розкладу спортивних подій відіграє значну роль у забезпеченні оптимального розкладу проведення турніру чи змагань. Потрібно зважати на різноманітні чинники, адже розробка цього алгоритму вимагає уважного врахування різноманітних факторів, таких як кількість учасників, розподіл команд, часові обмеження та особливості конкретного виду спорту.

Темою проекту є адміністрування любительських футбольних ліг і власне однією із задач проекту є генерація розкладу для ліги. Враховуючи що за спортивний сезон одна команда повинна зіграти з кожною командою дивізіону, було вирішено використати RoundRobinTournament алгоритм для генерації розкладу.

RoundRobinTournament (Круговий турнір) – це алгоритм, за яким кожен учасник зустрічається з усіма іншими учасниками по черзі. В одному круговому розкладі учасник грає з іншим учасником лише один раз [1]. Ця система вважається найбільш справедливою, але водночас вимагає найбільшого числа ігор для розподілу місць, порівняно з іншими турнірними системами.

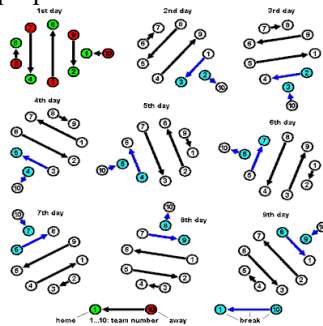


Рис. 1. Візуалізація алгоритму на прикладі 10 учасників

Якщо спростити опис алгоритму, то для його реалізації нам потрібно розрахувати кількість раундів, після цього потрібно опрацювати кожен з раундів і згенерувати матчі між командами. Кількість раундів напряму залежить від кількості команд; якщо кількість команд парна, то кількість раундів розраховується за формулою - $(n - 1)$, де n це кількість команд. Якщо кількість команд непарна, то кількість раундів відповідатиме кількості команд. Кількість матчів, що відбудуться за раунд, можна розрахувати такими формулами:

- $\binom{n}{2}(n - 1)$, якщо n парне
- $\binom{n-1}{2}n$, якщо n непарне.

Перейдемо власне до реалізації алгоритму. Так як генерація розкладу це тільки частина проекту і сам проект являє собою набір різних компонентів (мобільний додаток, API, web-портал для адміністрування), то реалізація алгоритму була виконана на стороні API. Для написання API частини було використано Node.js технологію, для спрощення процесу розробки був використаний Nest.js фреймворк.

Nest.js – це фреймворк для створення ефективних, масштабованих серверних програм Node.js [2]. Перевагою фреймворку є те, що Nest.js повністю підтримує Typescript і базується на DependencyInjection (DI) підході. Головна ідея DI полягає в тому, щоб відокремити процес створення та управління залежностями від основної логіки програми.

API компонент побудовано за підходом SOA. SOA (Service-Oriented Architecture) – це підхід до розробки програмного забезпечення, при якому функціональність програми поділяється на незалежні служби, що можуть взаємодіяти між собою [3]. Основні принципи SOA:

- незалежність служб;
- стандартизовані інтерфейси;
- відкритий доступ до служб.

Слідуючи підходу SOA, для генерації розкладу було створено окремий модуль Schedule. Schedule модуль об'єднує в собі такі компоненти:

- schedule.module – основний файл модулю, який об'єднує в собі всі потрібні компоненти і створює необхідні залежності;
- schedule.controller – відповідає за маршрутизацію, і власне в цьому компоненті створено маршрути, за якими мобільний додаток зможе отримати розклад;
- schedule.service – відповідає за бізнес логіку, власне в цьому компоненті реалізовано генерацію розкладу.

В `schedule.service` створено метод, який реалізує Round Robin Tournament. В загальному реалізація цього алгоритму виглядає як подвійний цикл, перший цикл відповідає за кількість раундів, вкладений цикл відповідає за генерацію пар команд та зсув команд у списку для наступного раунду. Якщо сильно спростити, то загальна структура коду виглядатиме приблизно так:

```
function generateRoundRobin(teams) {
  const numTeams = teams.length;
  const rounds = numTeams % 2 === 0 ? numTeams - 1 : numTeams;
  const factor = numTeams % 2 === 0 ? numTeams / 2 : (numTeams - 1) / 2;
  const schedule = [];
  for (let round = 0; round < rounds; round++) {
    const roundMatches = [];
    for (let i = 0; i < factor; i++) {
      const match = [teams[i], teams[numTeams - 1 - i]];
      roundMatches.push(match);
    }
    schedule.push(roundMatches);
    // Зсув команд у списку для наступного раунду
    teams.splice(1, 0, teams.pop());
  }
  return schedule;
}
```

Отже, після аналізу алгоритмів для генерації розкладу, основним алгоритмом було вибрано Round Robin Tournament, так як цей алгоритм задовольняє всі необхідні критерії для футбольних спортивних ліг. Було розроблено API частину проекту яка, в тому числі, і реалізує алгоритм генерації. Використання додатку дозволяє значно спростити адміністрування спортивної ліги, особливо коли це стосується формування розкладу на сезон.

Список використаних джерел

1. Optimizing Game Scheduling With Round-Robin Algorithms. URL: <https://cactusware.com/blog/round-robin-scheduling-algorithms#:~:text=It's%20a%20scheduling%20algorithm%20where,all%20the%20matches%20are%20completed>
2. Nest.js. URL: <https://docs.nestjs.com/>
3. What is SOA (Service-Oriented Architecture)? URL: <https://aws.amazon.com/what-is/service-oriented-architecture/>

УДК 004

Хімич В. О., магістрант,

Чижмотря О. В.ст.викладач

Державний університет «Житомирська політехніка»

АНАЛІЗ ФОРМАТІВ ФАЙЛІВ ДЛЯ ПОШИРЕННЯ ЗАСТОСУНКІВ ДЛЯ ОС ANDROID

З самого початку зародження інформаційних технологій одним з питань для вирішення були способи поширення програмного забезпечення, які разюче змінилися за відносно коротку історію індустрії. Так, наприклад, колись це були дискети, максимальна місткість яких складала лише 2880 кілобайт, згодом були винайдені CD-приводи, що відкрили дорогу для нових, значно більш ємнісних носіїв. Та все ж з широких поширенням інтернету фізичні носії для застосунків стали непотрібні і розповсюдження програмного забезпечення здійснюється через мережу. Однак кожна операційна система має власні особливості щодо вимог таких файлів, це стосується і Android, який вперше побачив світ у 2008 році.

З самого початку зародження ОС Android застосунки компілювалися в файл з розширенням .apk, який по своїй суті був ZIP-архівом, котрий зберігав у собі всю необхідну інформацію, програмний код, ресурси та інше, що було необхідним для встановлення за стосунку на будь-якому пристрої з підтримкою цих файлів. Це було хороше рішення для свого часу, адже робило простим поширення застосунків не лише через офіційні магазини застосунків, а й з інших джерел. Але з прогресом смартфонів та мобільних застосунків в цілому стала явною проблема підходу пакування застосунку в ZIP-архів – великий розмір цих файлів. До того ж значну частину місця в .apk файлах займали строкові та графічні ресурси застосунку, котрі могли навіть не використовуватися на окремому пристрої користувача.

Google розуміли цю проблему і на Google I/O 2018 представили новий спосіб поширення застосунків під їх мобільну ОС, вона отримала назву Android App Bundle з новим розширенням файлу .aab. На абстрактному рівні цей файл залишився тим же архівом, але зі значними допрацюваннями. Тепер архів ділиться на 3 частини:

1. Базовий APK – частина, що зберігає спільний код та ресурси застосунку;
2. Конфігураційний APK – включає в себе нативні бібліотеки та ресурси для конкретної щільності, розміру екрану, мови та інше;

3. APK динамічних функцій – частина функціоналу застосунку, що може бути завантажен апізніше.

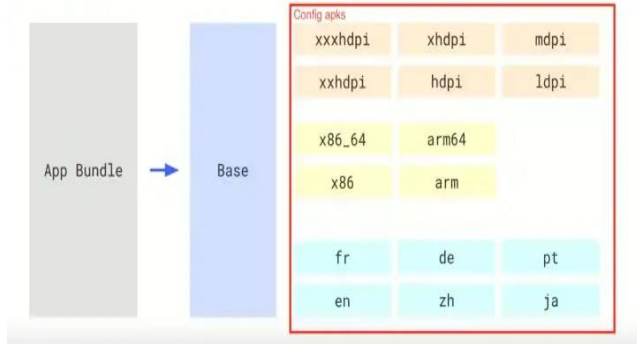


Рис. 1. Будова AndroidAppBundle

Саме конфігураційна частина APK дозволила в середньому зменшити розмір завантажуваного файлу з Google Play на 20%.

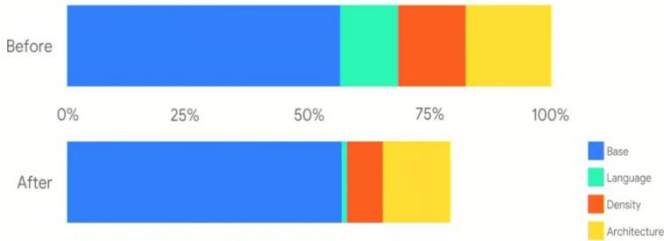


Рис. 2. Середній розмір .aab файлу в порівнянні з .apk

Проте найбільшим недоліком цього підходу є те, що .aab файли не можна напряму встановити на пристрій і на цей момент вони завантажуються лише в Google Play, де хмарні сервіси компанії Google роблять можливими оптимізації файлів цього формату. Саме через це .apk та .aab файли продовжують існувати разом, слугуючи різним цілям.

Отже, Google здійснила велику роботу щодо зменшення розміру завантажуваного застосунку за допомогою Android App Bundle, але його обмеження змушують досі використовувати Android Package Kit файли. Такий симбіоз підходів дозволяє гнучко задовольняти потреби і користувачів, і розробників.

Список використаних джерел

1. Android App Bundle documentation [Електронний ресурс] –Режим доступу до ресурсу: <https://developer.android.com/guide/app-bundle>

УДК 004.77

*Коренівська О. Л., к.т.н., доцент,
Коротун О.В., к.пед.н., доцент,
Франчук В.О., магістрант*

Державний університет «Житомирська політехніка»

ГНУЧКА СИСТЕМА РЕЄСТРАЦІЇ В МОБІЛЬНОМУ БАНКІНГУ ЗА ДОПОМОГОЮ SERVER-SIDE RENDERING (SSR)

В сучасному світі мобільних технологій компанії постійно стикаються з вимогою максимально зручної та гнучкої взаємодії з клієнтами. Особливо в сфері фінансових технологій, де надійність та зручність грають першорядну роль, реєстраційний процес стає одним із ключових компонентів. Наукова практика, проведена в компанії «Restart Financial», спрямована на дослідження та реалізацію гнучкої системи реєстрації в мобільному банкінгу з використанням підходу Server-Side Rendering (SSR).

Однією з важливих задач було розробити універсальний інструмент для реєстрації, який забезпечував би гнучкий флоу для різних проектів, використовуючи одну спільну кодову базу. Для цього було прийняте рішення використовувати Server-Side Rendering (SSR), що дало змогу генерувати та відправляти клієнтам індивідуальні реєстраційні форми в залежності від їхніх потреб.

Завдяки SSR під час завантаження сторінки реєстрації на сервері генерується вміст, який відповідає специфікаціям кожного проекту. Клієнт отримує зручний інтерфейс, що підлаштовується під його потреби. Це дозволяє заощадити ресурси обробки даних, уникнути непотрібних кроків у флоу реєстрації та забезпечити кожного клієнта мобільного банкінгу індивідуальною та зручною реєстраційною формою.

Впровадження SSR в реєстраційні процеси стало здатним розширити можливості та функціональність нашого додатку. За допомогою динамічної генерації реєстраційних форм на сервері, ми можемо забезпечити гнучкий підхід до реєстрації, де кожен клієнт може вибрати опції, що відповідають його потребам.

SSR дозволив створити спеціальну бібліотеку, що об'єднує різні аспекти реєстрації для різних проектів. Це значно спростило розробку та підтримку, а також дало можливість швидко реагувати на зміни та вимоги клієнтів.

Однією з ключових переваг SSR є можливість створення індивідуальних реєстраційних форм для кожного клієнта. Ми здатні

адаптувати реєстраційний процес під потреби різних груп користувачів, створюючи приємне та особисте враження.

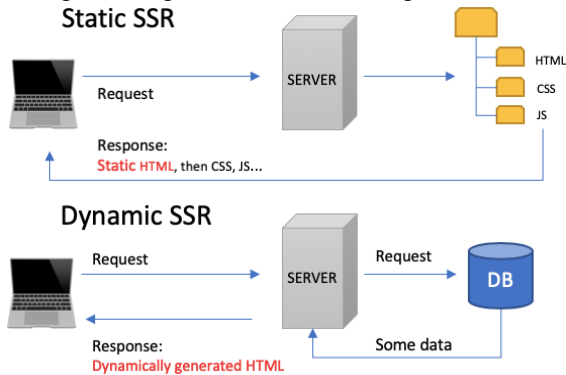


Рис. 1. Процес роботи SSR

Гнучкість і персоналізація є необхідними в мобільному банкінгу, де вимоги користувачів можуть значно відрізнятись. За допомогою SSR ми можемо забезпечити гармонійний баланс між загальною логікою реєстрації та індивідуальним підходом до кожного клієнта.

Використання Server-Side Rendering стало ключовим етапом нашого зусилля у вдосконаленні реєстраційних процесів та користувацького досвіду. Це підвищило якість обслуговування клієнтів, забезпечивши миттєве завантаження, гнучкість та персоналізацію.

Загалом, використання SSR для гнучкої реєстрації виявилось ключовим чинником у розвитку нашого мобільного банкінгу. Цей підхід став можливістю реалізувати нашу візію ідеального користувацького досвіду, де кожен клієнт може отримати унікальну та зручну реєстраційну форму, а компанія «Restart Financial» – зберегти час та ресурси при розробці.

Список використаних джерел

1. Miola A. Flutter complete reference: create beautiful, fast and native apps for any device. Independently Published, 2020.

2. Sufyan bin Uzayr. Mastering flutter: a beginner's guide. Boca Raton : CRC Press, 2022. 348 p.

3. The Road to React with Firebase: Your journey to master advanced React for business web applications. Chicago, Illinois : Independently Published, 2019. 199 p.

4. Waleed A. Managing State in Flutter Pragmatically: Discover how to adopt the best state management approach for scaling your Flutter app. Birmingham : Packt Publishing, 2021. 246 p.

УДК 004.054

*Шаңуріна Д. С., здобувачка
Державний університет «Житомирська політехніка»*

СУЧАСНІ МЕТОДИ ДОСЛІДЖЕННЯ UX

У світі сучасних технологій та цифрових інновацій питання користувацького досвіду (UX) стає все більш важливим для досягнення успіху в онлайн середовищі. Розуміння, як користувачі сприймають та взаємодіють з продуктами та сервісами, є вирішальним для розробників та дизайнерів. У цьому контексті широкий спектр дослідницьких методів UX надає незамінні інструменти для отримання цінних уявлень.

У галузі дослідження користувацького досвіду існує великий вибір методів дослідження, починаючи від перевірених часом, таких як лабораторні випробування користування, і закінчуючи новітніми, наприклад, немодерованими оцінками UX.

В багатьох випадках дизайнерські команди залишаються в рамках своєї зони комфорту, використовуючи лише кілька методів, які для них є найбільш знайомими. Проте стає ключовим питання: які саме методи обрати та у яких випадках? Для кращого розуміння, коли використовувати кожен метод, корисно аналізувати їх, використовуючи тривимірну рамку з такими осями:

1. Ставлення проти поведінки. Цю відмінність інакше можна визначити як різниця між «що люди говорять» та «що люди роблять». UX-спеціалісти, як правило, більшою мірою покладаються на поведінкові дослідження, тому що часто те, що люди повідомляють у дослідженнях ставлення, не збігається з тим, що вони насправді роблять у поведінкових дослідженнях.

2. Якісне проти кількісного. Якісні за своєю природою дослідження генерують дані про поведінку чи уявлення, базуючись на безпосередньому спостереженні чи почутому, тоді як у кількісних дослідженнях дані збираються опосередковано, через вимірювання або інструмент, такий як опитування чи інструмент аналітики.

3. Контекст використання.

Діаграма нижче (рис. 1) ілюструє, де саме розташовані 20 популярних методів дослідження вздовж цих вимірів.

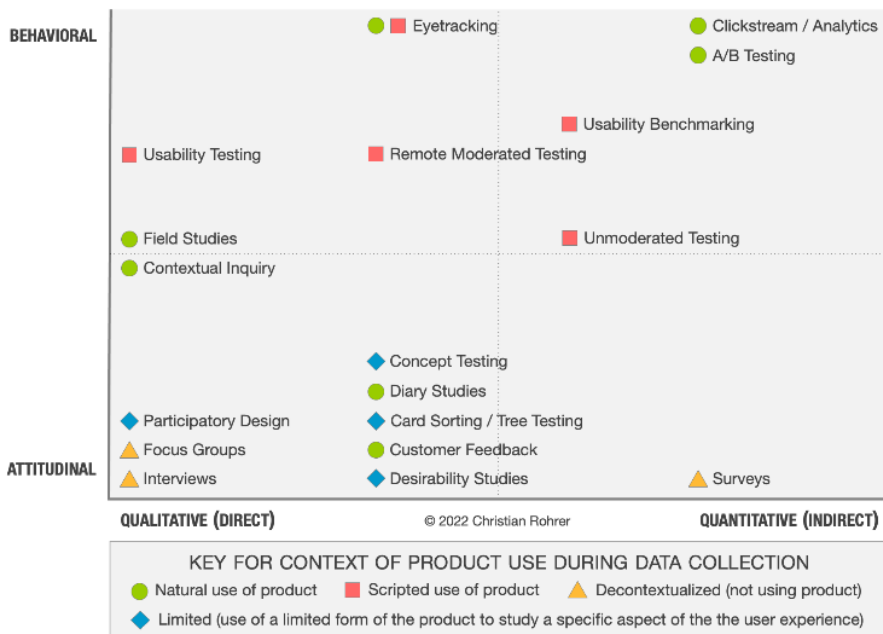


Рис. 1. Розташування методів дослідження UX

З них можна виділити такі найбільш корисні та актуальні методи:

1. Польові дослідження. Вивчення учасників у їхньому природному оточенні, де, ймовірно, вони найбільше взаємодіють з продуктом чи послугою в реальних умовах.

2. Участь у дизайні. Учасники отримують елементи дизайну або творчі матеріали для створення свого ідеального розташування, яке виражає їхні найважливіші цінності та причини.

3. Відстеження очей. Використовується пристрій для вимірювання того, куди дивляться учасники при взаємодії з веб-сайтами, додатками, фізичними продуктами або оточенням.

Список використаних джерел

1. When to Use Which User-Experience Research Methods. URL :<https://www.nngroup.com/articles/which-ux-research-methods/>.

УДК 004

*Чос А.С., здобувач,
Терещук С.О., асистент
Державний університет «Житомирська політехніка»*

АЛГОРИТМИ ХАНОЙСЬКОЇ ВЕЖІ: АНАЛІЗ ТА ОПТИМІЗАЦІЯ В КОНТЕКСТІ РОЗВ'ЯЗАННЯ КОМБІНАТОРНИХ ПРОБЛЕМ

Сучасний розвиток обчислювальної науки та інформаційних технологій визначає актуальність вивчення та оптимізації алгоритмів Ханойської вежі, що є ключовим елементом в теорії обчислювальної складності. Алгоритми Ханойської [1] вежі є фундаментальними для обчислювальної науки та технологій. Вони використовуються для розв'язання багатьох комбінаторних задач, таких як сортування, пошуки та розпізнавання.

Ця теза присвячена вивченню та оптимізації алгоритмів Ханойської вежі. Дослідження спрямоване на покращення якості та швидкодії вирішення комбінаторних задач за допомогою алгоритмів Ханойської вежі. Це важливо для розвитку обчислювальної математики та інформаційних технологій.

Лістинг коду:

```
...
void hanoi(int n, int i, int k){
    if (n == 0){
        printf("\n\tMove disk 1 from pin %d to %d", i, k);
    }
    else{
        int tmp = 6 - i - k;
        hanoi(n - 1, i, tmp);
        printf("\n\tMove disk %d from pin %d to %d", n, i, k);
        hanoi(n - 1, tmp, k);
    }
}
int main(){
    system("chcp 1251");
    system("cls");
    int choice_1, choice_2, choice_3;
    printf("\n\tВведіть розмір вежі: ");
    scanf_s("%d", &choice_1);
    printf("\n\tВведіть номер стовпця з якого перекладаємо: ");
    scanf_s("%d", &choice_2);
    printf("\n\tВведіть номер стовпця який перекладаємо: ");
    scanf_s("%d", &choice_3);
}
```

```
    hanoi(choice_1, choice_2, choice_3);  
    printf("\n");  
    return 0;  
}
```

Алгоритм Ханойської вежі включає переміщення дисків різного розміру між трьома стовпцями: початковим, допоміжним та цільовим. Основна ідея – переміщати диски один за одним, дотримуючись двох основних правил: диск завжди може бути розміщений лише на диск меншого розміру, і переміщення відбувається тільки між трьома стовпцями.

Рекурсивний алгоритм Ханойської вежі включає три основні етапи:

- Переміщення (n-1) дисків з початкового стовпця на допоміжний.
- Переміщення найбільшого диска з початкового стовпця на цільовий.
- Переміщення (n-1) дисків з допоміжного стовпця на цільовий.

Цей процес повторюється рекурсивно для кожної підзадачі, поки всі диски не будуть переміщені на цільовий стовпець. Алгоритм Ханойської вежі є ефективним способом вивчення рекурсії та стратегій алгоритмізації.

Існують різні способи оптимізації алгоритму Ханойської вежі. Ось деякі з них:

Ітеративний метод. З допомогою цього метода можна уникнути накопичення великої кількості рекурсивних викликів, що може бути важливо для оптимізації часу виконання.

Паралельне виконання. Можливість паралельного виконання алгоритму за допомогою конкурентних або розподілених обчислень покращує швидкодію, особливо для великих обсягів даних.

Оптимізація для конкретних випадків. Враховуючи особливості задачі Ханойської вежі, можна розглянути оптимізації для конкретних випадків, наприклад, для задачі з меншою кількістю дисків.

Отже, оптимізація алгоритму Ханойської вежі може покращити його швидкодію та ефективність. Існують різні способи оптимізації, які можна використовувати окремо або в комбінації.

Список використаних джерел:

1. Алгоритм «Ханойська вежа» [Електронний ресурс] – Режим доступу до ресурсу: <https://ua5.org/osnprog/255-algoritm-khanoijska-vezha.html>

2. Ханойські вежі [Електронний ресурс] – Режим доступу до ресурсу: <https://www.eolymp.com/uk/problems/6187>

УДК 004.054

*Кравченко С. М., ст. викладач,
Горбачевська Д. А., здобувачка
Державний університет «Житомирська політехніка»*

ОСОБЛИВОСТІ ЮЗАБІЛІТІ ТЕСТУВАННЯ

Для порівняння кількох інтерфейсів користувача в одному дослідженні існує два способи планування дослідження, а саме:

1. Дизайн міжпредметного дослідження (between-subjects), в якому різні люди перевіряють кожну умову, тому кожна особа має лише один інтерфейс користувача.

2. Дизайн дослідження в межах суб'єкту (within-subjects), в якому одна й та сама особа перевіряє всі умови, тобто всі інтерфейси користувача.



Рис. 1. Способи планування дослідження

Проаналізувавши рис. 1 можна порівняти на прикладі двох сайтів для прокату автомобілів А та Б, дивлячись на те, як учасники бронюють автомобілі на кожному сайті, дослідження можна було б спланувати двома різними способами:

1. Між предметами: кожен учасник міг протестувати один сайт прокату автомобілів і забронювати автомобіль лише на цьому сайті.

2. Всередині предметів: кожен учасник міг протестувати обидва сайти прокату автомобілів і забронювати автомобіль на кожному з них.

Будь-який тип дослідження користувачів, який включає більше ніж одну умову тестування, повинен визначити, чи бути між суб'єктами чи всередині суб'єктів. Однак ця різниця особливо важлива для кількісних досліджень.

Простої відповіді на питання «Що краще: між предметами чи всередині предметів?» – немає, адже в багатьох ситуаціях можливі обидва варіанти. Перевагами «Між предметами» є відсутність переходу між умовами, коротші навчальні сесії та легко налаштовуються, особливо при наявності кількох незалежних змінних. А перевагами «Всередині предметів» є мінімізація шуму у своїх даних, менші вимоги до кількості учасників та дешевші, а, отже доступніші.

Незалежно від того, чи планується експеримент усередині суб'єктів чи між суб'єктами, рандомізацією доведеться займатись, хоча й дещо іншими способами. Для міжпредметних дизайнів потрібно переконатись, що учасники розподіляються випадковим чином за умовами, щоб не вплинути на результати дослідження (тобто має внутрішню валідність). Таким чином, якщо дослідник вирішує, що всі учасники, які йому подобаються, повинні взаємодіяти з сайтом А, а потім він виявляє, що сайт А працює краще, ніж сайт Б, він не знатиме, чи виявив він справжню різницю між сайтами, чи результат просто відображає його завдання. У цій ситуації присвоєння є змінною, що змішує.

Кожен тип експериментального дизайну має свої переваги та недоліки; проектування в межах предметів вимагає менше учасників і збільшує шанси виявити справжню різницю між умовами; дизайни між предметами мінімізують вплив навчання в різних умовах, призводять до коротших сесій і можуть бути легшими для налаштування та аналізу.

Юзабільність тестування є ключовим етапом в розробці програмного забезпечення, оскільки вона дозволяє виявити та врахувати особливості користувачів, покращуючи їхній досвід та забезпечуючи оптимальний рівень задоволення від використання продукту. Акцент на юзабільності в тестуванні сприяє створенню дружнього та легкозасвоєного інтерфейсу, що впливає на успішність та прийняття програмного рішення користувачами.

Список використаних джерел

1. Between-Subjects vs. Within-Subjects Study Design [Electronic resource] – Access mode: <https://www.nngroup.com/articles/between-within-subjects/>

УДК 004.08

Кравченко С. М., ст. викладач,

Ігнатів О. С., здобувач

Державний університет «Житомирська політехніка»

КОРИСТУВАЦЬКИЙ І КЛІЄНТСЬКИЙ ДОСВІД: АСПЕКТИ ВЗАЄМОДІЇ З КОМПАНІЄЮ

В тезах розглядається розуміння динаміки: навігація між сферами взаємодії з користувачем і взаємодії з клієнтом.

Чи взаємозамінні терміни користувацький досвід (UX) і клієнтський досвід (CX), чи вони мають різні значення? Відповідь, як виявилось, і так, і ні. Щоб розгадати цю головоломку, потрібно заглибитись в розвиток UX і CX.

Еволюція від UX до CX

Спочатку термін «користувацький досвід» охоплював усі аспекти взаємодії людини з компанією, її послугами та продуктами. Однак його рання концепція, що сягає корінням в епоху, орієнтовану на комп'ютери, призвела до вузького тлумачення, зосередженого на окремій взаємодії, а не на повних відносинах клієнт-компанія. Щоб подолати це обмеження, з'явився термін «користувацький досвід» (CX), який представляє кульмінацію взаємодії користувача з організацією протягом певного часу.

Різні масштаби та значення

Розуміння нюансів досвіду користувачів і клієнтів передбачає розпізнавання трьох різних рівнів:

1. Рівень взаємодії:

Зосереджено на розробці досвіду однієї взаємодії, цифрової чи фізичної. Приклади включають підтримку по телефону, особисті транзакції в банку або подання страхової претензії онлайн. - Принципи дизайну, рекомендації та шаблони, специфічні для кожного каналу, керують досвідом взаємодії на рівні.

2. Рівень подорожі:

Охоплює наскрізний процес, який проходить клієнт для досягнення мети з часом. Включає кілька пристроїв і каналів взаємодії, таких як веб-сайти, програми, електронні листи та телефонні взаємодії. Проблеми включають підтримку узгодженості між каналами, плавні переходи та цілісні елементи дизайну.

3. Рівень відносин:

Вивчає загальний життєвий досвід і сукупне враження людини про організацію. Виходить за межі ізольованих взаємодій чи подорожей, враховуючи цілісні відносини між клієнтом і компанією. Потрібна ефективна інтеграція різних компонентів, включаючи шляхи клієнта, рекламні кампанії та пропозиції продуктів.

Взаємопов'язані рівні

- **UX рівня взаємодії:** в першу чергу стосується окремого завдання або транзакції, часто в центрі уваги дизайнерів UX.

- **UX на рівні подорожі:** передбачає низку пов'язаних взаємодій, що створює унікальні виклики, як-от узгоджене обмін повідомленнями та міжканальні переходи.

- **UX рівня взаємовідносин:** найширший спектр, зосереджений на цілісному досвіді клієнта протягом тривалого часу, що вимагає інтеграції різноманітних елементів.

Уніфікований підхід і термінологія

Використання термінів «UX» чи «CX» не має першорядного значення; послідовність в інтерпретації є ключовою. Організації повинні прагнути оптимізувати роботу на всіх рівнях, уникаючи розрізненого дизайну, який може добре працювати окремо, але дає збій, коли інтегрований у реалістичну подорож користувача. Ефективна комунікація та координація між рівнями мають вирішальне значення для запобігання збоям, які можуть вплинути на загальний досвід користувача.

Розвиток користувацького та клієнтського досвіду вимагає уваги до рівнів взаємодії, подорожі та відносин. Терміни UX і CX, хоч і взаємозамінні, мають свої відтінки. Успішна реалізація вимагає не лише оптимізації на кожному рівні, але й ефективної комунікації та координації. Взаємопов'язаність та уніфікований підхід є важливими для забезпечення позитивного досвіду для користувачів і клієнтів.

Список використаних джерел

1. User Experience vs. Customer Experience: What's The Difference? URL: <https://www.nngroup.com/articles/ux-vs-cx/>
2. User Experience vs. Customer Experience: What's The Difference? URL: <https://www.nngroup.com/articles/ux-vs-cx/>
3. Do Not Confuse User Experience With Customer Experience <https://usabilitygeek.com/confuse-user-experience-customer-experience/>
4. UX vs CX: What's the Difference? <https://careerfoundry.com/en/blog/ux-design/difference-between-ux-and-cx/>

УДК 004.08

Кравченко С. М., ст. викладач,

Предчук Т. В., магістрант

Державний університет «Житомирська політехніка»

ЗГОРТКОВА НЕЙРОННА МЕРЕЖА ДЛЯ РОЗПІЗНАВАННЯ ОБ'ЄКТІВ

Згорткова нейронна мережа (CNN) – це особливий вид нейронної мережі, який значно зменшує кількість параметрів у глибокій нейронній мережі з багатьма одиницями, не надто втрачаючи якість моделі. CNN застосовується в обробці зображень і тексту, та це одна з основних категорій для розпізнавання зображень, класифікації зображень, виявлення об'єктів, розпізнавання обличчя тощо.

За рахунок застосування спеціальної операції, власне згортки, згорткова нейронна мережа дозволяє водночас зменшити кількість інформації, що зберігається в пам'яті інформації, за рахунок чого краще справляється з картинками більш високої роздільної здатності, і виділити опорні ознаки зображення, такі як ребра, контури або грані. На наступному рівні обробки з цих ребер і граней можна розпізнати повторювані фрагменти текстуру, які далі можуть скластися в фрагменти зображення.

Архітектура згорткової нейронної мережі.

CNN зазвичай має три рівні: згортковий рівень, рівень об'єднання та повністю зв'язаний рівень (рис 1.).

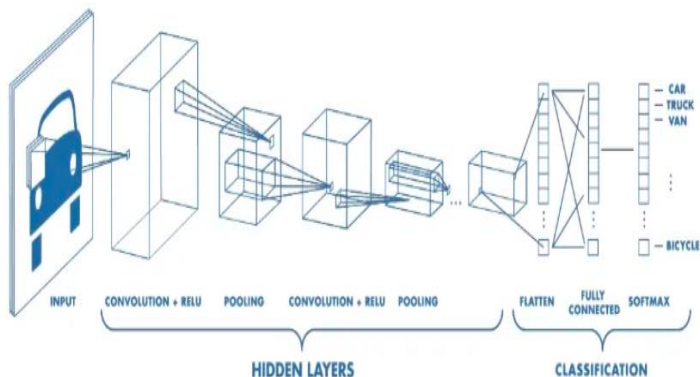


Рис. 1. Типова структура роботи. Архітектура CNN

На сьогоднішній час можна виділити наступні згорткові нейронні мережі, які використовуються:

1. Виявлення об'єктів. Завдяки CNN тепер є такі складні моделі, як R-CNN, Fast R-CNN і Faster R-CNN, які є основною системою для багатьох моделей виявлення об'єктів, що застосовуються в автономних транспортних засобах, розпізнавання обличчя тощо.

2. Семантична сегментація – це мережа для глибокого аналізу на основі CNN.

3. Субтитри до зображень: CNN використовуються з рекурентними нейронними мережами для написання титрів до зображень і відео. Це можна використовувати для багатьох програм, наприклад для розпізнавання активності або опису відео та зображень для людей із вадами зору.

Існують різні архітектури CNN, які відіграють ключову роль у побудові алгоритмів, які забезпечують і будуть підтримувати ІІІ в цілому в майбутньому. Деякі з них: LeNet, AlexNet, VGGNet, GoogLeNet, ResNet, ZFNet.

Класична згорткова нейронна мережа:

1. Згортковий шар.
2. Операція активації після кожного згорткового шару.
3. Рівень об'єднання, особливо рівень максимального об'єднання, а також інші на основі вимог.
4. Нарешті повністю підключений рівень.

Виявлення об'єктів

CNN може виявляти об'єкти на зображеннях у реальному часі, а також маркувати та класифікувати їх. Тому ця техніка широко використовується в автоматизованих транспортних засобах [1]. Це також дозволяє розумним будинкам і пішоходам розпізнавати обличчя власника автомобіля. Він також використовується в системах спостереження на основі ІІІ для виявлення та позначення об'єктів.

Виявлені області (рис. 2) об'єднуються за різними проміжками кольорів та показниками подібності. Кожна пропозиція відеопотоку змінюється так, щоб відповідати входу CNN, з якого отримується векторні ознаки розміру 4096 bit. Вектор ознак надходить в декілька класифікаторів для отримання імовірностей, що належать до кожного класу.

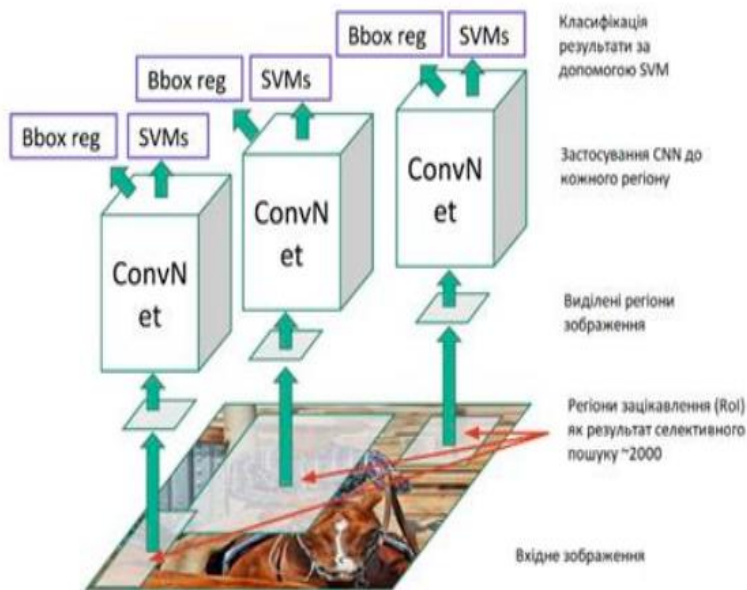


Рис. 2. Типова структура роботи R-CNN: на основі [2]

CNN на сьогодні широко використовується в області нейронних мереж. Це відбувається переважно для вирішення завдань комп'ютерного зору, хоча може застосовуватися також для роботи з аудіо і будь-якими даними, які можна представити у вигляді матриць.

Список використаних джерел

1. A Comprehensive Guide to Convolutional Neural Networks-the ELI5 way. URL :<https://towardsdatascience.com/a-comprehensive-guide-to-convolutional-neural-networks-theeli5-way-3bd2b1164a53>.
2. R. Girshick, «Fast R-CNN» 2015 IEEE International Conference on Computer Vision (ICCV), Santiago, 2015, pp. 1440-1448.

УДК 004.054

*Кравченко С.М., ст. викладач,
Чуприна В.А., здобувач
Державний університет «Житомирська політехніка»*

ШТУЧНИЙ ІНТЕЛЕКТ ДЛЯ ДОСЛІДЖЕННЯ UX

Штучний інтелект (ШІ) все більше використовується в різних галузях, включаючи дослідження користувацького досвіду (UX). Штучний інтелект (ШІ) використовує різні технології та алгоритми для опрацювання інформації та ухвалення рішень. Одним із ключових підходів у ШІ є машинне навчання, яке дає змогу комп'ютерній системі самостійно навчатися на основі великих обсягів даних, а також розпізнавати образи, виконувати аналіз тексту, прогнозувати тренди та багато іншого.

У сфері графічного дизайну ШІ може оптимізувати робочі процеси, покращувати творчі ресурси, аналізувати конкурентів та багато іншого. Ось чому дизайнерам варто звернути увагу на подібні сервіси:

1. Вони вдало виконують рутинні задачі.
2. Вони генерують безліч варіантів графіки.
3. Вони аналізують дані.

Штучний інтелект пропонує нові справді захопливі можливості для створення кращого користувацького досвіду. Розглянемо декілька корисних інструментів ШІ для UI/UX дизайнерів:

1. **DALL-E 2** – Нейромережа від OpenAI, яка створює оригінальні зображення з текстового опису.

2. **Midjourney** – Генерація банерів для сайту, статті у блозі, генерація логотипів, персонажів, патернів, рекламних креативів, зображень, дизайн продуктів.

3. **Stable Diffusion** – Дозволяє максимально швидко згенерувати зображення на основі тексту чи вхідного зображення.

4. **OpenArt** – велика бібліотека створених штучним інтелектом картинок.

Загалом нові інструменти на основі ШІ, які входять на ринок, пропонують великі обіцянки, такі як автоматичний аналіз даних, зменшення упередженості в дослідженнях та аналіз даних з будь-якого джерела. Однак ці обіцянки часто виявляються передчасними, і потрібно бути обережними при розгляді підписки на такі інструменти.

Є два типи ШІ-інструментів, які використовуються в дослідженні UX:

1. **Генератори інсайтів ШІ:** Ці інструменти генерують підсумки сесій дослідження користувачів, виключно на основі транскриптів цих сесій. Вони не приймають інші типи інформації від дослідника, що може стати великою проблемою, оскільки ці інструменти не можуть враховувати контекст.

2. **Співробітники ШІ:** Ці інструменти, на відміну від генераторів інсайтів, можуть приймати деяку контекстуальну інформацію від дослідника. Вони можуть аналізувати ваші текстові дані та виробляти інсайти.

Інструменти ШІ дозволяють дизайнерам заощадити час, оптимізувати робочі процеси, покращувати творчі ресурси, а також аналізувати конкурентів. Однак, варто пам'ятати, що ШІ не може замінити людський творчий процес і “душу” дизайну, яка надає йому унікальність і емоційну глибину. Хоча інструменти штучного інтелекту можуть автоматизувати багато рутинних завдань, вони не здатні відтворити той особливий елемент, який приносить людський художник або дизайнер. Творчість, інтуїція та особистий погляд залишаються ключовими компонентами успішного дизайну, які неповторно виражають власність ідеї чи продукту. Таким чином, використання інструментів штучного інтелекту має бути розглядане як підтримка та доповнення творчого процесу, а не його заміна.

Інструменти ШІ, безумовно, відіграють велику роль у недалекому майбутньому UX-досліджень. Важливо пам'ятати, що ШІ – це лише інструмент, і він може бути корисним лише тоді, коли використовується правильно. ШІ може допомогти автоматизувати деякі процеси та зробити їх більш ефективними, але він не може замінити людський розум і досвід. Тому дослідники повинні завжди залишатися критичними та обережними при використанні ШІ-інструментів для дослідження UX. Завжди важливо перевіряти результати, які надає ШІ, і не сліпо довіряти їм.

Список використаних джерел

1. AI – Powered Tools for UX Research. URL: <https://www.nngroup.com/articles/ai-powered-tools-limitations/>

2. ШІ в роботі дизайнера. URL: <https://ux.pub/designjam/shtuchnii-intieliekt-v-roboti-dizainiera>

3. Продуктивність ШІ в UX. URL: <https://dou.ua/forums/topic/43596/>

4. UX дизайн на основі штучного інтелекту URL: <https://seo24.kiev.ua/ui-ta-ux/yzdizajn-ux-na-osnovi-shtuchnogo-intelektu/>

УДК 004.054

Петришин А. О., здобувач

Державний університет «Житомирська політехніка»

ШАБЛони СКАНУВАННЯ ТЕКСТУ

Шаблони сканування тексту – це ефективний інструмент для структуризації та аналізу текстової інформації. Вони дозволяють систематизувати дані, виділяти ключову інформацію та автоматизувати процес обробки текстових документів. Ми розглянемо різні типи шаблонів сканування тексту та їх використання у практиці.

1. F-шаблон добре працює для розпізнавання тексту в ситуаціях, коли зображення може бути пошкоджено чи спотворене. Завдяки використанню цього шаблону можна точно розпізнавати символи навіть у випадку помилок або шумів у зображенні.

2. Плямистий візерунок – це метод, який базується на розпізнаванні особливих плям і текстур, які можна знайти на поверхні тексту. Цей шаблон дозволяє виділяти основні характеристики текстового матеріалу та точно визначати символи.

3. Ідея поділу тексту на шари, схожі на шари тіста в торті, використовується в шаблоні сканування листкового торта. Кожен шар відображає частину тексту, наприклад структуру абзаців, графічні елементи чи ключові слова. Таким чином можна проводити більш деталізоване сканування та розпізнавання тексту.

4. Основні елементи тексту, які вказують на обов'язки сторін, визначаються шаблоном зобов'язання. Це може бути лексичний візерунок, вживані вирази та ключові слова, які вказують на мету документа. Цей шаблон допомагає автоматизувати процес визначення змісту та ступеня зобов'язання сторін.

Розглянемо сфери використання шаблонів сканування тексту на прикладах (рис. 1).



Рис. 1. Шаблони сканування тексту

Бізнес-аналітика:

При вивченні фінансових звітів можна використовувати F-шаблон для автоматичного визначення витрат та доходів, що допомагає аналізувати фінансовий стан компанії.

Медицина діагностика:

Застосування плямистого візерунка для аналізу медичних записів може допомогти виявляти особливості та тенденції у симптомах пацієнтів.

Фінансовий менеджмент:

Шаблон сканування листкового торта може використовуватися для визначення ефективності різних інвестицій та розподілу ресурсів в бюджеті.

Юридична справа:

Використання шаблону зобов'язання в юридичних документах допомагає автоматизувати процес визначення зобов'язань між сторонами.

В юридичних справах шаблон зобов'язання використовується для автоматичного аналізу текстів контрактів та угод для виявлення та класифікації умов та обов'язків сторін. Шаблони сканування тексту є життєво необхідними для підвищення точності та ефективності розпізнавання інформації в сучасному світі. Вони дозволяють швидко та ефективно визначати ключові аспекти тексту, полегшуючи подальший аналіз та прийняття рішень, а їх використання дозволяє оптимізувати роботу з текстовою інформацією в різних сферах діяльності.

Список використаних джерел

1. Text Scanning Patterns: Eyetracking Evidence [Electronic resource] – Access mode: <https://www.nngroup.com/articles/text-scanning-patterns-eyetracking/>

2. 4 Types of Eye Tracking Patterns: How People (Don't) Read on Web | Creative Handles [Electronic resource] – Access mode: <https://creativehandles.com/blog-posts/79/4-types-of-eye-tracking-patterns-how-people-don-t-read-on-web>

3. 6 принципів візуальної ієрархії. Спочатку були кам'яні скрижалі, папірус... | by UIUXUA | Medium [Electronic resource] – Access mode: [https://medium.com/@uixukr/6-принципів-візуальної-ієрархії-326e7dc9c23c#:~:text=1\)%20Патерни%20сканування%20сторінок&text=Візерунки%20сканування%20звичай%20приймають%20одну,згори%20донизу%20з%20лівого%20боку.](https://medium.com/@uixukr/6-принципів-візуальної-ієрархії-326e7dc9c23c#:~:text=1)%20Патерни%20сканування%20сторінок&text=Візерунки%20сканування%20звичай%20приймають%20одну,згори%20донизу%20з%20лівого%20боку.)

УДК 004.08

*Кравченко С.М., ст. викладач,
Предчук Т.В., магістрант
Державний університет «Житомирська політехніка»*

ПОШУК ЗОБРАЖЕНЬ ЗА ДОПОМОГОЮ КОМП'ЮТЕРНОГО ЗОРУ

Комп'ютерний зір – це сфера штучного інтелекту (ШІ), яка дозволяє комп'ютерам і системам отримувати значущу інформацію з цифрових зображень, відео та інших візуальних вхідних даних і вживати дій або давати рекомендації на основі цієї інформації. Якщо ШІ дозволяє комп'ютерам мислити, то комп'ютерний зір дозволяє їм бачити, спостерігати та розуміти.

Комп'ютерний зір навчає машини виконувати ці функції, але робити це потрібно набагато швидше за допомогою камер, даних і алгоритмів, а не сітківки, зорових нервів і зорової кори. Оскільки система, навчена перевіряти продукти або спостерігати за виробничим активом, може аналізувати тисячі продуктів або процесів за хвилину, помічаючи непомітні дефекти чи проблеми, вона може швидко перевершити людські можливості [1].

Завдання, які вирішує технологія комп'ютерного зору:

- Класифікація зображень.
- Пошук дублікатів і схожих зображень.
- Розпізнавання тексту.
- Розуміння сцени і розпізнавання об'єктів на зображеннях.

Пошук зображень на основі вмісту використовує комп'ютерний зір для перегляду, пошуку та отримання зображень із великих сховищ даних на основі вмісту зображень, а не пов'язаних із ними тегів метаданих. Це завдання може включати автоматичне анотування зображення, яке замінює ручне тегування зображення. Ці завдання можна використовувати для систем управління цифровими активами та можуть підвищити точність пошуку та вилучення [1].

Застосування нейромереж в комп'ютерному зорі:

- Класифікація зображень
- Пошук схожих зображень.
- Виявлення (детекція) об'єктів на зображенні.
- Сегментація зображення.
- Пошук та розпізнавання тексту на зображенні.
- Генерація зображень

Сегментація – це об'єднання об'єктів в групи за загальними ознаками. Однокласова і багатокласова сегментація використовується, наприклад, для безпілотних автомобілів. Нейромережа розподіляє об'єкти по класах: машини, тротуар, будинки, люди. У всіх об'єктів є чіткі межі. Це робиться по одному знімку без жодної додаткової інформації. Алгоритми враховують не лише зовнішній вигляд об'єктів, а й їх взаємне розташування, що значно ближче до людського мислення, ніж формальний пошук зовні схожого об'єкта (рис.1).

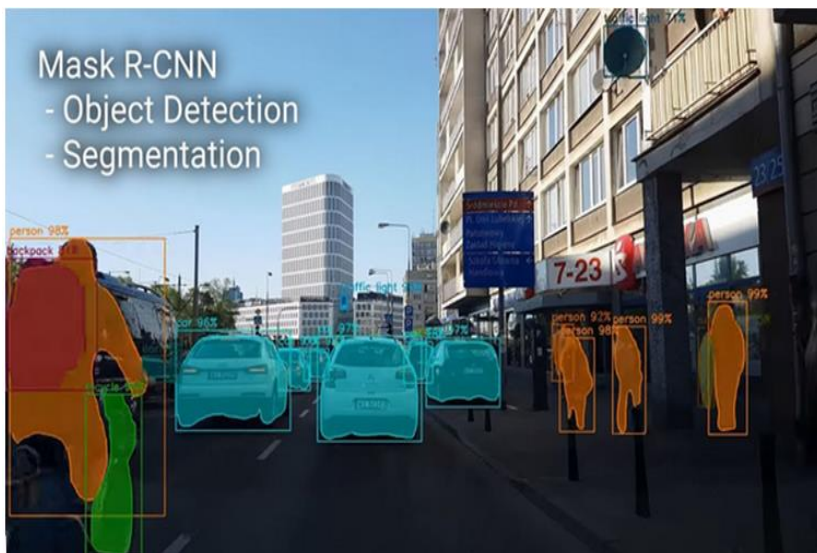


Рис. 1. Сегментація та розпізнавання об'єктів зображення

Список використаних джерел

1. What is computer vision? URL: <https://www.ibm.com/topics/computervision> Computer+vision+applications.

УДК 004.4

*Лобанчикова Н. М., к.т.н., доцент,
Захаров Д. М., доктор філософії, доцент
Державний університет «Житомирська політехніка»,*

ОСОБЛИВОСТІ РОЗРОБКИ ВЕБ-СИСТЕМ ДЛЯ ПЛАНУВАННЯ ТА ОРГАНІЗАЦІЇ ПРОЦЕСУ НАВЧАННЯ

Розробка веб-систем для планування та організації процесу навчання залишається надзвичайно актуальною у сучасному освітньому середовищі.

Основна задача розробки веб-системи для планування і організації процесу навчання – забезпечити зручний і ефективний інструмент для управління розкладом, реєстрацією студентів і викладачів, сповіщеннями та відстеженням навчальних відомостей, формування звітністю та аналітикою. Розробка веб-системи для планування і організації процесу навчання може мати наступні основні завдання:

- **Управління розкладом.** Система повинна дозволити створювати і змінювати розклад занять для учасників освітнього процесу. Вона повинна враховувати різні види занять, групи, аудиторії та інші фактори.

- **Реєстрація студентів і викладачів.** Система повинна мати можливість реєстрації нових користувачів (студентів і викладачів) та зберігати їхні дані.

- **Сповіщення і нагадування.** Система повинна надсилати сповіщення і нагадування користувачам про найближчі заняття, важливі події або зміни у розкладі.

- **Формування і відстеження успішності і відомостей.** Система повинна дозволити викладачам і студентам вносити і відстежувати оцінки, завдання, рейтинги і інші відомості, пов'язані з навчанням.

- **Спільнота і комунікація.** В системі повинні бути форуми, чати або інші інструменти для спілкування між студентами і викладачами, а також можливість обміну матеріалами та ресурсами для навчання.

- **Аналітика і звіти.** Система повинна збирати дані про навчання, відвідуваність, успішність і інші параметри, щоб допомогти адміністраторам і викладачам приймати рішення з удосконалення провадження освітньої діяльності.

- **Безпека та захист від несанкціонованого доступу до особистих даних користувачів і конфіденційної інформації,** що є однією з найважливіших функцій.

- **Інтеграція з іншими системами.** Система повинна інтегруватися з іншими системами, такими як системи управління

навчанням (LMS), електронними бібліотеками, системами електронної пошти тощо.

– Мобільний доступ. Забезпечення можливості доступу до системи через мобільні пристрої та планшети може бути важливим аспектом для зручності користувачів.

– Масштабованість. Система повинна бути здатна розширюватися і працювати ефективно навіть при зростанні обсягу користувачів і даних.

Розробка такої веб-системи вимагає детального аналізу вимог користувачів і планування, а також ефективного програмного забезпечення, забезпечення безпеки для даних користувачів. Сформуємо орієнтовний план розробки такої системи:

Етап 1. Аналіз потреб та вимог. Визначимо вимоги і розуміння потреб користувачів, а саме які функції потрібно включити в систему і які основні завдання будуть вирішуватися цією системою.

Етап 2. Проектування архітектури. На даному етапі спроекуємо загальну архітектуру системи. Визначимо, які компоненти будуть включені, і як вони взаємодіятимуть між собою.

Етап 3. Проектування бази даних. На цьому етапі важливо розробити оптимальну структуру для зберігання бази даних для зберігання інформації про дисципліни, студентів, викладачів, розклади, матеріали та інше.

Етап 4. Розробка інтерфейсу користувача. При цьому слід врахувати зручність використання та інтуїтивно зрозумілу навігацію.

Для досягнення поставленої мети, і розв'язку задачі визначено функціональні можливості системи. Таким чином, поставлена задача, визначений план та функціональні особливості системи є опорними елементами та сприятимуть процесу розробки веб-системи для планування та організації процесу навчання, яка відповідає потребам користувачів та навчального закладу.

Список використаних джерел

1. Awang, Norkhushaini & Darus, Mohamad. (2012). Evaluation of An Open Source Learning Management System: Claroline. *Procedia – Social and Behavioral Sciences*. 67. 416–426.

2. Pontoan, Michelle&Sihotang, Jay&Lompoliu, Erienika. (2023). Information Security Analysis of Online Education Management System using Information Technology Infrastructure LibraryVersion 3. *MATRIK : Jurnal Manajemen, Teknik Informatikadan Rekayasa Komputer*. 22. 207-216. 10.30812/matrik.v22i2.2474.

УДК 004.42

*Плечистий Д. Д., к.т.н., доцент,
Войтюк О. В., аспірант
Державний університет «Житомирська політехніка»*

БАГАТОЗАЛЕЖНІ ЗВ'ЯЗКИ У РЕКУРСИВНІЙ СТРУКТУРІ ФРОНТЕНД ДОДАТКУ

Побудова рекурсивного дерева елементів є однією із задач для кожного фронтенд розробника і потребує багато часу для аналізу та пошуку правильного рішення. Рівень складності такої задачі полягає у виборі правильних інструментів розробки, коректності їх налаштувань та реалізації складних програмних структур. Рівень складності підвищується еквівалентно збільшенню вхідних умов задачі які визначають фінальний набір функціональності додатку. Одним з таких умов є підтримка багатозалежності зв'язків між різними елементами. Прикладом може бути процес онлайн заповнення форми адреси для відправки пошти: результат вибору країни має автоматично змінити поле для вибору міста, що у свою чергу змінює набір опцій по вибору вулиці. Цей приклад є видом лінійної залежності, тому що усі елементи розташовані у логічній послідовності і під час розробки додатку будуть знаходитись у одній зоні видимості. Популярні випадки залежностей часто знаходяться на одному й тому самому рівні вкладеності і легко можуть бути пов'язані між собою. Водночас гарантією таких випадків є відсутність рекурсивної побудови додатку або спрощена архітектура вхідних об'єктів даних. Проблема багатозалежних зв'язків полягає у можливості існування одного або більше факторів впливу на елемент взаємодії з користувачем, тобто, декілька елементів додатку можуть змінити видимість або поведінку іншого елемента, який може існувати в іншому просторі видимості даних.

Для вирішення проблеми зв'язків у рекурсивних деревах елементів треба вибрати інструмент, який дозволить спостерігати за станом інших елементів та оновлювати цю інформацію на різних рівнях вкладеностей, а не тільки на самому вищому рівні. Вбудовані можливості React дозволять працювати з таки поняттям як «форми», що і є рішенням поставленої проблеми, однак ці можливості обмежені у функціональності та потребують більше часу і знань для впровадження складного рішення.

Проаналізувавши низку інструментів, які можуть легко інтегруватись у складну структуру зв'язків, було знайдено бібліотеку яка володіє зручною системою підписки на зміни даних – це Formik. Основними перевагами цієї бібліотеки є:

- **Спрощений код:** можливість написати менше коду для управління станом форми, обробки подій та валідації. Він надає компактний та зручний інтерфейс для роботи з формами.

- **Управління станом:** автоматично вирішує питання стану форми та обробки подій, дозволяючи зосередитися на логіці додатка, а не на деталях форм.

- **Інтеграція з валідацією:** легко інтегрується з валідацією форм, дозволяючи визначити правила валідації для кожного поля та миттєво отримувати звіти про помилки.

- **Вбудовані компоненти введення:** має вбудовані компоненти введення, такі як `<Field>`, які допомагають зробити код більш читабельним та лаконічним.

- **Форми на основі об'єктів:** Formik працює з формами, що базуються на об'єктах. Це дозволяє зберігати всі значення форми в одному об'єкті, спрощуючи управління станом.

- **Підтримка асинхронних операцій:** легко інтегрується з асинхронними операціями, такими як відправка форми на сервер, дозволяючи легко обробляти такі сценарії.

- **Можливість власних реалізацій:** якщо потрібно, Formik надає можливість власних реалізацій для деяких частин форми, забезпечуючи гнучкість для специфічних вимог.

У підсумку, можна сказати, що обґрунтований вибір технології спостереження за зв'язками пришвидшить вирішення основної проблеми оптимізації промалювання ВЕБ застосунку, а малий поріг входження у таку технологію зменшить кількість часу на побудову складного рішення.

Список використаних джерел

1. Titus Kamunya «8 Best React Form Libraries for Developers»
URL: <https://geekflare.com/best-react-form-libraries/>
2. Jared Palmer «Formik docs» URL: <https://formik.org/>
3. Jordan Walke «React Form» URL:
<https://legacy.reactjs.org/docs/forms.html>

Секція 2
КОМП'ЮТЕРНА ІНЖЕНЕРІЯ ТА КІБЕРБЕЗПЕКА

УДК 614.842.4(075.8)

*Котенко В. М., к.т.н, доцент,
Пархомчук О. Ю., магістрант
Державний університет «Житомирська політехніка»*

**ІНТЕГРОВАНА СИСТЕМА ОХОРОННО-ПОЖЕЖНОЇ
СИГНАЛІЗАЦІЇ**

Забезпечення безпеки об'єктів, будівель, приміщень та інших об'єктів життєдіяльності вимагає комплексного підходу та використання передових технологій. У цьому контексті програмно-апаратний комплекс інтегрованої системи охоронно-пожежної сигналізації набуває все більшої актуальності і важливості.

Найбільш прогресивний та перспективний вид – інтегровані (комплексні) системи охорони та пожежної сигналізації. Такі системи дозволяють об'єднати розрізнені системи, такі як системи управління доступом, охоронні системи, пожежні системи та системи відеоспостереження, в єдиний комплекс безпеки з можливістю управління, обробки та моніторингу всіх підсистем в одному місці. Це дозволяє скоротити витрати по впровадженню, підтримці і використанню підсистем, а також виводить охоронне забезпечення на новий рівень, дозволяючи впроваджувати інтелектуальні алгоритми автоматичної обробки та реагування.

Актуальність досліджень обумовлена необхідністю розробки інтегрованої системи охоронно – пожежної сигналізації, на основі об'єднання інформації чутливих елементів (датчиків) систем охоронної сигналізації і систем пожежної сигналізації в єдиному пристрої прийомо-контрольному (ППК), дослідженню можливостей такого об'єднання, розробки макета стенда інтегрованої системи і проведенні експериментальних досліджень його працездатності, виявлення недоліків системи і розробки технічних рішення на їх подолання.

При проведенні досліджень проведено порівняльний аналіз охоронних та пожежних систем захисту різних фірм-виробників. Встановлено, що системи відрізняються застосуванням сучасних технологій, вимогами надійності та розширеним функціоналом. Встановлено, що на ринку відсутні інтегровані охоронно-пожежні дротові системи захисту для невеликих офісних приміщень.

На основі проведеного аналізу технічних характеристик ППК і складових елементів інтегрованої системи охорони для обладнання

охоронно-пожежною сигналізацією невеликого офісу вибрано ППК Orion NOVA 4 та клавіатуру K-LED4.

Для реалізації макета стенда в якості чутливих елементів вибрано сповіщувач розбиття скла LC-105DGB, комбінований датчик руху і розбиття скла Crow Swan PGB, сповіщувачі пожежні димові СПД-КАДЕТ та СПД-3 та сповіщувача пожежний ручний SPR-L.

Аналіз програмного забезпечення oLoader 2 показав, що його функціональні можливості надають можливість налаштувати сценарій роботи інтегрованої системи охоронно-пожежної сигналізації.

На основі проведено аналіз характеристик вхідних і вихідних портів ППК Orion NOVA 4, клавіатури K-LED4 та вибраних чутливих елементів розроблена схема електрична функціональна яка включає ППК та елементи сигналізації, контролю і управління інтегрованою системою та розроблений макет інтегрованої системи охоронно-пожежної сигналізації представлений на рис 1.



Рис. 1. Макет охоронно-пожежної сигналізації

Проведені результати експериментальних досліджень підтвердили працездатність розробленого макету охоронно-пожежної сигналізації, та технічну можливість використання ППК системи охоронної сигналізації для реалізації інтегрованої системи охороннопожежної сигналізації для невеликого офіса.

Список використаних джерел

1. Технічні характеристики ППК Orion NOVA 4. [Електронний ресурс]. – Режим доступу: URL: <https://tiras.technology/devices/orion-nova-4/>
2. Кушнір А. П., Чалий Д. О. Системи пожежної та охоронної сигналізації : Навч. посіб. Львів : СПОЛОМ, 2022. – 298 с.

UDC 004.056.55:003.26.09

*Humeniuk I., Cand. Tech. Sc., Assoc. Prof.,
Lahodnyi O., Cand. Tech. Sc.,
Kosheva I.
Korolov Zhytomyr Military Institute*

INFORMATION ENCRYPTION METHOD IS BASED ON A COMBINATION OF CRYPTOGRAPHIC AND STEGANOGRAPHIC PROPERTIES OF ALGORITHMS

Problem statement. With the beginning of a full-scale invasion of Russian Federation in Ukraine, the objects of cyber influence were primarily the government, energy, military and financial sectors of the state. In the current conditions, the task of improving existing methods of protecting information at the data, host and network levels, synthesis of cryptographic and steganographic encryption algorithms is becoming relevant. That is why the purpose of this work is to ensure high cryptographic stability of encrypted information during its transmission through the channels of the network of information and communication systems and reduce the level of threat of unauthorized access to it or attack on the cipher.

Research method. The main properties of information, the maintenance of which is one of the tasks of ensuring cybersecurity, include confidentiality, data integrity and accessibility to electronic information resources. Their complex set is called the security model (triad).

To achieve this goal, it is proposed to improve the method of information protection, which is based on the use of the alphabet of a monochrome image. The proposed method consists of three stages: primary, main (encryption) and final (decryption). Detailed scheme of the method functioning is given in Fig. 1.

In the first step, each character that can be used in the message is assigned a certain static range of values [000; 255], which corresponds to the brightness scale of the image pixels. If you select a color bitmap, this range is tripled by using all channels (R, G, and B). As a result, the number of alphabet variants increases, for example, the value for English characters is selected from [0; 255] the R channel, for punctuation marks and special characters – the G channel and digits – B, etc.

It is worth noting that the alphabet is synthesized on one side of the information exchange and sent to the other by closed channels of data transmission, or agreed without any third party.

Another step of the current stage is the formation of a pixel map. It arbitrarily selects an image with the same color model and the number of blocks to which it will be distributed and numbered.

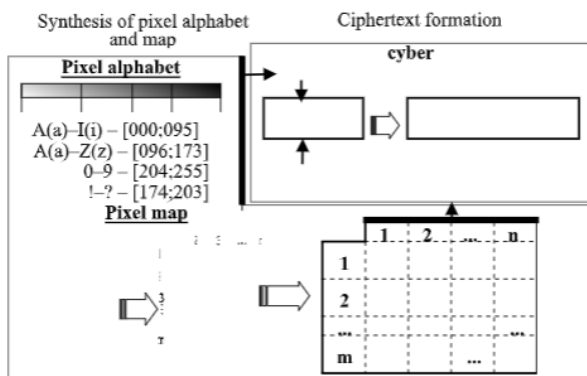


Fig. 1. Method operation scheme

For each block, average pixel brightness values are calculated and recorded in the table. The alphabet, the image should be changed with a certain periodicity.

The main stage is intended directly for encrypting the message of the original message, transmitting by the sender and receiving by the addressee. Its essence lies in the following: the message using the synthesized alphabet is replaced by the corresponding value from the range assigned to it. Further, pixel map block numbers and corresponding average pixel brightness values are randomly selected. Accordingly, these numbers determine the encryption key. Using the formulas given in the scheme, a ciphertext is formed. A feature of the method is that several characters can be assigned the same block.

The result is a ciphertext that looks like a sequence of pairs of values and for each character of the message.

Conclusion. The proposed method is advisable to use during the organization of the transfer of confidential information and in the presence of a potential threat of unauthorized access to it.

References

1. R. Hryshuk, Yu. Danik Fundamentals of Cybernetic Security : monograph, Zhytomyr. : ZhNAEU, 2016. 636 p.
2. V. Trysnyuk, K. Smetanin, I. Humeniuk, O. Samchyshyn, T. Trysnyuk Information Encryption Method based on a Combination of Steganographic and Cryptographic Algorithm's Features: Cybersecurity Providing in Information and Telecommunication Systems II, Kyiv, Ukraine, October 26, 2021. pp. 150–159.

УДК 004.056

*Ячменьова С.О., здобувач,
Шелуха О.О., к.т.н., доцент*

Державний університет «Житомирська політехніка»

МЕТОДИ ЗАХИСТУ WI-FI-МЕРЕЖ ВІД СПУФІНГУ

Останні роки зростає кількість кібератак через відкриті точки доступу в мережі стандарту IEEE 802.11 (Wi-Fi). Зловмисники завдяки відкритому характеру середовища мають можливість виявляти MAC адреси інших пристроїв у мережі, що дає змогу здійснити спуфінг атаки, так звану як «Злий двійник» («Evil twin»). Задля протидії поданій проблеми безпеки використовуються спостереження та аналіз кадрів у підключенні, зокрема моніторинг за допомогою систем штучного інтелекту.

Стандарт IEEE 802.11 є одним із основних видів бездротового зв'язку, який часто використовується Wi-Fi-мережами через велику кількість мобільних пристроїв. Не зважаючи на низку переваг у використанні, описаний стандарт працює за допомогою радіоефіру і широкомовної природи фізичного рівня, що робить мережу вразливою до здійснення атак на безпечній відстані. Зокрема, виокремлюють атаки: спрямовані на різні рівні мережевої моделі OSI; рекогносцирування; доступності; посередника; спуфінг.

Атака спуфінгу, зокрема «Злий двійник», націлена на перепідключення користувачів до шахрайської точки доступу для витягання конфіденційної інформації. Цей тип атаки може використовувати бездротові системи з низьким рівнем захисту, що стає особливо небезпечним з урахуванням розвитку мікрочипів та Інтернету речей. Зловмисники можуть використовувати вразливі пристрої, такі як смарт-годинники, фітнес-браслети, кардіо системи, для отримання конфіденційної інформації. Кінцевий результат атаки полягає в переважанні мережі шляхом відправки завдань з високим пріоритетом і цілеспрямованому перехопленні доступу до інтернет-трафіку від ключових пристроїв клієнта [1].

На сьогоднішній день стандартними заходами для запобігання такого роду атаки є низка заходів, що включають забезпечення тактових відміток з'єднання, нагляд за підозрілою активністю у бездротовій мережі та забезпечення шифрованого доступу до підключення. Спостереження мережі стандарту IEEE 802.11 та моніторинг кадрів-маяків підключення використовують для визначення несанкціонованих точок доступу, що піддалися атаці чи підозрілій активності.

Моніторинг Wi-Fi зазвичай здійснюють за допомогою мережного аналізатора, налаштувавши фільтрацію по Mac-адресі і певному типу

кадрів. Проте, варто зазначити, що процес контролю системи є складним та витратним, тому сьогодні актуальним є використання програм-оптимізаторів чи систем штучного інтелекту для полегшення поставленої задачі.

Можна виділити низку переваг використання штучного інтелекту для боротьби зі спуфінгом типу «Злий двійник» («Evil twin»), а саме: гнучкість та адаптація до змін в мережі; висока швидкість обробки; оптимальний аналіз мережі; доступність до системи знань; нескладний процес зміни даних.

У комплексі моніторингу підключень використовується алгоритм k-найближчих сусідів з використанням штучного інтелекту. Цей метод аналізує мережеві пакети, зберігає дані на основі часових рядів і визначає категорію пристроїв за рівнем сигналу від точки доступу. Основна мета алгоритму – створення моделі класифікації для нових зразків на основі їх подібності до найближчих зразків у наборі даних. Слід зазначити, що метод k-найближчих сусідів з використанням аналізу за допомогою штучного інтелекту, було протестовано і оцінено під час дослідження науковими працівниками «Львівської Політехніки» у 2023 році [2].

Отримані результати, а саме 100 % тестових випадків (більше 7 тисяч), було класифіковано правильно, що вказує, на те, що обраний метод аналізу даних дозволить значно підвищити безпеку інформаційно-комунікаційних системах державного та приватного рівнів [2].

Важливо відмітити деякі негативні сторони використання описаного методу аналізу даних, а саме: необхідність технічного забезпечення для повного функціонування системи, постійне навчання мережі штучного інтелекту, ризик неточності виявлення атаки.

Отже, у сучасному світі є реалізація ефективних методів з використанням штучного інтелекту в моніторингу кадрів для захисту в мереж стандарту IEEE 802.11 від кібератак типу «Злий двійник».

Таким чином, подальші дослідження будуть спрямовані на вдосконалення існуючих методів та систем протидії спуфінг-атак, розробку нових технологій для поліпшення моніторингу та покращення захисту від стороннього втручання в безпроводних мережах стандарту IEEE 802.11(Wi-Fi).

Список використаної літератури

1. Корольков Р.Ю. Сценарій атаки з використанням несанкціонованої точки доступу у мережах IEEE 802.11. Кібербезпека: освіта, наука, техніка. 3 (11), 2021, с. 144-154. – URL: <https://doi.org/10.28925/2663-4023.2021.11.144154>

УДК 004.7

*Магурін О. О., здобувач,
Шелуха О. О., к.т.н., доцент
Державний університет «Житомирська політехніка»*

ІНФРАСТРУКТУРА ЯК КОД, ХМАРНА ІНТЕГРАЦІЯ ТА НОВІ ТЕНДЕНЦІЇ

Інфраструктура як код (IaC) фундаментально переосмислює традиційний підхід до управління та впровадження ІТ-інфраструктури. У своїй суті IaC передбачає представлення конфігурацій інфраструктури через код, що дозволяє автоматизовано виконувати розгортання, конфігурацію та масштабування ресурсів [1]. Цей перехід від ручних, вразливих до помилок процесів до автоматизації, що базується на коді, керується кількома ключовими принципами. Перш за все – це концепція кодифікації інфраструктури, де конфігурації виражаються у форматі, що сприймається комп'ютерами. Цей принцип сприяє контролю версій, дозволяючи командам відстежувати зміни, ефективно співпрацювати та повертатися до попередніх станів за необхідності. Крім того, IaC підкреслює ідемпотентність конфігурацій, що означає, що однаковий набір інструкцій, який виконується кілька разів, дає однаковий результат, забезпечуючи передбачуваність у розгортанні. Оброблюючи інфраструктуру як код, організації можуть досягти гнучкості, швидкості та надійності у керуванні своїми ІТ-ресурсами.

Впровадження IaC включає ключові компоненти для визначення та оркестрації бажаного стану інфраструктури. Шаблони, представлені мовами типу YAML або JSON, служать схемами для ресурсів інфраструктури, описуючи конфігурацію, залежності та взаємозв'язки між компонентами. Системи контролю версій, такі як Git, використовуються для контролю версій шаблонів. Автоматизовані засоби впровадження, такі як Terraform або Ansible, інтерпретують шаблони та реалізують ресурси в хмарних середовищах [2]. Інтеграція цих компонентів дозволяє організаціям оптимізувати весь життєвий цикл інфраструктури, включаючи створення, зміни, масштабування та виведення з експлуатації.

Автоматизація та оркестрація є невід'ємними аспектами реалізації повного потенціалу IaC [3]. Автоматизація передбачає систематичне виконання заздалегідь визначених завдань без ручного втручання. В IaC автоматизація дозволяє швидке та послідовне надання інфраструктурних ресурсів, зменшуючи ймовірність помилок, пов'язаних з ручними процесами. Оркестрація цих завдань стає важливою при роботі з складними, багатокomпонентними системами.

В контексті IaC оркестрація вказує на координацію та управління кількома автоматизованими процесами для досягнення бажаного стану. Це забезпечує синхронне розгортання різних компонентів інфраструктури, сприяючи загальній ефективності та надійності системи.

Багато інструментів полегшують впровадження IaC, кожен зі своїми унікальними можливостями та функціоналом [3]. Terraform дозволяє користувачам визначати та надавати інфраструктуру за допомогою декларативної мови конфігурації. Ansible, з іншого боку, дотримується імперативного підходу, фокусуючись на завданнях з автоматизації та управлінні конфігурацією. Chef та Puppet – це додаткові інструменти, які акцентують на автоматизації процесів управління конфігурацією.

Інфраструктура як код (IaC) в хмарних обчисленнях принесла численні переваги: швидкість та гнучкість при управлінні ресурсами, автоматизація розгортання, що скорочує час масштабування і налаштування. Однорідність конфігурацій на різних етапах розробки забезпечує їхню однаковість, а IaC дозволяє динамічно виділяти та звільняти ресурси згідно із вимогами хмарових послуг. Підтримка спільної мови та процесу сприяє співпраці між розробниками та операторами, сприяючи культурі DevOps і прискорюючи постачання додатків.

В майбутньому кілька нових технологій готуються визначити майбутню картину IaC. Одним із помітних трендів є зростання serverless архітектур, де акцент переноситься з управління компонентами інфраструктури на виконання окремих функцій [3]. Безсерверне обчислення абстрагує базову інфраструктуру, дозволяючи розробникам зосередитися лише на написанні коду, тим самим підвищуючи гнучкість та ефективність використання ресурсів. Ще однією новою методологією є GitOps, парадигма, які дуже глибоко використовують репозиторії Git як джерело для конфігурацій інфраструктури. Цей підхід сприяє управлінню інфраструктурою, яке базується на контролі версій, аудиті та співпраці, додатково інтегруючи робочі процеси розробки та операцій. Оскільки організації продовжують приймати практику мікросервісів та контейнеризації, очікується, що ці нові технології відіграють ключову роль у розвитку практик IaC.

Список використаної літератури

1. Infrastructure as Code: What Is It? Why Is It Important? URL: <https://www.hashicorp.com/resources/what-is-infrastructure-as-code>
2. What is Terraform? URL: <https://developer.hashicorp.com/terraform/intro>
3. J. Geerling. Ansible for DevOps: Server and configuration management for humans. 2nd edition. 2023. 469 p. URL: <https://www.ansiblefordevops.com/>

УДК 004.056

*Дячук О. Ю., магістрантка,
Єфіменко А. А., к.т.н., доцент
Державний університет «Житомирська політехніка»*

АНАЛІЗ ОСНОВНИХ МЕТОДІВ ЗАХИСТУ КОМП'ЮТЕРНИХ МЕРЕЖ

Інформаційна безпека та захист інформації нерозривно пов'язані. Захист інформації – це комплекс операцій для забезпечення безпеки (цілісності та секретності) під час збирання, обробки, зберігання та передачі. Безпека інформації включає конфіденційність, скритність і цілісність даних. У розширеному розумінні захист інформації – це сукупність заходів (організаційних, законодавчих, технічних), спрямованих на нівелювання потенційних небезпек та ліквідацію їхніх наслідків. Суть захисту інформаційних даних полягає у виявленні та усуненні можливих загроз, шкідливих джерел і критичних причин, що можуть пошкодити інформацію.

Основні методи захисту інформації:

1. Неформальні методи захисту.

Неформальні методи захисту інформації включають законодавчі, адміністративні та морально-етичні засоби. Законодавча база, надана державою, регулює захист даних через різноманітні законодавчі проекти та документи. Адміністративні заходи є основою для формування ефективних механізмів захисту інформаційних даних, оскільки багато загроз пов'язані з неправомірними діями осіб та порушенням посадових повноважень.

Для зниження небезпек інформаційної безпеки важливо створити стійку базу, яка об'єднає законодавчо-правові та організаційно-технічні заходи. Морально-етичні методи включають норми і правила, сформовані в суспільстві чи колективі, які, хоча не врегульовані державною правовою системою, проте гарантують збереження інформаційних даних. Порушення цих норм може призвести до втрати довіри та підриву авторитету особи чи компанії.

2. Технічні способи захисту інформації.

У захисному програмному забезпеченні немає сенсу, якщо зловмисники можуть без зусиль отримати доступ до жорстких дисків з інформацією. Тому важливо спочатку забезпечити фізичний захист для технічних пристроїв і приміщень. Це можна здійснити за допомогою віконних ґрат, дверей з кодовими замками, сигналізації та камер цілодобового відеоспостереження.

Приміщення також слід захищати від природних катаклізмів і надзвичайних подій, використовуючи пожежну сигналізацію, датчики води і диму. Фізичні засоби забезпечення інформаційної безпеки не гарантують захист від отримання доступу через мережу, проте ефективно оберігають комп'ютерне обладнання та носії інформаційних даних.

3. Програмні способи захисту інформації.

Інструментарій для захисту відомостей включає програмні компоненти для комп'ютерів, ноутбуків та серверів. Серед програмних методів захисту виділяють такі:

- Антивірусні програми для виявлення та видалення вірусів;
- Обмеження доступу до інформаційної системи через особисті кабінети та паролі;
- Віртуалізація для створення «пісочниць» для неперевірених програм;
- Міжмережні брандмауери для контролю вхідного трафіку;
- DLP-системи, що обмежують копіювання і перенос відомостей;
- SIEM-системи для відстеження підозрілих активностей.

Важливо пам'ятати, що окремі програми захищають від обмеженого числа загроз. Для максимального рівня захисту потрібна взаємодія між програмами і технічними засобами, де кожен компонент «прикриває тили» іншого.

4. Апаратні способи захисту інформації.

Апаратні технічні методи захисту інформації включають:

- Спеціалізовані генератори цифрового шуму, які шифрують дані та створюють інформаційний шум для маскування каналів зв'язку.
- Апаратні реєстри паролів, що зберігають паролі і обов'язкові для доступу до інформаційних даних.
- Апаратні системи довіреного завантаження, які обмежують установку сторонніх операційних систем та програмного забезпечення для захисту даних на жорсткому диску.

Хоча апаратні методи можуть здаватися подібними до програмних, вони виявляються продуктивнішими і надійнішими, маючи підвищену стійкість перед атаками. Забезпечення максимального рівня інформаційної безпеки вимагає поєднання програмних та апаратних інструментів. Важливо віддавати перевагу сертифікованим та ліцензійним програмам для гарантії надійності, контрольованої органами держави.

5. Криптографічні способи захисту інформації.

Криптографія використовує спеціальні методи шифрування для захисту даних від змін, забезпечуючи безпеку інформації без обмеження доступу. Це дозволяє зберігати дані в зашифрованому вигляді, недоступному без відповідного криптографічного ключа.

Криптографія поділяється на чотири групи:

- Симетричні криптосистеми: Використовує один і той самий ключ для шифрування і розшифрування інформації.
- Криптосистеми з відкритим ключем: Використовують два пов'язаних ключі – відкритий і закритий – для кодування та розкодування.
- Криптосистеми на основі електронного підпису: Використовуються для підтвердження достовірності документів і авторства.
- Системи управління ключами: Взаємодіють з інформаційними даними на основі розподілу ключів між працівниками.

Криптографічні засоби застосовуються для передачі конфіденційної інформації, підтвердження автентичності, авторства та для зберігання закодованих даних на зовнішніх носіях. Це надійний метод забезпечення інформаційної безпеки.

6. Мережеві способи захисту інформації.

Для забезпечення інформаційної безпеки в комп'ютерних мережах використовують спеціалізовані програмно-технічні продукти, такі як фільтрувальні пакетні засоби, маршрутизатори та програмні шлюзи для контролю доступу. Однак основним засобом захисту від несанкціонованих атак є Firewall, який забезпечує зовнішній захист і обмежує доступ до мережі.

Firewall відбиває атаки, фільтрує вхідний трафік, обмежує доступ до ресурсів, фільтрує небажану кореспонденцію через електронну пошту. Ще один ефективний інструмент – маршрутизатор, який фільтрує пакети відомостей, обмежує доступ до певних адрес і хостів, а також контролює відправників і одержувачів.

Мережеві засоби дозволяють захищати дані як у глобальній мережі Інтернет, так і всередині корпоративних систем. Комплексний захист включає в себе організацію програмно-апаратних комплексів для забезпечення безпеки інформаційних даних на підприємстві.

7. Способи захисту інформації в Інтернеті

Для захисту інформаційного контенту компанії в Інтернеті потрібно розробити внутрішній документ, що визначає види інформації, етапи отримання дозволу на її розміщення, місце та доступність для різних категорій користувачів. Важливо розділити

інформацію на конфіденційну та загальну, забезпечуючи захист корпоративних даних.

Забезпечення інформаційної безпеки включає захист конфіденційних корпоративних даних. Важливо встановити різні рівні доступу для співробітників та визначити, яка інформація доступна для загального використання.

При наявності веб-сайту слід обдумати рівні доступу до збережених відомостей. Рекомендується розділити співробітників на групи та надавати відповідний рівень доступу, зокрема для вищого адміністративного апарату, керівників підрозділів та пересічних фахівців.

Для клієнтів важливо розміщувати відкриту інформацію про вартість товарів і послуг, знижки та акції. Якщо необхідно обмежити доступ конкурентам, ці дані можуть бачити лише зареєстровані користувачі.

У підсумку, можна визначити, що забезпечення інформаційної безпеки в сучасному цифровому середовищі є надзвичайно складним завданням, яке вимагає комплексного підходу та поєднання різноманітних програмних і технічних засобів захисту. Успішна імплементація заходів із забезпечення безпеки включає в себе не лише застосування передових технологій, але й врахування законодавчих, адміністративних та морально-етичних аспектів.

Таким чином, сучасний підхід до забезпечення інформаційної безпеки передбачає використання широкого арсеналу інструментів, які взаємодіють між собою для створення повноцінної та надійної системи захисту. Поєднання апаратних методів зі спеціалізованими програмними компонентами стає запорукою найвищого рівня інформаційної безпеки, враховуючи різноманітні вектори загроз і високий рівень вимог до збереження конфіденційності та цілісності даних.

Список використаної літератури

1. E. Knipp et al., *Managing Cisco Network Security*. Elsevier Inc., 2002
2. S. Wilkins, T. Smith *CCNP Security. SECURE 642-637 Official Cert Guide*. Cisco Press, 2011
3. A. D wankhade and P. N. Dr Chatur *Comparison of Firewall and Intrusion Detection System*, *Int. J. Comput. Sci. Inf. Technol.* vol. 5, no 1. 674-678 pp., 2014, URL: <http://ijcsit.com/docs/Volume 5/vol5issue01/ijcsit20140501145.pdf/>.

УДК 004.4

Goncharov M., master's student
Zhytomyr Polytechnic State University

MODERN FRONTEND ARCHITECTURES ANALYSIS

Frontend architecture comprises a bunch of practices and tools that upgrade application's code quality. What's more, it also presents the opportunity to create a productive, scalable, and sustainable workflow. Frontend architecture can be divided into two main categories: micro frontends and monolithic frontends.

In micro frontend approach each team is responsible for a small self sufficient application which implements part of big system functionality. All applications built and delivered separately. The shell application composes all micro frontend applications into one system and delivers it to the end user. Micro frontend approach improves flexibility, scalability and maintainability of the systems.

Micro frontend advantages:

- **Technology agnostic:** Teams are independent in technology choice and able to upgrade and maintain their stack without coordination with other teams. It gives teams more flexibility to choose the best technology for each micro frontend.
- **Codebase isolation:** Micro frontend application codebase isolated from other development teams, which simplify structuring and maintenance.
- **Developer productivity:** Micro frontends can help to improve developer productivity by allowing teams to work on different parts of the application independently. This is because micro frontends can be developed and deployed independently, without affecting the rest of the application.
- **Active usage of native browser features:** The micro frontend encourages teams to use native browser features instead of custom API's for communication between applications.

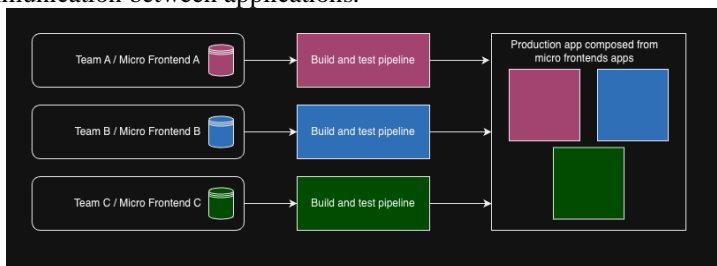


Fig. 1. Micro frontend delivery architecture

Monolithic frontend architecture is a traditional web application architecture in which all of the frontend code is contained in a single codebase. This means that the entire user interface (UI) and all of the functionality of the application are implemented in a single, large codebase.

Main advantages of monolithic frontend architecture:

- **Simplicity:** Monolithic frontends are easy to understand and develop. All of the code for the UI is in a single place, making it easy to find and modify.
- **Performance:** Monolithic frontends can often perform better than Micro Frontends due to reduced overhead. There is no need to communicate between different Micro Frontends, and the code is typically more optimized.
- **Cost:** Monolithic frontends are typically less expensive to develop and maintain than Micro Frontends. There is no need to develop and maintain separate codebases for different Micro Frontends.

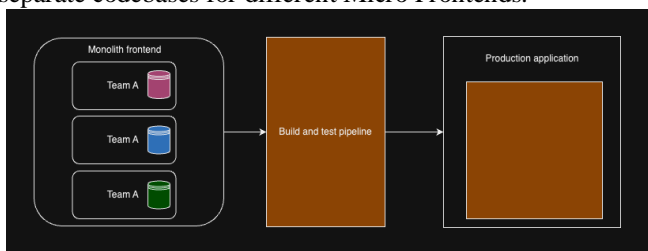


Fig. 2. Monolith frontend delivery architecture

Choosing right frontend architecture depends on project requirements, budget and resources. Micro frontend will fit for large and complex applications with a lot of development teams, it will allow quickly and easily scale and provides freedom for the teams in the technologies usage. Monolith frontend is ideal for small and simple applications, it will speed up development, simplify maintenance, reduce product delivery time and budget expenses.

RESOURCES

1. Luca Mezzalira, Building Micro-Frontends: Scaling Teams and Projects, Empowering Developers
2. Michael Geers, Micro Frontends in action
3. Micro Frontends URL: <https://martinfowler.com/articles/micro-frontends.html>
4. Microfrontends vs. Monolithic Frontend: Which Is Right for Your Project? URL: <https://levelup.gitconnected.com/microfrontends-vs-monolithic-frontend-which-is-right-for-your-project-2980c6939a36>

УДК 621.3: 455.63

*Капітон А. М., д.пед.н., професор,
Прокудін А. Ю., здобувач*

Національний університет «Полтавська політехніка ім. Юрія Кондратюка»

КІБЕРБЕЗПЕКА В ЕПОХУ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

Кібербезпека в епоху цифрової трансформації є однією з найбільш актуальних та важливих проблем сучасного світу. Зростання кількості цифрових атак та загроз вимагає постійного удосконалення методів захисту, а також розробки нових стратегій та підходів до кібербезпеки. Цифрова трансформація призводить до значного збільшення обсягу цифрових даних, що потребують захисту, до появи нових векторів атак, пов'язаних з розробкою та впровадженням нових технологій.

Із поширенням цифрових технологій та зростанням кількості цифрових даних зростає й загроза їх незаконного доступу та використання. Тому важливо розглядати нові підходи до кібербезпеки, такі як штучний інтелект, машинне навчання, блокчейн технології та інші інноваційні методи. Використання штучного інтелекту та машинного навчання може допомогти у виявленні та усуненні загроз безпеці, а також у попередженні цифрових атак. Блокчейн технології можуть забезпечити додатковий рівень безпеки для цифрових даних та транзакцій, що є особливо важливим у сферах фінансів та медицини.

Також важливо розглядати вплив цифрової трансформації на загальний рівень кібербезпеки, зокрема на захист особистих даних, інфраструктури критичних систем, корпоративних мереж та інших сфер. З поширенням «Інтернету речей» (IoT) з'являються нові можливості для кібератак на обладнання, пристрої, що може призвести до серйозних наслідків для людей та організацій. Тому необхідно активно досліджувати цей напрямок та розробляти методи захисту в умовах швидкого розвитку цифрових технологій.

Дослідження цих питань дозволить розробити більш ефективні стратегії захисту в умовах цифрової трансформації, а також виявити потенційні загрози та вразливості, пов'язані з швидким розвитком цифрових технологій. Враховуючи постійне зростання кількості атак, важливо активно працювати над покращенням кібербезпеки в епоху цифрової трансформації, щоб забезпечити стабільну та безпечну роботу цифрових систем у майбутньому.

Соціальна інженерія, фішинг та інші види атак, спрямовані на отримання доступу до систем через маніпуляцію людьми, стають все більш поширеними. Тому нам слід обговорити питання психології кібербезпеки, навчання персоналу та розвиток свідомості про безпеку

серед користувачів. У цьому контексті, спеціалісти з кібербезпеки мають велику відповідальність за забезпечення безпеки цифрових систем та захист особистих даних користувачів. Вони повинні постійно вдосконалювати свої навички та знання, щоб бути готовими до виявлення та усунення потенційних загроз. Також важливо сприяти своєчасному виявленню нових загроз та розробці ефективних методів захисту.

Усе більше компаній та установ розуміють, що ефективна програма з кібербезпеки включає фахівців, процеси й технологічні рішення, які разом зменшують ризик перерв у роботі компаній, фінансових втрат і підриву репутації внаслідок атак і виділяють значні кошти на захист своєї інформації та інфраструктури. Проте, безпека мереж та систем повинна бути постійною та систематичною, оскільки загрози постійно змінюються і розвиваються разом із цифровими технологіями.

Отже, кібербезпека є лідером та одним із найбільш актуальних питань у сучасному світі, особливо в умовах швидкого розвитку цифрових технологій. Вивчення нових підходів до кібербезпеки, таких як штучний інтелект, машинне навчання, блокчейн-технології та інші інноваційні методи, дозволить стабілізувати ситуацію і забезпечити безпечне функціонування цифрових систем у майбутньому.

Список використаних джерел

1. Що таке кібербезпека? URL: <https://www.microsoft.com/uk-ua/security/business/security-101/what-is-cybersecurity> (дата звернення: 14.11.2023).
2. Цифровізація як нова реальність України. URL: <https://lexinform.com.ua/dumka-eksperta/tsyfrovizatsiya-yak-nova-realnist-ukrayiny/>
3. Когут Ю. І. Кібербезпека та ризики цифрової трансформації компаній. навч. посіб., Київ : Сідкон, 2021. 372 с.
4. Kali Linux 2018: Захист безпеки за допомогою тестування на проникнення.: посіб. / Парасрам Ш., та ін. 5-те вид., 2020. 448с.
5. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О. Довгань; упоряд. О. Довгань, Л. Литвинова, С. Дорогих; Науково-дослідний інститут інформатики і права НАПрН України; Національна бібліотека України ім. В. І. Вернадського. – К., 2019. – №3. – 80 с.

УДК 004.056

*Трокоз Є. М., ст. викладач,
Таргонський О. В., магістрант
Державний університет «Житомирська політехніка»*

СУЧАСНІ ІНСТРУМЕНТИ ТА ТЕХНОЛОГІЇ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

Час не стоїть на місці. Глобальна всесвітня комп'ютеризація зіткнулася з глобальною кіберзлочинністю. Міжнародні експерти стверджують, що кожне третє злочинне діяння у світі відбувається у віртуальному світі. Одним із найнебезпечніших типів атак є соціальна інженерія.

Соціальна інженерія (у контексті інформаційної безпеки) – це наука, яка вивчає методи та фактори впливу на людську свідомість та її переконання. У контексті кібербезпеки – соціальна інженерія є одним з найнебезпечніших типів атак та серйозною загрозою інформаційній безпеці. Метою соціальної інженерії є спонукання людей робити певні дії, які вони за звичних умов ніколи б не вчинили. Американський консультант з комп'ютерної безпеки, письменник Кевін Митник, а в минулому один із найвідоміших у світі комп'ютерних хакерів, стверджував, що «зламати людину набагато простіше, ніж комп'ютер, оскільки комп'ютери дотримуються інструкцій, а люди піддаються емоціям» [1].

Кіберзлочинці знаходять все нові і нові способи експлуатації людського фактору. Найпоширенішими є повідомлення про терміновість порятунку рідної людини, про проблеми із банківською карткою і т.д. Маніпулювання людською свідомістю відбувається настільки професійно, що жертва стає співавтором виконання задумів злочинців (особливо зараз, коли ми знаходимося у стані війни та психіка громадян надзвичайно травмована). Тому для ефективного захисту від атак кіберзлочинців надзвичайно важливо володіти знаннями про психологічні підходи, якими вони володіють, та про сучасні інструменти та технології, які вони використовують.

Відомий психолог Роберт Чалдіні виділив шість психологічних прийомів, на яких базується весь арсенал інструментарію та технологій соціальної інженерії, а саме: взаємність (людина намагається відповісти добром на добро, послугою на послугу, щоб не бути у «боргу»); послідовність (хакер спочатку проковує жертву розкрити малий обсяг інформації та, користуючись принципом «послідовності», досягає своєї мети); конформізм (людина погоджується з тим, що робить більшість); авторитет (людині

притаманно слідувати за тими, кому вона довіряє, кого знає, хто для неї є авторитетом); симпатія (людина охочіше та швидше виконує прохання тих, хто їй симпатичний, або зробить те, що їй подобається); дефіцит (людина завжди більше бажає того, що їй недоступно) [2].

В залежності від поставленої мети зловмисника, використовуються і відповідні інструменти та технології соціальної інженерії. Фішинг – найпопулярніший сучасний інструмент соціальної інженерії. Зловмисник надсилає електронний лист або інше повідомлення, яке містить посилання на підроблений веб-сайт. Жертва переходить за посиланням, вводить свої облікові дані або іншу конфіденційну інформацію, яка потім може бути використана для злому її облікового запису. Вішинг – телефонне шахрайство, метою якого є отримання реквізитів банківських карток або будь-якої іншої конфіденційної інформації. Смішинг – використовуються текстові SMS-повідомлення, які містять шкідливі посилання або вміст. Претекстинг – вид атаки, який передбачає використання голосових засобів, таких як Skype, телефон і т.п. Попередньо проводиться збір персональних даних жертви. Підманювання – зловмисники використовують привабливі пропозиції або стимули, щоб заманити жертву в пастку. Соціальна інженерія на основі штучного інтелекту – вид атаки, в якому зловмисники використовують штучний інтелект для створення більш реалістичних і ефективних атак соціальної інженерії [3].

Таким чином, соціальна інженерія є досить актуальною проблемою, яка впливає на людську свідомість. Сценарії, за якими працюють шахраї, є досить різноманітними. Атаки соціальної інженерії можуть бути спрямовані на отримання фінансової вигоди, отримання конфіденційної інформації, нанесення збитків, можуть мати політичні мотиви та ін. Важливо розуміти, що атаки соціальної інженерії можуть стати загрозою для будь-якої особи або організації, незалежно від їх статусу чи потреб.

Список використаних джерел

1. Mitnick, Kevin, and William L. Simon. *The Art of Deception: Controlling the Human Element of Security*. Wiley, 2002. – 368 p.
2. Cialdini R.B. *Influence: The psychology of persuasion* / Robert B. Cialdini. – New York: Harper Business, HarperCollins Publishers, 2007. – 322 p.
3. Social engineering attack techniques. URL: <https://www.imperva.com/learn/application-security/social-engineering-attack/>

УДК 004.056

Трокоз Є.М., ст. викладач,

Сірик А.Ю., магістрант

Державний університет «Житомирська політехніка»

ЗАСТОСУВАННЯ БЕЗПЕЧНИХ АРІ ДЛЯ ОБМІНУ ДАНИМИ: МЕТОДИ ТА ТЕХНОЛОГІЇ

В сучасному світі, де інформаційні технології визначають нові стандарти розвитку, обмін даними між програмами та сервісами виявляється ключовим аспектом розробки програмного забезпечення. Процес обміну даними потребує не лише ефективності та швидкості, але й високого рівня безпеки.

АРІ, або інтерфейс програмування додатків, є механізмом, що визначає взаємодію між різними програмами чи сервісами. Це забезпечує ефективну комунікацію та обмін даними між різними компонентами програмного забезпечення. Серед різних архітектур АРІ можна виділити RESTful, SOAP, GraphQL, WebSocket та Open API (Swagger).

RESTful API (Representational State Transfer) орієнтований на ресурси. Кожен ресурс має свій унікальний URI. В RESTful API використовуються стандартні методи HTTP. Також він спрощує роботу з даними та підтримує швидку та ефективну взаємодію. SOAP API (Simple Object Access Protocol) заснований на обміні повідомленнями у форматі XML. Використовується для обміну структурованими та типізованими даними. Підтримує більш жорсткі стандарти в порівнянні з RESTful і частіше використовується у великих корпоративних системах. GraphQL API дозволяє клієнтам запитувати саме ті дані, які їм потрібні, замість отримання всього об'єму даних. Визначає структуру запитів та формат повернених даних на стороні клієнта. Також GraphQL API забезпечує більш гнучку та ефективну взаємодію для клієнтів. WebSocket API забезпечує двосторонню взаємодію між клієнтом та сервером в режимі реального часу. Використовує постійне підключення для передачі даних в обидві сторони. WebSocket API ідеальний для відстеження подій, онлайн-чатів та інших сценаріїв, де необхідна миттєва взаємодія. Open API (Swagger) визначає стандарти та специфікації для документації та розробки АРІ. Забезпечує чітку специфікацію для структури та взаємодії з АРІ. Крім того, він дозволяє автоматично генерувати код для взаємодії з АРІ на різних мовах програмування [1].

Один із важливих аспектів безпеки в обміні даними – це використання протоколу HTTPS. Він забезпечує захищену передачу

даних за допомогою шифрування, зменшуючи ризик перехоплення чи модифікації інформації. Однією з ключових функцій HTTPS є використання шифрування для захисту даних під час їхньої передачі. Для цього використовуються криптографічні протоколи, такі як TLS (Transport Layer Security) або його попередник SSL (Secure Sockets Layer). Сертифікати видаються авторитетними сертифікаційними центрами та підтверджують ідентичність сервера. Шифрування унеможливує зловмисникам читання чи модифікацію даних, які передаються між клієнтом та сервером. HTTPS використовує різні криптографічні алгоритми для забезпечення конфіденційності та цілісності даних. Сайти, які використовують протокол HTTPS, можуть отримати позитивний вплив на їхній рейтинг у пошукових системах. Крім того, браузерери можуть позначати незахищені сайти як небезпечні, тоді як захищені сайти відзначаються символом замку чи іншими позначками безпеки.

OAuth 2.0 є важливим інструментом для забезпечення безпеки під час обміну авторизаційними даними між різними системами. Він дозволяє надавати обмежений доступ до ресурсів без передачі облікових даних. Токени в OAuth 2.0 використовуються для ідентифікації та авторизації користувачів під час доступу до ресурсів. Вони використовуються для забезпечення безпеки обміну даними та відокремлення від передачі справжніх облікових даних.

Застосування безпеки на рівні даних. Шифрування та хешування грають важливу роль у забезпеченні безпеки обміну даними через API. Шифрування забезпечує конфіденційність, а хешування допомагає перевірити цілісність отриманих даних [2, 3].

Методи та технології обміну даними з використанням безпечних API є визначальним елементом сучасного програмування. Вони забезпечують не тільки ефективну комунікацію, а й гарантують безпеку обміну даними відповідно до найвищих стандартів. Розуміння та використання цих методів та технологій стає важливим завданням для розробників у всіх сферах індустрії.

Список використаних джерел

1. Jacobson, Daniel. APIs: A Strategy Guide. O'Reilly Media, 2012. – 148 p.
2. API Security. URL: <https://www.imperva.com/learn/application-security/api-security>
3. What is API Security? URL: <https://nonamesecurity.com/learn/api-security/>

УДК 004.42

Болотіна В. В., ст. викладач,

Адамчук Р. С., здобувач

Державний університет «Житомирська політехніка»

ЗАХИСТ ДАНИХ У ВЕБ-ДОДАТКАХ СТВОРЕНИХ ЗА ДОПОМОГОЮ МОВИ ПРОГРАМУВАННЯ JAVASCRIPT

У світі, де кожен клік – це новий цифровий слід, безпека даних у веб-додатках стає справжньою битвою проти зловмисників. Захист даних – від персональних даних користувачів до фінансових секретів – є фундаментальним елементом веб-екосистеми. Дані, як скарб сучасного Інтернету, стають мішенню для хакерів. Уявімо, наприклад, що ви робите покупки в Інтернет-магазині і вводите певну інформацію. Якщо ця інформація не зашифрована, хакери можуть зловити вас і легалізувати ваш банківський рахунок. Тут безпека даних – це щит, який може вас врятувати.

Шифрування HTTPS інкапсулює ваші дані в захищену оболонку. У реальності онлайн-платежів цей щит шифрування перетворює ваші фінансові дані на віртуальний сейф, недоступний для небажаних зловмисників. Це схоже на сучасну магію, що виключає можливість несанкціонованого доступу або невдалих спроб вилучення цінного цифрового контенту. Щоб запобігти зловживанню, системи використовують валідацію. Наприклад, розуміючи, що в поле пароллю не можна вставити SQL-запит, ви уникаєте потенційної атаки, що може порушити всю систему.

Взаємодія з просунутими бібліотеками, такими як Vue.js та Svelte – це не просто технічний код, а високоякісне мистецтво взаємодії. Прикладом використання такого підходу є відомий сервіс Twitter. Він реалізує розгалужений frontend для безперервної трансляції твітів. Це не лише стимулює активне залучення, але й надає можливість швидко оновлювати дані користувачів. Використання передових технологій, таких як Sequelize для PostgreSQL, відображає ефективний спосіб взаємодії з базою даних. Наприклад, в ігрових додатках Sequelize можна використовувати для зберігання і оновлення статистики гравців в режимі реального часу, забезпечуючи високоефективний інструмент для обробки даних в контексті гри. Функції, такі як DOMPurify в JavaScript, – це аналог таємного агента, який перевіряє кожен символ, щоб уникнути ураження шкідливого коду на сторінці. Важливо, коли ви взаємодієте з введенням користувача.

Впроваджуючи атрибути HttpOnly і Secure для файлів cookie, можливо додати рівень безпеки, подібний до надійного залізничного

замка на вході в інформаційне сховище. Ця стратегія особливо важлива для ефективного управління сесансами у веб-додатках.

У веб-додатках на основі JavaScript, де безпека даних є критично важливою, акцент робиться на правильній обробці вхідних даних і забезпеченні безпеки виконання скриптів. Використання спеціальних бібліотек, таких як Validator.js, може допомогти уникнути несанкціонованих атак, пов'язаних з несанкціонованим введенням даних, і допомагає забезпечити надійний рівень захисту. Ще однією важливою складовою є обережне використання асинхронних запитів. Використання технік, таких як CORS (Cross-Origin Resource Sharing), може запобігти атакам типу Cross-Site Request Forgery (CSRF), забезпечуючи, що запити на сервер відбуваються лише з дозволених джерел.

Використання мови програмування JavaScript у веб-додатках не лише втілює технічні аспекти інтерактивності, але й покладає на нас відповідальність за забезпечення найвищого рівня безпеки. Щоб цінні дані не потрапили до рук зловмисників, ми повинні забезпечити дотримання найкращих практик та постійного вдосконалення безпеки відповідно до динаміки технологічних змін. У цьому контексті важливе значення мають керівні принципи найкращих практик і постійне вдосконалення механізмів безпеки, що відображають вимоги сучасної цифрової екосистеми.

Список використаних джерел

1. JavaScript Security | JavaScript Vulnerabilities | Snyk. Snyk. URL: <https://snyk.io/learn/javascript-security/> (date of access: 19.11.2023).
2. Why is JavaScript Security Important?. What is JavaScript Security?. URL: <https://www.checkpoint.com/cyber-hub/cloud-security/what-is-secure-coding/what-is-javascript-security>. (date of access: 19.11.2023).
3. What is Web Application Security?. Cloudflare. URL: <https://www.cloudflare.com/learning/security/what-is-web-application-security/> (date of access: 19.11.2023).
4. What Is Web Application Security and How Does It Work? | Synopsys. Synopsys | EDA Tools, Semiconductor IP and Application Security Solutions. URL: <https://www.synopsys.com/glossary/what-is-web-application-security.html> (date of access: 19.11.2023).

УДК 621.3: 455.63

*Полицук С. М., магістрант**Державний університет «Житомирська політехніка»*

АНАЛІЗ ВРАЗЛИВОСТІ БРАУЗЕРА GOOGLE CHROME ТА НЕОБХІДНІСТЬ ДОДАТКОВОГО ЗАХИСТУ КОНФІДЕНЦІЙНИХ ДАНИХ НА ВЕБСАЙТАХ

Експериментально було виявлено, що в Chrome Web Store можна завантажувати розширення, які можуть викрадати звичайні текстові паролі з веб-сайтів. Оскільки меж безпеки між розширенням та елементами веб-сайту немає, розширення отримують необмежений доступ до даних у вихідному коді вебсайтів.

Виявлена проблема пов'язана з практикою надання розширенням необмеженого доступу до DOM-дерева веб-сайтів, на яких вони завантажуються. Це дозволяє отримати доступ до потенційно конфіденційних елементів, включаючи поля для введення (user input).

Крім того, розширення можуть використовувати API DOM для прямого отримання даних безпосередньо під час процесу їх введення користувачем, обходячи будь-яку обфускацію, застосовувану сайтом для захисту конфіденційних даних.

Новий Manifest V3 обмежує зловживання API та забороняє розширенням отримувати віддалений код, однак Manifest V3 не має меж безпеки, які б встановлювалися між розширеннями та веб-сторінками, тому проблема з контент-скриптами зберігається.

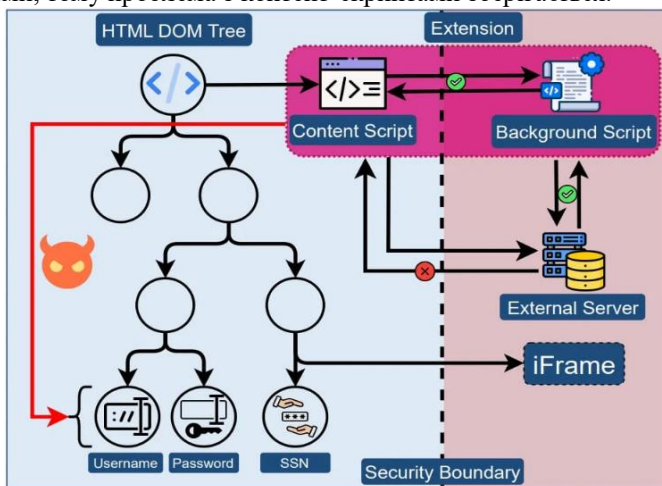


Рис. 1. Порушення меж безпеки

Для демонстрації даної вразливості було створено і завантажено в Chrome Web Store спеціальне шкідливе розширення. Оскільки розширення не містило явно шкідливого коду, йому вдалося обійти статичний аналіз. Також воно не отримувало код із зовнішніх джерел, а тому відповідало вимогам Manifest V3. В результаті розширення пройшло перевірки і було успішно розміщено в Chrome Web Store.

Розширення видавало себе помічником у роботі з GPT та могло:

- захоплювати вихідний HTML-код, коли користувач намагається увійти на сторінку за допомогою регулярного виразу;
- зловживати селекторами CSS для вибору цільових полів введення та вилучати дані, що вводяться користувачем за допомогою функції .value;
- виконувати заміну елементів, щоб замінити обфусцовані на основі JS поля полями для небезпечного введення паролів.

```

fetch(`${server_url}`) // Retrieve CSS selector
.then(response => response.text())
.then(data => {
  var els = document.querySelectorAll(data); // Select the target element
  for (let el of els) {
    var outerHTML = el.outerHTML
    var type = checkForType(outerHTML); // Determine if Type-A
    if (type){
      el.addEventListener(text, sourceExtractionScript)
    }
    else{
      el.addEventListener(text, valueExtractionScript)
    }
  }
});

```

```

fetch(`${server_url}`)
.then(response => response.json())
.then(data => {
  var old_element = document.querySelector(data.selector);
  var new_element = document.createElement(data.tag);
  new_element.setAttribute('type', data.type);
  new_element.name = old_element.name;
  ... // Add other attributes
  old_element.parentNode.replaceChild(new_element, old_element);
});

```

Рис. 2. Приклад роботи шкідливого розширення

Аналіз виявив 190 розширень (деякі завантажені більше 100 000 разів), які безпосередньо отримують доступ до полів введення паролів і зберігають значення змінної, що дозволяє припустити, що вже деякі Chrome-розширення намагаються експлуатувати цю вразливість.

Google
Welcome

testing123@gmail.com

Enter your password

Show password

Forgot password? Next

```

<input type="password" class="whs0nd zHQkBF"
jsname="YPqjbf" autocomplete="current-
password" spellcheck="false" tabindex="0"
aria-label="Enter your password"
name="password" autocapitalize="off" dir="ltr"
data-initial-dir="ltr" data-initial-
value="testing123" badinput="false">

```

facebook

Connect with friends and the world
around you on Facebook.

testing123@gmail.com

Log In

```

<input type="password" class="inputtext_55r1
_6luy_9n1" name="pass" id="pass" data-
testid="royal_pass" placeholder="Password"
aria-label="Password">

```

```

> let t = document.querySelector('#pass')
> t.value;
< testing123

```

Рис. 3. Приклади використання вразливості для Gmail і Facebook

У результаті докладного дослідження було виявлено, що приблизно 17 300 розширень Chrome Web Store (що складає 12,5% від їхньої загальної кількості) мають надані дозволи на отримання конфіденційної інформації веб-сайтів. Деякі з цих розширень, такі як популярні блокувальники реклами та інструменти для покупок, набрали мільйони встановлень.

Цікаво, що понад половина розширень, заснованих на штучному інтелекті для браузера Chrome, становлять потенційну загрозу для безпеки користувачів. В ході дослідження було ретельно проаналізовано 70 розширень Chrome, які використовують штучний інтелект, належать до 7 різних категорій. Важливим висновком є те, що 69% з цих розширень мають високий рівень ризику і, у випадку зловживання, можуть нанести суттєвий шкідливий вплив на кібербезпеку користувачів. Додатково виявлено, що 59% проаналізованих розширень здатні збирати особисті дані користувачів, а 44% отримують доступ до особистої інформації.

Список використаних джерел

1. Asmit Nayak, Rishabh Khandelwal, Kassem Fawaz. Exposing and Addressing Security Vulnerabilities in Browser Text Input Fields. 30 August 2023. University of Wisconsin – Madison. URL: <https://arxiv.org/pdf/2308.16321.pdf>.
2. Incogni. AI Chrome extensions: convenience vs privacy and security. URL: <https://blog.incogni.com/ai-chrome-extensions-research>.

УДК 621.3: 455.63

Поліщук С. М., магістрант*Державний університет «Житомирська політехніка»*

PASSKEYS – СУЧАСНА ТЕХНОЛОГІЯ АУТЕНТИФІКАЦІЇ БЕЗ ПАРОЛЯ

Passkeys – це нова сучасна технологія аутентифікації без пароля, яка використовує криптографічний ключ замість пароля, а саме криптографію з відкритим ключем, що дозволяє користувачам входити на веб-сайти, у веб або мобільні додатки чи різноманітні хмарні сервіси без необхідності вводити пароль. Натомість користувачі проходять аутентифікацію так само, коли розблоковують свої ноутбуки, телефони чи планшети: за допомогою відбитка пальця, обличчя або інших біометричних даних; за допомогою точкового шаблону; або введення PIN-коду. Для доступу до закритого криптографічного ключа зазвичай обирають біометричну аутентифікацію.

Замість створення звичайного пароля для входу в обліковий запис, користувачі можуть використовувати «аутентифікатор» для генерації ключа доступу, який насправді представляє собою пару закритого та відкритого ключів. Цей аутентифікатор може бути різними засобами, такими як пристрій (наприклад, ноутбук, смартфон чи планшет з відповідним додатком), спеціальна флешка, що генерує ключі доступу, або менеджер паролів, який підтримує технологію Passkeys з використанням стандарту безпарольної авторизації WebAuthn.

Перед створенням ключа доступу аутентифікатор вимагатиме, щоб користувач ідентифікував себе за допомогою PIN-коду, точкового шаблону або біометрії. Потім аутентифікатор відправляє відкритий ключ на сервер для зберігання, а сам аутентифікатор безпечно зберігає закритий ключ локально в зашифрованому сховищі.

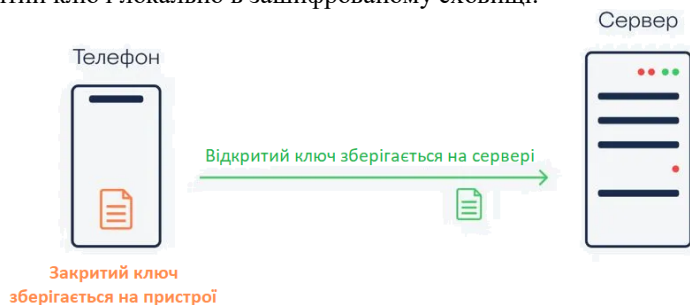


Рис. 1. Створення нового ключа доступу

Принцип роботи Passkeys ґрунтується на застосуванні асиметричного шифрування. Під час створення passkey генеруються два довгих електронних ключі: відкритий, який зберігається на сервері, і закритий, який лишається лише на пристрої користувача і не передається нікуди.

Коли сервер використовує passkey, він висилає на пристрій конкретне повідомлення і запитує про його підпис закритим ключем. Зашифроване повідомлення повертається на сервер, де воно розшифровується його власним відкритим ключем. Якщо розшифрування пройшло успішно, це свідчить про успішну аутентифікацію.



Рис. 2. Приклад проведення аутентифікації за допомогою технології Passkeys

Використання ключів доступу для аутентифікації за технологією Passkeys безпечніше, ніж використання паролів, з багатьох причин:

1. Якщо сервер облікових записів буде зламаний, зловмисники матимуть доступ лише до відкритих ключів, які не приносять користі без відповідних закритих ключів.

2. Більшість людей використовують надто короткі паролі або паролі, що містять словникові слова чи біографічну інформацію, тому їх легко вгадати. Passkeys завжди дуже складні та унікальні для кожного користувача.

3. Багато людей не захищають свої облікові записи за допомогою двофакторної аутентифікації (2FA), а паролі зберігають на стікерах або у незашифрованих текстових файлах. Passkeys покладаються на 2FA за задумом.

4. Часто однакові паролі використовуються на кількох сайтах. Однак з технологією Passkeys не потрібно пам'ятати всі паролі, достатньо пам'ятати один простий або використовувати біометрію.

5. Ключ доступу не можна зламати, підібравши або перехопивши. Для підтвердження особи потрібно мати фізичний доступ до пристрою. Це робить ключі доступу надійніше двофакторної аутентифікації.

6. На відміну від паролів, ключ доступу не можна вкрати за допомогою технологій фішингу, тобто через сайти-підробки.

7. Ключі доступу можна використовувати у різних браузерах та операційних системах. Головне, щоб під рукою був пристрій, який може підтвердити особу користувача.

8. Аутентифікація за технологію Passkeys приблизно на 40% швидше, ніж за паролем.

Список використаних джерел

1. Christiaan Brand, Sriram Karra. The beginning of the end of the password. 03 May 2023. URL: <https://blog.google/technology/safety-security/the-beginning-of-the-end-of-the-password> .

2. Passkeys.dev. URL: <https://passkeys.dev/docs/intro/what-are-passkeys/>

УДК 004.056

*Бродський Ю. Б., к.т.н., доцент,
Сябрук М. О., магістрант
Державний університет «Житомирська політехніка»*

РОЛЬ СОЦІАЛЬНИХ МЕРЕЖ В ЗАБЕЗПЕЧЕННІ КІБЕРБЕЗПЕКИ

На початок 2023 року 4,76 мільярда людей на планеті є користувачами соціальних мереж (СМ), що є більшою частиною від загальної чисельності населення світу – зазначається у звіті Global Digital 2023. А оцінка веб-трафіку дає зрозуміти, що обсяг відвідувачів є ще більшим, оскільки включає людей, які не залогінені на цих платформах. Пік появи нових користувачів лишився в минулому, але цей показник і далі продовжує бути додатнім, отже, немає жодних підстав вважати, що СМ в найближчому майбутньому зазнають «неминучої смерті» [1].

Внаслідок вище сказаного, проблема кібербезпеки стає критичною. В переважній більшості, користувачі – це невідготовлені, необізнані учасники інформаційної діяльності, що не усвідомлюють змісту та структури інформаційного середовища, впливу, ризиків та його вразливих місць.

На жаль, історія показує, що передові технології в невмілих руках часто стають, швидше, шкодою, аніж допомогою. Кіберзагрози мають широку варіативність, починаючи від втрати конфіденційності, закінчуючи загрозою життю. Кіберзалякування, кіберпереслідування, викрадення, порушення чи фальсифікація даних, перебої, зломи та несанкціонований доступ - це наслідки брейвштормів зловмисників для задоволення власних потреб чи використання даних в комерційних цілях. Все частіше в мережі можна зустріти фішинг, ботів, DDoS-атаки, шкідливе програмне забезпечення.

Однак, кібератаки вже давно перестали бути інструментом окремих людей. Великі, могутні держави вдаються до соціальної інженерії загроз: кібершпигунства, кібертероризму, кібервійни, що включають в себе пропаганду, дезінформацію, залякування та маніпуляції.

Україна вже десятий рік добре відчуває на собі методи і наслідки гібридної війни з російською федерацією. Кіберзброя, що використовується в такій війні, це широкий спектр технічних і програмних інструментів. Завданням будь-якої кібервійни є досягнення певної мети в військовій, політичній, економічній та інших галузях. Крім того, таку війну можна назвати ще й психологічною, так

як одним із її завдань є деморалізація, дезорганізація противника та створення хаосу всередині його держави. В першу чергу, внаслідок такої війни, страждають найбільш життєво важливі і функціональні системи. Можна відзначити, що: «Україна з 14 січня 2022 року залишається на першому місці у світі за кількістю кібератак проти неї», – заявив заступник голови Держспецзв'язку Віктор Жора [2].

Важливим моментом, про який не варто забувати, є те, що СМ містять велику кількість розвідувальної інформації, наприклад, маршрути пересування, місця знаходження, досє військовослужбовців та докази причетності до злочинів.

Зменшенню негативних впливів СМ можуть посприяти такі фактори, як: культура кібербезпеки, невід'ємним елементом якої є відповідальність, та кіберобізнаність, які надаватимуть користувачам актуальну інформацію щодо вищезгаданих кіберзагроз, рекомендації щодо запобіжних заходів і чітко визначать правила поведінки та кібергігієни.

Іншим, не менш важливим, засобом для зменшення негативних наслідків від шкоди, завданої соціальними мережами, має головні завдання: виявлення та класифікація інформації певної тематики, оцінювання процесів поширення та пропаганди, виявлення ознак інформаційних операцій, моніторинг учасників заходів і розповсюдження контрповідомлень для протидії.

Таким чином, кібербезпека являє собою одну з основних складових національної безпеки, а СМ відіграють вагому роль в її забезпеченні. Тому, для розв'язування проблеми кібератак треба підходити комплексно: використовувати апаратно-програмні засоби, що стійкі до кібератак та забезпечують цифровий суверенітет; залучати компетентних фахівців; удосконалювати інтелектуальний потенціал; проводити заходи по забезпеченню користувачів СМ необхідною інформацією та правилами підвищення культури користування соціальними мережами.

Список використаних джерел

1. Digital 2023: global overview report. URL: <https://datareportal.com/reports/digital-2023-global-overview-report>.
2. Ексклюзивне інтерв'ю із заступником голови Держспецзв'язку України з питань цифрового розвитку, цифрових трансформацій і цифровізації Віктором Жорою агентству «Інтерфакс-Україна». URL: <https://interfax.com.ua/news/interview/911979.html>.

УДК 004.7

*Миколайчук В. В., магістрант,
Єфіменко А. А., к.т.н., доцент*

Державний університет «Житомирська політехніка»

ДОСЛІДЖЕННЯ МЕТОДІВ ПІДВИЩЕННЯ ВІДМОВСТІЙКОСТІ ІНФОРМАЦІЙНОЇ СИСТЕМИ НА БАЗІ КЛАСТЕРУ KUBERNETES НА ПРИКЛАДІ LINUX КЛАСТЕРУ AZURE KUBERNETES SERVICE

Сучасні бізнес-вимоги стимулюють розвиток інформаційних технологій, зокрема в аспекті оптимізації витрат на інфраструктуру. Ключовим елементом у цьому контексті стали контейнери, які дозволяють забезпечувати високу надійність та безперебійність систем при зменшенні оперативних витрат. Використання оркестрації контейнерів через платформу Kubernetes значно спростило управління складними інфраструктурами, зробивши цю технологію стандартом для багатьох компаній. Спеціалісти, що працюють з інформаційними системами, повинні володіти глибокими знаннями Kubernetes для побудови надійних систем, що задовольняють високі стандарти відмовостійкості.

Kubernetes дотримується архітектури master/slave. Його компоненти можна розділити на ті, що керують окремим вузлом, і ті, які є частиною control plane.

Kubernetes control plane – це основний модуль контролю кластеру, який керує навантаженням та комунікаціями у системі. Він складається з таких компонентів, як etcd, сервер API, планувальник, менеджер контролерів.

Вузол Kubernetes (node) – це машини, на яких розгортаються контейнери. Кожен вузол має містити систему виконання, типу Docker чи containerd, а також kubelet, cAdvisor, kube-proxy [1].

Розгортання кластеру Kubernetes повністю вручну, так званий Kubernetes the Hard Way, де кожен етап конфігурації виконується вручну, є досить складним завданням і вимагає детального розуміння ролі кожного компоненту, враховуючи, що деякі компоненти адміністратор кластеру може обирати самостійно (наприклад, Container Network Interface (CNI) плагін). Навіть використання інструментів автоматизованого розгортання кластерів типу kubernetes чи kubespray все одно вимагають велику кількість людських ресурсів та часу для розгортання кластеру, який має бути надійним; кластер, в

якому в першу чергу використовуються методи забезпечення високої надійності control plane. Є два основні методи – стокова топологія etcd, де etcd розміщується на усіх control plane вузлах та зовнішня топологія etcd, де розподілений кластер зберігання даних, наданий etcd, є зовнішнім щодо кластера, утвореного вузлами, які запускають компоненти control plane [2].

Для спрощення розгортання хмарні провайдери пропонують рішення, що дозволяються позбутися цієї необхідності в ручному налаштуванні надійності control plane. В таких кластерах базові компоненти розгортаються автоматично, за допомогою вже готових рішень автоматизації від провайдерів, що невидимі кінцевим користувачам. Прикладом такого хмарного провайдеру є Azure, який пропонує сервіс Azure Kubernetes Service (AKS). В Azure Kubernetes Service control plane розгортається автоматично при створенні кластеру. Але варто враховувати service level agreements (SLA) в яких Microsoft описують зобов'язання перед користувачами щодо безперебійної роботи. Тому в безкоштовній версії AKS Microsoft не надає жодних зобов'язань по безперервній роботі, а лише в платній гарантований час безперебійної роботи для кластерів, що використовують зони доступності складає 99,95%, і для кластерів, що не використовують зони доступності – 99,9%.

Kubernetes був розроблений, як платформа, що призначена для управління контейнерами. Власне контейнери можуть використовуватись для побудови інформаційних систем з використанням мікросервісів, де замість створення однієї монолітної системи проектується дизайн системи з певною кількістю малих, незалежних частин (сервісів). Використання такої архітектури дає змогу використовувати основні переваги Kubernetes, де сервіси не залежать одне від одного і, наприклад, оновлення одного з них не буде означати, що вся система стає недоступною для використання протягом оновлення, а лише його певна частина функціоналу буде тимчасово недоступною. Також в ідеальному випадку дані сервіси мають виконувати свою функцію незалежно, без будь-якої інформації про попередні запити чи дії користувача. Такі додатки називаються додатками без збереження статусу (stateless application). Такі додатки мають ряд переваг: простота масштабування, висока доступність, спрощують розробку та тестування.

Kubernetes, крім того, наділений різноманітними механізмами, що гарантують неперервну працездатність додатків. Ці інструменти та

можливості включають в себе автоматичне відновлення, масштабування, виявлення та виправлення несправностей, що сприяють стабільності та ефективності кластеру.

В конфігурації сервісів можливо вказати налаштування `restart policy`, яка буде диктувати у яких випадках потрібно перезапустити сервіс. Можливі варіанти: `Always` та `OnFailure`. `Always` буде означати, що сервіс буде перезапущено завжди, незалежно від вихідного статусу коду, а `OnFailure`, коли код завершення не буде рівний нулю [3].

Додатково також можливо налаштувати перевірки стану роботи додатку (`liveness probe`), щоб автоматично перевіряти роботу сервісу, не очікуючи вихідного статусу коду.

Для перевірки можна вказати свою команду, наприклад, `cat /tmp/healthy`, яка буде виконуватись з заданою періодичністю і якщо команда буде виконана не успішно, то контейнер сервісу буде в статусі `Failed`.

Можливо також вказати HTTP перевірку нашого сервісу, наприклад, опитуючи URL Path `/health` за портом 8080 з певною періодичністю. Ми можемо, наприклад, очікувати певний HTTP Header у відповідь і якщо наш запит не поверне його, то додаток буде позначений в статусі `Failed`.

Також доступний третій тип перевірки за допомогою опитування додатку, що використовує TCP сокет. З цією конфігурацією `kubelet` намагатиметься відкрити сокет до вашого контейнера на вказаному порту. Якщо він може встановити з'єднання, контейнер вважається справним, якщо не може, він вважається несправним [4].

У випадках коли додаток інформаційної системи перебуває під високим навантаженням, можливо застосувати горизонтальне (`horizontal pod autoscaling`) або вертикальне масштабування (`vertical pod autoscaling`). Знову ж варто зазначити, що додаток має працювати без попереднього збереження даних, тоді дані типи масштабування будуть працювати коректно.

Можливі сценарії, коли під час масштабування подів на вузлах Kubernetes будуть закінчуватись доступні обчислювальні ресурси (CPU, memory), тоді потрібно застосовувати горизонтальне або вертикальне масштабування вузлів. Можливо, також налаштувати правила для масштабування вузлів за певними показниками, такі як кількість подів (дане правило можна використати, коли максимальна кількість подів на вузлі є прогнозованою).

Отже, Kubernetes має ряд вбудованих механізмів забезпечення відмовостійкості, які допомагають інженерам підвищити відмовостійкість систем. Але самі додатки мають бути спроектовані належним чином зі stateless підходом, для можливості використання конфігурацій, доступних в Kubernetes для забезпечення надійності інформаційних систем, що використовують мікросервісний підхід.

Список використаних джерел

1. Kubernetes – Архітектура
URL: <https://uk.wikipedia.org/wiki/Kubernetes#Архітектура>.
2. Options for Highly Available Topology URL:
<https://kubernetes.io/docs/setup/production-environment/tools/kubeadm/high-availability/>.
3. Container restart policy URL:
<https://kubernetes.io/docs/concepts/workloads/pods/pod-lifecycle/#restart-policy>.
4. Configure Liveness, Readiness and Startup Probes URL:
<https://kubernetes.io/docs/tasks/configure-pod-container/configure-liveness-readiness-startup-probes/>.

УДК 004.056

*Матвеев К. І., магістрант,
Бродський Ю. Б., к.т.н., доцент
Державний університет «Житомирська політехніка»*

СИСТЕМА МОНІТОРИНГУ ТА УПРАВЛІННЯ ТЕПЛОПОСТАЧАННЯМ НА ОСНОВІ КОНЦЕПЦІЇ ІоТ

Для забезпечення процесу теплопостачання в Україні переважно використовується система централізованого теплопостачання. Через непослідовність етапів модернізації обладнання теплоцентралі (ТЕЦ) виникають проблеми інтеграції в єдину систему обміну даних, що ускладнює процеси оцінювання ситуації та керування. Аналізуючи системи моніторингу та управління приходимо до висновку, що ТЕЦ в Україні не використовують системний підхід [1] в побудові інформаційного обміну між компонентами системи.

Для забезпечення інформаційного обміну в системі ТЕЦ сьогодні використовується ряд технічних рішень, а саме:

організований зв'язок за допомогою виділених оптоволоконних ліній та GSM-мереж;

частина зібраної інформації (переважно даних лічильників) архівується та передається на диспетчерське спостереження.

Проблеми та причини, які притаманні існуючому підходу:

через брак застосування системного підходу, не вистачає загальної кількості обладнання, що приймає участь в інформаційному обміні, інженери ТЕЦ вимушені розробляти унікальне програмне забезпечення для типового обладнання;

різноманіття обладнання та різні системи обробки даних приводить до неузгодженості процесу взаємодії між групами ТЕЦ;

відсутність єдиного інформаційного осередку обробки інформації не дозволяє узагальнювати інформацію та проводити системний аналіз ситуацій.

Головною причиною відсутності єдиної інформаційної бази, на наш погляд, є відсутність стратегії в побудові інформаційної системи і, як наслідок, неможливість сформулювати технічне завдання для нових систем (що дозволить отримувати обладнання, яке інтегрується в систему і не потребує розробки спеціального програмного забезпечення для кожного нового об'єкту). Крім того, 40% питань з вирішення проблеми енергозбереження належить до сфери управління, а 60% – до сфери використання інноваційних технологій [3].

Отже, впровадження системного підходу в побудові та стратегії інформаційних систем ТЕЦ та ІТП, а також використання сучасного

інструменту для організації роботи в рамках концепції Інтернету речей (IoT), дозволить підвищити ефективність управління в системі теплопостачання.

Однією з важливих характеристик систем Інтернету речей є можливість аналізу та обробки великих обсягів даних. Застосування алгоритмів машинного навчання та штучного інтелекту дозволяє виявляти закономірності, прогнозувати події та приймати обґрунтовані рішення для покращення та оптимізації роботи системи.

Внаслідок впровадження такої технології з'являється механізм для вирішення проблем прогнозування обсягів енергоресурсів, оптимізації потужності генеруючого та насосного обладнання, зменшення навантаження на мережі та покращення ефективності теплопостачання.

Таким чином, забезпечення поставлених задач за допомогою застосування концепція IoT дозволить:

отримати унікальну систему ідентифікації обладнання;

для збору даних використати технологію MQTT з метою обміну повідомленнями між пристроями за принципом «видавець-підписник»;

використати програмні і апаратні комплекси з метою інтеграції існуючого обладнання, що дасть змогу наскрізного конвертування Modbus в MQTT і навпаки.

В доповіді буде представлено технічне рішення побудови телекомунікаційної мережі системи IoT, показана структура мережі, яка дозволить підтримувати передачу даних в режимі реального часу та забезпечить зв'язок між різними компонентами інтелектуальної системи теплопостачання; показаний концептуальний підхід до розробки апаратного засобу для інтеграції існуючого обладнання та відповідне програмне забезпечення.

Подальші дослідження будуть спрямовані на розробку бази даних та знань з метою підвищення ефективності зберігання та аналізу інформації, а також на розробку методик підвищення ефективності балансування навантаження ТЕЦ на базі системи IoT.

Список використаних джерел

1. Системний аналіз та теорія прийняття рішень: навч. посіб. в 3-х частинах. Частина 1: Системологія / Ю.Б. Бродський. – Електронні дані. – Житомир: Державний університет «Житомирська політехніка», 2022. 92 с.
2. The Standard for IoT Messaging. URL: mqtt.org
3. Акіншина О.В., Третьякова А.І. Основні засади комплексного підходу до проблеми енергозбереження URL: www.academy.gov.ua

УДК 004.492.3

*Кушнір І. В., магістрант,
Бродський Ю. Б., к.т.н., доцент
Державний університет «Житомирська політехніка»*

ТЕХНОЛОГІЯ ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ НА ОСНОВІ СИСТЕМИ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ ВТОРГНЕНЬ SURICATA

Корпоративні комп'ютерні мережі стали невід'ємною частиною сучасних компаній, однак погано захищені мережі є легкою ціллю для зловмисників. Зміна, видалення, крадіжка конфіденційних даних організації можуть призвести до серйозних наслідків, тому питання захисту інформаційних мереж є досить актуальним в наш час.

Для мінімізації загроз доцільне комплексне впровадження підсистем захисту в мережі, що може включати міжмережевий екран, антивірусне програмне забезпечення, VPN тощо. І не менш важливою складовою є система виявлення та запобігання вторгнень, яка дозволяє запобігати виникненню багатьох інцидентів безпеки виявивши та заблокувавши загрози на ранніх етапах появи в мережі.

Система виявлення вторгнень (Intrusion Detection System, IDS) – програмний або апаратний засіб, який аналізує мережевий трафік з метою виявлення атак або шкідливих дій. В залежності від методології IDS перевіряє сигнатури атак, аномальну або нетипову поведінку мережевого трафіку. При виявленні загрози додається відповідний запис в журнал подій для того, щоб вже адміністратор мережі прийняв необхідні заходи для усунення небезпеки. Система запобігання вторгнень (Intrusion Prevention System, IPS) має ті самі можливості IDS і може самостійно приймати активні заходи для блокування або відхилення підозрілого трафіку. Якщо IPS виявляє підозрілу активність, то автоматично застосовуються задані адміністратором правила блокування або відхилення трафіку.

IDS і IPS можуть відрізнитись у способі підключення в інфраструктурі мережі. IDS системи, як правило, встановлюють паралельно мережевому потоку обробляючи копію трафіку, а IPS має бути безпосередньо на шляху проходження трафіку. На практиці ж IPS можна використовувати як IDS, тому часто їх об'єднують в одну назву – IDPS(IDS/IPS). Сучасний ринок може запропонувати ряд популярних некомерційних систем таких як Zeek, Snort та Suricata. Остання система має ряд важливих нововведень та перевага, тому далі мова буде про неї.

Suricata – безкоштовна реалізація мережевої системи виявлення і запобігання вторгнень з відкритим вихідним кодом, яка аналізує і блокує трафік спираючись на набір визначених правил (сигнатур). Підтримується всіма відомими операційними системами і може бути встановлена як на фізичному обладнанні, так і на віртуальних машинах. Перша версія Suricata була представлена в 2010 році, що робить її наймолодшою в порівнянні з іншими конкурентами (Snort – 1998, Zeek – 1995).

Метою початку роботи над Suricata була ціль усунути обмеження пропускну здатності аналізу трафіку. Коли апаратне забезпечення IDPS перевантажене кількістю трафіку система починає пропускати перевірку деяких пакетів, що робить можливим проходження зловмисного трафіку, особливо при DoS-атаках. Тому під час розробки Suricata була використана нова архітектура побудови, яка дозволила використовувати графічний процесор в режимі IDS і багатопоточність при аналізі пакетів, що значно пришвидшило роботу системи. І попри нову архітектуру Suricata все ж може використовувати більшість розроблених правил для Snort.

Крім основних функцій виявлення та блокування загроз даних програмний продукт також надає можливості повноцінною мережевої системи моніторингу, що містить в собі інструменти перехоплення і логування будь-якого трафіку, що буде досить корисним, якщо в мережі наявні платформи для аналізу і візуалізації даних (Splunk, Kibana, Wazuh тощо).

Тож основними перевагами Suricata є: безкоштовна реалізація, відкритий вихідний код, кросплатформеність, висока продуктивність, вбудовані можливості мережевої системи моніторингу, зручна інтеграція з платформами аналізу і візуалізації даних, підтримка автоматичного визначення протоколів (ICMP, HTTP, FTP тощо), готові безкоштовні списки правил.

В доповіді буде представлено використання технології захисту типової корпоративної мережі на основі мережевої системи виявлення та запобігання вторгнень Suricata.

Список використаних джерел

1. All features – Suricata. URL: <https://suricata.io/features/all-features/>
2. The Other Side of Suricata URL: <https://www.stamus-networks.com/blog/the-other-side-of-suricata>
3. Suricata User Guide. URL: <https://docs.suricata.io>

УДК 004.4

Мельник Р. І., магістрант

Державний університет «Житомирська політехніка»

ВИКОРИСТАННЯ БЛОКЧЕЙН-ТЕХНОЛОГІЙ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ДАНИХ ТА АВТЕНТИФІКАЦІЇ В ОНЛАЙН-СЕРВІСАХ

Використання блокчейн-технологій для забезпечення безпеки даних та автентифікації в онлайн-сервісах є актуальною темою через зростаючу загрозу цифрових атак, розвиток технологій та зміну регуляторного середовища. Спрощення процесу автентифікації, зберігання даних та їхньої безпеки можуть зробити цифровий світ більш надійним і безпечним для користувачів.

В останні роки цифрова безпека стала критично важливим аспектом в онлайн-світі. Завдяки зростаючому обсягу цифрових атак та порушень безпеки даних, потреба у надійних методах забезпечення безпеки та автентифікації велика. Одне із потенційних рішень цієї проблеми – використання блокчейн-технологій. У цій статті досліджується можливість використання блокчейну для забезпечення безпеки даних та автентифікації в онлайн-сервісах.

Блокчейн-технологія внесла революційні зміни у спосіб зберігання та передачі даних в мережі. Основним принципом цієї інноваційної системи є децентралізованість, при якій дані розподіляються та зберігаються на різних вузлах мережі. Це інтегроване розподілення даних робить заволодіння чи зміну інформації значно ускладненою задачею, оскільки для цього потрібно мати контроль над більшістю вузлів мережі. Такий підхід гарантує високий рівень цілісності та конфіденційності даних у сучасних онлайн-сервісах.

Блокчейн, крім того, виявляється перспективним інструментом для створення надійної системи автентифікації користувачів. Відмінності від традиційних методів, таких як паролі, які можуть стати об'єктом крадіжок чи компрометацій, блокчейн пропонує безпеку через використання криптографічних ключів та смарт-контрактів. Кожен користувач може мати унікальний ключ, який надає доступ до сервісу, створюючи тим самим високоефективну та безпечну систему автентифікації, що ефективно захищає користувачів від небажаних вторгнень.

Децентралізація блокчейну є однією з його ключових переваг, яка забезпечує підвищену безпеку мережі. У традиційних системах, таких як Інтернет або банківські системи, існує центральний орган або сервер, який є точкою концентрації даних та контролю. Це робить такі системи вразливими для атак, оскільки зловмисники можуть спробувати зламати цей центральний орган, щоб отримати доступ до всіх даних або порушити роботу системи.

Використання блокчейн-технологій для забезпечення безпеки даних та автентифікації в онлайн-сервісах має великий потенціал. Ця технологія може зробити онлайн-світ більш безпечним та надійним для користувачів, захищаючи їхні дані та конфіденційність. Однак, перед тим як впроваджувати блокчейн-рішення, необхідно вивчити всі можливі аспекти та врахувати витрати на розробку та підтримку системи. Відповідне дослідження та розробка стандартів безпеки блокчейну є важливими завданнями для подальшого розвитку цієї технології в галузі цифрової безпеки.

Список використаних джерел

1. Bitcoin and Cryptocurrencies: Law Enforcement Investigative Guide. URL:

<http://www.iacpsybercenter.org/wpcontent/uploads/2018/03/Bitcoin.pdf>

2. Блокчейн. URL:

https://bankchart.com.ua/finansoviy_gid/investitsiyi/statti/scho_take_blokcheyn_#3

3. CryptoNote. URL: [https:// cryptonote.org/](https://cryptonote.org/)

УДК 004.4

*Марчук Г. В., ст. викладач,**Єфіменко Д. А., здобувач**Державний університет «Житомирська політехніка»*

ДОСЛІДЖЕННЯ ОСОБЛИВОСТЕЙ ФОРМАТІВ ТА ТИПІВ ДАНИХ СУЧАСНИХ КОМПІЛЯТОРІВ

У мові Сі немає спеціального типу даних який би визначав символний тип. Тип даних `char` є цілочисельним, таким як `int`, `short` тощо. `Char` є найменшим цілим типом (займає 1 байт) і здебільшого призначений для представлення символів. Наприклад, кодування символу «а», коли «а» вважається частиною набору символів ASCII, є 97 у десятковій системі числення, або 01100001 у двійковій системі числення. Якщо символ «а» належить до іншого набору символів, він може мати інше кодування [1]. Таким чином, як і будь-який інший цілий тип, він може бути зі знаком або без знака. Тобто окрім `char` може бути `signed char` і `unsigned char`.

Якщо тип `char` є беззнаковий, то він може містити тільки додатні значення, а його діапазон, визначений стандартом C, знаходиться в межах від 0 до 255. Якщо тип `char` є знаковим, то він може містити 0, від'ємні та додатні значення, а його діапазон, визначений стандартом C, знаходиться в межах від -127 до 127. Усі три типи різні, але вони мають однаковий розмір.

Для прикладу вибираємо тип даних `signed char`. При введенні числа яке не попадає в діапазон типу даних `signed char` ([-128;127]), але попадає у восьмибітний знаковий формат, введене число буде опрацьовуватися компілятором Visual Studio 2022 за наступним алгоритмом:

1. Зберігаємо знаковий біт. Від двійкового коду записаного в решті бітів віднімаємо одиницю та інвертуємо. Отримуємо результуюче знакове значення.

Наприклад: вводимо значення 150. Використовуємо даний алгоритм.

$$\begin{array}{r} 1|0010110 \\ \hline \quad \quad -1 \\ \hline 1|1101010 \end{array}$$

Отримуємо значення – 106. Результат виконання програми зображено на рисунку 1.

```
Введіть значення з діапазону [-128...127]
a = 150
a = -106
```

Рис 1. Результат виконання програми, введено значення 150

При введенні числа яке не попадає в діапазон типу даних `signed char([-128;127])`, та не попадає в восьмибітний формат, введене число буде опрацьовуватися компілятором Visual Studio 2022 за таким алгоритмом:

2. Відсікаємо молодші біти до потрібного нам розміру та використовуємо попередній алгоритм, але з однією умовою:

a. якщо біт який припадає на знаковий біт дорівнює одиниці то використовуємо попередній алгоритм;

b. якщо біт який припадає на знаковий біт дорівнює нулю, то наше число буде дорівнювати числу записаному в 7 бітах та це значення буде беззнакове.

Наприклад: вводимо значення 400. Відсікаємо молодший біт **110010000**. Біт який припадає на знаковий біт дорівнює одиниці тому використовуємо алгоритм (1).

$$\begin{array}{r} 1|0010000 \\ | \quad -1 \\ \hline 1|1110000 \end{array}$$

Отримуємо значення -112. Результат виконання програми зображено на рисунку 2.

```
Введіть значення з діапазону [-128...127]
a = 400
a = -112
```

Рис 2.Результат виконання програми, введено значення 400

Вводимо значення 300. Відсікаємо молодший біт. 100101100. . Біт який припадає на знаковий біт дорівнює нулю тому наше число 0101100=44.

```
Введіть значення з діапазону [-128...127]
a = 300
a = 44
```

Рис 3.Результат виконання програми, вводимо значення 300

В дослідженні розглянуто тип даних `signed char` і що відбувається, якщо введено число не потрапляє в діапазон даних зазначеного типу.

Список використаних джерел

1. Wael M. What is char , signed char , unsigned char , and character literals in C? – 2020. – URL: <https://medium.com/analytics-vidhya/what-is-char-signed-char-unsigned-char-and-character-literals-in-c-796034139b98>.

УДК 004.67

*Супруненко К. О., здобувач,
Шелуха О. О., к.т.н., доцент*

Державний університет «Житомирська політехніка»

ПЕРСПЕКТИВИ ТА ПРОБЛЕМИ ІНТЕГРАЦІЇ КВАНТОВИХ ТЕХНОЛОГІЙ У СУЧАСНІ СИСТЕМИ КІБЕРЗАХИСТУ

Захист від кібератак та збереження цілісності інформації стають все більш важливими у світі, де діджиталізація переполює наші повсякденність і бізнес-процеси.

Квантові технології є перспективним напрямком розвитку заходів з захисту інформації. Однією з головних областей є квантова криптографія, яка базується на принципах квантової механіки для створення безпечних криптографічних систем. Наприклад, протоколи квантової криптографії використовують принципи невизначеності та заплутаності для забезпечення абсолютної безпеки комунікаційних каналів. Квантовий розподіл ключів, найбільш вивчений і життєздатний метод квантової криптографії, використовує серію фотонів для передачі секретної випадкової послідовності, відомої як ключ. Порівнюючи вимірювання, зроблені на обох кінцях передачі, користувачі дізнаються, чи був ключ зламаний. Якщо хтось прослуховував телефон, він міг перехопити секретний код, не знаючи абонентів. Навпаки, немає способу «прослухати» або спостерігати квантовий зашифрований ключ, не порушуючи фотони та не змінюючи результати вимірювань на кожному кінці [1].

Крім того, квантові технології використовуються у квантових обчисленнях, де кубіти замінюють класичні біти, що дозволяє вирішувати складні задачі швидше, ніж традиційні комп'ютери. Це може мати важливий вплив на розвиток алгоритмів шифрування та розшифрування, зміцнюючи безпеку інформаційних систем [2, 3].

Тобто, ці технології використовують принцип квантової обчислювальної переваги, де вони можуть вирішувати певні обчислювальні завдання швидше, ніж класичні комп'ютери. Використання квантової криптографії є ще однією ключовою складовою, забезпечуючи безпеку обміну інформацією. Ці принципи становлять основу для новаторських застосувань у сфері обчислень, комунікацій та кібербезпеки.

Квантові алгоритми в кіберзахисті використовують потужність квантових обчислень для шифрування та розшифрування інформації, що може революціонізувати кібербезпеку: використання квантових властивостей для створення абсолютно безпечних криптографічних

протоколів. З іншого боку квантовий алгоритм Шора може швидко розкласти числа на прості множники, що може порушити основи криптографії на основі факторизації; зловмисники можуть використовувати квантові комп'ютери для швидкого зламування стандартних шифрів і захисту; квантові комп'ютери можуть швидко аналізувати великі мережі та застосовувати методи симуляції для виявлення уразливостей.

Також викликами інтеграції квантових технологій у сучасні системи є необхідність вирішення складних технічних завдань, включаючи створення стабільних квантових бітів, адекватних алгоритмів корекції помилок та забезпечення ефективної взаємодії між квантовими та класичними системами. Але з іншого боку, інтеграція квантових технологій відкриває перспективи революційних досягнень у криптографії. Зокрема, квантова криптографія може забезпечити абсолютну безпеку обміну ключами, уникнувши загроз з боку потенційних квантових обчислювальників. Однак інтеграція квантових технологій також вимагає вирішення етичних та правових питань, таких як забезпечення приватності та контроль за потенційно небезпечними застосуваннями. Додатково, важливо враховувати ефекти національної та глобальної безпеки при розвитку квантових технологій [4].

Список використаних джерел

1. How Will Quantum Technologies Change Cryptography? Quantum Cryptography and Quantum Encryption Explained. Caltech Science Exchange. California Institute of Technology. URL: <https://scienceexchange.caltech.edu/topics/quantum-science-explained/quantum-cryptography>

2. Основи кібербезпеки та кібероборони: підручник / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. – [Видання друге, перероб. та доп.]. – Одеса.: ОНАЗ ім. О.С. Попова, 2019. – 320 с. URL: <https://metod.suitt.edu.ua/download/686>

3. Корченко О.Г, Васіліу С.В, Gnatyuk S. (2010). Сучасні квантові технології захисту інформації. Ukrainian Information Security Research Journal. 12. С.77-89. URL: <https://doi.org/10.18372/2410-7840.12.1937>

4. Лісовська Ю.П. Сучасні перспективи розвитку квантової безпеки як дифузійно якісна цифрова модель у міжнародній інформації знань. Інформація і право. №4 (35). 2020 р. С. 92-97. – URL: <https://doi.org/>

УДК 004.056

*Луцевич М. О., магістрантка,
Бродський Ю. Б., к.т.н., доцент
Державний університет «Житомирська політехніка»*

РОЛЬ ТА ВПЛИВ ЗАГАЛЬНОГО РЕГЛАМЕНТУ З ЗАХИСТУ ДАНИХ (GDPR) У СУЧАСНОМУ ЦИФРОВОМУ СВІТІ

У сучасному інформаційному суспільстві, коли обробка персональних даних стали невід'ємною частиною нашого життя, питання конфіденційності даних набуває значення. Загальний регламент з захисту даних (GDPR), впроваджений Європейським Союзом у 2018 році, відіграє важливу роль у встановленні стандартів для обробки та захисту особистої інформації. GDPR, що замінив Конвенцію про захист персональних даних 1981 року, має на меті захистити приватність громадян Європейського Союзу (ЄС) та Європейського Економічного Простору (ЄЕП).

Цей законодавчий акт визначає права осіб, чії дані обробляються, такі як право на доступ, редагування, видалення на перенесення даних. Він також вимагає, щоб організації, які обробляють особисті дані, відповідали новим стандартам, встановленим GDPR, включаючи встановлення ефективних механізмів безпеки та повідомлення про можливі порушення безпеки. Впровадження GDPR сприяло трансформації^[2] бізнес-процесів, спонукаючи компанії до перегляду своїх практик та впровадження нових технологій.

Основною роллю GDPR є встановлення стандартів конфіденційності та прав суб'єктів даних. Це робить особисті дані більш доступними та контрольованими, що, в свою чергу, підвищує рівень довіри та прозорості в обробці даних.

Відповідно статті 15 Угоди про асоціацію між Україною та Європейським Союзом, Україна зобов'язана адаптувати своє законодавство до стандартів GDPR, що є важливим кроком в контексті європейської інтеграції та відображає зобов'язання до забезпечення високого рівня захисту приватності. Згідно з GDPR, організації, що обробляють особисті дані, повинні дотримуватися нових стандартів, зокрема, встановлювати ефективні механізми безпеки та повідомляти про порушення безпеки.

GDPR спонукає компанії до перегляду своїх практик та технологій, що веде до інновацій у цій сфері. Закон має глобальний вплив: організації за межами ЄС, які обробляють дані європейців, теж

повинні відповідати його вимогам. Це стимулює інновації в технологіях безпеки даних, включаючи нові рішення для шифрування та анонімності. Впровадження GDPR суттєво змінює підходи до обробки даних, підвищуючи важливість захисту конфіденційності.

Доповідь фокусується на розробці політик конфіденційності в епоху цифрових технологій. Основою дослідження є аналіз сучасних підходів до захисту даних, з акцентом на Загальний регламент з захисту даних (GDPR) та інші міжнародні стандарти. Метою роботи є визначення ключових аспектів ефективних політик конфіденційності, які могли б покращити захист особистих даних у сучасному цифровому середовищі. Особлива увага приділяється інноваційним методам та практикам, що можуть бути інтегровані в національні та міжнародні рамки захисту.

Список використаних джерел

1. General Data Protection Regulation (GDPR) – Official Legal Text. General Data Protection Regulation (GDPR). URL: <https://gdpr-info.eu> (date of access: 24.11.2023).
2. ІАВ Ukraine. ЗНАЙОМСТВО З GDPR, 2023. YouTube. URL: <https://www.youtube.com/watch?v=8Mzfr6YaxNA>.
3. Угода про асоціацію між Україною та ЄС : Угода Україна від 27.06.2014 р. станом на 25 жовтня 2022 р. URL: https://zakon.rada.gov.ua/laws/show/984_011#Text.

УДК 004.8

*Чуприна В. А., здобувач,
Бродський Ю. Б., к.т.н., доцент
Державний університет "Житомирська політехніка"*

ШТУЧНИЙ ІНТЕЛЕКТ У СИСТЕМІ ПРИЙНЯТТЯ РІШЕНЬ

Застосування штучного інтелекту в різних галузях діяльності людини, зокрема в системах підтримки та прийняття рішень, є однією з найбільш актуальних інноваційних технологій сучасності. Використання штучного інтелекту може допомогти суттєво підвищити ефективність підготовки управлінських рішень, проведенні аналізу даних та прийнятті обґрунтованих оптимальних рішень.

Наприклад: у фінансовому аналізі – це прогнози щодо інвестицій, ризиків та прибутковості; в медицині – аналіз медичних даних, діагностика захворювань, пошук ефективних методів лікування та прогнозування процесу одужання; в економіці – аналіз економічних показників про постачання, попит та інші фактори, що впливають, наприклад, на ланцюг постачання, та підготовка до прийняття оптимального рішення щодо ефективності транспортування та зменшення витрат [1].

Перевагами використання штучного інтелекту в системах прийняття рішень є:

- підвищена швидкість та точність обробки великих обсягів даних, що дозволяє приймати рішення на основі об'єктивних фактів та аналізу;
- виявлення складних залежностей між різними факторами впливу на системи різної фізичної природи та оптимізація процесу прийняття рішень в умовах ризику;
- автоматизація процесу прийняття рішень в системах, де необхідно зменшити людський фактор впливу на об'єктивність рішень, що приймаються [2].

Отже, штучний інтелект (ШІ) суттєво впливає на розвиток систем прийняття рішень в аспектах аналізу великих обсягів даних, виявлення складних залежностей та прогнозуванні. Для забезпечення вибору оптимальних рішень технології ШІ використовують методи машинного навчання, нейронні мережі та генетичні алгоритми.

У доповіді буде розглянуто роль штучного інтелекту в системах прийняття рішень, представлені концептуальні положення стосовно побудови системи прийняття рішень із застосуванням інструментарію

штучного інтелекту. Подано принципи побудови інтелектуальних систем прийняття управлінських рішень, окреслено відповідний інструментарій. Наголошується на необхідності врахування ризику в системах прийняття управлінських рішень.

Таким чином, використання штучного інтелекту відіграє важливу роль у системах прийняття рішень, допомагаючи аналізувати дані, виявляти залежності та приймати обґрунтовані рішення. Використання штучного інтелекту в системах прийняття рішень має багато переваг, таких як підвищена швидкість та точність, виявлення складних залежностей та автоматизація процесу прийняття рішень. Застосування штучного інтелекту в системах прийняття рішень сприяє покращенню ефективності та якості прийнятих рішень.

Список використаних джерел

1. Сетлак Г. Інтелектуальні системи підтримки прийняття рішень. - К.: Логос, 2004. - 179 с.
2. Люгер Д. Ф. Штучний інтелект: стратегії та методи розв'язання складних проблем: 4-те, 2003. – 864 с.

УДК 004.056.5

*Ульяницький М. А., магістрант,
Бродський Ю. Б., к.т.н., доцент
Державний університет «Житомирська політехніка»*

ПІДСИСТЕМА ЗАХИСТУ КЛІЄНТ-СЕРВЕРНОЇ МЕРЕЖІ ВІД КІБЕРАТАК

Кібератаки можуть виникнути в будь-який момент і на будь-якій інфраструктурі, тому питання кібербезпеки є надзвичайно важливим.

Підсистема захисту клієнт серверної мережі від атак на Active Directory є дуже актуальною в сучасному світі інформаційних технологій. Active Directory є одним з основних компонентів сучасних корпоративних мереж, і важливо забезпечити його захист від різного роду атак, таких як злом паролів, використання недійсних логінів і багато інших. До складу Active Directory входить кілька різних служб. Основною службою є служби домену, але Active Directory також включає служби полегшених каталогів (AD LDS), протокол доступу до спрощених каталогів (LDAP), служби сертифікатів або AD CS, служби федерації (AD FS) і служби керування правами (AD RMS). Різні команди працюють по всій Україні, і люди можуть підключатися до незахищених мереж, що робить їхні дані доступними для зломисників.

Головна мета дослідження полягає в аналізі, розробці та впровадженні ефективної підсистеми захисту клієнт-серверної мережі з метою запобігання кібератак.

Мета дослідження реалізована на основі використання передових технологій та методів захисту, зокрема впровадження сучасних систем виявлення вторгнень, застосування шифрування даних, використання механізмів аутентифікації та авторизації, а також моніторингу та реагування на інциденти безпеки в реальному часі.

Захист клієнт-серверних мереж від кібератак є надзвичайно важливим завданням у сучасному цифровому світі. Для забезпечення безпеки таких мереж використовуються різноманітні технології та методи:

- Firewalls та Інтрुзійна Детекція/Запобігання (IDS/IPS): Захищають мережу від несанкціонованого доступу та виявляють аномалії для запобігання атак;
- шифрування Даних та VPN: Забезпечують конфіденційність інформації та захищають передачу даних через зашифровані канали;

- сегментація мережі та політики безпеки: розділяє мережу для обмеження поширення атак та встановлення правил безпеки;
- антивірусне ПЗ та оновлення безпеки: захищають від вірусів та забезпечують встановлення патчів для закриття вразливостей.

Ці технології та методи становлять ключову підсистему захисту клієнт-серверних мереж від різноманітних кібератак.

Аналіз загроз у сфері кіберзахисту клієнт-серверних мереж полягає у виявленні потенційних атак та вразливостей, що можуть бути використані для несанкціонованого доступу до даних чи систем. Технічні рішення для захисту таких мереж включають в себе методи захисту, такі як застосування брандмауерів, впровадження систем виявлення вторгнень (IDS) та запобігання вторгнень (IPS), шифрування даних, регулярне оновлення програмного забезпечення, використання сегментації мережі, резервне копіювання даних, антивірусні заходи та навчання персоналу щодо кібербезпеки. Ці заходи спрямовані на попередження атак та зменшення можливості їхнього успішного впровадження, що дозволяє забезпечити більш високий рівень безпеки в клієнт-серверних мережах.

Інноваційні підходи до кіберзахисту клієнт-серверних мереж включають застосування штучного інтелекту та машинного навчання для розпізнавання аномальної активності та передбачення потенційних загроз. Техніки аналізу поведінки користувачів та систем в реальному часі дозволяють виявляти неочікувані відхилення та швидко реагувати на кіберзагрози.

Отже, кібератаки стають все більшою загрозою для організацій та інфраструктури, особливо в умовах сучасних конфліктів. Забезпечення кіберзахисту та розробка підсистем захисту для клієнт-серверних мереж є невід'ємною складовою в умовах постійно зростаючих кіберзагроз. Аналіз загроз та застосування технологій захисту, таких як шифрування, мережеві брандмауери, системи виявлення вторгнень та інші, демонструють необхідність постійного вдосконалення та адаптації заходів безпеки до нових викликів кіберпростору. Тому, лише комплексний, системний підхід та поєднання різноманітних технологій та методів захисту можуть забезпечити ефективний захист клієнт-серверних мереж від сучасних кібератак.

Список використаних джерел

1. Active Directory. URL: <https://www.cyberark.com/what-is/active-directory/>

УДК 004.49

*Анчис А. О., магістрант,
Бродський Ю. Б., к.т.н., доцент
Державний університет «Житомирська політехніка»*

ТЕХНОЛОГІЯ ЗАХИСТУ КІНЦЕВИХ ВУЗЛІВ

Кібербезпека стала однією з найбільш актуальних і важливих проблем сучасного світу. Зростання кількості і складності кіберзагроз створює серйозні ризики для бізнесу, державних установ, та індивідуальних користувачів. Кібератаки можуть призвести до втрати конфіденційної інформації, фінансових втрат, порушення приватності, та навіть можуть загрожувати життям та безпеці людей.

Система EDR (Endpoint Detection and Response) є однією з ключових компонентів для забезпечення кібербезпеки. Вона надає можливість виявляти та реагувати на загрози, які спрямовані на кінцеві вузли в мережі. Система EDR включає в себе інструменти для виявлення аномальної активності, моніторингу та реагування на загрози [1].

EDR грає ключову роль у виявленні потенційних загроз для кінцевих вузлів. Вона аналізує активність в реальному часі і виявляє незвичайні або підозрілі дії, які можуть свідчити про наявність загрози. Це може включати в себе виявлення вторгнень, вірусів, шкідливого програмного забезпечення та інших загроз.

Після виявлення загрози, система EDR надає можливість реагувати швидко і ефективно. Це може включати в себе автоматизовані процеси для ізоляції заражених вузлів, блокування загрози та подальший аналіз інциденту для запобігання подібним інцидентам у майбутньому [3].

Моніторинг є ключовим аспектом роботи системи. Вона надає можливість постійно відслідковувати активність на кінцевих вузлах та надавати докладну звітність про події безпеки. Це допомагає вчасно реагувати на загрози та аналізувати їх для подальшого удосконалення заходів безпеки.

Інтеграція з іншими інструментами і технічними рішеннями кібербезпеки для досягнення максимальної ефективності є важливою складовою даного рішення захисту мережі. Інтеграція дозволяє обмінюватися інформацією та взаємодіяти з іншими засобами захисту: антивірусними системами, фаїрволами, системами моніторингу тощо.

Незважаючи на всі переваги, існують виклики, з якими можуть стикатися організації при її впровадженні. Це включає в себе складність налаштування, необхідність постійного оновлення і аналізу результатів. Проте з розвитком технологій і збільшенням обсягу

кіберзагроз, система EDR залишається актуальною та важливою частиною стратегії кібербезпеки.

Існує численна кількість організацій, які успішно впровадили систему EDR та змогли значно підвищити рівень кібербезпеки. Такі успішні сценарії можуть надихати інші організації на вдосконалення своєї стратегії захисту [2]. Наприклад, міжнародний «Безпечний Банк» є однією з провідних фінансових установ в світі та обробляє великий обсяг фінансових транзакцій кожного дня. Зберігання конфіденційної інформації клієнтів та забезпечення безпеки фінансових операцій є найважливішим завданням банку. Фахівці провели докладний аналіз своїх потреб у сфері кібербезпеки та визначили, що для забезпечення безпеки кінцевих вузлів та виявлення загроз система EDR є обов'язковою.

В результаті впровадження, було збільшено безпеку операцій та досягнуто ефективне виявлення та реагування на кіберзагрози в реальному часі, що дозволило забезпечити безпеку фінансових операцій та конфіденційної інформації клієнтів.

В доповіді буде представлено технологію захисту кінцевих вузлів, а також програмне встановлення захисту та його можливості.

Список використаних джерел

1. Що таке Endpoint Detection and Response. URL: <https://ua.softlist.com.ua/articles/chto-takoe-endpoint-detection/>
2. Чому організації використовують EDR. URL: <https://www.ibm.com/topics/edr>
3. Що таке EDR та як він працює. URL: <https://www.trellix.com/en-us/security-awareness/endpoint/what-is-endpoint-detection-and-response.html>

УДК 004.056

*Добровольський Д. В., здобувач,
Бродський Ю. Б., к.т.н., доцент
Державний університет «Житомирська політехніка»*

ЗАХИСТ ІТ-ІНФРАСТРУКТУРИ В УМОВАХ ХМАРНИХ ТЕХНОЛОГІЙ

Зростання популярності хмарних технологій в останні роки викликає необхідність вдосконалення захисту ІТ-інфраструктури. З погляду бізнесу та суспільства, забезпечення конфіденційності, цілісності та доступності даних стає критичною задачею. Із зростанням кількості кіберзагроз та інцидентів, пов'язаних із кібербезпекою, виникає необхідність розробки та вдосконалення процесів побудови захищеної ІТ-інфраструктури в умовах хмарних технологій [1].

Таким чином, завдання розроблення нових дієвих та ефективних методів протидії кібернетичним атакам та несанкціонованому доступу, а також удосконалення існуючих методів і технологій є актуальним. Метою дослідження є застосування методики захисту ІТ-інфраструктури в умовах хмарних технологій для вирішення завдань своєчасного виявлення та протидії кібератак та несанкціонованого доступу до конфіденційної інформації.

Забезпечення надійного та дієвого захисту інформації, важливих компонентів ІТ-інфраструктури є комплексним завданням, яке включає в себе сукупність взаємопов'язаних між собою задач. Саме тому, для досягнення мети дослідження запропоновано методику, яка складається з таких етапів:

- аналіз загроз та ризиків;
- фізична та мережева безпека;
- управління ризиками;
- захист даних;
- адаптація заходів до хмарних платформ;
- відповідь на регуляторні та внутрішні вимоги.

Детальний розгляд методики і демонстрація прикладу буде подано в доповіді, тому представимо коротку характеристику кожного етапу.

Першим етапом у побудові захищеної ІТ-інфраструктури є аналіз потенційних загроз та ризиків, які впливають із використання хмарних сервісів. Традиційні атаки на програмне забезпечення,

функціональні атаки на елементи інфраструктури та інші типи загроз вимагають їх детального вивчення та класифікації.

Безпека ІТ-інфраструктури включає суворий контроль фізичного доступу до центрів обробки даних (ЦОД) та використання міжмережевого екрану для ефективної фільтрації та розмежування внутрішніх мереж. Захист від вторгнень є ключовим елементом в цьому контексті.

Застосування моделі управління ризиками для хмарної інфраструктури дозволяє ефективно виявляти, оцінювати та мінімізувати потенційні ризики. Це включає в себе розробку індивідуальних систем захисту для вирішення високорівневих завдань, пов'язаних із керуванням хмарним середовищем.

Основою безпеки в хмарному середовищі є шифрування даних, які зберігаються та передаються. Забезпечення захисту інформації при передачі даних, автентифікація користувачів та їх ізоляція один від одного, стають невід'ємною частиною ефективної архітектури безпеки.

З урахуванням віртуалізації, як ключового фактору у хмарних технологіях, виникає потреба в адаптації існуючих заходів безпеки до хмарних платформ. Це включає в себе контроль та управління хмарними сервісами, а також розробку спеціалізованих заходів для вирішення нових викликів.

З урахуванням росту вимог з боку зовнішніх регуляторів та внутрішніх питань політики захисту, необхідно встановити ефективну систему відповіді на ці вимоги. Це включає в себе вдосконалення технічних аспектів та розробку політики безпеки ЦОД.

Таким чином, проблема забезпечення безпеки в хмарному середовищі є достатньо складним завданням, яке вимагає системного підходу та постійного вдосконалення. Захист ІТ-інфраструктури в умовах хмарних технологій вимагає врахування специфічних загроз та впровадження сучасних методів захисту даних. Тільки так можна забезпечити надійність та безпеку використання хмарних обчислень в сучасних умовах.

Список використаних джерел

1. S. Singh. A survey on cloud computing security : Issues, threats, and solutions. – 2016. –

URL:

<https://www.sciencedirect.com/science/article/abs/pii/S1084804516301990>.

УДК 004.056

*Бродський Ю. Б., к.т.н., доцент,
Рудюк Б. М., здобувач*

Державний університет «Житомирська політехніка»

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ТА РІВНЯ БЕЗПЕКИ КОРПОРАТИВНОЇ МЕРЕЖІ НА БАЗІ ТЕХНОЛОГІЇ CISCO DMVPN

Корпоративні мережі є ключовою інфраструктурою для бізнесу. Вони використовуються для зберігання, обробки та передачі важливої інформації, а також для забезпечення зв'язку між співробітниками, клієнтами та партнерами. Внаслідок цього корпоративні мережі є привабливою мішенню для хакерів та інших зловмисників.

Забезпечення безпеки корпоративних мереж є вельми важливим завданням для будь-якої компанії. Несанкціонований доступ до цих мереж може призвести до витоку конфіденційної інформації, фінансових втрат та завдати серйозної шкоди репутації компанії. Тому компанії повинні активно працювати над вдосконаленням заходів безпеки і регулярно проводити аудит своїх мереж, щоб виявити потенційні слабкі місця і вразливості. Підтримка безпеки корпоративних мереж стає невід'ємною частиною сучасного бізнесу, і важливо приділяти їй належну увагу.

Одним із найбільш актуальних завдань захисту корпоративної мережі є забезпечення безпеки тунельного зв'язку між віддаленими філіями. Технологія Cisco DMVPN дозволяє вирішити це завдання шляхом використання динамічного тунелю (Dynamic Multipoint VPN), який забезпечує шифрування трафіку між філіями, а також аутентифікацію і авторизацію учасників тунелю.

Основна перевага DMVPN полягає в можливості створення динамічних тунелів без необхідності ручного налаштування на кожному з вузлів. Вона використовує протоколи IPsec і GRE (Generic Routing Encapsulation), що дозволяє створити шифровані тунелі для безпечної передачі даних через незахищені мережі, такі як Інтернет. Крім того, DMVPN дозволяє ефективно використовувати ресурси мережі, зменшуючи трафік і обчислювальні витрати.

Також, DMVPN надає можливість створювати мережі з точки-до-точки або з точки-до-багатьох, що робить її ідеальним рішенням для організацій з розподіленою інфраструктурою. Це спрощує побудову складних мереж і дозволяє забезпечувати зв'язок між різними вузлами в мережі, навіть якщо вони розташовані в різних фізичних локаціях.

Таким чином, DMVPN є потужним і гнучким інструментом для забезпечення зв'язку і безпеки в розподілених мережах.

Безпека в DMVPN забезпечується за рахунок наступних механізмів:

Зашифрований тунель: DMVPN використовує різні методи шифрування, такі як IPSec, для створення зашифрованого тунелю між різними вузлами мережі. Це дозволяє захистити передачу конфіденційних даних через незахищені мережі, такі як Інтернет;

Динамічне налаштування тунелів: DMVPN дозволяє автоматично налаштовувати тунелі між вузлами, що спрощує керування VPN і дозволяє додавати нові підключення без необхідності ручного налаштування;

Централізоване управління: Cisco DMVPN може бути інтегрованим з централізованими системами управління, такими як Cisco Identity Services Engine (ISE). Це дозволяє контролювати доступ до мережі, вимагаючи аутентифікації, авторизації та обліку (AAA) для кожного підключення;

Мультифакторна аутентифікація: підключає додатковий шар безпеки;

Перевірка безпеки мережі: за допомогою Cisco DMVPN можна встановити засоби моніторингу та реагування на інциденти для виявлення та відповіді на потенційні загрози безпеці мережі [2].

Отже, DMVPN дозволяє заощадити час та зусилля при налаштуванні мережі, спрощує розгортання та управління мережею, зменшує ймовірність помилок та підвищує загальну надійність і безпеку інфраструктури. Таким чином, DMVPN стає потужним інструментом для організацій, що прагнуть поєднати безпеку та ефективність у своїй корпоративній мережі.

Список використаних джерел

1. Cisco Dynamic Multipoint VPN. URL: https://www.cisco.com/c/en/us/products/collateral/security/dynamicmultipoint-vpndmvpn/data_sheet_c78-468520.html.

2. DMVPN – Concepts & Configuration. URL: <https://learningnetwork.cisco.com/s/article/dmvpn-conceptsamppconfiguration>.

УДК 004.056

*Умінський І. О., здобувач,
Бродський Ю. Б., к.т.н., доцент
Державний університет «Житомирська політехніка»*

ОПТИМІЗАЦІЯ ЕФЕКТИВНОСТІ ТА ЗАБЕЗПЕЧЕННЯ ВИСОКОГО РІВНЯ БЕЗПЕКИ КОРПОРАТИВНОЇ МЕРЕЖІ ЗА ДОПОМОГОЮ РЕАЛІЗАЦІЇ ТЕХНОЛОГІЇ OPENVPN

Корпоративні мережі – це спеціалізовані комп'ютерні мережі, що забезпечують зв'язок між різними комп'ютерами, пристроями та іншими ресурсами в межах однієї організації чи підприємства. Вони призначені для обміну даними, спільної роботи над проектами, обміну ресурсами та забезпечення безпеки і конфіденційності внутрішніх інформаційних потоків. Такі мережі можуть включати в себе внутрішній Інтранет, електронну пошту та інші засоби зв'язку, спрямовані на підтримку внутрішньої діяльності компанії.

Безпека в корпоративних мережах – це критичний аспект, оскільки вони містять важливі дані, конфіденційну інформацію та доступ до ресурсів компанії. Незаконний доступ до цих мереж може призвести до розголошення конфіденційної інформації, фінансових втрат та серйозної шкоди репутації компанії. Тому компанії повинні активно працювати над удосконаленням заходів безпеки та регулярно проводити аудит своїх мереж, щоб виявити потенційні слабкі місця і вразливості. Забезпечення безпеки корпоративних мереж стає невід'ємною частиною сучасного бізнесу, тому важливо приділяти цьому питанню належну увагу.

Однією з ключових та актуальних задач забезпечення безпеки корпоративної мережі є забезпечення захисту тунельного зв'язку між віддаленими філіями. OpenVPN забезпечує безпеку тунельного зв'язку, створюючи зашифрований канал між різними точками мережі. Це дозволяє працівникам підключатися до корпоративної мережі з будь-якого місця, використовуючи Інтернет, забезпечуючи захист даних під час передачі через небезпечні мережі, такі як громадські Wi-Fi мережі.

Основна перевага OpenVPN – кросплатформеність. OpenVPN підтримується на різних операційних системах, таких як Windows, macOS, Linux, і може бути використаний на різних пристроях, що робить його універсальним для багатьох потреб.

Крім того, OpenVPN надає можливість створення мереж з точки-до-точки або з точки-до-багатьох, що робить її оптимальним вибором для організацій з розподіленою інфраструктурою. Це спрощує

розгортання складних мереж та забезпечує зв'язок між різними вузлами мережі, навіть якщо вони розташовані у різних фізичних місцях. Таким чином, OpenVPN є потужним і гнучким інструментом для забезпечення зв'язку та безпеки у розподілених мережах.

OpenVPN славиться своєю високою безпекою, яка базується на декількох ключових аспектах:

Шифрування: OpenVPN використовує різні методи шифрування, такі як AES (Advanced Encryption Standard) або Blowfish, для захисту передачі даних через тунель. Це забезпечує конфіденційність інформації під час її транспортування.

Протоколи автентифікації: OpenVPN використовує протоколи автентифікації, такі як HMAC (Hash-based Message Authentication Code), які дозволяють перевіряти цілісність даних та підтверджувати їх автентичність під час передачі.

Сертифікати та ключі: використання цифрових сертифікатів та ключів для автентифікації і шифрування даних в тунелі, що забезпечує захист від несанкціонованого доступу.

Керування сесіями: OpenVPN має можливість контролювати сесії та автоматично перезавантажувати ключі для підтримки безпеки тунелю.

Захист від атак: OpenVPN має вбудовані заходи безпеки для запобігання різного роду атак, таких як атаки типу «перехоплення людини посередника» (Man-in-the-Middle), DNS-отруєння та інші.

Аудит безпеки: відкритий код OpenVPN дозволяє громадськості аудитувати його безпеку, що сприяє виявленню та усуненню можливих вразливостей.

Ці аспекти забезпечують високий рівень безпеки для тунельних з'єднань у OpenVPN, що робить його популярним та надійним засобом для захисту передачі даних через відкриті мережі, такі як Інтернет.

Отже, OpenVPN вирізняється своєю здатністю забезпечувати високий рівень безпеки та ефективності у створенні захищених тунельних з'єднань. Він спрощує процес налаштування мережі, забезпечуючи широкі можливості для безпечного обміну даними. OpenVPN знижує ризик помилок завдяки своїм методам шифрування та протоколам автентифікації, що підвищує надійність і безпеку інфраструктури. Таким чином, OpenVPN стає важливим інструментом для організацій, які прагнуть забезпечити найвищий рівень захисту даних та оптимізувати роботу корпоративної мережі.

УДК 004.056

*Хоменко В. Р., здобувач,
Бродський Ю. Б., к.т.н., доцент
Державний університет «Житомирська політехніка»*

БАЛАНСУВАННЯ НАВАНТАЖЕННЯ ТА БЕЗПЕКА: РОЛЬ PFSense У ВИСОКОДОСТУПНИХ МЕРЕЖАХ

Сучасні високодоступні мережі вимагають ефективного управління трафіком та високого рівня безпеки для забезпечення стабільності та надійності функціонування. PFSense виконує ключову роль у досягненні таких цілей, поєднуючи балансування навантаження та високий рівень безпеки.

Балансування навантаження є важливою функцією для високодоступних мереж, оскільки воно дозволяє розподіляти трафік між декількома серверами. Це може допомогти підвищити продуктивність мережі, оскільки трафік не надходить лише на один сервер. Балансування навантаження також може допомогти підвищити доступність мережі, оскільки якщо один сервер вийде з ладу, інший сервер зможе продовжувати обробляти трафік.

Основна мета балансування навантаження – це оптимізація використання ресурсів, максимізація пропускної здатності, зменшення часу відгуку і запобігання перевантаження будь-якого одного ресурсу. Використання декількох компонентів балансування навантаження, замість одного компонента, може значно підвищити надійність і доступність за рахунок резервування. Саме балансування навантаження передбачає, зазвичай, наявність спеціального програмного забезпечення або апаратних засобів, таких як багаторівневий комутатор або система доменних імен, серверний процес [1].

PFSense підтримує кілька методів балансування навантаження. Статичне балансування розподіляє трафік між серверами на основі статичного правила, наприклад, на основі IP-адреси або номера порту. Динамічне балансування розподіляє трафік між серверами на основі динамічних факторів, таких як навантаження на сервер або час відгуку. Балансування за допомогою IP-адрес розподіляє трафік між серверами на основі IP-адреси клієнта.

Безпека також є важливою для високодоступних мереж, оскільки вони є більш привабливими для хакерів. Зловмисники можуть

використовувати високодоступні мережі для запуску атак на велику кількість користувачів.

PFSense надає широкий спектр функцій безпеки, які можуть допомогти захистити високодоступні мережі від атак. Фільтрація пакетів може блокувати несанкціонований трафік, який може використовуватися для запуску атак. PFSense підтримує широкий спектр правил фільтрації пакетів, які можна використовувати для блокування різних типів несанкціонованого трафіку. Системи виявлення та запобігання вторгненням (IDS/IPS) можуть виявляти та запобігати атакам, використовуючи різні методи. Віртуальні приватні мережі (VPN) можуть шифрувати трафік між пристроями, що перешкоджає зловмисникам відстежувати та атакувати його.

Для підвищення безпеки мережі за допомогою мережевого екрану PFSense рекомендується регулярно оновлювати програмне забезпечення, перевіряти журнали безпеки PFSense на наявність ознак атак, створювати резервні копії конфігурації PFSense.

Таким чином, PFSense – це потужний інструмент підвищення ефективності функціонування та безпеки високодоступних мереж.

В доповіді буде показано, як використовувати функції балансування навантаження та безпеки PFSense в процесі створення стійкої та захищеної мережі [2].

Список використаних джерел

1. Динамічне балансування трафіку між декількома провайдерами. URL: <http://journals.khnu.km.ua/vestnik/wp-content/uploads/2021/01/12-7.pdf>
2. pfSense® – World's Most Trusted Open Source Firewall. URL: <https://www.pfsense.org/>

УДК 004.451.9+004.94

*Головня О. С., к.пед.н., доцент,
Магурін О. О., здобувач,
Дехтяр М. С., здобувач*

Державний університет «Житомирська політехніка»

ДОБІР ВІРТУАЛІЗАЦІЙНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ПРОТОТИПУ ХМАРНОЇ МЕРЕЖНОЇ ІНФРАСТРУКТУРИ

Хмарні технології дозволяють організувати клієнту доступ як до окремих програм у хмарі, так і до мережної інфраструктури. Розповсюдженню хмарних сервісів додатково сприяла пандемія Covid-19, а повномасштабна російсько-українська війна спричинила підвищений інтерес українських організацій до розміщення мережної інфраструктури у хмарі з метою захистити сервіси і дані від фізичної втрати та хакерських атак. Необхідний контроль над хмарною інфраструктурою надають хмарні сервіси моделі IaaS (інфраструктура як сервіс). Організувати таку інфраструктуру можна за двома підходами: використання *платформ, наданих провайдерами хмарних сервісів* (Azure Virtual Machines, Amazon EC2, Google Compute Engine та ін.), та використання *спеціалізованого хмарного програмного забезпечення* (Eucalyptus, OpenStack, CloudStack, OpenNebula та ін.). Крім того, хмарна інфраструктура на базі спеціалізованого хмарного ПЗ також може надаватися провайдерами на їхньому обладнанні. Обидва підходи мають переваги, однак у межах даного дослідження увагу зосереджено на другому підході через його гнучкість, що відповідає потребам освітнього й дослідницького використання.

Метою роботи є добір спеціалізованого хмарного програмного забезпечення для прототипу хмарної мережної інфраструктури.

Розроблюваний прототип є частиною більшого дослідження, описаного у роботах [1] та [2], і у довшій перспективі повинен забезпечувати можливість масштабування у хмарну лабораторію для навчання операційної системи Linux. *Вимоги до прототипу хмарної мережної інфраструктури* є наступними: використання віртуальних середовищ з ОС Linux, об'єднаних за допомогою віртуальних комп'ютерних мереж; розгортання за моделлю приватної хмари (лабораторія використовуватиметься лише студентами університету); відносно невисокі системні вимоги; висока масштабованість.

У статті [2] здійснено порівняльний аналіз чотирьох популярних вільно поширюваних хмарних платформ (Eucalyptus, OpenStack, CloudStack та OpenNebula). Усі вони загалом відповідають заявленим

вимогам. Обрано платформу OpenStack, що має високу гнучкість і відповідає відкритим стандартам. Загалом, OpenStack складається з багатьох компонентів і може бути адаптована для широкого кола потреб. Водночас, наявні й рішення на основі OpenStack, які підходять для розроблюваного прототипу, передусім завдяки невисоким системним вимогам: OpenStack Training Labs; MicroStack на базі Sunbeam; невеликий кластер на основі Microstack з інстансами CirrOS. Здійснено аналіз та тестування перелічених рішень і, як результат, для реалізації прототипу хмарної мережної інфраструктури обрано невеликий кластер на базі Microstack з інстансами CirrOS. В OpenStack Training Labs використано старіші технології (Python 2, Ubuntu 20.04), тому під час тестування виявлено проблеми сумісності з Ubuntu 22.04. Для роботи рішення MicroStack на базі Sunbeam потрібні 16 Гб вільної оперативної пам'яті, і на комп'ютері з 16 Гб RAM рішення не працює.

Для розгортання прототипу хмарної інфраструктури використано ноутбук HP 250 G5 з процесором Intel Core i5-6200U @ 2.30GHz × 4, 16 ГіБ RAM та ОС Ubuntu 22.04.3 LTS. Розгорнуто мінімальну конфігурацію MicroStack за допомогою команд

```
sudo snap install microstack --devmode --beta
sudo microstack init --auto --control
microstack launch cirros --name test
```

На рис. 1 показано тестовий інстанс у веб-інтерфейсі Horizon.

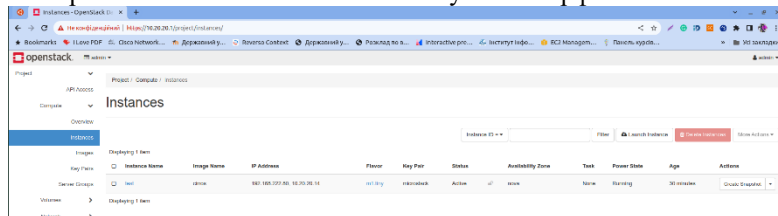


Рис. 1. Інстанс test (CirrOS) в інтерфейсі Horizon

Для під'єднання до інстансу використовується протокол SSH.

Висновки. Для створення прототипу хмарної мережної інфраструктури вибрано платформу OpenStack. Успішно розгорнуто невеликий кластер на базі Microstack з інстансами CirrOS.

Список використаних джерел

1. Holovnia O. Linux online virtual environments in teaching operating systems. Proceedings of the 16th International Conference on ICT in Education, Research and Industrial Applications. – 2020. – Vol. 2. pp. 964 – 973.
2. Holovnia O., Oleksiuk V. Selecting cloud computing software for a virtual online laboratory supporting the Operating Systems course. Proceedings of the 9th Workshop on Cloud Technologies in Education. 2021. – pp. 216 – 227.

УДК 004.056.5

*Ищук К. О., здобувач,
Покотило О. А., ст. викладач,
Щур Н. О., ст. викладач*

Державний університет «Житомирська політехніка»

ДОСЛІДЖЕННЯ ФУНКЦІОНАЛУ, ЕФЕКТИВНОСТІ ТА БЕЗПЕКИ КРИПТОГРАФІЧНИХ БІБЛІОТЕК У СЕРЕДОВИЩІ JAVASCRIPT

Криптографічні бібліотеки в середовищі JavaScript виступають як ключовий елемент забезпечення безпеки. Вони дозволяють забезпечити захист конфіденційної інформації, такої як паролі, особисті дані, фінансові транзакції, а також допомагають здійснювати безпечну передачу даних через мережу шляхом їх шифрування перед відправкою та розшифрування при отриманні, що унеможливорює перехоплення та злам доступу до них. Актуальність та важливість теми криптографічних бібліотек у JavaScript у сфері безпеки не може бути недооцінена. Вони є необхідними для перевірки цілісності та аутентифікації користувачів, а їх використання зменшує ризик зламу системи або зловживання даними.

Метою даного дослідження є аналіз ключових аспектів основних криптографічних бібліотек в середовищі JavaScript з подальшим порівнянням їх характеристик задля визначення оптимального рішення для використання в практичних розробках.

До найбільш відомих криптографічних бібліотек відносять CryptoJS [1], Forge [2], SJCL (Stanford JavaScript Crypto Library) [3], SubtleCrypto (Web Crypto API) [4], libsodium.js [5]. Результат їх порівняння за основними критеріями наведено в табл.1.

Результати дослідження вищенаведених криптографічних бібліотек демонструють їх основні відмінності. CryptoJS, хоча і підтримує багато алгоритмів, використовує застарілі методи шифрування, що може вплинути на безпеку та ефективність у сучасних сценаріях. Forge і SJCL забезпечують високий рівень безпеки та підтримки сучасних стандартів, проте Forge потребує багатьох ресурсних витрат у зв'язку з великим обсягом, тоді як SJCL може не враховувати деякі новіші розробки в галузі криптографії.

SubtleCrypto, яка вбудована у браузері через Web Crypto API, має високу безпеку та дозволяє використовувати сучасні алгоритми, але її функціонал може бути обмежений залежно від браузера. libsodium.js виділяється високою безпекою та ефективністю завдяки сучасним алгоритмам та швидкодії, але можуть бути питання по швидкості завантаження веб-додатків.

Таблиця 1

Порівняльна характеристика криптографічних бібліотек у середовищі JavaScript

Критерій	<i>CryptoJS</i>	<i>Forge</i>	<i>SJCL</i>	<i>SubtleCrypto</i>	<i>libsodium.js</i>
Алгоритми шифрування	<i>AES, DES, Triple DES, інші</i>	<i>AES, DES, Triple DES, інші</i>	<i>AES, DES, RC4</i>	<i>AES, DES, RSA, інші</i>	<i>AES, ChaCha20, інші</i>
Хеш-функції	<i>MD5, SHA-1, SHA-256, інші</i>	<i>MD5, SHA-1, SHA-256, інші</i>	<i>SHA-1, SHA-256</i>	<i>SHA-1, SHA-256, інші</i>	<i>SHA-256, SHA-512, інші</i>
Підтримка RSA	+	+	-	+	+
Підтримка ECC	-	+	-	+	+
Web Crypto API сумісність	-	-	-	+	-
Розмір	<i>Близько 300-400 KB (зжатиий вигляд)</i>	<i>Близько 200-300 KB</i>	<i>Близько 100-200 KB</i>	<i>Залежить від браузера</i>	<i>Близько 200-300 KB</i>
Підтримка / спільнота	<i>Малоактивна</i>	<i>Активна</i>	<i>Обмежена</i>	<i>Активна</i>	<i>Активна</i>
Ліцензія	<i>BSD, MIT</i>	<i>BSD</i>	<i>BSD</i>	<i>MIT</i>	<i>ISC</i>
Ефективність	<i>Середня</i>	<i>Висока</i>	<i>Середня</i>	<i>Висока</i>	<i>Висока</i>
Безпека	<i>Низька</i>	<i>Висока</i>	<i>Висока</i>	<i>Висока</i>	<i>Дуже висока</i>

Враховуючи отримані результати, визначення оптимального рішення для практичних розробок буде залежати від конкретних потреб. Для веб-додатків, де важлива вбудована підтримка браузерів, кросплатформених платформ, мобільних додатків та інших обмежених середовищ, де важливий обсяг завантаження, кращим вибором буде SubtleCrypto. У випадку розробки додатків, які вимагають високого рівня безпеки, доцільно зупинити вибір на libsodium.js або SJCL.

Використання криптографічних бібліотек у JavaScript є важливим кроком для забезпечення безпеки в інтернет-просторі, і їхня правильна інтеграція є важливою частиною розробки безпечних та надійних веб-застосунків.

Список використаної літератури

1. CryptoJS. URL: <https://cryptojs.gitbook.io/docs/>
2. Forge. GitHub Pages. URL: <https://digitalbazaar.github.io/forge/>
3. Stanford Javascript Crypto Library (SJCL). URL: <https://crypto.stanford.edu/sjcl/>
4. Web Crypto API – Web APIs. URL: <https://developer.mozilla.org/en-US/docs/Web/API>
5. Libsodium documentation: Introduction. URL: <https://libsodium.gitbook.io/doc/>

УДК 004.056.5

*Драчевський Н. В., здобувач,
Покотило О. А., ст. викладач,
Щур Н.О., ст. викладач*

Державний університет «Житомирська політехніка»

ЗАСТОСУВАННЯ АЛГОРИТМІВ ХЕШУВАННЯ ДЛЯ ЗАХИСТУ ПАРОЛІВ У ПРОГРАМАХ НА МОВІ PYTHON

У сучасному цифровому середовищі, де зберігаються великі обсяги конфіденційної інформації, їх захист стає однією з найбільш актуальних проблем для багатьох компаній, розробників програмного забезпечення і користувачів. Використання надійних алгоритмів хешування для захисту паролів дозволяє забезпечити безпеку інформації, зокрема у веб-розробці, де дані зберігаються в базах даних. Тому питання їх застосування є актуальним.

Метою даного дослідження є аналіз різних алгоритмів хешування, виявлення їх вразливостей та методів підвищення безпеки за допомогою хешування паролів у програмах, написаних на Python.

Python дозволяє широко використовувати різноманітні бібліотеки та модулі, що сприяють високому рівню безпеки при збереженні паролів. Зазвичай, на практиці застосовуються наступні: `passlib`, `hashlib` та `bcrypt`.

`Passlib` – це бібліотека, спеціалізована на роботі з паролями, яка надає багато функцій для їх безпечного зберігання та перевірки. Вона підтримує різні алгоритми хешування, зокрема SHA-1, SHA-2, SHA-3, `bcrypt`, `scrypt` і `Argon2` та має можливість працювати з різними системами збереження паролів. `Passlib` може застосовуватися для роботи з системами аутентифікації веб-фреймворків, таких як `Flask` або `Django`, а також для безпечного зберігання та перевірки паролів користувачів в системах аутентифікації. Проте використання `passlib` може бути складним через широкий спектр можливостей, а інтеграція у деякі існуючі системи вимагатиме додаткових зусиль.

Модуль `hashlib` входить до стандартної бібліотеки Python, та надає можливість взаємодіяти з хеш-функціями MD5, SHA-1, SHA-2, SHA-3 і BLAKE2. Крім того, в ньому є можливість використання функції `pbkdf2_hmac()`, яка реалізує алгоритм PBKDF2 (Password-Based Key Derivation Function 2), який кілька разів проводить хешування пароля та солі (`salt` – випадкове унікальне значення, яке додається до пароля перед тим, як його хешувати). Даний модуль не надає спеціалізованих інструментів для безпечного зберігання паролів, а деякі з підтримуваних хеш-функцій (MD5, SHA-1) є вразливі до атак колізій.

Його доцільно використовувати для зберігання хешів паролів та при перевірці цілісності файлів шляхом обчислення хеш-суми.

Бібліотека `bcrypt` спеціалізується на алгоритмі хешування з аналогічною назвою на основі шифру Blowfish. Він вважається одним з найбезпечніших для збереження паролів. Завдяки тому, що модуль `bcrypt` дозволяє керувати параметрами алгоритму, це перетворює його в ефективний засіб захисту паролів. Але при високому рівні складності алгоритм може бути повільнішим в порівнянні з іншими, та потребує більших обчислювальних ресурсів, що може впливати на продуктивність системи. `Bcrypt` найкраще застосовувати при захисті паролів веб-додатків та в системах аутентифікації Python для забезпечення міцності паролів [1].

Серед методів підвищення безпеки при збереженні паролів у програмах, розроблених на Python, можна виділити наступні:

- додавання випадкової унікальної інформації до паролю перед процесом хешування для ускладнення атак типу «rainbow table»;
- використання сучасних безпечних алгоритмів, що спеціально розроблювались для захисту паролів і здатні протистояти атакам;
- забезпечення обробки помилок аутентифікації при невдалих спробах входу, щоб уникнути надмірного розкриття інформації;
- використання функції хешування до паролю більше одного разу для ускладнення зловмисних атак [2].

Таким чином, застосування відповідних методів хешування паролів у програмах на Python є надзвичайно важливим для забезпечення захисту конфіденційної інформації користувачів. Сучасні алгоритми `bcrypt` або `Argon2` – найкращий варіант для зберігання паролів, оскільки вони володіють високою стійкістю до атак.

Важливо дотримуватися розглянутих методів підвищення безпеки та постійно слідкувати за оновленнями та рекомендаціями для використання найбільш сучасних та найбезпечніших шляхів зберігання паролів.

Список використаної літератури

1. Python: 3 Ways to Hash a Password. URL: <https://www.slingacademy.com/article/python-ways-to-hash-a-password/>
2. Password Hashing and Salting: Performance vs Security. URL: <https://www.linkedin.com/advice/0/how-do-you-balance-performance-security-when>

УДК 004.056.57

Пірог О.В., к.т.н., доцент

Державний університет «Житомирська політехніка»

СТАНДАРТИ ВЕРИФІКАЦІЇ БЕЗПЕКИ МОБІЛЬНИХ ДОДАТКІВ

У квітні 2023 року вийшов реліз версії 2.0.0 Стандарту верифікації безпеки мобільних додатків OWASP (OWASP Mobile Application Security Verification Standard – MASVS) [1]. Основними напрямками забезпечення безпеки мобільних додатків визначено: зберігання даних, криптографічні методи, аутентифікація та авторизація, мережевий зв'язок, взаємодія платформ, якість коду, стійкість до зворотного проєктування та втручання.

Мобільні додатки обробляють широкий спектр конфіденційних даних, таких як персональні дані (PII), криптографічний матеріал, секрети та ключі API, які часто потрібно зберігати локально. Ці конфіденційні дані можуть зберігатися у пам'яті додатку. Також конфіденційні дані зберігаються або розкриваються у загальнодоступних місцях (використання API, резервне копіювання, журнали). Тому потрібний контроль, що гарантує належний захист конфіденційних даних, що зберігаються додатком, та всіх їх витоків.

Криптографія є важливою для мобільних додатків, оскільки мобільні пристрої дуже портативні і їх можна легко втратити або вкрасти. Зловмисник, який отримує фізичний доступ до пристрою, потенційно може отримати доступ до всіх конфіденційних даних, що зберігаються на ньому (паролі, фінансова інформація та особиста інформація). Криптографія є засобом захисту цих конфіденційних даних шляхом їх шифрування, щоб неавторизований користувач не міг їх прочитати. Також необхідно керувати криптографічними ключами протягом усього їх життєвого циклу (генерація, зберігання та захист ключів). Погане керування ключами може поставити під загрозу навіть найнадійнішу криптографію. Тому потрібно переконатися, що додаток використовує криптографію відповідно до передових галузевих практик, які визначені в стандартах, таких як NIST.SP.800-175B [2] і NIST.SP.800-57 [3].

Аутентифікація та авторизація є важливими компонентами мобільних додатків. Важливо, щоб додаток дотримувалася найкращих практик, щоб забезпечити безпечне використання протоколів. Мобільні додатки, щоб підтвердити особу користувача, використовують різні форми аутентифікації (біометрія, PIN-код, багатофакторна аутентифікація). Ці механізми мають бути реалізовані

правильно, щоб забезпечити їх ефективність у запобіганні несанкціонованому доступу. Безпеку віддаленої кінцевої точки слід перевіряти за допомогою галузевих стандартів, таких як OWASP Application Security Verification Standard (ASVS) [4].

Забезпечення мережевої безпеки є критично важливим аспектом безпеки мобільних додатків. Щоб забезпечити конфіденційність і цілісність даних, що передаються, розробники зазвичай покладаються на шифрування, наприклад, за допомогою TLS. Однак існують способи вимкнення безпечних параметрів за замовчуванням або їх обходу (з використанням API або бібліотек сторонніх розробників). Мобільний додаток повинен встановлювати безпечні зашифровані з'єднання та перевіряти це. Розробник може довіряти лише певним центрам сертифікації (CA).

Безпека мобільних додатків значною мірою залежить від їх взаємодії з платформою, що передбачає розкриття даних за допомогою наданих платформою механізмів взаємодії між процесами (IPC), що можуть використовуватися зловмисниками. Конфіденційні дані (паролі, дані кредитних карток і одноразові паролі в сповіщеннях) відображаються в інтерфейсі користувача. Важливо переконатися, що ці дані не витікають через механізми платформи (автоматично створені знімки екрана), розкриття за допомогою «серфінгу через плече» або під час спільного використання пристрою. Тому потрібно безпечно використовувати надані платформою механізми IPC та безпечно відображати конфіденційні дані в інтерфейсі користувача.

Мобільні додатки мають точки введення даних (інтерфейс користувача, IPC, мережа та файлова система). Потрібно розглядати ці вхідні дані як ненадійні. Загрозами є ін'єкційні атаки (ін'єкція SQL, XSS або незахищена десеріалізація). Дефекти пам'яті, важко виявити під час тестування на проникнення, але їх можна запобігти за допомогою безпечної архітектури програмування. Існують вразливості програмування, які виникають із зовнішніх джерел (ОС і компоненти ПЗ сторонніх розробників). Розробники повинні дотримуватися найкращих практик, таких як OWASP Software Assurance Maturity Model (SAMM) [5] і NIST.SP.800-218 Secure Software Development Framework (SSDF) [6], перевіряти та дезінфікувати всі вхідні дані, щоб запобігти атакам ін'єкцій, а також забезпечувати оновлення додатків і платформ, щоб захистити від відомих вразливостей.

Заходи поглибленого захисту (обфускація коду, anti-debugging, anti-tampering тощо) важливі для підвищення стійкості додатків до зворотного проектування. Вони створюють нові рівні контролю безпеки, що ускладнює зловмисникам зворотне проектування. Такий

захист перешкоджає з'ясуванню того, як додаток працює за допомогою статичного аналізу, запобігає динамічному аналізу. Ці заходи створюють додатковий захист.

Список використаних джерел

1. OWASP Mobile Application Security Verification Standard URL: <https://mas.owasp.org/MASVS/11-MASVS-RESILIENCE/>
2. NIST.SP.800-175B Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms URL: <https://csrc.nist.gov/pubs/sp/800/175/b/r1/final>
3. NIST.SP.800-57 Recommendation for Key Management URL: <https://csrc.nist.gov/pubs/sp/800/57/pt1/r5/final>
4. OWASP Application Security Verification Standard URL: <https://owasp.org/www-project-application-security-verification-standard/>
5. OWASP Software Assurance Maturity Model URL: <https://owasp samm.org/model/>
6. NIST.SP.800-218 Secure Software Development Framework URL: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf>

УДК 004.056

*Колощук М. С., асистент,
Дячук О. Ю., ст. викладач
Державний університет «Житомирська політехніка»*

LI-FI: ТЕХНОЛОГІЯ БЕЗДРОТОВОГО ЗВ'ЯЗКУ ЧЕРЕЗ СВІТЛО

У світі бездротового зв'язку Wi-Fi був домінуючою технологією протягом кілька десятиліть. Однак в останні роки з'явилася нова технологія, яка має потенціал для революційної зміни способу бездротової передачі даних. Ця технологія називається Li-Fi, скорочено від Light Fidelity. Li-Fi – це технологія бездротового зв'язку, яка використовує видиме світло для передачі даних, на відміну від Wi-Fi, який використовує радіохвилі. Ця технологія привертає все більше уваги в останні роки завдяки своїм потенційним перевагам над традиційною технологією Wi-Fi. У цій статті ми розглянемо переваги та недоліки Li-Fi, як вона працює, як її можна використовувати та на якому етапі розвитку перебуває.

Переваги Li-Fi

1. Швидша швидкість передачі даних: Li-Fi може передавати дані зі значно більшою швидкістю, ніж Wi-Fi, з теоретичною швидкістю до 224 Гбіт/с. Це відбувається тому, що видиме світло має вищу частоту, ніж радіохвилі, що дозволяє передавати більше даних передавати більше даних за коротший проміжок часу.

2. Більш безпечний: Оскільки Li-Fi використовує світло для передачі даних, він не може проходити крізь стіни, що робить його більш безпечним, ніж Wi-Fi. Це означає, що хакерам набагато складніше перехопити дані, що передаються через Li-Fi.

3. Відсутність перешкод: Сигнали Wi-Fi можуть бути легко порушені іншими електронними пристроями, але на Li-Fi не впливають електромагнітні перешкоди. Це означає, що Li-Fi можна використовувати там, де Wi-Fi не може, наприклад, у лікарнях і літаках.

4. Енергоефективність: Li-Fi використовує світлодіодні лампи для передачі даних, які є більш енергоефективними, ніж традиційні передавачі Wi-Fi. Це означає, що Li-Fi потенційно може заощадити енергію та зменшити викиди вуглецю.

Недоліки Li-Fi

1. Обмежений радіус дії: Сигнали Li-Fi не можуть проходити крізь стіни, тому радіус дії Li-Fi обмежується кімнатою, в якій він

використовується. Це означає, що потрібно встановити кілька Li-Fi у великих будівлях або будинках потрібно встановлювати кілька передавачів Li-Fi.

2. Необхідна пряма видимість: Оскільки Li-Fi використовує світло для передачі даних, він вимагає чіткої прямої видимості між передавачем і приймачем. Це означає, що перешкоди такі як люди та меблі, можуть перешкоджати проходженню сигналу.

3. Дорогий: Технологія Li-Fi все ще перебуває на ранніх стадіях розвитку, і вартість обладнання, необхідного для її використання, наразі набагато вища, ніж у традиційного Wi-Fi обладнання.

4. Обмежена сумісність: Li-Fi наразі не сумісний з більшістю існуючих пристроїв, а це означає, що потрібно буде розробляти і встановлювати нові пристрої, щоб скористатися перевагами технології Li-Fi.

Як працює Li-Fi

Li-Fi використовує світлодіодні ліхтарі для передачі даних. Світлодіоди модулюються на високій частоті, що дозволяє їм передавати дані. Фотодетектор використовується для прийому сигналу, який потім перетворюється назад у дані. Модуляція світлодіодних ліхтарів відбувається таким чином, що вона непомітна для людського ока.

Як можна використовувати Li-Fi

Технологія Li-Fi має багато потенційних застосувань, серед яких

1. У лікарнях: Li-Fi можна використовувати в лікарнях для передачі медичних даних, оскільки сигнал не може проходити крізь стіни і не піддається впливу електромагнітних перешкод.

2. У літаках: Li-Fi може використовуватися в літаках для розваг пасажирів під час польоту, оскільки сигнал не заважає навігаційному обладнанню літака.

3. У будинках та офісах: Li-Fi можна використовувати в будинках і офісах для забезпечення високошвидкісного доступу до Інтернету, оскільки він може передавати дані зі значно більшою швидкістю, ніж Wi-Fi.

4. У роздрібних магазинах: Li-Fi можна використовувати в роздрібних магазинах для надання клієнтам послуг, що базуються на місцезнаходженні, таких як інформація про товари та акції.

5. У промислових умовах: Li-Fi можна використовувати в промислових умовах для забезпечення бездротового зв'язку, на який не впливають електромагнітні перешкоди.

6. У розумних містах: Li-Fi може використовуватися в розумних містах для забезпечення бездротового зв'язку, який є більш безпечним

і ефективним, ніж Wi-Fi. бездротового зв'язку, який є більш безпечним та енергоефективним, ніж Wi-Fi.

Сучасний стан розвитку Li-Fi

Технологія Li-Fi все ще перебуває на ранніх стадіях розвитку, і наразі існує лише кілька компаній, які активно працюють над розробкою Li-Fi продуктів. Однак інтерес до цієї технології дуже великий, і очікується, що в найближчі роки вона стане більш доступною. Дослідники також вивчають шляхи покращення діапазону та сумісності Li-Fi, що може зробити його життєздатною альтернативою Wi-Fi в майбутньому.

Висновок

Li-Fi – це перспективна технологія бездротового зв'язку, яка має потенціал для забезпечити вищу швидкість передачі даних, підвищити безпеку та енергоефективність. Незважаючи на те, що вона все ще перебуває на ранніх стадіях розвитку, Li-Fi має багато потенційних застосувань у різних галузях. Однак вона також має свої обмеження, такі як обмежений радіус дії та висока вартість. Оскільки технологія Li-Fi продовжує розвиватися, буде цікаво подивитися, як вона розвивається і як вона може бути інтегрована в наше повсякденне життя. З постійними дослідженнями і розробками в цій галузі та розробки в цій галузі, Li-Fi має потенціал, щоб змінити правила гри у світі бездротового зв'язку. у світі бездротового зв'язку.

Список використаних джерел

1. What is LiFi? Everything You Need to Know. LiFi.co. URL: <https://www.lifi.co/what-is-lifi/>

УДК 004.056.5

*Сушко Р. М., магістрант,
Пірог О. В., к.т.н., доцент
Державний університет «Житомирська політехніка»*

ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ПРИСТРОЇВ НА БАЗІ ОС ANDROID

За даними аналітичної компанії DataReportal, у 2022 році кількість користувачів смартфонів на ОС Android у світі склала понад 3 мільярди [1]. Водночас, за статистикою ESET, кіберзагрози для Android зростають щорічно на 20-25%. Тому питання забезпечення кібербезпеки пристроїв на Android є надзвичайно актуальним [2].

Метою даного дослідження є аналіз основних загроз кібербезпеці Android пристроїв та розробка рекомендацій щодо захисту від них.

Аналіз найбільш поширених джерел загроз виявив, що:

- За статистикою G DATA, найпоширеніший Android вірус GhostCtrl заразив понад 100 000 пристроїв. Його мета – крадіжка облікових даних жертв.

- У 2019 році виявлено понад 1500 шкідливих додатків у Google Play, які використовували для викрадення грошей користувачів.

Способами захисту, що рекомендовані, є:

- За результатами тестів AV-TEST у 2020 році, найкращі показники захисту від загроз продемонстрували антивіруси ESET та Avira.

- Дослідження показали, що шифрування AES з ключем 256 біт є оптимальним для захисту даних на Android пристроях [3].

Рекомендації користувачам щодо захисту кінцевих точок:

- Фахівці радять використовувати складні паролі довжиною не менше 10 символів для захисту пристроїв.

- Регулярне оновлення ПЗ та сканування системи дозволяє своєчасно виявляти уразливості й загрози безпеці [4].

Потрібно використовувати вбудовані засоби захисту:

- У Android 8.0 впроваджено механізм Google Play Protect для перевірки додатків на наявність вірусів та загроз.

- Шифрування даних в Android можна ввімкнути в налаштуваннях безпеки, встановивши PIN код або пароль.

- Блокування екрану, шифрування даних за допомогою протоколів AES, TLS, SSL.

– Пісочниця та ізоляція підозрілих додатків в окремому середовищі.

– Налаштування дозволів додаткам, обмеження доступу до функцій пристрою.

– Такі технології, як рандомізація розміщення адресного простору (ASLR), заборона виконання (NX), ProPolice, safe iop, OpenBSD dlmalloc і callocLinux mmap min addr для зменшення ризиків, пов'язаних із типовими помилками керування пам'яттю.

– Використання VPN для шифрування трафіку. Фільтрація з'єднань через брандмауер.

– Вбудовані засоби перевірки додатків на наявність вірусів [2].

Таким чином, проблема кібербезпеки мобільних пристроїв на Android є надзвичайно актуальною в сучасних умовах. Кількість загроз, таких як банківські трояни і фішингові додатки, неспинно зростає.

Поєднання сучасних антивірусних програм, VPN-захисту, надійного шифрування і регулярного оновлення ПЗ є оптимальним комплексним рішенням для кіберзахисту Android пристроїв.

Важливо також дотримуватися розроблених рекомендацій щодо кібергігієни та безпечної роботи з мобільними додатками. Систематичне використання вбудованих засобів захисту Android істотно підвищує загальний рівень безпеки.

Перспективним є подальший розвиток комплексних систем кіберзахисту з використанням новітніх технологій.

Список використаних джерел

1. Кількість користувачів смартфонів у світі з 2016 по 2021 рр. URL: <https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/>
2. McAfee. Mobile Threat Report 2020 – Santa Clara, CA: McAfee Corp., 2020. – 43 p.
3. Symantec. Internet Security Threat Report – Mountain View, CA: Symantec Corp., 2019. – 58 p.
4. Trend Micro. Стан постійних змін: Щорічний звіт Trend Micro про кібербезпеку 2020 – Даллас, TX: Trend Micro Inc., 2020. – 102 с.
5. Shostack A. Threat Modeling: Designing for Security / A. Shostack, M. Green. – Wiley, 2014. – 624 p.

УДК 004.056

*Ковальчук І. В., магістрант,
Бродський Ю. Б., к.т.н., доцент
Державний університет «Житомирська політехніка»*

МІЖМЕРЕЖЕВИЙ ЕКРАН НОВОГО ПОКОЛІННЯ PALO ALTO NETWORKS ЯК НОВИЙ ПІДХІД ДО ЗАХИСТУ КОРПОРАТИВНИХ МЕРЕЖ ОРГАНІЗАЦІЙ

Сучасний світ демонструє стрімкий розвиток цифрових технологій, і ця трансформація допомагає підняти ефективність бізнесу та поліпшувати якість життя громадян. Однак, разом з вигодами цифрового віку приходять і нові загрози. Кіберзагрози стали невід'ємною частиною нашого інформаційного життя, і організації повинні бути готові захищати свої корпоративні мережі від кіберзлочинців, які постійно вдосконалюють свої методи. У цьому контексті міжмережвий екран нового покоління Palo Alto Networks виявляється як інноваційний підхід до захисту корпоративних мереж, який надає нові можливості та інструменти для кібербезпеки.

З розвитком кібербезпеки корпоративних мережі стають все більш вразливими перед надходженням різних кіберзагроз. Від вірусів та шкідливих програм до складних атак типу «нульового дня», організації повинні впроваджувати заходи для захисту своїх мереж від цих загроз. Популярні атаки, такі як DDoS, фішинг та витоки даних [1], стають все поширенішими та деструктивними. Тому необхідно розглядати більш розвинуті та комплексні засоби для захисту.

Традиційні методи захисту мереж включають в себе брандмауери, антивіруси та виявлення інструкцій, але вони мають свої обмеження [2]. Загрози стають все більш винахідливими та важкими для виявлення, що ускладнює завдання забезпечення кібербезпеки.

Palo Alto Networks представляє інтегрований підхід до безпеки, зосереджуючись на виявленні та запобіганні загрозам, що робить його об'єктом інтересу для дослідників і спеціалістів у галузі інформаційної безпеки. Його інтегрована система забезпечує розширений аналіз трафіку, а також використовує технології машинного навчання для виявлення загроз. Palo Alto Networks дозволяє організаціям активно реагувати на атаки в реальному часі, що робить його важливим інструментом для кіберзахисту.

В доповіді буде представлений аналіз та оцінка міжмережевого екрана нового покоління від Palo Alto Networks [3], а також приведені результати дослідження технічних характеристик, функціоналу та

інновацій, які пропонує Palo Alto Networks, та оцінювання і перевірка ефективності застосування міжмережевого екрану в реальних умовах функціонування корпоративної мережі.

Результати дослідження показують, що міжмережевий екран Palo Alto Networks є ефективним інструментом для захисту корпоративних мереж від кіберзагроз. Він надає інтегровані засоби виявлення та запобігання атакам, а також забезпечує більшу видимість та контроль в мережі. Результати дослідження мають важливе практичне значення для організацій, які прагнуть забезпечити надійний захист своїх корпоративних мереж.

Отримані результати відкривають широкий простір для подальших досліджень у галузі мережевої безпеки та використання продуктів Palo Alto Networks, як інноваційного інструмента для забезпечення безпеки корпоративних мереж та захисту конфіденційної інформації.

Список використаних джерел

1. Smith J. (2020). Сучасні виклики мережевої безпеки в корпоративних мережах. Журнал інформаційної безпеки, 15(2), 45-62.
2. Doe A. (2019). Огляд інноваційних технологій Palo Alto Networks. Конференція з інформаційної безпеки, презентація.
3. Palo Alto Networks. (2022). Документація та технічна специфікація продукту. Доступно на сайті виробника: <https://www.paloaltonetworks.com/products/firewalls>.

УДК 004.77

Герус В. А., ст. викладач

Національний університет водного господарства та природокористування

ХАКЕРСЬКІ УГРУПУВАННЯ

У всесвітньому кіберпросторі існує таємничий та нестабільний світ хакерських угруповань, які, наче тіні, переслідують власну мету та інтереси. Вони є віртуозами в галузі комп'ютерної безпеки, порушуючи закони та залишаючи за собою сліди хаосу та руйнування. У цій статті ми розглянемо хакерські угруповання як феномен сучасного інтернет-суспільства, розгадаємо їх мотивацію, методи та вплив на сучасний світовий ландшафт інформаційної безпеки. Від таємничих колективів, які виходять на світло лише під час великих кібератак, до постійно активних груп, які підірвали традиційні уявлення про безпеку.

Кіберзлочинці активно шукають способи застосування нейромереж в атаках. Штучний інтелект допомагає зловмисникам підтримувати ілюзію осмисленого діалогу з жертвою, генерувати переконливі фішингові листи, створювати дипфейки голосів, зображень та відео. Ми можемо тільки прогнозувати зростання кількості атак з використанням нейромереж, які поступово поповнюють арсенал зловмисників. Кіберзлочинці не лише прагнуть обійти цензуру ChatGPT на створення шкідливого контенту, а й створюють власні набори інструментів. Наприклад, WormGPT – генеративна нейромережа для проведення фішингових та ВЕС-атак – створена зловмисниками на основі мовної моделі JPT-J з відкритим вихідним кодом спеціально для незаконної діяльності.

Хакерські угруповання залишаються невід'ємною частиною динамічної кіберпросторової реальності. Спробуємо перерахувати їх, вказавши альтернативні назви та цілі:

APT31 – група, відома з 2016 року; їй приписують атаки на організації Франції, США, уряду Норвегії, Фінляндії, Німеччини.

Альтернативні назви: JudgmentPanda, Zirconium, APT 31, TEMP.Avengers, BronzeVinewood.

Атаковані галузі: Фінансовий сектор, Авіаційно-космічна промисловість, Телекомунікації, Будівництво, Дослідницькі компанії, Неурядові організації, Медіа.

APT32. Кібершпигунська група APT32 активна щонайменше з 2012 року. Націлена на урядові, громадські та торговельні організації країн Східної та Південно-Східної Азії. Має різнобічний інструментарій, що постійно змінюється.

Альтернативні назви: OceanLotus, APT-C-00, CobaltKitty, SeaLotus, OceanBuffalo, TinWoodlawn, SectorF01, PondLoach

Атаковані галузі: Військово-промисловий комплекс, Державний сектор, Фінансовий сектор, Промисловий сектор, Телекомунікації, Медіа.

BronzeUnion – APT- угруповання, активне як мінімум з 2010 року. На думку різних дослідників, має китайське походження. Широко використовує для початкового проникнення техніки «атаки на водопій» (wateringhole), зокрема зараження веб-сайтів, відвідуваних жертвами, а також фішинг та вразливість мережевих сервісів. Група спеціалізується на кібершпиунстві, переважно в мережах державних установ, оборонних підприємств та політичних організацій. У 2020 році деякі дослідники (включно зі спеціалістами PT ExpertSecurityCenter) припустили появу у групи фінансової мотивації.

Альтернативні назви: LuckyMouse, EmissaryPanda, APT27, IronTiger, TG-3390, TEMP.Hippo, Group 35, ZipToken

Атаковані галузі: Державний сектор, Промисловий сектор, Інформаційні технології, Авіаційно-космічна промисловість, Освіта, Військово-промисловий комплекс, Медіа, Аналітичні центри.

Calypso. Вперше активність групи Calypso була виявлена фахівцями PT ExpertSecurityCenter у березні 2019 року під час робіт з виявлення кіберзагроз. Група активна як мінімум із вересня 2016 року. Основною метою групи є крадіжка конфіденційних даних, основні жертви – державні установи Бразилії, Індії, Казахстану, Росії, Таїланду, Туреччини.

Атаковані галузі: Державний сектор.

ChamelGang. У другому кварталі 2021 року Експертний центр безпеки PositiveTechnologies (PTESC) виявив діяльність невідомої раніше групи. Група була названа ChamelGang (від Chameleon) за вміння ефективно маскувати свою діяльність та оминати засоби захисту. Жертви цієї групи перебувають у світі навіть у Росії, де група скомпрометувала енергетичну організацію та організацію з авіаційно-промислового сектора.

Атаковані галузі: Державний сектор, Фінансовий сектор, Енергетика, Авіаційно-космічна промисловість, Телекомунікації.

Cobalt. Кіберзлочинна група Cobalt існує з 2016 року і атакує організації кредитно-фінансової сфери з метою крадіжки коштів через зламвання банкоматів, картковий процесинг, різні платіжні системи (SWIFT, АРМ КБР). Імовірно, деякі її учасники були членами групи Carbanak, яка існувала раніше. За оцінками ФінЦЕРТ, збитки від атак групи Cobalt у Росії в 2017 році перевищили 1 млрд рублів. Після

арешту одного з лідерів групи у 2018 році група продовжила свою активність. Один із гучних зломів, до яких була причетна група, – зламування системи швидких платежів Unistream.

Альтернативні назви: CobaltGang, CobaltSpider

Атаковані галузі: Фінансовий сектор

CozyDuke. Група CozyDuke – добре оснащена, організована та віддана своїй справі кібершпигунська група. На думку дослідників, група є російськомовною і існує щонайменше з 2008 року. Влада США інкримінує групі кібератаки на Білий Дім США, Держдепартамент США та Національний комітет Демократичної партії США.

Альтернативні назви: APT 29, TheDukes, Group 100, Yttrium, IronHemlock, Minidionis

Атаковані галузі: Державний сектор, Промисловий сектор, Телекомунікації, Освіта, Військово-промисловий комплекс, Дослідницькі компанії, Неурядові організації, Фармацевтика.

FancyBear – імовірно російськомовна група, що спеціалізується на шпигунстві. Група активна щонайменше з 2004 року. Має багатий інструментарій, що постійно змінюється.

Атаковані галузі: Державний сектор, Фінансовий сектор, Промисловий сектор, Інформаційні технології, Освіта, Військово-промисловий комплекс, Дослідницькі компанії, Неурядові організації, Медіа, Охорона здоров'я.

GoblinPanda вперше виявлена в 2013 році дослідниками з CrowdStrike і вважається групою, яка діє на користь Китаю. Група зосереджена на шпигунстві та має у своєму арсеналі ВПО здатне комунікувати у закритих мережах. У результаті аналізу ВПО було виявлено, що група має перетину з інструментами групи Calypso.

Альтернативні назви: Cycldek, Hellsing, Conimes

Атаковані галузі: Державний сектор

Higaisa. Кібершпигунський гурт Higaisa активний як мінімум з 2009 року. Націлена на державні, громадські та торгові організації у Північній Кореї. У списку атакованих країн також є Китай, Польща, Росія, Японія.

Атаковані галузі: Державний сектор.

Lazarus. Lazarus – АРТ-група, яку дослідники пов'язують з урядом Північної Кореї. Найбільш відома за шифрувальником WannaCry, від якого постраждали понад 150 країн, і злому SonyPictures. Група активна принаймні з 2009 року, організовує широкомасштабні кампанії кібершпигунства, операції із застосуванням програм-шифрувальників, а також атаки на криптовалютний ринок.

Альтернативні назви: Hidden cobra, Zinc, GuardiansofPeace, Group 77, Office 91, RedDot, Temp. -APT-15, NewRomanicCyberArmyTeam, Appleworm, SectorA01, ITG03

Атаковані галузі: Державний сектор, Фінансовий сектор, Інформаційні технології, Авіаційно-космічна промисловість, Військово-промисловий комплекс, Медіа, Фармацевтика, Охорона здоров'я, Криптовалютні біржі, Дослідники в галузі кібербезпеки.

RTM (ReadTheManual). Кіберзлочинна група RTM розпочала свою активність у 2015 році та атакує організації з різних галузей з метою крадіжки коштів з рахунків, крадіжки конфіденційних документів, облікових записів. Група використовує шкідливе ПЗ (ВПО) власної розробки. ВПО групи немає статичного контрольного сервера: воно отримує його через блокчейн.

Атаковані галузі: Державний сектор, Фінансовий сектор, Енергетика, Промисловий сектор, Інформаційні технології.

Silence. Кіберзлочинна група Silence з'явилася у 2016 році та атакувала організації кредитно-фінансової сфери, переважно в Росії. Метою групи є крадіжка коштів через зламані банкомати, картковий процесинг, АРМ КБР. З 2018 року група розширила географію атак та стала атакувати організації по всьому світу. У деяких атаках група використовувала інструменти групи TA505, що може говорити про їхню кооперацію. *Атаковані галузі:* Фінансовий сектор.

SpacePirates. Вперше угруповання SpacePirates було помічене фахівцями PT ExpertSecurityCenter наприкінці 2019 року під час робіт з виявлення кіберзагроз. Активна як мінімум із 2017 року. Основними цілями зловмисників є шпигунство та крадіжка конфіденційної інформації. Угруповання активно атакує різні галузі Росії. Крім цього, було виявлено жертви в Грузії, Узбекистані, Монголії, Китаї та Сербії.

Атаковані галузі: Фінансовий сектор, Інформаційні технології, Авіаційно-космічна промисловість, Освіта, Військово-промисловий комплекс, Охорона здоров'я, Сільське господарство, Паливно-енергетичний комплекс, Електроенергетика, Державні установи.

TA505. Одна з найнебезпечніших та найактивніших злочинних кібергруп, що діє більш ніж у 60 країнах. Основна мета групи – крадіжка або вимагання коштів.

Альтернативні назви: EvilCorp, ATK 103, SectorJ04, Hive0065, GRACEFUL SPIDER, GOLD TAHOE, Dudear, CHIMBORAZO.

Атаковані галузі: Фінансовий сектор, Державний сектор, Енергетика, Авіаційно-космічна промисловість, Дослідницькі компанії, Фармацевтика.

TaskMasters. Кібершпигунське угруповання TaskMasters виявлено у 2018 році фахівцями PT ExpertSecurityCenter. Група активна щонайменше з 2010 року. Серед атакованих організацій – великі промислові та енергетичні підприємства, державні структури, транспортні компанії. Угруповання атакує компанії з різних країн, але більшість жертв перебувають у Росії та країнах СНД.

Альтернативні назви: BlueTraveller.

Атаковані галузі: Державний сектор, Енергетика, Промисловий сектор, Транспортні компанії.

Turla – відома група кібершпигунства, що має величезну кількість інструментів, яка понад десять років пов'язана з операціями проти різних організацій по всьому світу. Особливістю групи є розробка своїх власних унікальних сучасних шкідливих програм та інструментів, а також нових методів атак та обфускації.

Альтернативні назви: Waterbug, WhiteBear, VenomousBear, Group 88, Snake, SIG23, IronHunter, Krypton, Pacifier APT

Атаковані галузі: Державний сектор, Енергетика, Освіта, Військово-промисловий комплекс, Дослідницькі компанії, Неурядові організації, Фармацевтика.

Winnti. Група активна з 2012 року, походить з Китаю і належить до класу спонсорованих урядом. Ключові інтереси – це шпигунство та отримання фінансової вигоди. Основний арсенал групи складається із власне розробленого ВПО. Winnti використовує складні методи атак серед яких supply-chain і wateringhole. Група точно знає хто їхня жертва, вона дуже обережно розвиває атаку і лише після детального аналізу зараженої системи завантажує основний інструментарій. Атакує країни по всьому світу: Білорусь, Бразилію, Німеччину, Індію, Монголію, Росію, США, Південну Корею, Японію ін.

Альтернативні назви: APT41, AXIOM, BARIUM, LEAD, BlackFly.

Атаковані галузі: Державний та Фінансовий сектор, Енергетика, Ігрова індустрія, Розробка ПЗ, Авіаційно-космічна промисловість, Телекомунікації, Будівництво, Освіта, Фармацевтика.

Загалом, ситуація з хакерськими угрупованнями вимагає постійної уваги та стратегічного підходу до кібербезпеки. Завдяки спільним зусиллям ми можемо забезпечити безпеку та захист в інтернет-середовищі, де інформація стає все більш цінним ресурсом, а загрози – більш вдосконаленими та складними.

Нові технології, такі як штучний інтелект та блокчейн, також можуть виконувати важливу роль у покращенні кібербезпеки. Штучний інтелект може виявляти та відповідати на загрози в реальному часі, а блокчейн може забезпечити додатковий рівень захисту даних.

Секція 3 ІНФОРМАЦІЙНІ СИСТЕМИ ТА ТЕХНОЛОГІЇ

УДК 004.4

Мельник Р. І., магістрант

Державний університет «Житомирська політехніка»

АВТОМАТИЗОВАНЕ ТЕСТУВАННЯ ТА ЯКІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ: РОЗРОБКА МЕТОДІВ ДЛЯ ВИЯВЛЕННЯ ТА УСУНЕННЯ ПОМИЛОК В ПРОГРАМАХ

Актуальність та постановка проблеми. В сучасному цифровому світі програмне забезпечення використовується майже у всіх аспектах нашого життя. Якість програмного забезпечення стала критично важливою, оскільки недоліки в програмах можуть призвести до серйозних наслідків, включаючи витрати на виправлення помилок, втрати даних та негативний вплив на користувачів. Автоматизоване тестування є ефективним інструментом для виявлення та усунення помилок в програмах. У цій статті розглядаються методи та підходи до автоматизованого тестування, спрямовані на покращення якості програмного забезпечення.

Основні матеріали дослідження. Автоматизоване тестування – це процес виконання тестів на програмному продукті з використанням автоматизованих інструментів і сценаріїв. Це дозволяє автоматично перевіряти функціональність, продуктивність та стійкість програмного забезпечення. Основні складові автоматизованого тестування включають створення тестових сценаріїв, виконання тестів та аналіз результатів.

Вибір відповідних тестових інструментів і мов програмування є важливим кроком у розробці автоматизованих тестів. Різні інструменти можуть бути придатними для різних типів тестів, включаючи функціональне, інтеграційне, навантажувальне тестування та інше. Мови програмування, такі як Python, Java та JavaScript, широко використовуються для написання автоматизованих тестів.

Створення ефективних тестових сценаріїв є важливою частиною автоматизованого тестування. Тестові сценарії визначають послідовність дій, які слід виконати для перевірки конкретної функціональності програми. Вони повинні бути детально спроектовані та відповідати специфікаціям програми.

Після створення тестових сценаріїв тести виконуються автоматично. Результати тестів записуються та аналізуються, щоб виявити помилки і недоліки. Важливо відслідковувати і реєструвати всі виявлені проблеми для подальшого усунення.

Однак автоматизоване тестування також вносить свої виклики та проблеми, які потребують уваги і розв'язання. Розробка та підтримка автоматизованих тестів може вимагати значних витрат ресурсів, часу та грошей. Необхідно створювати тестові сценарії, а також підтримувати їх оновлення у відповідності до змін в програмі. Автоматизоване тестування графічних інтерфейсів може бути важким завданням через їхню динамічність і різноманітність. Інструменти для автоматизованого тестування інтерфейсів повинні бути добре адаптовані до різних платформ і браузерів. Програмне забезпечення постійно розвивається, і це вимагає постійного оновлення тестових сценаріїв. Нові функції, зміни в інтерфейсі та архітектурі можуть вплинути на ефективність тестування. Тестування асинхронних та розподілених систем вимагає специфічних підходів та інструментів, оскільки вони взаємодіють з багатьма компонентами і можуть мати складну логіку обміну даними. Важливо забезпечити належне покриття всіх аспектів програмного забезпечення тестами. Недостатнє покриття може призвести до недоліків, які не будуть виявлені під час тестування. Впровадження автоматизованого тестування може потребувати зміни в культурі розробки. Розробники повинні бути готові до співпраці з командою тестування та враховувати тестові вимоги на кожному етапі розробки.

Висновки. Автоматизоване тестування важливе для забезпечення якості програмного забезпечення. Ця методика дозволяє ефективно виявляти і усувати помилки, зменшувати ризик витрат та негативного впливу на користувачів. Незважаючи на виклики, пов'язані з впровадженням автоматизованого тестування, його переваги більш ніж компенсують ці труднощі.

Список використаних джерел

1. Автоматизоване тестування. [Електронний ресурс]. Режим доступу: <https://qalight.ua/baza-znaniy/avtomatizovane-testuvannya/>
2. Авраменко А.С. Тестування програмного забезпечення. [Навчальний посібник]. Черкаси, 2017.
3. Сегеда Н. Є. Якість програмного забезпечення та тестування. [Навчальний посібник]. 2014.
4. Основи QA [Електронний ресурс]. Режим доступу: <https://lemon.school/blog/osnovy-qa>

УДК 004:42

*Стельмах А. О., здобувач,
Левківський В. Л., ст. викладач
Державний університет «Житомирська політехніка»*

АЛГОРИТМИ ВЗАЄМОДІЇ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

У сучасному світі інформаційні системи стають ключовим елементом в різних сферах, зокрема медицині, науці, бізнесі та технологіях. Зростання обсягу та різноманітності інформації вимагає постійного вдосконалення алгоритмів взаємодії для забезпечення ефективного та безпечного використання цієї інформації.

Аналіз потреб в інформаційних системах містить вивчення структури та формату даних, визначення вимог до обробки, передачі та збереження інформації. Досліджуються аспекти ефективності, зручності використання та безпеки для користувачів.

Розробка алгоритмів взаємодії в інформаційних системах – це комплексний процес, спрямований на створення ефективних та оптимальних механізмів для взаємодії між користувачами та системою. Основна мета полягає в поліпшенні обробки інформації, забезпеченні високої точності обчислень та максимальної швидкості доступу до потрібних даних.

Оцінка різних аспектів включає аналіз та вдосконалення інтерфейсу користувача, зробленого з урахуванням зручності та інтуїтивності. Також вивчається питання забезпечення конфіденційності інформації, зокрема розробка механізмів шифрування та заходів безпеки для запобігання несанкціонованому доступу.

Окрема увага приділяється можливостям інтеграції з іншими інформаційними системами, що дозволяє створювати єдиний та злагоджений інформаційний простір. Це важливо для забезпечення спільної роботи різних систем та обміну даними без проблем та затримок.

Такий підхід дозволяє створювати високоефективні та сучасні інформаційні системи, які відповідають сучасним вимогам швидкості, точності та безпеки обробки даних.

Впровадження розроблених алгоритмів – це багатоетапний процес, який включає не лише саму інтеграцію алгоритмів, але й комплексне тестування їхньої ефективності та стійкості в реальних умовах використання (рис. 1). Основною метою цього етапу є перевірка того,

що розроблені алгоритми працюють ефективно, надійно та безперерійно під час реального функціонування системи.



Рис. 1. Схема процесу впровадження алгоритму

Під час тестування важливо розглянути різні сценарії використання, щоб забезпечити високу адаптивність алгоритмів до різних умов та ситуацій. Це містить різноманітні сценарії обробки даних, взаємодії з користувачем, обробки великих обсягів інформації тощо. Тестування повинно також враховувати можливі внутрішні та зовнішні фактори, які можуть впливати на роботу системи.

У процесі вдосконалення алгоритмів взаємодії в інформаційних системах важливо також враховувати розвиток технологій та потреби користувачів, які стрімко змінюються. Нові можливості та інновації вносять свої власні виклики та можливості в області обробки та обміну інформацією.

Отже, постійне удосконалення алгоритмів взаємодії в інформаційних системах визначає ефективність та безпеку використання інформації. Аналіз, розробка та впровадження цих алгоритмів дозволяють створювати сучасні системи, які відповідають високим стандартам точності, швидкості та безпеки обробки даних, сприяючи розвитку різних галузей життя.

Список використаних джерел

1. Сухий О.Л., Міленін В.М., Тарадайнік В.М. (2015). Алгоритми пошуку в інформаційних системах: Методичні рекомендації. Київ. Retrieved from <https://lib.iitta.gov.ua/704951/1/>

УДК 004

*Граф М. С., Ph.D,
Райковський В. А., здобувач
Державний університет «Житомирська політехніка»*

АЛГОРИТМИ ОПТИМІЗАЦІЇ ДАНИХ

В наш час потоки даних стрімко зростають, їх стає забагато для послідовного аналізу та обробки. Великі корпорації, компанії та підприємства стикаються з безперервними потоком інформації, яка потребує обробки, класифікації та аналізу, виокремлення важливих даних та сортування їх, саме завдяки таким процесам виникає необхідність у розробці нових та покращених вже існуючих алгоритмів оптимізації даних. Над проблемою обробки великих масивів даних працюють сотні тисяч науковців, адже останнє десятиліття ця проблема актуальна як ніколи, і з кожним роком актуальність проблеми тільки збільшується.

Існує велика кількість алгоритмів оптимізації даних основа яких була закладена природою – це так звані метаевристичні алгоритми – мурашині алгоритми оптимізації. Такі алгоритми ґрунтуються подібно тому, як у природі мурахи хаотично нишпорять шукаючи їжу, а досягнувши бажаного повертаються до мурашника (колонії) разом з тим прокладаючи слід з феромонів по своєму маршруту. Інші члени колонії знайшовши залишений із феромонів слід починають рухатися тим же маршрутом. Загалом, коли мурашка знаходить найкоротший маршрут від їжі до колонії, то інші мурахи у переважній більшості дотримуватимуться цього маршруту. Ідея полягає в імітації руху умовних мурашок найвигіднішим маршрутом.

В розглянутому алгоритмі мураха є нічим іншим, як об'єктом, що рухається задля пошуку найкращого рішення поставленої проблеми. Для використання мурашиного алгоритму на практиці задачу потрібно звести до задачі пошуку кращого маршруту на зваженому графі. Така задача буде розв'язуватися у n -кількість ітерацій, кожна з яких міститиме декілька кроків: першим кроком мураха випадковим чином обирає порядок проходження ребер графу, якого слід дотримуватися; другим кроком здійснюється порівняння, аналіз маршрутів що пройшли різні члени колонії; третім кроком здійснюється оновлення значущості феромонів в кожній точці, на кожному ребрі.

Доцільно пояснити алгоритм на прикладі задачі комівояжера. Задача передбачає пошук найкращого кільцевого маршруту що пролягає через усі задані міста один раз. Для рішення задачі

використовується не лише одна мураха, а кілька мурах паралельно, кожна мураха відповідає за визначену ітерацію пошуку, тобто намагається знайти оптимальний маршрут.

Необхідно враховувати такі особливості: під час руху маршрутом мураха відкладає феромони, умовно на ребрі графу, об'єм феромону є обернено пропорційним до довжини шляху комівояжера між містами, що відповідають вершинам умовного графу. Щоб запобігти передчасній збіжності алгоритму існує випаровування феромону. Час випаровування є важливим фактором, адже досить велике, або навпаки, маленьке значення провидить до збою роботи алгоритму.

Перехід між містами залежить від: переліку пройдених міст, видимості та феромону. Розглянемо математично: мураці k необхідно подолати маршрут довжиною L_{ij} між містами i та j відповідно, з урахуванням видимості η_{ij} .

Варто зазначити що наявність на ребрі феромону підкріплює необхідність мурахи перейти між містами i та j . Феромоновий слід з ітераціями змінюється відповідно до набутого мурахами досвіду. Кількість феромону на поточному ребрі $i - j$ позначимо σ_{ij} . Ймовірність переходу мурахи між містами i та j визначається у вигляді пропорції:

$$\begin{cases} P_{ij}^k(t) = \frac{[\sigma_{ij}(t)]^\alpha [\eta_{ij}]^\beta}{\sum_{l \in J_i^k} [\sigma_{il}(t)]^\alpha [\eta_{il}]^\beta}, & \text{якщо } j \in J_i^k \\ P_{ij}^k(t) = 0, & \text{якщо } j \notin J_i^k, \end{cases}$$

де $P_{ij}^k(t)$ – ймовірність переходу мурахи k між містами i та j на ітерації t .

α та β – введені параметри що відображають силу феромону.

Приведений алгоритм має досить широке застосування в різних сферах, зокрема і в спорті. Якщо розглядати застосування мурашиного алгоритму на практиці, наприклад у футбольній сфері, то перше, що можна зауважити, ще те що запропонований алгоритм може забезпечити оптимізацію стратегії гри футбольного клубу шляхом аналізу стратегії суперників, особливостей захисту та нападу, складу команди та заявлених на гру гравців.

Список використаних джерел

1. Dorigo, M., Maniezzo, V., Colomi, A., The Ant System: Optimization by a Colony of Cooperating Agents, IEEE Trans. Systems, Man Cybernetics, Part B, 1996, том 26, вип.1, с. 29–41.

УДК 621.3: 455.63

*Паламарчук М. П., магістрант,
Граф М. С., Ph.D,
Колос К. Р., д.пед.н., професор*

Державний університет «Житомирська політехніка»

АЛГОРИТМИ СИНХРОНІЗАЦІЇ ПРОЦЕСІВ В ОНЛАЙН ГРІ

У сучасних он-лайн іграх синхронізація процесів є одним з найважливіших аспектів. Вона впливає не тільки на плавність ігрового процесу, а і на загальні враження гравців. Якщо для покровових стратегій синхронізація є чимось другорядним, то для шутерів, навпаки – перетворюється на визначальний фактор. В таких іграх кожен момент стає критичним і найменші затримки можуть вирішально вплинути на результат взаємодії гравців, визначити перемогу чи поразку. Саме тому вдосконалення синхронізації є важливим аспектом при створенні якісних он-лайн ігор. Метою дослідження є аналіз основних алгоритмів і підходів до синхронізації процесів в он-лайн грі.

Найбільша проблема при синхронізації процесів в он-лайн іграх – це час, затрачений на передачу даних. При цьому не завжди є доступ до швидкого та надійного мережевого з'єднання. Щоб компенсувати різницю у часі між сервером та гравцями, використовують обчислювальні потужності гаджетів та різноманітні алгоритми синхронізації процесів. Завдяки цьому, можна скинути частину навантаження з мережі на процесор. Це можна зробити за допомогою таких методів:

- **Застосування алгоритмів стиснення даних:** дозволяє зменшити розмір даних без втрати інформації. Однак цей варіант підходить лише для великих об'ємів інформації, адже час на кодування та розшифрування при невеликій кількості даних може навіть негативно вплинути на розмір даних та витратити час на обробку, що тільки сповільнить передачу [2].

- **Використання шаблонів, заготовок, словників тощо:** будь-яку інформацію, що часто використовується, можна скоротити. Це дещо схоже на алгоритми стиснення даних, але використовується лише для конкретної інформації, замінюючи довгі рядки короткою позначкою. Наприклад, ігровий простір можна розбити на квадрати, додавши кожному буквену позначку. І вже семизначна координата перетворюється на одну букву з двома-трьома цифрами, що змінились. Назви предметів замінити на унікальний номер, при передачі даних.

- **Використання алгоритмів передбачення стану об'єктів:** дозволяє зменшити кількість даних, що передаються, оскільки не завжди необхідно передавати повний стан об'єкта. Наприклад, можна передбачати напрямок руху персонажа на основі його попереднього стану, що дозволить промалювати дії гравця без жодної затримки [1].

- **Оптимізація та фільтрування інформації, що надсилається:**

- Ігнорування незначних змін в стані об'єктів.

Наприклад, персонаж змінює нахил камери на 1 градус. Такі зміни навіть візуально непомітні для інших гравців і їх не обов'язково передавати на сервер. Також можна проігнорувати анімації та події, що не несуть в собі певної інформації для інших гравців.

- Періодична синхронізація стану об'єктів.

Наприклад, персонаж горить і здоров'я гравця поступово падає. Серверу не обов'язково фіксувати кожну одиницю здоров'я гравця, ще й надсилати іншим.

- Паралельна обробка інформації.

Сервер може розподілити обчислювання інформації не тільки між ядрами своїх процесорів, а й змусити гравців самостійно обраховувати події. Повертаючись до попереднього прикладу, сервер може отримати та надіслати лише факт початку події горіння, при цьому кожен гравець самостійно обрахує падіння здоров'я конкретного персонажа, а в кінці сервер тільки перевірить коректність результату.

- Відправляти лише ту інформацію, яка стосується гравця.

На масштабній ігровій локації гравець бачить лише невелику частину, тому недоцільно відправляти йому усе що відбувається в кожному кутку гри.

Отже, оптимізація синхронізації в он-лайн іграх через використання алгоритмів і технік, що переносять частину навантаження з мережі на процесори, може значно поліпшити ігровий досвід, забезпечуючи ефективну взаємодію гравців при обмежених ресурсах мережі.

Список використаних джерел

1. Ferretti S., Rocetti M., Palazzi C. E. An Optimistic Obsolescence-Based Approach to Event Synchronization for Massively Multiplayer Online Games. *International Journal of Computers and Applications*. 2007. Vol. 29, no. 1. P. 33–43. URL: <https://doi.org/10.1080/1206212x.2007.11441830>.

2. Gregory J., Peters A. *Game Engine Architecture*. CRC Press, 2009. 1240 p. URL: <https://doi.org/10.1201/b10681>.

УДК 004:42

*Москалик О.С., магістрант,
Левківський В. Л., ст. викладач
Колос К.Р., д.пед.н, професор*

Державний університет «Житомирська політехніка»

АНАЛІЗ АЛГОРИТМІВ МАШИННОГО НАВЧАННЯ

У сучасному світі машинне навчання стало невід’ємною частиною нашого життя, воно відіграє важливу роль завдяки своєму широкому застосуванню і потужному впливу на різні сфери діяльності.

Алгоритми машинного навчання натреновані знаходити взаємозв’язки та закономірності в даних. Термін «машинне навчання» часто помилково плутають з поняттям «штучний інтелект» (ШІ), але машинне навчання насправді є підгалуззю ШІ. Термін «машинне навчання», введений американським вченим Артуром Семюелом у 1959 році, визначається як «здатність комп’ютера навчатися без явного програмування» [1].

На табл. 1 відображено наявні алгоритми та їх характеристику у машинному навчанні.

Таблиця 1

Алгоритми машинного навчання

Навчання під наглядом	Навчання без нагляду	Напівкероване навчання	Навчання з підкріпленням
Datascientists забезпечують вхідні, вихідні дані та зворотній зв’язок для побудови моделі (за визначенням) <i>Приклади алгоритмів:</i> - <i>лінійна регресія;</i> - <i>опорні вектори</i> - <i>дерево рішень</i>	Використовує глибоке навчання для отримання висновків і закономірностей на основі немаркованих навчальних даних	Створює модель на основі поєднання маркованих і немаркованих даних, набору категорій, пропозицій і прикладів міток.	Самоінтерпретована, але заснована на системі заохочень і покарань, отриманих шляхом спроб і помилок, з метою отримання максимальної винагороди

У навчанні під наглядом (supervised learning) машина навчається на прикладах. Оператор надає алгоритму машинного навчання відомий набір даних, який включає бажані вхідні та вихідні дані, а алгоритм повинен знайти метод, щоб визначити, як отримати ці вхідні

та вихідні дані. У той час, як оператор знає правильні відповіді на завдання, алгоритм виявляє закономірності в даних, вчиться на основі спостережень і робить прогнози. Алгоритм робить прогнози і коригується оператором, цей процес триває доти, доки алгоритм не досягне високого рівня точності або продуктивності [2].

Напівкероване навчання (semi-supervised) схоже на кероване навчання, але замість цього використовує як мічені, так і немічені дані. Марковані дані – це інформація, яка має значущі теги, щоб алгоритм міг зрозуміти дані, тоді як не марковані дані не мають такої інформації. Використовуючи цю комбінацію алгоритми машинного навчання можуть навчитися маркувати немарковані дані [3].

Алгоритм некерованого навчання вивчає дані для виявлення закономірностей. Тут немає ключа для відповідей, або людини-оператора, яка б давала вказівки. Замість цього машина визначає кореляції та взаємозв'язки, аналізуючи наявні дані. Алгоритм намагається організувати ці дані певним чином, щоб описати їхню структуру.

Навчання з підкріпленням фокусується на регламентованих процесах навчання, де алгоритм машинного навчання забезпечується набором дій, параметрів і кінцевих значень. Визначивши правила, алгоритм машинного навчання намагається дослідити різні варіанти та можливості, відстежуючи та оцінюючи кожен результат, щоб визначити, який з них є оптимальним. На відміну від інших алгоритмів, навчання з підкріпленням вчить машину методом проб і помилок. Вона вчиться на минулому досвіді і починає адаптувати свій підхід у відповідь на ситуацію, щоб досягти найкращого результату [3].

Отже, аналіз показав, що у кожного з цих алгоритмів є свої переваги та недоліки і вибір залежить від поставленої задачі та наявних даних. Зазвичай важливо правильно підібрати тип навчання для конкретного завдання, оскільки це може суттєво вплинути на результати та ефективність моделі машинного навчання.

Список використаних джерел

1. Tucci L., Burns E. What is Machine Learning and How Does It Work? In-Depth Guide. Enterprise AI. URL: <https://shorturl.at/vDEI6>. (date of access: 25.10.2023).

2. Wakefield K. A guide to the types of machine learning algorithms. URL: <https://shorturl.at/dwCL9>.

3. Wong W. StackPath. StackPath. URL: <https://www.electronicdesign.com/markets/automotive/article/21804976/whats-the-difference-between-machine-learning-techniques>.

УДК 621.3: 455.63

*Єфремов Ю. М., к.т.н., доцент
Павлішин М.С., магістрант*

Державний університет «Житомирська політехніка»

АНАЛІЗ ПРИЧИН ВИКОРИСТАННЯ МІКРОСЕРВІСНОЇ АРХІТЕКТУРИ В СУЧАСНИХ ПРОГРАМНИХ РІШЕННЯХ

У минулому, на початку 2000-х років, інженери компанії Amazon відзначали повільним темпом розгортання нового коду, що було далеко від сучасної середньої швидкості розгортання, яка становить приблизно 11,7 секунди. Для виконання цього завдання Amazon використовував спеціальний інженерний підрозділ, який здійснював ручне розміщення нових версій програмного забезпечення в виробничому середовищі компанії.

Що стало причиною таких змін? Amazon перейшов до більш гнучких методів розробки програмного забезпечення і впровадив архітектуру мікросервісів. В наші дні Amazon – це сукупність автономних сервісів, які майже не мають між собою сильних зв'язків або прямих залежностей і керуються командами «двох піщ». Кожна з таких команд складається з 6-8 інженерів, які мають повний контроль над одним або двома мікросервісами (окремими функціональними частинами програми). Гнучкі команди відповідають за усі аспекти життєвого циклу продукту, включаючи збір вимог, планування функціональності, проектування, розробку, тестування, розгортання та подальшу підтримку. Саме таким чином Amazon виконує до 50 мільйонів розгортань програмного забезпечення щорічно.

Архітектура мікросервісів, або ж просто мікросервіси, – це спосіб організації розробки програмного забезпечення, при якому програми структуруються як незалежні автономні сервіси. Інакше кажучи, великі та складні продукти розбиваються на невеликі окремі міні-додатки, які відповідають за конкретні бізнес-функції, такі як входи в соціальних мережах або корзина для електронної комерції. Мікросервіси можуть бути слабко зв'язаними і розгортатися незалежно один від одного, що дозволяє змінювати один сервіс, не впливаючи на інші.

Основна ідея архітектури мікросервісів (MSA) полягає у створенні незалежних програмних компонентів, які ефективно вирішують окремі завдання. Кожен мікросервіс має чітко визначену мету, таку як відстеження історії доставки або обробка платежів. При розробці

мікросервісів слід керуватися бізнес-процесами, а не горизонтальними шарами, такими як обмін повідомленнями або доступ до даних.

Кожен мікросервіс має власну межу, яка визначається контекстом домену, де він функціонує. Проте визначення відповідних меж для кожного мікросервісу може бути викликом, і тут важливим стає дизайн, орієнтований на домен (DDD). Основною ідеєю DDD є розробка архітектури, яка гармонійно поєднує всі бізнес-процеси та варіанти використання з відповідними артефактами коду. Це дозволяє створювати оптимальну архітектуру програмного забезпечення:

- Аналіз домену;
- Визначення обмеженого контексту;
- Визначення сутностей, агрегатів та сервісів;
- Визначення конкретних мікросервісів.

Використання методології проектування, орієнтованої на домен, має багато переваг. Ваше програмне забезпечення буде оптимально пристосоване до потреб конкретного домену, а не обмежене лише вимогами, такими як дружність інтерфейсу користувача. Ви отримуватимете продукт, який враховує потреби цього домену.

Зрозуміло, що архітектура мікросервісів надає великим компаніям гнучкість і можливість використовувати нові технології для задоволення зростаючих потреб клієнтів. Однак для успішного впровадження цієї архітектури потрібно величезне зусилля в рефакторингу та переформатуванні старих монолітних систем зі складними залежностями. Для підтримки нової архітектури також необхідна висококваліфікована команда DevOps, яка забезпечить правильну оркестрацію, автоматизацію процесів та впровадження моделі безперервної доставки.

Список використаних джерел

1. Важливість впровадження мікросервісної архітектури для побудови сучасних легко розширюваних програмних рішень. [Електронний ресурс]. Режим доступу: <https://www.infopulse.com/blog/the-importance-of-microservices-architecture-for-modern-applications>.

2. Архітектура мікросервісів: Початковий посібник. [Електронний ресурс]. Режим доступу: <https://www.infopulse.com/blog/the-importance-of-microservices-architecture-for-modern-applications>.

УДК 621.3: 455.63

*Єфремов Ю. М., к.т.н., доцент,
Павлішин М.С., магістрант
Державний університет «Житомирська політехніка»*

АНАЛІЗ ТЕНДЕНЦІЙ РОЗВИТКУ РИНКУ МУЗИЧНИХ СТРІМІНГОВИХ СЕРВІСІВ

Проаналізовано перспективи та тенденції розвитку музичних стрімінгових платформ. Дано характеристику головним представникам ринку та проаналізовано чинники зростання їх популярності.

У 2021 році світовий ринок потокового передавання музики оцінювався в 29,45 мільярдів доларів США, і очікується, що з 2022 до 2030 року він зростатиме на 14,7% у середньому на рік. Зростання проникнення цифрових платформ і використання інтелектуальних пристроїв є очікується прискорення зростання ринку протягом прогнозованого періоду. Платформи, які дозволяють користувачам слухати аудіо та підкасти та дивитися музичні відео, є прикладами сервісів потокової передачі музики. Ці платформи набувають популярності завдяки таким функціям, як рекомендації пісень, автоматична персоналізація списку відтворення та безпроблемне підключення до програм і браузерів. Крім того, розширення жанрів підкастів на цих порталах сприяє зростанню ринку.

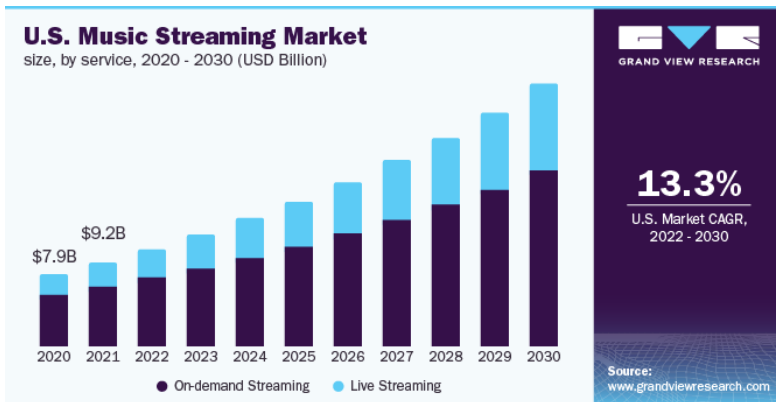


Рис. 1. Діаграма прогнозованого зростання ринку музичних стрімінгових платформ

У 2020 році спалах COVID-19 спонукав більшість країн запровадити карантинні заходи, щоб запобігти поширенню вірусу. Це призвело до збільшення кількості передплатників на музичних потокових платформах, таких як Spotify, Tencent Music Entertainment і Amazon Music. Більше того, кількість передплатників, які беруть участь у прямих трансляціях на таких платформах, як Instagram та YouTube, спостерігала сплеск.

Очікується, що сегмент прямих трансляцій зареєструє найвищий CAGR у 16,0% з 2022 по 2030 рік. Потенціал прямих трансляцій для охоплення більшої аудиторії є основним фактором, що стимулює цей сегмент. Пряма трансляція – це процес доставки живого вмісту окремим особам через Інтернет у режимі реального часу. Окрім служб, спеціально розроблених для прямих трансляцій, кілька соціальних мереж також підтримують прямі відео. Зростаюча популярність живих відео спонукає музикантів вести прямі трансляції на таких сайтах, як YouTube Live, Facebook, Instagram і Twitter Periscope. Очікується, що ця тенденція продовжить розвивати сегмент протягом прогнозованого періоду.

Послуги потокового передавання музики дозволяють доставляти музичний і відеоконтент через Інтернет без необхідності традиційного мовлення чи кабельних програвачів. Ці послуги надаються в програмах і браузерах на кишенькових пристроях споживачів, таких як планшети, смартфони та ноутбуки. Крім того, очікується, що глобальне розгортання інтернет-з'єднань 5G спричинить попит на технології потокового передавання, які можуть забезпечити користувачам безперервний досвід прослуховування без необхідності завантажувати файли на особисті пристрої.

Список використаних джерел

1. Розмір ринку потокового передавання музики, частка та звіт про аналіз тенденцій за послугами [grandviewresearch.com](https://www.grandviewresearch.com) [Електронний ресурс]. <https://www.grandviewresearch.com/industry-analysis/music-streaming-market>
2. Тенденції зростання музичного потокового ринку платформ, коротка аналітика музичного ринку [researchandmarkets](https://www.researchandmarkets.com/reports/5595773/music-streaming-market-size-share-and-trends) [Електронний ресурс]. <https://www.researchandmarkets.com/reports/5595773/music-streaming-market-size-share-and-trends>
3. Список найкращих тенденцій потокового передавання музики, на які варто звернути увагу у 2023 році [Dataart](https://www.dataart.com/blog/music-streaming-trends-for-2020) [Електронний ресурс]. <https://www.dataart.com/blog/music-streaming-trends-for-2020>

УДК 004.5: 004.92

Марчук Г. В., ст. викладач,

Дяченко В. В., здобувач

Державний університет «Житомирська політехніка»

ВАЖЛИВІСТЬ ВІЗУАЛЬНОЇ ЧАСТИНИ ІГОР

Ігри вже давно входять в наше життя, і одним із їх ключових аспектів є візуальна частина. Вона відповідає за гарний інтерфейс, відмінні ефекти та, як результат, допомагає створити неймовірні й захоплюючі світи.

Візуальний стиль з'єднує усі компоненти, що бачить гравець: персонажів, ігровий світ, анімацію, інтерфейс та меню. Вони повинні бути як ідентичними, так і унікальними, щоб додаток був впізнаний лише по шматочку інтерфейсу. У той же час, потрібно розуміти, що різні типи ігор вимагають унікального підходу до створення світу, та різного типу дизайну. Тому що графіка визначає емоційний вплив на гравця та відображає сутність гри.

Залежно від жанру, обирається найкращий стиль, що передасть не тільки атмосферу, але і головну думку всього проекту. У 2D іграх вони бувають абсолютно різні: художні (картунстичні), піксельні, сітчасті або скелетні. Для жанру Метроїдванія добре підходить піксельний стиль, що зазвичай намальовано від руки.

Піксельний стиль – це вид графіки, де зображення створюються шляхом розміщення пікселів на растровій сітці. Даний стиль може бути дуже привабливим для багатьох гравців, проте потрібно пам'ятати, що він не підходить для всіх ігор та аудиторій.

Коли визначилися зі стилем, наступним важливим питанням є GUI (Game User Interface), або графічний інтерфейс користувача. Це спосіб взаємодії з комп'ютерною програмою за допомогою графічних об'єктів, таких як кнопки, панелі, вікна, меню та інші візуальні елементи. Створення інтерфейсу гри – це завдання технічного художника, який працює комплексно і одночасно враховує ергономіку, логіку, стилістику, не забуваючи про UI (User Interface) в рамках інших аспектів сприйняття. Проектування інтерфейсів для ігор передбачає виділення одного екрану для кожного завдання. Розробники уникають «приховування» інших функцій, оскільки це призводить до значних ризиків непорозуміння. Чітке визначення «одного завдання» також створює труднощі, оскільки практично будь-який процес включає кілька етапів. Важливо організувати простір екрану так, щоб геймер міг інтуїтивно використовувати інтерфейс гри, розуміючи призначення

кожного елемента. Також він має бути актуальним, тобто ефективним і придатним до використання в поточному контексті. Це стосується усіх типів інтерфейсів: дієгетичного та мета-інтерфейсу (тобто HUD і меню).

Меню гри – це усім знайомий набір UI елементів, що зустрічають користувача при кожному запуску додатку, або паузі. Воно включає у себе контроль рівнями, налаштування, статистику і багато іншого. HUD (Heads-UpDisplay) в свою чергу надає усі інші, дійсно необхідні, дані для проходження гри. Стан гравця: життя, броня, енергія, монети, досвід тощо. Також міні-карта або радар, який допомагає гравцеві орієнтуватися в світі. Інформацію про «швидкий інвентар» та амуніцію. Годинник, таймери або інші дані про час у грі.

При правильному використанні усі частини GUI допомагає покращити геймплей та надає гравцю засоби для прийняття рішень.

Іншим важливим елементом графіки є Particle System (система частинок). Потужний інструмент у гральному движку Unity, який дозволяє створювати різноманітні ефекти: дим, вогонь, воду, сніг, вибухи, і багато інших. Вони додають реалізм і красу, дозволяючи створювати рухомі, живі ефекти відповідно до потреб. Також це дозволяє зображати ефекти, які зазвичай важко відтворити за допомогою мешів або спрайтів, оскільки вони часто представляють собою явища, які є рідкими та нематеріальними за своєю природою.

Математично Particle Systems базуються на рівняннях фізики та обчисленнях для кожної частинки в системі. Наприклад, вираховуються параметри, які визначають швидкість, рух і розсіювання, також можуть включати в себе обробку зіткнень та інші фізичні явища для створення реалістичних ефектів. Хоча Unity і не використовує конкретні фізичні формули для моделювання в системах частинок, але двигун має різні алгоритми та методи для досягнення бажаних візуальних результатів. Реалістичність та поведінка частинок визначаються на основі налаштувань і параметрів, які встановлюються у графічному інтерфейсі Unity.

Більшість ефектів створюються шляхом накладання кількох компонентів один на одного. Дані компоненти в іграх зазвичай пов'язані з технічними аспектами гри, і тому вкрай важливо постійно тестувати та вдосконалювати їх. У процесі створення ефектів необхідно нерідко змінювати параметри, такі як часові інтервали, масштаб та швидкість, щоб досягнути оптимального вигляду, коли ефект відтворюється.

Звісно ж робота з частинками та освітленням у 2D відрізняється від 3D. І щодо освітлення воно може бути використано у Particle

Systems, проте зазвичай, базується на інших системах. Існує декілька типів джерел світла:

- Global Illumination (Глобальне освітлення): складний підхід, який включає обчислення освітлення в реальному часі. Створює красиві ефекти, але вимагає багато ресурсів.

- Матеріали та Shader: шейдери також підтримують ефекти, такі як тіні, відбитки світла і багато інших.

- Масштабування. Unity дозволяє змінювати масштаб освітлення, щоб зробити об'єкти світлішими або темнішими.

- Тіні. Unity підтримує 2D тіні що додають глибину та реалізм в ігровий світ.

- Маски шарів. дозволяють керувати тим, як світло взаємодіє з об'єктами.

- Візуальні ефекти. Unity має багато готових візуальних ефектів, які можна використовувати для покращення освітлення в грі. Це може включати блискавки, світлофори, полум'я та інші ефекти.

Не дивлячись на усі можливості надані двигуном, важливо визначити, який рівень освітлення підходить для конкретного проекту, і налаштувати його відповідно до вашого бажаного візуального стилю і рівню продуктивності.

Окрім освітлення та тіні також існує додатковий спосіб створення візуального ефекту руху в просторі – паралакс. Він виникає через різницю у швидкості руху або перспективі об'єктів, і використовується для створення візуального вираження глибини в графіці. При використанні даного прийому сцени стають більш живими та менш монотонними. Існує два основних типи паралаксу:

- Паралакс проксимальності (Parallax Scrolling). Цей ефект використовується у 2D іграх. Фонові шари рухаються з різною швидкістю в залежності від їх відстані до глядача. Це дозволяє створити враження, що об'єкти рухаються один відносно одного.

- Паралакс при виведенні (Parallax Mapping). Цей ефект використовується в 3D-графіці для створення реалістичних текстур та рельєфу на поверхнях об'єктів. Він враховує точки світла і тіні, створюючи ілюзію виступаючих деталей.

Список використаних джерел

1. Сегол Р. І., Дегтярьова Є. О., Шевчук Г. О. (2022). Роль редактора у підготовці комп'ютерних ігор. Оптимізація дизайну. 1(11), 110-130. Retrieved from

https://ela.kpi.ua/bitstream/123456789/51120/1/OD_1%281%29_2022_p110-130.pdf

УДК 621.3: 455.63

Коваленко Я. П., магістрант

Державний університет «Житомирська політехніка»

ВИБІР АРХІТЕКТУРИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Архітектура програмного забезпечення системи або набору систем складається з усіх важливих проектних рішень з приводу структур програми і взаємодій між цими структурами, які складають системи.

Проектні рішення забезпечують бажаний набір властивостей, які повинна підтримувати система, щоб бути успішною. Проектні рішення надають концептуальну основу для розробки системи, її підтримки і обслуговування.

Як ми бачимо, вибір архітектури ПО, що розробляється, визначається завданнями, поставленими перед розробниками, функціональними і експлуатаційними вимогами.

З точки зору кількості користувачів, що працюють з однією копією ПО, розрізняють:

- розраховану на одного користувача архітектуру;
- розраховану (мережеву) на багато користувачів архітектуру.

Крім того, у рамках розрахованої на одного користувача архітектури розрізняють:

- програми. Програма (program, routine) – впорядкована послідовність формалізованих інструкцій для вирішення завдання за допомогою комп'ютера. Це найпростіший вид архітектури, який зазвичай використовується при рішенні невеликих завдань;

- пакети програм. Пакети програм є декількома окремими програмами, вирішальними завдання певної прикладної області. Наприклад: пакет графічних програм, та пакет математичних програм.

Пакет програм реалізується як набір окремих програм, кожна з яких сама вводить необхідні дані і виводить результати, т. е. програми пакету пов'язані між собою тільки приналежністю до деякої прикладної області;

- програмні комплекси. Програмні комплекси є сукупністю програм, що спільно забезпечують рішення невеликого класу складних завдань однієї прикладної області. При цьому для виконання деякого завдання програмним диспетчером послідовно викликаються декілька програм з програмного комплексу. Оскільки декілька програм для вирішення одного завдання працюють з одними і тими ж початковими даними і проміжними результатами, бажано зберігати ці дані і

результати викликів в оперативній пам'яті або у файлах в межах одного призначеного для користувача проєкту.

Програми комплексу можуть компілюватися як самостійні одиниці або спільно. Програма-диспетчер може мати примітивний інтерфейс і просту довідкову систему;

- програмні системи. Програмні системи є організованою сукупністю програм (підсистем), що дозволяє вирішувати широкий спектр завдань з деякої прикладної області.

Програми, що входять в програмну систему, взаємодіють через загальні дані. Програмні системи мають досить розвинений інтерфейс, що вимагає їх ретельного проєктування і розробки.

Розраховану на багато користувачів архітектуру реалізують системи, побудовані за принципом «клієнт – сервер». Також є основні класи архітектури програмних засобів.

Розрізняють наступні основні класи архітектури програмних засобів:

- цілісна програма;
- комплекс автономно виконуваних програм;
- шарувата програмна система;
- колектив паралельно виконуваних програм.

Цілісна програма представляє вроджений випадок архітектури ПС: до її складу ПС входить тільки одна програма. Таку архітектуру вибирають зазвичай у тому випадку, коли ПС повинна виконувати одну будь-яку яскраво виражену функцію, та її реалізація не представляється занадто складною.

Природно, що така архітектура не вимагає будь-якого опису (окрім фіксації класу архітектури), оскільки відображення зовнішніх функцій на цю програму тривіально, а визначати спосіб взаємодії не вимагається (через відсутність зовнішньої взаємодії програми, окрім як взаємодії її з користувачем, де останнє описується в документації по застосуванню ПС).

Список використаних джерел

1. Іващук В.В. Курс лекцій «Засоби мультимедіа в нових інформаційних технологіях» Національний університет харчових технологій: НУХТ. 2011. С.77.

2. Проць О.А., Данилюк Т.Б. Автоматизація неперервних технологічних процесів. Навчальний посібник для технічних спеціальностей вищих навчальних закладів. Тернопіль: ТДТУ ім. І.Пулюя. 2008. С.239.

УДК 004.78

*Кадькало В. В., магістрант,
Чижмотря О. В., ст. викладач,
Кузьменко О. В., ст. викладач*

Державний університет «Житомирська політехніка»

ВИКОРИСТАННЯ МЕТОДІВ МАШИННОГО НАВЧАННЯ ДЛЯ АНАЛІЗУ ФІНАНСОВИХ РИНКІВ

На сьогоднішній день, використання методів штучного інтелекту для аналізу інформації, зокрема машинного навчання, відкриває перед спеціалістами небачені раніше можливості. Завдяки здатності швидко обробляти великі масиви інформації, а також робити достатньо точні припущення на основі побудованих моделей, використання штучного інтелекту може доповнити роботу спеціалістів або навіть перевершити результати роботи людини.

Інструменти які надає нам штучний інтелект знаходять своє застосування у багатьох галузях людської діяльності. Так, наприклад, в медицині штучний інтелект застосовується в діагностуванні захворювань і дозволяє лікарям швидше і точніше ставити діагнози пацієнтам. У сільському господарстві штучний інтелект часто використовується для аналізу ґрунтів, прогнозування врожайності і навіть для створення сільськогосподарської техніки що не потребує керування людиною. Сфери його застосування не обмежуються наведеними прикладами, системи штучного інтелекту мають величезний потенціал у найрізноманітніших галузях.

Аналіз фінансових ринків є однією з таких сфер людської діяльності, де використання штучного інтелекту успішно застосовується і має великий потенціал для подальших розробок. За допомогою методів машинного навчання спеціалісти можуть аналізувати історичні дані та будувати моделі, що будуть передбачати майбутні ціни на ті чи інші фінансові інструменти. В багатьох випадках прогнози, отримані за допомогою моделей машинного навчання, можуть бути навіть ефективніші, ніж прогнози надані аналітиками.

Серед методів машинного навчання, що широко використовуються в аналізі фінансових ринків, можна виділити штучні нейронні мережі, метод опорних векторів та дерева рішень. Штучні нейронні мережі – це моделі побудовані на основі спостережень структури людського мозку. Метод опорних векторів та дерева рішень – це алгоритми, які однаково добре виконують завдання як регресії, так і класифікації, і

можуть бути використані для визначення ринкових тенденцій. Згадані методи, як і багато інших можуть, застосовуватись як окремо так і в поєднанні один з одним.

Моделі, побудовані за допомогою машинного навчання, можуть здійснювати аналіз біржових настроїв – обробку різноманітних даних таких як новини, дописи в соціальних мережах, публікації на тематичних сайтах з метою виявити динаміку зміни інтересу до того чи іншого фінансового інструменту. Такі моделі можуть здійснювати оптимізацію інвестиційного портфелю, тобто проводити аналіз ефективності активів з метою урівноваження ризиків та створення збалансованого інвестиційного рішення. Також можливе здійснення корекції існуючих торгових стратегій за допомогою навчання з підкріпленням. Також є можливим використання методів машинного навчання для побудови алгоритмічних торгових стратегій, де рішення про купівлю або продаж активу приймається безпосередньо програмою на основі прогнозу наданого моделлю.

На відміну від класичних алгоритмічних торгових стратегій, у яких правила, за якими програма здійснює торгові операції, описує людина за допомогою тієї чи іншої мови програмування, стратегії реалізовані завдяки методам машинного навчання самі знаходять закономірності при аналізі зміни цін, та використовують їх для побудови прогнозів, або навіть здатні самі змінювати свою стратегію з огляду на зміни динаміки цін. Такі рішення часто можуть знаходити приховані закономірності які людина помітити не в змозі, в зв'язку з цим торгові програми в яких використані методи машинного навчання в багатьох випадках якісніше аналізують ринкову інформацію ніж програми які написані з використанням класичного підходу.

Велика кількість вже реалізованих таким чином програмних продуктів підтверджує успішність використання методів машинного навчання для аналізу ринкової інформації. Одними із таких продуктів є інвестиційна платформа "Robinhood", яка надає користувачам персоналізовані рекомендації щодо інвестицій та хедж-фонд "Numerai", який аналізує ринкову інформацію та приймає рішення, щодо інвестування, покладаючись на прогнози надані штучним інтелектом.

Таким чином використання методів штучного інтелекту для аналізу фінансових ринків має надзвичайно великий потенціал, надаючи фахівцям нові інструменти що можуть вивести їх ефективність на новий рівень та завдяки цьому значно збільшити прибутки.

УДК 004.92

*Штиль М.Р., здобувач,
Фуріхата Д.В., ст. викладач
Державний університет «Житомирська політехніка»*

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ AIUPSCALING У ВІДЕОІГРАХ

Протягом існування ігрової індустрії спостерігається постійна тенденція на покращення графіки у відеоіграх. До недавнього часу цей тренд розвивався у тандемі з розвитком апаратного забезпечення. Наразі швидкість розвитку відеокарт уповільнюється через ряд невітшних причин, а ціни на сучасні моделі зростають, так як ці пристрої також отримали застосування у сфері штучного інтелекту.

Враховуючи наведені вище причини, виробники відеокарт обрали інший шлях підвищення продуктивності, а саме – покращення програмної частини. Одним із найкращих методів збереження продуктивності відеочіпу було зменшення роздільної здатності рендеру. З метою збільшення продуктивності та водночас збереження якості зображення вони почали використовувати технології масштабування за допомогою штучного інтелекту (AI upscaling) у драйверах відеокарт.

Масштабування (upscaling) [1] – перетворення зображень із нижчою роздільною здатністю на вищу. Масштабування за допомоги штучного інтелекту (aiupscaling) це процес, який використовує алгоритми машинного навчання для покращення роздільної здатності та якості зображень із дуже високою швидкістю роботи та кращою точністю.

Традиційне масштабування починається із зображення низької роздільної здатності та намагається покращити його візуальну якість при вищій роздільності. Розширення штучного інтелекту використовує інший підхід: враховуючи зображення з низькою роздільною здатністю, модель глибокого навчання передбачає зображення з високою роздільною здатністю, яке буде зменшуватися, щоб виглядати як оригінальне зображення з низькою роздільною здатністю.

Щоб прогнозувати масштабовані зображення з високою точністю, модель нейронної мережі має бути навчена на великій кількості зображень. Потім розгорнута модель AI може знімати відео з низькою роздільною здатністю та створювати неймовірну різкість і покращені деталі, які не може відтворити жоден традиційний алгоритм масштабування. Краї виглядають гострішими, волосся – чітким, а пейзажі зберігають свої деталі.

Найпотужнішою нішею для масштабування зображення – стали відеоігри. Найвідомішими технологіями масштабування стали **Deep Learning Super Sampling (DLSS)** [2] від **NVIDIA** та **FidelityFX Super Resolution (FSR)** [3] від **AMD**. Обидві ці технології спрямовані на покращення візуальних ефектів гри, зберігаючи високу продуктивність і частоту кадрів, але вони роблять це за допомогою різних підходів. DLSS використовує потужні графічні процесори NVIDIA та алгоритми глибокого навчання для високоякісних зображень у реальному часі, надаючи геймерам чіткіші зображення без шкоди для продуктивності. З іншого боку, FSR – це рішення з відкритим вихідним кодом, яке базується на техніці просторового масштабування та сумісне з більш широким спектром обладнання. Обидві технології мають свої плюси та мінуси, але ясно одне: масштабування III стає все більш важливим у світі ігрової графіки.



Рис. 1. Порівняння продуктивності гри без DLSS та з DLSS



Рис. 2. Порівняння продуктивності гри без FSR та з FSR

Пізніше до них додалась ще **Xe Super Sampling (XeSS)** [4] від **Intel**. За принципом роботи технологія Intel XeSS близька до Nvidia DLSS. Вона також базується на алгоритмах машинного навчання, але разом із цим може працювати на всіх більш-менш сучасних відеокартах. Щоправда, у разі графічних процесорів Intel Arc Alchemist її ефективність буде вищою, ніж на GPU конкурентів.



Рис. 3. Порівняння продуктивності гри без XeSS та з XeSS

Масштабування з використанням штучного інтелекту відзначається численними перевагами. Перш за все, цей підхід надає розробникам можливість продовжувати вдосконалювати графіку та технології у відеоіграх, не турбуючись про ефективність апаратної частини. Зменшення навантаження на апаратну інфраструктуру сприяє зниженню вартості відеокарт, зменшення енергоспоживання та збільшенню загального ресурсу їх експлуатації. Використання таких підходів також породжує певні проблеми. Розробники вкладають менше зусиль у оптимізацію своїх ігор та включають підтримку технологій масштабування у системні вимоги для зменшення витрат на розробку. Проте, найбільш суттєвим недоліком є уповільнення прогресу у розробці нового апаратного забезпечення.

Узагальнюючи, масштабування зображень із застосуванням штучного інтелекту у відеоіграх представляє собою ефективний метод для поліпшення продуктивності, при цьому не втрачаючи в якості графіки.

Список використаних джерел

1. Масштабування зображення [Електронний ресурс] – Режим доступу до ресурсу:

https://uk.wikipedia.org/wiki/Масштабування_зображення

2. NvidiaRTXDLSS[Електронний ресурс] – Режим доступу до ресурсу: <https://www.digitaltrends.com/computing/everything-you-need-to-know-about-nvidias-rtx-dlss-technology/>

3. AMD FidelityFX Super Resolution [Електронний ресурс] – Режим доступу до ресурсу: <https://www.digitaltrends.com/computing/what-is-amd-fidelityfx-super-resolution/>

4. XeSS Super Sampling[Електронний ресурс] – Режим доступу до ресурсу: <https://www.intel.com/content/www/us/en/products/docs/discrete-gpus/arc/technology/xess.html>

УДК 004.92

*Гайдай І. Я., здобувач,
Граф М. С., PhD*

Державний університет «Житомирська політехніка»

ВИКОРИСТАННЯ ФРЕЙМВОРКУ ANDROIDJETPACK ДЛЯ СПРОЩЕНОГО СТВОРЕННЯ МОБІЛЬНИХ ДОДАТКІВ

Фреймворк – інфраструктура програмних рішень, що полегшує розробку складних систем. Спрощено дану інфраструктуру можна вважати своєрідною комплексною бібліотекою, але при цьому вона має ряд обмежень, що задають правила створення структури проекту та написання коду.

Android Jetpack – це набір бібліотек та інструментів, які спрощують створення мобільних додатків, зменшувати шаблонний код на платформі Android. Jetpack включає в собі компоненти, які можна використовувати для вирішення різних, завдань.

Використання в розробці мобільних додатків

Перед тим як використовувати фреймворк треба розібрати переваги та недоліки (рис. 1).



Рис. 1. Переваги та недоліки Android Jetpack

Набір бібліотек і їх типи можна переглянути на рис. 2.

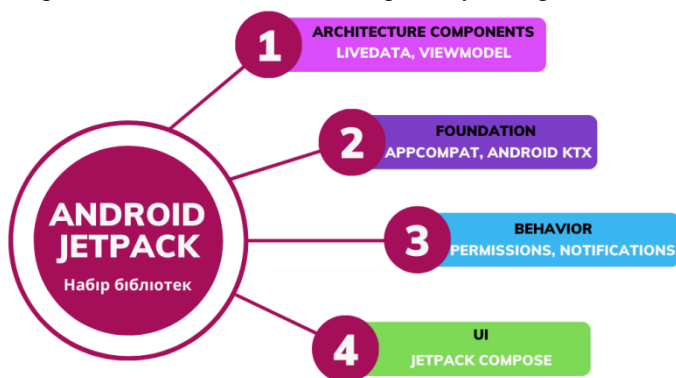


Рис. 2. Набір бібліотек

Набір бібліотек які містить фреймворк:

1. Foundation – базові бібліотеки, які допомагають зменшити бойлерплейт-код. Сюди входять AppCompat, Android KTX.

2. Architecture Components – це бібліотеки, що використовуються для побудови архітектури програми. Серед них LiveData, ViewModel.

3. Behavior – бібліотеки для функціональності, що надається Android SDK. Створені для покращення стандартного Android API: Permissions, Notifications.

4. UI – компоненти, що допомагають працювати з фрагментами, лейаутами та анімацією. Сюди входить Jetpack Compose.

Android Jetpack дозволяє розробникам писати більш стабільні та продуктивні додатки, спрощуючи та прискорює процес розробки, забезпечуючи кращу підтримку нових функцій Android. Він ідеально підходить для створення різноманітних додатків, від простих до складних. Однак, перш ніж починати використовувати Jetpack, необхідно уважно вивчити його основи та зрозуміти, як він працює.

Список використаних джерел

1. Android Developers. [Електронний ресурс] – Режим доступу до ресурсу: <https://developer.android.com/jetpack>

2. Stack Overflow. [Електронний ресурс] – Режим доступу до ресурсу: <https://stackoverflow.com/questions/50251658/what-exactly-is-android-jetpack>

УДК 621.3: 455.63

*Горопашин О.С., магістрант,
Колос К.Р., д.пед.н., професор
Державний університет «Житомирська політехніка»*

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ТА МАШИННОГО НАВЧАННЯ ДЛЯ ОПТИМІЗАЦІЇ МЕТОДІВ НАУКОВИХ ДОСЛІДЖЕНЬ

Використання технологій штучного інтелекту (ШІ) та машинного навчання (МН) в методах наукових досліджень пропонує революційну зміну парадигми, дозволяючи дослідникам розширювати, вдосконалювати та оптимізувати свої дослідницькі підходи [1].

Принципи використання ШІ та МН для оптимізації наукових досліджень:

- **Автоматизація та оптимізація:** ШІ та МН дозволяють автоматизувати рутинні процеси в наукових дослідженнях, підвищуючи ефективність та зменшуючи помилки;

- **Гнучкість та адаптивність:** ці технології дозволяють створювати адаптивні моделі, які пристосовуються до змін в даних або дослідницькому середовищі, підвищуючи точність та актуальність;

- **Прогнозування та прогнозування:** використання ШІ та МН допомагає будувати прогнозні моделі на основі даних, сприяючи передбаченню майбутніх результатів і тенденцій в дослідженнях;

- **Дослідження та відкриття:** Ці технології допомагають виявляти нові закономірності, зв'язки та ідеї в даних, сприяючи висуненню нових гіпотез і напрямків досліджень;

- **Системний і цілісний підхід:** впровадження ШІ та МН може допомогти розробити більш комплексні моделі, що враховують множинні фактори та взаємозв'язки;

- **Моніторинг та верифікація результатів:** вони дозволяють створювати системи для моніторингу та верифікації результатів досліджень, забезпечуючи об'єктивність і надійність наукових досліджень;

- **Постійне вдосконалення:** принцип постійного вдосконалення та розвитку моделей на основі отриманих результатів є важливим для підтримки актуальності та точності даних.

Ці принципи разом сприяють підвищенню якості, швидкості та об'єктивності наукових досліджень за рахунок використання ШІ та МН, тим самим розширюючи можливості для наукового прогресу.

Переваги використання ШІ та МН для оптимізації методів наукових досліджень:

1. **Покращена обробка даних:** ШІ і МН забезпечують швидку і ефективну обробку великих наборів даних, виявляючи складні закономірності та взаємозв'язки в даних, які можуть уникнути людського аналізу [2].

2. **Прогнозне моделювання:** використовуючи алгоритми МН, прогносні моделі на основі існуючих даних можуть передбачати потенційні результати та тенденції в наукових дослідженнях.

3. **Автоматизація процесів:** ці технології автоматизують повторювані дослідницькі завдання, такі як збір та аналіз даних, звільняючи час для вчених, щоб зосередитися на складних аналітичних аспектах.

4. **Покращена точність та швидкість:** ШІ і МН забезпечують більш точні та швидкі результати порівняно з традиційними методами, дозволяючи глибше зрозуміти складність даних.

5. **Об'єктивне прийняття рішень:** вони сприяють наданню об'єктивних даних, зменшуючи суб'єктивність у прийнятті рішень і забезпечуючи більш обґрунтовані та переконливі результати досліджень.

6. **Виявлення нових ідей:** використання цих технологій допомагає виявляти нові зв'язки і ідеї в даних, сприяючи інноваціям і розвитку нових гіпотез.

7. **Адаптивні структури:** застосування ШІ і МН дозволяє створювати адаптивні структури, які розвиваються разом з виникаючими шаблонами даних, сприяючи динамічним та ітеративним дослідницьким практикам.

8. **Ефективне використання ресурсів:** оптимізація дослідницьких методологій за допомогою ШІ і МН призводить до кращого використання ресурсів, економії часу та зусиль на аналіз даних та експериментування.

Отже, використання ШІ і МН в наукових дослідженнях оптимізує процеси, сприяє інноваціям і підвищує точність та ефективність дослідницьких пошуків.

Список використаних джерел

1. Пономаренко С.М., Слободянюк О.В. Штучний інтелект у наукових дослідженнях: можливості та перспективи. Вісник НТУУ КПІ «Інформатика, комп'ютерні системи та мережі». 2023. № 1. С. 19–28.

2. Пірс Д., Гетевей Е. Як штучний інтелект може допомогти освіті | «Освіторія». Освіторія Медіа. URL: <https://osvitoria.media/experience/yak-shtuchnyj-intelekt-mozhe-dopomogty-osviti/>

УДК 004.08

*Фуріхата Д.В., ст. викладач**Державний університет «Житомирська політехніка»***ГЕНЕРАТИВНІ МОДЕЛІ НЕЙРОННИХ МЕРЕЖ**

Генеративні моделі нейронних мереж здобувають все більше уваги у сучасному машинному навчанні, відзначаючись високою ефективністю у генерації нових даних. Ці моделі, засновані на глибоких нейромережах, пропонують новий підхід для вирішення завдань генерації відображень та побудови структури даних. Важливим аспектом вивчення генеративних моделей є розгляд теоретичних основ, а саме архітектури, на якій вони базуються. Серед найбільш поширеної архітектури виділяються варіаційні автокодекери (VAEs) та генеративні припущення adversarial networks (GANs).

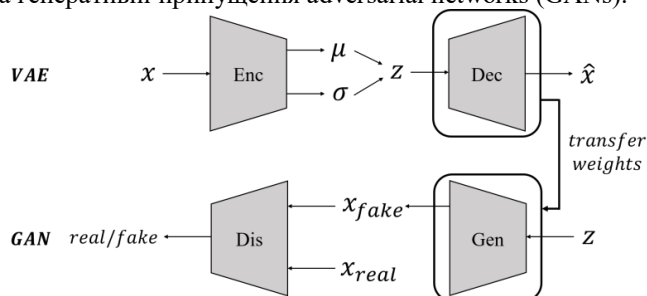


Рис. 1. Методи генеративних моделей

VAEs базуються на ідеї варіаційного байєсівського підходу, де нейромережа навчається генерувати розподіл у просторі можливих представлень. Вони використовують енкодер для перетворення вхідних даних у вектор з параметрами розподілу, а генератор використовує ці параметри для генерації нових екземплярів даних. Ця архітектура широко використовується в завданнях генерації обличчя, зображень та рукописного тексту. З іншого боку, GANs працюють на основі конкурентного навчання, де генератор та дискримінатор взаємодіють у процесі навчання. Генератор намагається максимізувати ймовірність того, що його згенеровані зразки будуть сприйняті дискримінатором як реальні, тоді як дискримінатор прагне правильно класифікувати між справжніми та синтетичними даними. Цей конкурентний підхід дозволяє GANs досягати вражаючої якості генерації, що призводить до широкого застосування в сучасних технологіях.

Генеративні моделі знайшли широкий спектр застосувань, включаючи генерацію зображень та тексту, що робить їх корисними в задачах створення вмісту для мультимедійних додатків. Порівняння з іншими методами генерації дозволяє оцінити їхню точність, різноманітність та здатність відтворення структури оригінальних даних.

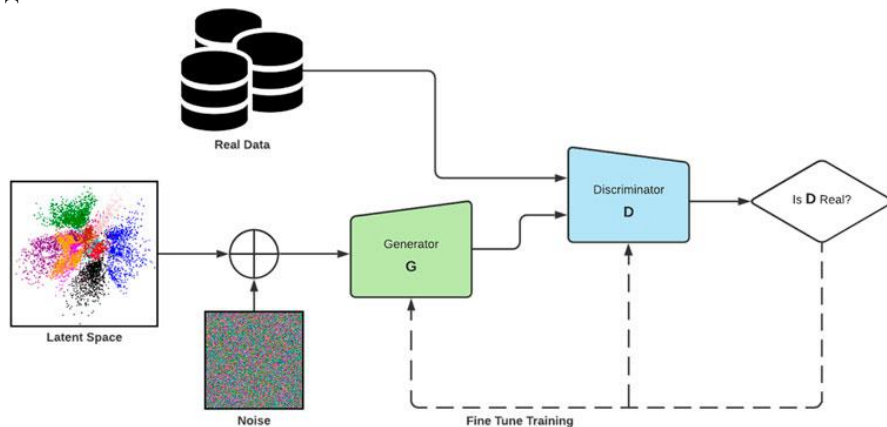


Рис. 2. Приклад GAN архітектури

Підсумовуючи, найбільш поширені генеративні моделі, такі як VAEs та GANs, стали основним інструментарієм у вивченні та розвитку сучасних методів генерації даних. Майбутні дослідження в напрямку розширення функціональності генеративних моделей та здатності їх адаптації до різних завдань мають продовжити розвиток цього захопливого напрямку машинного навчання.

Список використаних джерел

1. Hughes R. T., Zhu L., Bednarz T. (2021). Generative Adversarial Networks–Enabled Human–Artificial Intelligence Collaborative Applications for Creative and Design Industries: A Systematic Review of Current Approaches and Trends. *Frontiers in Artificial Intelligence and Image Processing*. Retrieved from: <https://www.frontiersin.org/articles/10.3389/frai.2021.604234/full>
2. Ham H., Jun T. J., Kim D. (2020). Unbalanced GANs: Pre-training the Generator of Generative Adversarial Network using Variational Autoencoder. *arXiv*. Retrieved from: <https://www.arxiv-vanity.com/papers/2002.02112/>

УДК 004.8

*Варганова Д. О., ст. викладач,
Кушнір Н. О., ст. викладач,
Москаль М.В., здобувач*

Державний університет «Житомирська політехніка»

ГЕНЕРАЦІЯ ЗОБРАЖЕНЬ ЗА ДОПОМОГОЮ ШТУЧНОГО ІНТЕЛЕКТУ

За допомогою зображень кожен із нас має можливість виразити та втілити свої фантастичні мрії. З розвитком технологій штучного інтелекту (ШІ) ми маємо можливість прослідкувати за їх досягненнями у різних сферах. Однією з них є генерація зображень за допомогою штучного інтелекту.

Розглянемо, що являють собою ШІ-генератори зображень. Це системи, які створюють унікальні зображення на основі вхідних параметрів і використовують машинне навчання на великих наборах зображень, щоби генерувати схожі за стилем та змістом зображення. Галузі застосування ШІ-генераторів зображень різні.

Розглянемо принципи роботи основних із них і відповідно здійснимо генерацію зображень.

1. Natural Language Processing(NLP)

Ця модель передбачає розуміння промптів користувача, перетворюючи їх на числові представлення за допомогою моделей обробки природної мови, таких як CLIP. Такий підхід дозволяє генераторам створювати зображення, які відповідають текстовим описам, шляхом інтерпретації тексту як навігаційної карти для створення композиційних і візуальних аспектів зображення.

2. Generative Adversarial Networks (GANs)

У такій моделі дві нейронні мережі змагаються поміж собою. Одна мережа є генератором та відповідає за створення зображень, тоді як друга мережа, розпізнавач, використовується для визначення того, чи є зображення справжніми, чи підробленими [1].

3. Diffusion Models

Така модель є найпопулярнішою моделлю, яка передбачає навчання ШІ на сотнях мільйонів зображень, кожне з яких має опис зображення словами, що б зрозуміти зв'язок між текстом і зображенням. Після навчання моделі вона може приймати текстові підказки від користувача, створюючи спочатку зображення з низькою роздільною здатністю, а потім поступово додавати нові деталі, щоби перетворити його на повноцінне зображення. Цей процес повторюється доти, доки не буде створено остаточне зображення з високою роздільною здатністю [2].

DIFFUSION MODELS

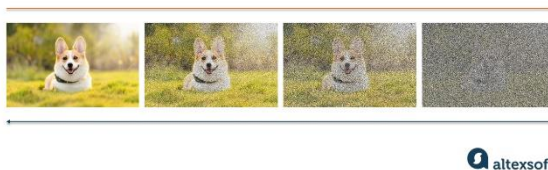


Рис. 1. Принцип роботи моделі дифузії

4. Neural Style Transfer (NST)

Це модель глибокого навчання, яка поєднує вміст одного зображення зі стилем іншого, щоби створити абсолютно новий витвір мистецтва. NST використовує попередньо навчену мережу для аналізу візуальних зображень, а після цього додаткові заходи, щоби запозичити стиль одного зображення і застосувати його до іншого. Таким чином створюється нове зображення, яке об'єднує стилі обох зображень.

NEURAL STYLE TRANSFER (NST)



Рис. 2. Принцип роботи моделі NST

Отже, генерація зображень за допомогою штучного інтелекту – це не просто технологічне досягнення, а інструмент, який відкриває шлях до безмежно широкого застосування у таких сферах, як медицина, мистецтво, дизайн, розробка ігор, кіноіндустрія та інші, спрощуючи роботу та допомагаючи людям досягти раніше недосяжних результатів за короткий проміжок часу.

Список використаних джерел

1. AI Image Generators: How They Work And Why They Are Important [Електронний ресурс] – Режим доступу до ресурсу: <https://www.hypotenuse.ai/blog/ai-image-generator>.
2. AI Image Generation Explained: Techniques, Applications, and Limitations [Електронний ресурс] – Режим доступу до ресурсу: <https://www.altexsoft.com/blog/ai-image-generation/>.

УДК 621.3: 455.63

*Вольних І. В., магістранта,
Концидайло А. М., аспірант
Державний університет «Житомирська політехніка»*

ГЕНЕРАЦІЯ ТЕСТОВИХ ДАНИХ ЗА ДОПОМОГОЮ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ RESTFULAPI

У сучасному світі ІТ індустрії активно розвивається використання штучного інтелекту для оптимізації розробки програмного забезпечення, а також процесів тестування. Саме завдяки ефективним технікам тест-дизайну та використанню можливостей генеративних моделей, а також машинному навчанню, ми можемо досягти високого рівня якості програмного забезпечення.

RESTful API є найбільш поширеним підходом для розробки програмного інтерфейсу сьогодення. Саме тому, забезпечення коректності та стійкості роботи таких застосунків є ключовим етапом у процесі розробки програм, оскільки вони виступають важливим інтерфейсом для взаємодії між різними компонентами системи а також між різними зовнішніми системами.

Ця робота присвячена вивченню та розробці методів генерації тестових даних для RESTful API для оптимального покриття тестових сценаріїв та скороченню ресурсів для ручного дизайну тестових даних. Тестові дані можуть бути використані у параметрах запитів API у тілі запиту або у параметрах шляху. Використання згенерованих та готових даних скорочує час на ручне заповнення тіла запиту і може бути корисне для розробників програмного забезпечення та тестувальників, сприяючи покращенню якості та швидкості розробки API-інтерфейсів та забезпеченню їхньої стабільності у різних умовах використання. Оскільки тестування API методів базується саме на використанні певного набору даних для отримання перевірки очікуваної відповіді сервера основні завдання роботи включають аналіз існуючих методів дизайну тестових даних, розробку та реалізацію нових підходів на основі штучного інтелекту, а також експериментальне порівняння їхньої ефективності та точності у контексті тестування RESTful API.

Розглянемо декілька прикладів як штучний інтелект може генерувати тестові дані для параметрів запитів. Використання GPT(Generative Pre-trained Transformer 3) відображає передовий підхід до «pre-training» та «fine-tuning». Генерація тестових даних відбувається шляхом використання контекстуального розуміння,

отриманого від передового навчання, для прогнозування наступного символу чи токена в послідовності. Механізм уваги дозволяє моделі взаємодіяти з різними частинами вхідного тексту, враховуючи їхній відносний внесок у генерацію тексту. Таким чином, GPT-3 може адаптуватися до конкретного контексту та завдання, що робить його потужним інструментом для генерації текстового вмісту, включаючи тестові дані, з високою логічністю та врахуванням мовної структури.

Рекурентні нейронні мережі (RNN) відзначаються унікальною математичною структурою, що дозволяє їм ефективно враховувати послідовність даних та зберігати внутрішній стан. Це властивість знайшла особливе застосування в генерації тестових даних для тестування, де RNN може адаптуватися до контексту та структури послідовностей. Математично це виражається через рекурентну функцію, що ураховує поточний вхід, попередній стан та параметри мережі. З використанням удосконалених архітектур, таких як Long Short-Term Memory (LSTM) та Gated Recurrent Unit (GRU), RNN набуває здатності довго враховувати залежності в даній послідовності, зробивши його потужним інструментом для генерації тестових даних з високим рівнем наукової та математичної точності.

Генерація та використання синтетичних тестових даних мають практичні застосування в контексті тестування RESTful API. Ось декілька прикладів:

- генерація тестових даних може бути використана у автоматизованому тестуванні для уникнення ефекту пестициду і дозволяє при кожному запуску регресійного тестування отримувати ефективніше покриття.
- використання алгоритмів штучного інтелекту, що використовуються в некерованому навчанні, реалізовані системою двох штучних нейронних мереж дозволяють уникнути використання реальних даних користувачів що може призвести до порушення регламенту з питань захисту даних.
- використання генеративних мовних моделей дозволяє суттєво зменшити час на ведення тестової документації а саме на написання тестових випадків для тестування відповіді сервера при використанні різних груп даних(валідних та невалідних), що у випадку тестування API є доволі об'ємним завданням.
- тестові дані, згенеровані за допомогою генеративної змагальної мережі можуть бути використані у об'ємному тестуванні навантаження як реалістичні значення параметрів API запитів, оскільки дані не вважатимуться синтетичними і базуватимуться на початкових навчальних даних для дискримінатора.

Можемо зробити висновок, що використання таких методів штучного інтелекту, як рекурентна нейронна мережа або генеративних мовних моделей дозволяє суттєво оптимізувати щоденні задачі інженерів з забезпечення якості при роботі з тестуванням API.

Список використаних джерел

1. Bhadeshia H. K. D. H. (1999). Neural Networks in Materials Science. ISIJ International 39 (10): 966–979.
2. Synthetic Data Generation Using Conditional-GAN [Електронний ресурс] – Режим доступу до ресурсу: <https://towardsdatascience.com/synthetic-data-generation-using-conditional-gan>
3. Challenges in API testing [Електронний ресурс] – Режим доступу до ресурсу: <https://www.webomates.com/blog/api-testing/top-5-api-testing-challenges-solved-with-ai/>
4. How AI Test Automation Can Boost Your Business Growth – Режим доступу до ресурсу: <https://www.webomates.com/blog/ai-test-automation-for-business-growth/>.
5. Generative Adversarial Network (GAN)-Based Autonomous Penetration Testing for Web Applications [Електронний ресурс] – Режим доступу до ресурсу: <https://www.mdpi.com/1424-8220/23/18/8014>
6. Hitaj, B.; Gasti, P.; Ateniese, G.; Perez-Cruz, F. Passgan: A deep learning approach for password guessing. In Proceedings of the International Conference on Applied Cryptography and Network Security, Bogota, Colombia, 5–7 June 2019; Springer: Cham, Switzerland, 2019; pp. 217–237.
7. Load Testing API Endpoints: Simulating real-world API traffic with Poisson Distributions [Електронний ресурс] – Режим доступу до ресурсу: <https://medium.com/sage-ai/load-testing-api-endpoints-simulating-real-world-api-traffic-with-poisson-distributions-b1e4fca7085d>
8. What Is a REST API? Examples, Uses, and Challenges [Електронний ресурс] – Режим доступу до ресурсу: <https://blog.postman.com/rest-api-examples/>.
9. How to prepare realistic test data via OpenAI API in Postman [Електронний ресурс] – Режим доступу до ресурсу: https://dev.to/n_demia/how-to-prepare-test-data-via-openai-api-in-postman-5con.

УДК 004:42

Горницький О. В., магістрант

Державний університет «Житомирська політехніка»

ДОСЛІДЖЕННЯ ПСИХОЕМОЦІЙНОГО СТАНУ РОЗРОБНИКІВ ІНТЕРНЕТ-МАГАЗИНУ

Стрес – стан психічної напруги, що виникає в процесі діяльності в найбільш складних і важких умовах. Організм реагує на це захисно-приспосувальною реакцією підвищеного порушення. За допомогою порушення організм намагається пристосуватися до подразника. Це неспецифічне для організму порушення і є станом стресу [1].

Психічна напруга може негативно впливати на якість роботи працівника, завдавати шкоди його здоров'ю, а також можуть призвести до прямих збитків бізнес-партнерів шляхом збільшення кількості логічних помилок програмному коді та нестабільної роботи інформаційної системи.

В працях психологів можна знайти кореляцію індивідуальних психічних особливостей з реакцією на впливи середовища. Сюди відносяться дослідження тривожності, або занепокоєння. Тривожність діагностувалась за допомогою наборів питань приналежних до середовища впливів за допомогою так званої шкали Тейлора «відкритої тривожності» [2], яка будується по типу опитування.

Також відомі й інші методики діагностування стресу, такі як метод Холмса-Раге, тест самовідчуття Вісман, Рікс, тест здоров'я Голдберг, Тест САН – самопочуття, активність, настрій, Самооцінка психічних станів Г.Айзенка, Шкала реактивної та особистісної тривожності Спілбергера-Ханіна, Опитувальник нервово-психічної напруги Немчіна, Шкала депресії Балашова, Диференціальна шкала емоцій К.Ізарда, та інші [3]. Всі вони побудовані на основі опитування та збору інформації про персональний емоційний стан людини.

Для досліджень на основі співбесід діагноз виробляється за допомогою спостереження за зміною відповіді співробітника на питання, що стосуються безпосередньо відчуття впливу.

Класифікатори для створення опитування був і наступні:

- Participation (співучасть)
- eNPS (лояльність співробітників)
- Engagement (залученість)
- Recognition (визнання)
- Feedback (зворотній зв'язок)

- Relationships with peers (відносини з колегами)
- Relationships with manager (відносини з менеджером)
- Satisfaction (загальна задоволеність)
- Allignment (слідування цілям компанії/власним цілям)
- Happiness (задоволення від виконання роботи)
- Wellness (самопочуття)
- Personal growth (можливість самоствердження)
- Ambassadorship (умотивованість)

На основі класифікаторів було сформовано список тематичних питань та проведено періодичні опитування співробітників.

Після збору даних проведений перерахунок середнього арифметичного значень відповідей на питання по класифікатору. На основі даних приведеної таблиці побудовано графіки зміни середнього психоемоційного стану співробітників двох команд за весь період спостереження(рис. 1).



Рис. 1. Графіки зміни середнього психоемоційного стану команд співробітників.

В ході аналізу було виявлено залежність у психоемоційному стані двох команд. В першій команді чітко виражені піки покращення стану працівників в червні-липні та листопаді-грудні, проте в кінці року та в період вересень-жовтень стан значно погіршується в обох командах. З початку року стан співробітників в цілому стабільний та навіть покращується в першій команді.

Цікаво, що команди працюють з різними менеджерами та різними проектами. Значні зміни вірогідніше за все створюють зовнішні чинники.

Список використаних джерел

1. Психологія стресу: підручник / Л. Б. Наугольник. – Львів: Львівський державний університет внутрішніх справ, 2015. – 324 с.
2. Janet A. Taylor. Taylor Manifest Anxiety Scale, TMAS, 1953.
3. S. Cohen, G. Williamson. Perceived Stress Scale, PSS-10, 1988.

УДК 004

*Олексійчук М. В., магістрант,
Чижмоторя О. В., ст. викладач
Державний університет «Житомирська політехніка»*

ЕТИЧНІ ПРОБЛЕМИ РОЗВИТКУ І ВИКОРИСТАННЯ ТЕХНОЛОГІЙ МАШИННОГО НАВЧАННЯ ТА NLP ТА ПІДХОДИ ДО ЇХ ВИРІШЕННЯ

З перспективи сьогодення навіть відносно близьке минуле для багатьох може здаватись кам'яним віком технологій, коли не було широкого розголосу про практичне використання штучного інтелекту поза колами вчених та розробників. Поки виробництво розвивалось у сторону автоматизації та заміни людського фактору, робота з текстом здебільшого лишалась незмінною. З розвитком інформаційних технологій та таких галузей штучного інтелекту, як машинне навчання (з англ. Machine Learning, ML) та обробки природної мови (з англ. Natural Language Processing, NLP), автоматизація та алгоритмізація роботи, що з першого погляду не може бути повністю автоматизована, призводить до багатьох морально-етичних проблем та питань.

Технології обробки тексту, засновані на ML та NLP, потребують великої кількості даних для навчання, формування внутрішніх алгоритмів та розуміння порядку слів, значення словосполучень, виокремлення теми тексту та насиченості його емоційно, інформаційно тощо. У процесі створення технологій, розробники та дослідники мають знайти та організувати дані, виділити ключові особливості текстів, що може призвести до суб'єктивності та упередженості системи, а у випадку несерйозного ставлення до майбутньої системи – грубої та неадекватної поведінки [1].

Мета розроблених моделей та систем може варіюватись від обробки публічних даних, починаючи від коментарів до медіа-публікацій до наукових статей, так і особистих в додатках, що спеціалізуються на пошуку співрозмовників по спільним інтересам, організації побачень, отримання порад від спеціалістів, або системах рекомендації товарів та підбору реклами тощо. Неприйнятний тренд на періодичні порушення безпеки та витік даних великих компаній може значно посилитись із втратою даних, зібраних завдяки чат-ботам на основі ML та NLP [2, 3].

Нарешті, разом з відсутністю прозорості в процесі розробки та при випуску цих програмних продуктів, особливо в комбінації вище зазначених проблем, довіра до розроблених моделей підривається, та

бажання користуватись системами зменшується чи повністю зникає, незважаючи на можливі корисні можливості та заяви про забезпечення безпеки [3].

Ці та інші проблеми, пов'язані з доступом до користувацьких даних, часто пов'язані з невідповідальним ставленням компаній та команд розробки стосовно програмного продукту. Процес розробки систем на основі технологій штучного інтелекту має дотримуватись головних принципів та практик, нормативних декларацій, що об'єднують спільною назвою «Відповідальний ШІ» (з англ. «Responsible AI»). Згідно них, компанії мають виробити та поширити етику використання інструментів на основі технологій ШІ, яка доповнює корпоративну етику розробки піклуванням про безпеку даних, їх анонімізацію за необхідності зберігання, ефективність роботи систем через якомога якісніші розробку та тестування [4].

Зі сторони клієнтів користування системами на основі ML та NLP потребує відповідального ставлення до особистих даних. Незважаючи на постійні успіхи в розвитку сфери, найбільшою проблемою при роботі з даними є людський фактор та необережне користування Інтернетом. Розвиток критичного мислення та вивчення небезпек Всесвітньої Мережі все ще залишається ефективним способом захисту.

Список використаних джерел

1. Jovi Umawing. Now it's BlenderBot's turn to make shocking, inappropriate, and untrue remarks – Malwarebytes. [Електронний ресурс] Режим доступу до ресурсу: <https://www.malwarebytes.com/blog/news/2022/08/its-now-blenderbots-turn-to-make-shocking-inappropriate-and-untrue-remarks>

2. Wisdom Sablah, Lauren Mak. Privacy Risks of AI Chatbots: ChatGPT and AI Privacy Issues – VPNO verview. [Електронний ресурс] – Режим доступу до ресурсу: <https://vpnoverview.com/privacy/apps/ai-privacy-risks/>

3. Catherine Thorbecke. Don't tell anything to a chatbot you want to keep private – CNN Business. [Електронний ресурс] – Режим доступу до ресурсу: <https://edition.cnn.com/2023/04/06/tech/chatgpt-ai-privacy-concerns/index.html>

4. Marcin Frąckiewicz. The Potential and Risks of Machine Learning in Privacy and Data Protection – TS2 Space. [Електронний ресурс] – Режим доступу до ресурсу: <https://ts2.space/en/the-potential-and-risks-of-machine-learning-in-privacy-and-data-protection/>

УДК 004.92

*Байло О.В., здобувач,
Левченко А. Ю., к.т.н., ст. викладач
Державний університет «Житомирська політехніка»*

ЗАСТОСУНОК GAEA: АНАЛІЗ ЗАСТОСУВАННЯ АЛГОРИТМІВ В СУЧАСНИХ ІТ-СИСТЕМАХ

З розвитком технологій в галузі комп'ютерної графіки, виокремлюється програмне забезпечення Gaea як інноваційний інструмент [1], спеціалізований на створенні природних об'єктів та ландшафтів. За допомогою програми, користувачі можуть легко втілити в життя величезні гори, річки, долини та інші природні об'єкти з вражаючою деталізацією, надаючи реалістичний вигляд створеним візуальним образам.

Gaea володіє модульною та добре структурованою архітектурою, що визначає його ефективність та зручність для користувачів. Тобто програма розділена на логічні модулі, що спрощує внесення змін і дозволяє легко додавати нові функції та інтегрувати їх з існуючими. Архітектура програми оптимізована для роботи з великими обсягами даних, що важливо для обробки деталізованих ландшафтів та природних об'єктів.

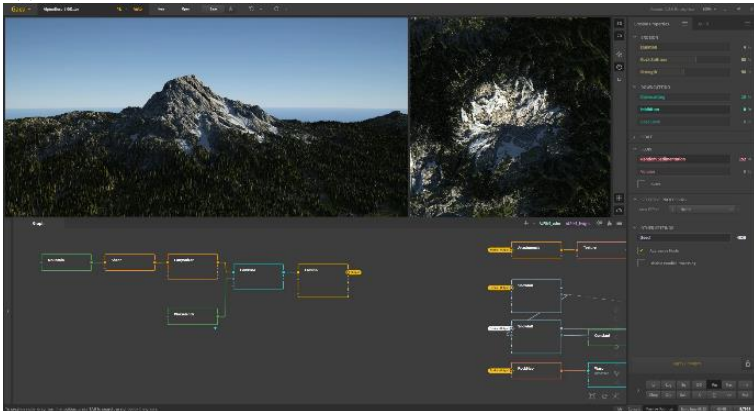


Рис. 1. Інтерфейс програми Gaea

Однією з головних інновацій Gaea є використання штучного інтелекту для полегшення та поліпшення творчого процесу. Алгоритми машинного навчання допомагають автоматизувати рутинні

завдання, забезпечуючи художникам можливість фокусуватися на творчості та експериментах.

Ключовий пункт у використанні Gaea – це його здатність інтегруватися з іншими графічними редакторами та програмами для 3D-моделювання забезпечуючи велику гнучкість у творчому процесі.

Gaea виявляється надзвичайно цінним інструментом у сфері візуальної графіки, забезпечуючи неперевершені можливості для створення реалістичних природних об'єктів та ландшафтів. Його вдоскоалена архітектура та ключові функції роблять Gaea важливим активом для різних галузей, таких як:

1) Графічний дизайн – дозволяє художникам та дизайнерам створювати вражаючі природні сцени, розширюючи їх творчий потенціал та пропонуючи нові можливості для вираження ідей.

2) Ігрова індустрія – використання Gaea в ігровій індустрії дозволяє створювати великі та деталізовані ігрові світи, забезпечуючи гравцям неповторні враження та високий рівень занурення.

3) Кінематографія – в Gaea вбудовані засоби для створення реалістичних природних сцен та ефектів, що визначають високу якість візуальних елементів у фільмах та рекламних відеороликах.

4) Архітектурне проектування – Gaea використовується для візуалізації зовнішнього середовища будівельних об'єктів, надаючи архітекторам та дизайнерам можливість досліджувати та вдосконалювати свої концепції.

5) Наука – у галузі науки Gaea використовується для моделювання та візуалізації екологічних систем, допомагаючи вченим розуміти та досліджувати природні процеси.

Розвиток програми Gaea у напрямку збільшення функціональності, використання новітніх технологій наприклад VR і покращенням використання штучного інтелекту та покращення користувальницького досвіду визначатиме її значущість у майбутньому дизайну та графічній індустрії. Відкриваючи нові можливості для творчості та взаємодії, Gaea стане не тільки інструментом для створення вражаючих візуальних образів, але й підтримкою для нових ідей та інновацій у сучасному дизайні. А також визначає новий стандарт у створенні природних об'єктів в галузі візуальної графіки. Його функції, спрямовані на полегшення творчого процесу та створення реалістичних візуальних образів, покликані визначити майбутнє графічного дизайну та візуального мистецтва.

Список використаних джерел

1. Quad Spinner. [Електронний ресурс] – Режим доступу до ресурсу: <https://quadspinner.com/>

УДК 621.3: 455.63

*Каранет Б. В., магістрант,
Савіцький Р. С., викладач
Державний університет «Житомирська політехніка»*

ЗНАХОДЖЕННЯ ВІДМІННОСТЕЙ ПРИ ПОРІВНЯННІ ЗОБРАЖЕНЬ З ДРОНУ, ЗНАХОДЖЕННЯ ПОТЕНЦІЙНОЇ ЦІЛІ

Сучасний світ переживає еру активного використання інформаційних технологій, де важливим завданням стає аналіз та обробка великих обсягів даних. Однією з ключових галузей є комп'ютерний зір, яка визначається як область машинного зору та обробки зображень. Ця галузь розвивається завдяки постійному вдосконаленню методів та інструментів для порівняння зображень та виявлення об'єктів.

Ключовими аспектами при вирішенні завдань комп'ютерного зору та обробки зображень є інструменти порівняння зображень, методи трансформації фотографій та способи пошуку об'єктів за допомогою моделей машинного навчання.

У великій мірі, розвиток і застосування цих методів визначається інноваційними можливостями та практичним застосуванням у багатьох галузях, таких як системи безпеки, онлайн-сервіси для обробки зображень та доповнена реальність. Використання комп'ютерного зору стає надзвичайно важливим для досягнення високої продуктивності та точності в обробці зображень та розпізнаванні об'єктів.

Для висвітлення проблеми було детально розглянуто інструменти порівняння зображень, трансформацію фотографій та пошук об'єктів, а також визначено їх важливість і застосування в сучасному світі інформаційних технологій [1].

Інструменти порівняння та комп'ютерний зір:

- Повзунок порівняння зображень: важливий інструмент для візуального порівняння двох зображень та визначення їх схожості чи відмінностей [2].
- Попіксельне порівняння за допомогою cv2.absdiff з підсвічуванням різниці: застосування cv2.absdiff дозволяє виділити області, де зображення відрізняються, що корисно для визначення різниці між ними [3].

- Накладання двох BGR2GRAY фотографій: перетворення зображень у чорно-білі за допомогою BGR2GRAY і їх подальше накладання для аналізу подібності і відмінностей [4].
- Порівняння за допомогою модулю PIL: використання бібліотеки Python Imaging Library для порівняння зображень та визначення їхньої схожості.

Трансформація фото з подальшим порівнянням:

- Трансформація перспективи: можливість зміни кута огляду зображення для подальшого порівняння [5].
- Порогова зміна зображення. Глобальне порогове значення ($V=127$): використання фіксованого порогового значення для бінаризації зображень.
- Порогова зміна зображення. Адаптивне середнє порогове значення: застосування адаптивного порогового значення на основі середнього значення пікселів для покращення бінаризації [6].
- Порогова зміна зображення. Адаптивне порогове значення Гауса: аналогічно до попереднього пункту, але з використанням Гаусівського фільтру для підсилення результату [7].
- Виявлення країв: використання фільтрів для виявлення контурів на зображенні для подальшого порівняння.

Пошук об'єктів за допомогою моделі машинного навчання:

- Послідовна модель: створення послідовної моделі для виявлення об'єктів на зображеннях.
- Знаходження об'єктів за допомогою ImageAI та YOLOv3 моделі: використання ImageAI бібліотеки та YOLOv3 моделі для виявлення та локалізації об'єктів на зображеннях.

Комп'ютерний зір та алгоритми порівняння зображень мають різноманітні практичні застосування в контексті порівняння зображень, отриманих з дронів, а також в пошуку потенційних цілей. Ось декілька прикладів:

- Моніторинг лісових пожеж: дрони можуть зафіксувати зображення лісних масивів, а комп'ютерний зір допомагає порівнювати ці зображення з попередніми записами для виявлення пожеж та їхнього розповсюдження.
- Пошук цілей у воєнних операціях: воєнні дрони можуть збирати інформацію про територію та потенційні цілі. Комп'ютерний зір може аналізувати зображення для виявлення рухомих об'єктів, визначення типу та розташування ворожих техніки та інфраструктури.

- Моніторинг стану інфраструктури: дрони можуть облітати мости, будівлі та інші інженерні споруди для отримання зображень. Комп'ютерний зір може використовуватися для порівняння цих зображень з раніше отриманими даними для виявлення будь-яких дефектів чи змін у структурі.

- Пошук людей в рятувальних операціях: дрони можуть допомагати в пошуку втрачених або заблокованих осіб у важкодоступних областях. Комп'ютерний зір може аналізувати зображення, виявляти людей та надавати координати для швидкого рятування.

Ці приклади демонструють, як комп'ютерний зір та порівняння зображень можуть використовуватися для різних цілей, включаючи безпеку, військові операції, моніторинг і рятувальні операції. Вони допомагають покращити надійність та ефективність процесів, що вимагають аналізу великих обсягів візуальної інформації.

Список використаних джерел

1. OpenCV. [Електронний ресурс] – Режим доступу до ресурсу: <https://opencv.org/about/>.

2. How TO – Image Comparison Slider. [Електронний ресурс] – Режим доступу до ресурсу: https://www.w3schools.com/howto/howto_js_image_comparison.asp.

3. Program Creek. Python cv2.absdiff() Examples. [Електронний ресурс] / programcreek – Режим доступу до ресурсу: <https://www.programcreek.com/python/example/89428/cv2.absdiff>.

4. BGR2GRAY в документації OpenCV. [Електронний ресурс] – Режим доступу до ресурсу: http://www.devdoc.net/linux/OpenCV-doc-4.3.0/dc/d38/group__gapi__colorconvert.html#ga3e8fd8197ab16811caf9b31cb1e08a05

5. Shaikh R. OpenCv Perspective Transformation. [Електронний ресурс] / Raqeeb Shaikh. – Режим доступу до ресурсу: <https://medium.com/analytics-vidhya/opencv-perspective-transformation-9edffefb2143>.

6. Image Thresholding. [Електронний ресурс] – Режим доступу до ресурсу: https://docs.opencv.org/4.x/d7/d4d/tutorial_py_thresholding.html.

7. Maximinusjoshus. Dive deeper into OpenCV's Adaptive Thresholding [Електронний ресурс] / Maximinusjoshus. – 1404. – Режим доступу до ресурсу: <https://medium.com/featurepreneur/dive-deeper-into-opencvs-adaptive-thresholding-3f29dda8c908>.

УДК 621.3: 455.63

*Венгловська Ю. В., магістрант,
Марчук Г. В., ст. викладач,
Колос К. Р., д.пед.н., професор
Державний університет «Житомирська політехніка»*

ІДЕАЛЬНІ ЛАБІРИНТИ ТА АЛГОРИТМИ ЇХ СТВОРЕННЯ

Процедурна генерація лабіринту часто стає у нагоді при розробці ігор, наприклад, для створення унікальних рівнів. Однак, найчастіше використовують стандартний вигляд алгоритму, що позбавляє ринок певної унікальності та псує досвід гравця. Одним із можливих рішень цієї проблеми є розширене дослідження різних методів, та, в перспективі, створення нових. Метою дослідження є аналіз основних алгоритмів генерації ідеальних лабіринтів у середовищі Unity.

Лабіринт вважається ідеальним, якщо в нього немає замкнутих і зациклених ділянок, і від будь-якої точки до будь-якої іншої точки існує один шлях.

Recursive backtracker (рис. 1): він вимагає стека, обсяг якого може сягати розмірів лабіринту. Прохід завжди вирізається у нествореній частині, якщо вона існує поруч із поточним осередком. Щоразу, під час переміщення до нового осередку, здійснюється запис попереднього осередку у стек. Якщо поруч із поточною позицією немає нестворених осередків, то повертається значення стека з попередньої позиції. Лабіринт завершено, коли в стеку більше нічого не залишається. Це призводить до створення лабіринтів з максимальним показником плинності, глухих кутів менше, але вони довші, а рішення зазвичай виявляється дуже довгим і звивистим. При правильній реалізації алгоритм виконується швидко, швидше працюють лише дуже спеціалізовані алгоритми.

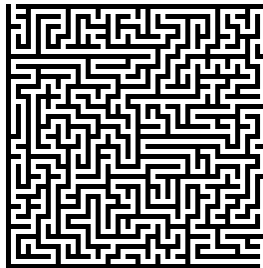


Рис. 1. Лабіринт, побудований алгоритмом Recursive backtracker [1]

Алгоритм Крускала (рис. 2): це алгоритм, що створює мінімальне сполучне дерево. Він не «вирощує» лабіринт подібно до дерева, а вирізає сегменти проходів по всьому лабіринту випадковим чином, проте в результаті створює в кінці ідеальний лабіринт. Для його роботи потрібно обсяг пам'яті, пропорційний розміру лабіринту, а також можливість перерахування кожного ребра або стіни між осередками лабіринту у випадковому порядку (зазвичай для цього створюється список всіх ребер і перемішується випадковим чином). Кожен осередок позначається унікальним ідентифікатором, потім усі ребра обходяться у випадковому порядку. При правильній реалізації цей алгоритм працює досить швидко, але повільніше більшості через створення списку ребер та управління множинами.

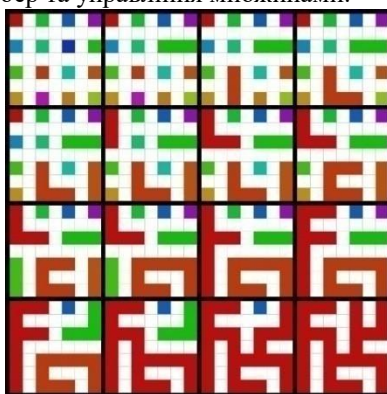


Рис. 2. Ітерації побудови лабіринту за допомогою алгоритму Крускала [2]

Алгоритм Еллера (рис. 3): це особливий алгоритм, тому що він не тільки найшвидший, але й не має очевидних недоліків; крім того, при створенні пам'ять використовується найбільш ефективно. Для нього навіть не потрібно, щоб у пам'яті знаходився весь лабіринт, він використовує об'єм, пропорційний розміру рядка. Він створює лабіринт рядково, після завершення генерації рядка алгоритм більше його не враховує. Створення рядка і двох частин: випадковим чином з'єднуються сусідні у межах рядка осередки, тобто вирізаються горизонтальні проходи, потім випадковим чином з'єднуються комірки між поточним і наступним рядками, тобто вертикальні проходи. Створення починається з того, що перед з'єднанням осередків у першому рядку кожен осередок має власну безліч. Створення завершується після з'єднання осередків в останньому рядку.

Існує особливе правило завершення: до моменту завершення кожен осередок повинен знаходитися в однаковій множині, щоб уникнути ізольованих областей. Найкраще реалізовувати множину за допомогою списку осередків виконувати за постійний час вставку, видалення та перевірку знаходження сусідніх осередків в одній множині. Проблема цього алгоритму полягає у незбалансованості обробки різних країв лабіринту; щоб уникнути плям у текстурах потрібно виконувати з'єднання та пропуск з'єднання осередків у правильних пропорціях.

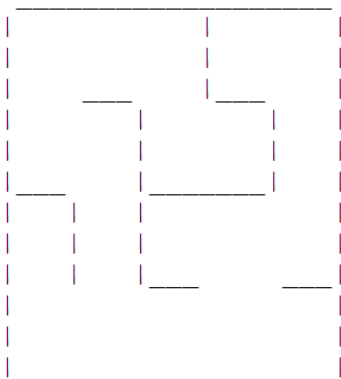


Рис. 3. Лабіринт, побудований алгоритмом Еллера [3]

Отже, процедурна генерація лабіринту є важливою складовою розробки ігор, яка може зробити геймплей більш цікавим та непередбачуваним для гравців. Однак, стандартні алгоритми генерації можуть призвести до відчуття одноманітності та втрати цікавості в грі. Тому важливо проводити дослідження та розглядати різні методи генерації лабіринтів у пошуках нових способів покращення якості гри та підвищення задоволення гравців.

Список використаних джерел

1. Алгоритм Recursive backtracker [Електронний ресурс] – Режим доступу до ресурсу: <https://aryanab.medium.com/maze-generation-recursive-backtracking-5981bc5cc766>.
2. Алгоритм Крускала [Електронний ресурс] – Режим доступу до ресурсу: <https://vishald.com/blog/kruskals-maze-generation/>.
3. Алгоритм Еллера [Електронний ресурс] – Режим доступу до ресурсу: <https://weblog.jamisbuck.org/2010/12/29/maze-generation-eller-s-algorithm>.

УДК 550.34.01

Пількевич І. А., д.т.н. проф.

Гордієнко Ю. О., к.т.н.

Мірошніченко С. І., викладач

Житомирський військовий інститут імені С. П. Корольова

МЕТОДИКА АВТОМАТИЧНОГО ВИЗНАЧЕННЯ ОСЕРЕДКУ СЕЙСМІЧНОЇ ПОДІЇ ТРИКОМПОНЕНТНОЮ СЕЙСМІЧНОЮ СТАНЦІЄЮ

Безпосереднім результатом діяльності людини є надзвичайні ситуації (НС) техногенного характеру, які виникають у результаті порушення нормальних умов життя й діяльності людей на об'єктах або територіях. За даними ООН від НС щорічно в Україні гине більше 70 тисяч осіб, а держава зазнає значних матеріальних збитків.

Для якісного захисту населення від НС техногенного характеру необхідно своєчасно отримувати інформацію про надзвичайні події та їх наслідки. Для цього згідно з Кодексом цивільного захисту України створено систему моніторингу надзвичайних ситуацій (СМНС), побудовану на зборі й аналізі інформації, яка надходить із різноманітних засобів контролю та спостереження, про стан відповідних об'єктів або територій, що є небезпечними [1]. Саме тому актуальним завдання є підвищення можливостей СМНС за рахунок розширення методів моніторингу.

Метою роботи є розробка методики визначення місцезнаходження осередку сейсмічної події за результатами аналізу даних трикомпонентної сейсмічної станції (ТКСС), яка входить до складу мережі сейсмічних спостережень Головного центру спеціального контролю (ГЦСК).

У даний час обробка вимірювальних даних сейсмічного спостереження здійснюється в ручному та автоматичному режимах. Однак рішення про параметри сейсмічної події та можливі наслідки приймається оперативним черговим ГЦСК за результатами аналізу інформації про параметри сейсмічного сигналу (час вступу основних типів сейсмічних хвиль, їх амплітуда та період), отриманої з кожного з пунктів спостереження [2]. Тимчасова втрата Кримського півострова призвела до територіальної обмеженості мережі сейсмічних спостережень ГЦСК. Це зумовило необхідність розробки алгоритмів ідентифікації природи сейсмічного джерела за результатами обробки сейсмічних даних в автоматичному режимі окремих пунктів спостереження.

У доповіді запропоновано використання особливостей ортогональності кутових характеристик об'ємних хвиль, що покладено в основу методики визначення осередку сейсмічної події. Методика визначення сейсмічної події на основі використання особливостей кутових характеристик складових об'ємних хвиль сейсмічного сигналу за результатом обробки вимірювальних даних окремої ТКСС включає такі етапи:

- 1) виявлення вступу сейсмічного сигналу (Р-хвилі);
- 2) оцінювання кутових характеристик вступу сейсмічного сигналу (Р-хвилі);
- 3) пошук ділянок запису сейсмічного сигналу з кутовими характеристиками, які відповідають S-хвилі (виконання умови ортогональності кутових характеристик Р і S-хвиль);
- 4) визначення координат осередку сейсмічного джерела (азимуту на джерело відносно пункту спостереження та відстань між ним та джерелом сейсмічної події).

На першому етапі виявлення вступу сейсмічного сигналу здійснюється за амплітудним критерієм із застосуванням детектору STA/LTA (перевищення порогу $STA/LTA \geq 3$).

На другому етапі для першого вступу сейсмічного сигналу застосовується апарат поляризаційного аналізу, результатом якого є значення ступеня лінійності, кутове положення великої вісі еліпсоїда, яке у свою чергу визначає азимут надходження сейсмічної хвилі.

На третьому етапі здійснюється пошук ділянки запису, для якої виконується умова – кутове положення головної піввісі еліпсоїду для отриманої вибірки ортогональне положенню Р-хвилі.

Розроблена методика автоматичного визначення осередку сейсмічної події ТКСС ґрунтується на застосуванні апарату поляризаційного аналізу, що дозволяє суттєво зменшити час обробки сейсмічного запису порівняно з обробкою в ручному режимі.

Список використаних джерел

1. Кодекс цивільного захисту України. № 5403-VI, 2 жовтня 2012 року // Голос України. – 2012. – № 220(5470). – С. 4–20.
2. Vakaliuk T. A., Pilkevych I. A., Hordiienko Y. O., Loboda V. V. Application of Polarization-Time Model Seismic Signal for Remote Monitoring of Potential Sources Emergencies by Three-Component Seismic Station // The Sixth International Workshop on Computer Modeling and Intelligent Systems (CMIS 2023) Zaporizhzhia, Ukraine. 2023. P. 52–64. <https://doi.org/10.32782/cm/3392-5>

УДК 004

*Менес Ю. В., магістрант,
Марчук Г. В., ст. викладач,
Колос К. Р., д.пед.н., професор
Державний університет «Житомирська політехніка»*

МЕТОДОЛОГІЧНІ ОСНОВИ ВИКОРИСТАННЯ КОЛЬОРІВ У ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЯХ

Зв'язок між теорією кольору та інформаційно-комунікаційними технологіями (ІКТ) є важливим у світі, де ми багато часу проводимо онлайн і використовуємо різні гаджети. ІКТ допомагають нам краще розуміти, як кольори впливають на наші почуття та як їх можна використовувати в Інтернеті, в мультимедійних проектах та інших місцях.

Метою дослідження є визначити, як інформаційно-комунікаційні технології впливають на сприйняття та застосування кольорів у різних аспектах сучасного життя, зокрема у веб-дизайні, мультимедійних проектах, інтерактивних інтерфейсах та інших областях.

Теорія кольору – це і наука, і мистецтво використання кольору. Вона пояснює, як люди сприймають колір і візуальні ефекти того, як кольори змішуються, збігаються або контрастують один з одним. Теорія кольору також включає повідомлення, які передають кольори і методи, що використовуються для відтворення кольору.

У теорії кольору кольори організовані на кольірному колі (рис.1) та згруповані в 3 категорії: основні кольори (Primarycolors), вторинні кольори (Secondarycolors) та третинні кольори (Tertiarycolors) [1].



Рис. 1. Кольорове коло [2]

Перші згадки про теорію кольору відносяться до античності [3], але справжній прорив в цій області був зроблений в середньовіччі, коли Альхазен та Ібн аль-Хайтам вивчали властивості світла та колірну спектральну розкладку [4]. Важливі внески в розвиток теорії кольору зробили Іоганнес Кеплер, Гюйгенс, Ісаак Ньютон та інші.

Фізичний підхід до теорії кольору розглядає колір як результат взаємодії світла і об'єктів. Найважливішими концепціями є спектральний розклад світла, дисперсія, абсорбція та відбиття кольору. Психологічний підхід до теорії кольору досліджує, як колір впливає на сприйняття та емоційний стан людини. Відомі теорії, такі як теорія кольорового контрасту та теорія кольорової асоціації, грають важливу роль у цьому контексті.

Теорія кольору має безліч практичних застосувань у різних сферах життя, включаючи мистецтво, дизайн, маркетинг, психологію та науку. Наприклад, в дизайні – використовується для створення ефективних логотипів та пакувань продуктів. Правильний підбір кольорової палітри має залучити користувача та створювати внутрішнє відчуття порядку, рівноваги у візуальному досвіді. Має бути гармонією.

Коли щось не гармонійно – це або нудно, або хаотично. Людський мозок відкидає те, що не може організувати, чого не може зрозуміти. Саме гармонія кольорів створює візуальний інтерес і відчуття порядку [5].

Існує багато теорій гармонії. Наступні ілюстрації та описи представляють деякі основні формули.

1. Колірна схема на основі аналогічних кольорів.

Аналогічними кольорами (рис. 2) є будь-які три кольори, які розташовані поруч на кольоровому колі, наприклад жовто-зелений, жовтий і жовто-помаранчевий. Зазвичай переважає один із трьох кольорів [6].



Рис. 2. Приклад застосування аналогічних кольорів [2]

2. Колірна схема на основі комплементарних кольорів.

Комплементарні кольори (рис. 3) – це будь-які два кольори, які знаходяться прямо протилежно один одному, наприклад червоний і зелений, червоно-фіолетовий і жовто-зелений [6].



Рис. 3. Приклад застосування комплементарних кольорів [2]

3. Колірна схема на основі розділених комплементарних кольорів.

Роздільно-комплементарна колірна схема (рис. 4) використовує один основний колір і два додаткових кольори [7].



Рис. 4. Приклад вибору розділених комплементарних кольорів [2]

4. Колірна схема на основі тріади кольорів.

Тріада (рис. 5) – це колірна схема, особливий варіант роздільно-комплементарної колірної схеми з рівною відстанню між усіма кольорами [8].



Рис. 5. Приклад застосування тріади кольорів [2]

5. Колірна схема на основі тетради кольорів.

Тетрада (рис. 6) – це колірна схема, особливий варіант подвійної колірної гами з рівною відстанню між усіма кольорами. Усі чотири кольори рівномірно розподілені навколо колірного кола, тому немає чіткого домінування одного кольору [9].



Рис. 6. Приклад застосування тетради кольорів [2]

Теорія кольору залишається активною областю досліджень, і в майбутньому можливі нові відкриття та застосування. Розвиток нових технологій, таких як штучний інтелект, може розширити наше розуміння та можливості використання кольору.

Отже, дослідження теорії кольору є важливим компонентом нашого розуміння світу навколо нас і впливає на багато сфер нашого життя, особливо під час використання ІКТ. Фізичні та психологічні аспекти кольору доповнюють один одного, дозволяючи нам краще розуміти, як кольори впливають на наше сприйняття і поведінку.

Список використаних джерел

1. The fundamentals of understanding color theory. [Електронний ресурс] – Режим доступу до ресурсу: <https://99designs.com/blog/tips/the-7-step-guide-to-understanding-color-theory/>

2. Color Theory: Get Inspired by Color! [Електронний ресурс] – Режим доступу до ресурсу: <https://www.skillshare.com/en/classes/Color-Theory-Get-Inspired-by-Color/1952660760?via=user-profile>

3. Коротка історія теорії кольору. [Електронний ресурс] – Режим доступу до ресурсу: <https://romasheva.com/uk/2021/a-brief-history-of-color-theory.html>

4. Ібн аль-Хайтам. [Електронний ресурс] – Режим доступу до ресурсу: <https://ibib.ltd.ua/ibn-haytam-27271.html>

5. Basic Color Theory. [Електронний ресурс] – Режим доступу до ресурсу: <https://www.colormatters.com/color-and-design/basic-color-theory>

6. The fundamentals of understanding color theory. [Електронний ресурс] – Режим доступу до ресурсу: <https://99designs.com/blog/tips/the-7-step-guide-to-understanding-color-theory/>

7. 7 колірних схем для гармонійного дизайну. [Електронний ресурс] – Режим доступу до ресурсу: <https://blog.depositphotos.com/ua/kolirni-shemy.html>

8. Triadic color scheme. [Електронний ресурс] – Режим доступу до ресурсу: https://paletton.com/wiki/index.php/Triadic_color_scheme

9. Tetradic color scheme. [Електронний ресурс] – Режим доступу до ресурсу:

https://www.paletton.com/wiki/index.php/Tetradic_color_scheme#:~:text=From%20Colorpedia,clear%20dominance%20of%20one%20color.

УДК 004.92: 004.4

Марчук Г. В., ст. викладач,

Кірій Д. О., здобувач

Державний університет «Житомирська політехніка»

МЕХАНІКИ ТА ДИЗАЙН РІВНІВ В ЖАНРАХ «METROIDVANIA» ТА «SOULS-LIKE»

Жанри «Metroidvania» та «Soulslike» представляють собою цікавий сегмент в світі відеоігор, що завжди привертає увагу геймерів та розробників. Ці два жанри стали відомими завдяки своїм унікальним особливостям та геймплею, а також вони доповнюють один одного, створюючи нові можливості для розробників і враження для гравців.

Жанр «Metroidvania» виник в результаті поєднання двох ігор «Metroid» та «Castlevania». Ці ігри відзначаються великим світом для дослідження та необхідністю отримання нових інструментів чи навичок для просування вперед.

Жанр «Soulslike» отримав свою назву від ігри «Dark Souls» розробленою FromSoftware. Відзначається не тільки важкістю, але і атмосферністю, заглибленою історією світу та моральними виборами гравця.

Незважаючи на різні коріння, «Metroidvania» і «Soulslike» мають деякі спільні риси, що можуть бути поєднані в одній грі:

- Необхідність дослідження. Гравцю доводиться досліджувати структурований світ, розгадувати та долати перешкоди.
- Збирання ресурсів та інвентарю. Обидва жанри передбачають збирання ресурсів, предметів і покращення інвентарю гравця.
- Високий ступінь виклику. Геймплей в цих іграх може бути надзвичайно важким, і гравцям доводиться навчатися на власних помилках.

Жанри «Metroidvania» і «Soulslike» можна об'єднати в одній грі, створюючи унікальний гібрид. Наприклад, гра може поєднувати високий рівень виклику та бойову систему «Soulslike» з необхідністю дослідження та відкриття нових областей, яка характерна для «Metroidvania». В цих жанрах існують унікальні механіки геймплею, які визначають їхні особливості. «Metroidvania» відомий своєю системою геймплею, де гравцеві необхідно ретельно досліджувати великі, зв'язані локації та вдосконалювати свої навички та обладнання для просування вперед. Основні механіки геймплею включають:

- Переміщення та подолання перешкод. Герой зазвичай володіє набором навичок які дозволяють подолати різноманітні перешкоди.

– Збирання предметів та інструментів. Гравцю потрібно знаходити ключові предмети та інструменти, які розблоковують нові можливості і локації.

– Карта та навігація. Важливою частиною геймплею є карта та навігація, оскільки гравцю потрібно пам'ятати структуру світу та знаходити оптимальні шляхи.

– Бойова система. «Metroidvania» може містити елементи бою, де гравцю доводиться вступати в битву з ворогами та босами.

«Soulslike» відомий своєю високою важкістю та інноваційним підходом до геймплею. Основні механіки геймплею включають:

– Бойова система, надає глибокий рівень взаємодії гравця з ворогами, де кожен крок та удар мають велике значення.

– Відновлення здоров'я та ресурсів. Гравцеві доводиться ретельно керувати своїм рівнем здоров'я та ресурсами.

– Збирання душ та досвіду це головна валюта в «Soulslike».

– Засоби комунікації з гравцями і внутрішньою історією. «Soulslike» часто використовує загадковий підхід до розповіді, де гравцеві слід вивчати приклади внутрішньої історії гри з опису предметів та діалогів.

Існують певні спільні механіки та можливості взаємодії, які можуть бути використані для створення унікальних ігор:

– Бойова система і розвиток навичок. Об'єднуючи глибоку бойову систему «Soulslike» з можливістю вдосконалення навичок головного героя, гра може створити цікавий баланс між важкістю та розвитком персонажа.

– Дослідження та відкриття нових локацій. Ідеї «Metroidvania» можуть доповнити світ «Soulslike», надаючи гравцю додатковий стимул для розкриття гри.

– Моральні вибори та наратив. Повністю зрозумілі моральні вибори та глибокий наратив «Soulslike» можуть доповнити гру «Metroidvania» та зробити її насиченою сюжетними елементами.

Інтеграція механік цих двох жанрів може дозволити розробникам створити гру з більшою глибиною геймплею, більшою варіативністю і цікавими комбінаціями елементів. Відмінності між ними також створюють можливості для креативності у геймдеві, що може призвести до виняткових ігрових досвідів для гравців.

Дизайн рівнів у жанрах «Metroidvania» і «Soulslike» грає ключову роль у створенні глибокого іммерсивного досвіду для гравців і виразної наративної структури. Обидва жанри мають свої унікальні принципи та методи дизайну рівнів, які впливають на геймплей і глибину світу гри.

У «Metroidvania» рівні призначені для створення відчуття розгорнутого світу і гравцю дозволяється вільно досліджувати їх. Доступ до різних областей може залежати від здобуття певних навичок чи обладнання. Рівні можуть містити важливу інформацію для розкриття сюжету. Відомості про минуле гри і її персонажів часто приховуються у вигляді залишених записів, графіті чи розташування об'єктів у світі.

У «Soulslike» рівні виконують іншу функцію, вони розроблені так, щоб бути викликом для гравця, містять сильних ворогів, пастки та босів, які вимагають від гравця навичок і стратегії. Створення атмосфери гри важливо для «Soulslike», рівні мають темну та містичну атмосферу, що допомагає підсилити іммерсивність гри. Головний сюжет і найважливіші об'єкти гри часто приховані у секретних місцях, які гравцеві доводиться відкрити, досліджуючи рівні.

При об'єднанні двох підходів до дизайну рівнів, гра може представляти великий та зв'язаний світ, який характеризує «Metroidvania». Гравцеві доведеться досліджувати цей світ, знаходячи нові навички та здібності, щоб отримати доступ до різних областей. В різних частинах світу можуть бути розташовані сильні вороги та боси, що характеризують «Soulslike». Ці вороги вимагатимуть від гравця високого рівня навичок та стратегії. Об'єднуючи два жанри, гра може створити глибокий і насичений сюжет, який розкриватиметься через дослідження світу та взаємодію з персонажами, аналогічно «Metroidvania». У той же час, важлива сюжетна інформація може бути прихована у секретах і записах, які бути важко знайти, як у «Soulslike». Результатом такої комбінації стане ігровий досвід, який використовує найкращі аспекти обох жанрів, надаючи гравцям глибокий іммерсивний світ для дослідження.

Об'єднання жанрів «Metroidvania» і «Soulslike» в одній грі може створити глибокий і захопливий ігровий досвід, який буде цікавим для гравців з різними смаками і вимогами. «Metroidvania» пропонує великі інтерконектовані світи з акцентом на дослідження та збільшення навичок персонажа. З іншого боку, «Soulslike» славиться високою важкістю гри і складною бойовою системою. Поєднання цих двох жанрів може призвести до створення гри з цікавим сюжетом, глибокими рівнями і наголосом на розвиток персонажа та стратегічну боротьбу.

Список використаних джерел

1. D. I. Klymenko. Metroidvanias and Souls-likes: A Comparative Analysis of Level Design and Gameplay Mechanics. *International Journal of Game Design and Development*. 2023. Vol. 13, No. 2, P. 1–16.

УДК 004

*Хімич В. О., магістрант,
Чижмоторя О. В., ст. викладач
Державний університет «Житомирська політехніка»*

МИНУЛЕ, ТЕПЕРІШНЄ ТА МАЙБУТНЄ СПОСОБІВ РОЗРОБКИ КОРИСТУВАЦЬКИХ ІНТЕРФЕЙСІВ ДЛЯ ОС ANDROID

Проаналізовано шлях розвитку способів розробки користувацьких інтерфейсів для ОС Android. Описано переваги нових підходів та способів розробки та зроблено висновки щодо майбутнього цих підходів.

Користувацькі інтерфейси пройшли довгу історію розвитку з самого початку створення ЕОМ. Спочатку взаємодія користувача відбувалася за допомогою строкових інтерфейсів, які керували комп'ютерами, що займали чи не цілу кімнату. Потім комп'ютери стали набувати більшого поширення та набувати популярності серед звичайних користувачів. Однак при цьому інтерфейси залишалися застарілими. Вирішенням цього стала розробка графічних інтерфейсів, з якими ми взаємодіємо і донині.

Хоч інтерфейси для користувача не змінили своєї суті, засоби їх розробки постійно змінюються і покращуються для кожної технології чи операційної системи. Android порівняно молода ОС, але при цьому постійно розвивається, і для розробників теж.

З самого початку користувацькі інтерфейси для застосунку під цю операційну систему мали досить типовий спосіб визначення - опис елементів інтерфейсу через теги в файлах з розширенням .xml, котрі були окремими ресурсами для модулю застосунку. Далі ці файли розмітки мали поєднуватися з програмним кодом через Activity/Fragment в окремих Java-файлах, де писалася логіка для інтерфейсу та обробка подій..

Google розуміли цю проблему і в 2016 році представили новий спосіб розробки інтерфейсів – databinding. Його суть полягала в тому, що для кожного .xml файлу застосунку, де корінним тегом є layout, автоматично генерувався код з елементами інтерфейсу, котрі мали атрибут id, тому тепер доступ до всіх потрібних елементів інтерфейсу в Activity/Fragment здійснювався лише через одну змінну з Binding необхідного екрану. Ще однією перевагою цього способу є те, що можна встановлювати значення для атрибутів елементів. До того ж з часом розвитку ОС Android та смартфонів користувацькі інтерфейси

стали значно більш складні та навантажені, а головна концепція залишилася на рівні 2008 року.

Однак у 2019 році на GoogleI/O [1] було перевинайдено концепцію та інструменти створення інтерфейсу для Android-застосунків, що отримало назву JetpackCompose. Це декларативний спосіб побудови інтерфейсу, на ідеї модульної розробки інтерфейсів з використанням можливостей головної мови розробки для Android – Kotlin.

З його застосуванням всі елементи інтерфейсу описуються у звичайних функціях з анотацією Composable, що дозволяє ділити інтерфейс на групи елементів, розмір та суть яких обирає сам розробник. Таким чином при роботі з JetpackCompose розробник по суті створює бібліотеку елементів інтерфейсу, необхідних саме його застосунку. Ще однією перевагою JetpackCompose є ідея використання принципу UnidirectionalDataFlow для оновлення стану UI в самій основі технології, що дозволяє значно зменшити кількість багів та проблем, пов'язаних з оновленням даних. Значним покращенням в порівнянні з .xml є те, що при зміні стану UI відбувається рендеринг лише тих Composable функцій, стан яких було змінено, і таким чином, якщо це зміна стану лише певного, навіть малого, елемента, то вона буде стосуватися лише його, зменшуючи навантаження на процесор мобільного пристрою. Разом зі стислістю коду, потрібного для опису інтерфейсу, та акцентом компанії Google, цей інструмент поступово набирає популярність.

Згідно досліджень з цієї статті [2] Compose має більшу продуктивність, коли елементи JetpackCompose підзавантажуються завчасно, наприклад, при переході з одного екрану написаного таким способом на інший. В порівнянні з .xml такий комплексний підхід матиме меншу кількість “заморожених” кадрів, але повільнішу швидкість завантаження екрану.

Отже, Android мав типову для свого часу концепцію побудови інтерфейсу, що давала достатню продуктивність, але з розвитком смартфонів та користувацьких інтерфейсів стала надто громіздкою та надлишковою для розробки. Цю проблему інженери Google вирішили гнучким, модульним та продуктивним інструментом.

Список використаних джерел

1. GoogleI/O Compose presentation [Електронний ресурс] – Режим доступу до ресурсу: <https://www.youtube.com/watch?v=VsStyq4Lzxo>.

2. Comparing Jetpack Compose performance with XML. [Електронний ресурс] – Режим доступу до ресурсу: <https://medium.com/okcredit/comparing-jetpack-compose-performance-with-xml-9462a1282>

УДК 621.3: 455.63

*Єфремов Ю. М., к.т.н., доцент,
Крискун С. І., магістрант*

Державний університет «Житомирська політехніка»

ОБҐРУНТУВАННЯ ВИБОРУ ІНСТРУМЕНТАЛЬНИХ ЗАСОБІВ ДЛЯ РОЗРОБКИ ВЕБ-САЙТУ

Веб-програмування стрімко розвивається кожного дня. Мною було обрано саме створення веб-сайту, через те, що я хочу розвиватися у сфері Front-End Development. Почнемо розгляд цього питання саме з програм, в яких і створювався мій програмний продукт. Задля того, щоб виконати завдання магістерської дипломної роботи я використовувала такі програми та технології: Adobe Photoshop, Visual Studio Code, HTML5, CSS3, JavaScript. Почнемо розгляд цього питання саме з програм, в яких і створювався цей програмний продукт.

Adobe Photoshop: продукт компанії Adobe Systems. Даний редактор є лідером серед дизайнерів, розробників та простих користувачів в області редагування різних типів зображень. Скорочено програму називають Фотошоп. Visual Studio Code: серед розробників йменованій як IDE, тобто середа розробки та редагування сучасних веб-програм, веб-застосунків та програм для хмарних систем, яка є безкоштовною для користувача. HTML5 (HyperTextMarkupLanguage) – мова гіпертекстової розмітки сторінки, яка допомагає створювати семантичну архітектуру сучасної веб-сторінки за допомогою блочних та вбудованих елементів, які можливо стилізувати. Cascading Style Sheets (CSS) – каскадна таблиця стилів. Мова, яка використовується для візуалізації та стилізації сторінок написаних на HTML (HTML5/XHTML). JavaScript є високорівневою, інтерпретованою мовою програмування, яка використовується для розробки динамічних веб-сайтів. Вона підтримує об'єктно-орієнтовану, подійно-орієнтовану та функціональну парадигми програмування. JavaScript використовується в браузерях для взаємодії з користувачем, а також на стороні сервера (за допомогою Node.js) для розробки серверних додатків. розробки різноманітних застосунків. Отже, як висновок, ми обґрунтували вибір технологій для розробки веб-сайту. Вище описані технології на сьогодні є найбільш розвиненими та мають самі сучасні версії для створення веб-програм.

Список використаних джерел

1. W3SCHOOLS [Електронний ресурс] – Режим доступу до ресурсу: <https://www.w3schools.com/JavaScript>;
2. Дуглас Крокфорд. JavaScript The Good Parts 2016. – 264 с.

УДК 621.3: 455.63

Крискун С. І., магістрант

Державний університет «Житомирська політехніка»

КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ: ІННОВАЦІЇ, ПРОБЛЕМИ, РІШЕННЯ

У світі стрімко розвиваючихся комп'ютерних технологій відбуваються значущі інновації, які переписують правила гри в різних галузях. Однак цей швидкий прогрес супроводжується низкою викликів, які потребують уважної уваги та вирішення.

Інновації в комп'ютерних технологіях: Інновації в комп'ютерних технологіях на сучасному етапі визначають темпи та напрямки технологічного розвитку. Кілька ключових напрямків інновацій включають: 1. Штучний інтелект (ШІ). 2. Блокчейн. 3. Інтернет речей (ІоТ). 5. Кібербезпека та блокування. З інноваціями комп'ютерних технологій виникають численні проблеми, деякі з них включають: 1. Кібербезпека: Недостатньо ефективний захист може призвести до витоку конфіденційної інформації, порушення приватності та фінансових втрат. 2. Етичні питання: Питання автономних систем, алгоритмів прийняття рішень та впливу на робочі місця вимагають уваги. 3. Приватність даних: Збільшення обсягів збирання та обробки даних, зокрема в рамках Інтернету речей, підвищує ризик порушення приватності користувачів. 4. Цифровий розрив: У деяких випадках інновації можуть призводити до посилення розриву між тими, хто має доступ до передових технологій, і тими, хто залишається позаду. 5. Залежність від технологій: Зростання залежності від комп'ютерних технологій може призвести до проблем при відмові систем або випадку технічних неполадок. Рішення та перспективи: Впровадження ефективних стратегій кібербезпеки, створення етичних стандартів для розробників ШІ та постійний контроль за використанням основних технологій є кроками у правильному напрямку.

Отже, як висновок, комп'ютерні технології, приносять неймовірний потенціал для розвитку суспільства та покращення якості життя. Для досягнення успішного розвитку в цьому цифровому епохальному контексті, важливо вдосконалювати кібербезпеку, вирішувати етичні питання та активно працювати над забезпеченням прозорості та захисту приватності.

Список використаних джерел

1. CORE. [Електронний ресурс] – Режим доступу ресурсу: <https://core.ac.uk/download/pdf/83099886.pdf>

УДК 004

Болотіна В. В. ст. викладач,

Панібратець О. Д., здобувач

Державний університет «Житомирська політехніка»

ОБРОБКА ЗОБРАЖЕНЬ ЗАСОБАМИ ADOBE PHOTOSHOP З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

З розвитком технологій та можливостей у сучасному суспільстві навряд чи знайдеться людина, яка б не чула про Adobe Photoshop або Adobe загалом. На це є просте пояснення: ми живемо у світі, який прямо пропорційно залежить від нових розробок та покращення інформаційного середовища. Ми вже просто не можемо відмовитись від величезної кількості медіа, що представляє собою фотографії, відео, рекламу, банери, сайти і т.д. Тобто це вже є частиною нас. Така програма, як Photoshop перетворює сірі непримітні зображення на справжні витвори мистецтва. Люди звикли, що творчість – це лише щось створене руками на папері, за допомогою фарб, дерева, глини і т.д. Але вже це не зовсім так. Новітні технології дозволяють витратити менше ресурсів, але створювати так само багато контенту. Завдяки своїй універсальності він став однією з найкращих програм для редагування фотографій майже у всьому світі.

Adobe Photoshop простий у використанні і має багато інструментів та функцій, які можна швидко освоїти. Перше, що варто відмітити – це редагування фотографій. Редактор дозволяє змінювати насиченість, пропорції, перспективу та налаштування світла. Це дозволяє покращити вигляд оригінальної фотографії або створити щось абсолютно нове.

Ще однією перевагою є нова функція «GenerativeExpand», яка використовує згенерований ШІ вміст для розширення зображення. Щоб скористатися цією функцією, потрібно перетягнути інструмент обрізання за межі початкового розміру зображення і додати текстові підказки. Adobe вважає, що ця функція буде корисною для творців контенту, які хочуть змінити співвідношення сторін, замінити обрізані об'єкти та якимось модифікувати ілюстрації. До речі, текстові підказки Generative наразі існують приблизно на 100 мовах і ця цифра постійно збільшується. Варто зазначити, що штучний інтелект став основоположником нової ери в Adobe Photoshop, дозволивши маніпулювати зображеннями в складні способи без необхідності вивчати нове програмне забезпечення. Наприклад, генеративна заливка надає дуже зручний спосіб замінити частини існуючого зображення. Він називається «inpainting», де ви вибираєте те, що

хочете змінити, і вводите те, що повинно бути включено і цю область. І це виходить далеко за межі існуючих інструментів штучного інтелекту, які різні компанії використовують для виправлення дефектів і покращення фото.

Штучний інтелект Photoshop є ідеальним способом, щоб за кілька секунд робити впливові підробки, які потім можуть негативно впливати на чиєсь життя. Адже сама технологія штучного інтелекту, яка допомагає прибрати якихось птахів із зображення, може також створити дуже переконливе зображення повністю вигаданої пожежі в Пентагоні (таке зображення якийсь час було досить вірусним у твіттері). Тому на кожен позитивний відгук отримується близько п'яти відповідей незадоволених користувачів. Основна проблема полягає в тому, що штучний інтелект Photoshop просто не вміє генерувати певні типи об'єктів, тому реалізація деяких запитів може виглядати безглуздо, недомальовано або просто фальшиво. І якщо говорити про людей, ШІ Photoshop найгірше справляється з ними. Область, яка вибирається на вихідному зображенні, значно впливає на результат. Штучний інтелект Adobe розроблений таким чином, що реагує саме на форму виділення. Adobe Photoshop став незамінним інструментом у багатьох сучасних професіях.

Із появою штучною інтелекту працювати стало дещо швидше, адже певну частину завдань можна передати йому. Замінити фон, збільшити зображення та додати частину фото, якої не існує, прибрати недоліки на фото та багато інших вище перелічених можливостей, що має ШІ. Також такі картинки можуть слугувати натхненням для творців, тому це неабияка перевага. Проте, варто ставитись до цього з обачністю та правильно вводити запити. В результаті використання існує дуже мала ймовірність, що ШІ зможе повністю замінити художників, дизайнерів, бо без аналізу поставленої задачі людським мозком іноді важко створити те, що хочеться.

Список використаних джерел

1. Photoshop нині: як графічний редактор став інструментом для всіх – Bazilik Media. BazilikMedia. URL: <https://bazilik.media/photoshop-puni-ia-k-hrafichnyj-redaktor-stav-instrumentom-dlia-vsikh/>

2. Камінський Б. Компанія Adobe оновила бета-версію Photoshop функцією Generative Expand, яка збільшує зображення за допомогою ШІ. Speka – онлайн медіа про технології та підприємництво. | SPEKA.media | SPEKA.media. URL: <https://speka.media/photoshop-teper-vikoristovuje-si-dlya-rozsirennya-zobrazen-p645n9>.

УДК 658.7

*Багрій В. В., аспірант,
Граф М. С., PhD*

Державний університет «Житомирська політехніка»

ОГЛЯД МЕТОДІВ ТА ПРОГРАМНИХ ЗАСОБІВ ДЛЯ ОПТИМІЗАЦІЇ ЛОГІСТИЧНИХ ПРОЦЕСІВ У ВАНТАЖНИХ ПЕРЕВЕЗЕННЯХ

Від моменту зародження галузі вантажних перевезень і до сучасності, важливим аспектом залишається впровадження ефективного планування усіх етапів логістичних процесів, а також складання найбільш оптимальної стратегії раціонального розподілу ресурсів та максимального зниження ризиків під час здійснення рейсів. Поява і розвиток електронно-обчислювальних машин (ЕОМ) створили сприятливі умови для появи нових методів оптимізації, але, попри це, через великі об'єми, складність і високу динамічність розвитку технологій, ці методи постійно потребують вдосконалення. Для розуміння проблематики цього питання, спочатку потрібно провести аналіз існуючих методів та програмних засобів оптимізації логістичних процесів.

Серед науковців, важливий вклад в загальні принципи логістичних процесів і методів їх оптимізації зробили: Крістофер М., Хау Л. Лі, Сімчі-Леві Д., Глок К.Х., Датта П.П., Елрам Л.М., Огдрен Дж.А., Фосетт С.Е., Ламберт Д.М., Купер М.С., Менцер Дж.Т., ДеВітт В., Кіблер Дж.С., Мін. С., Сміт К.Д., Захарія З.Д., Шимонік А., Окслі Дж., Краучер Ф., Стро М.Б., Шеффі Й., Вайс Г., Слоун Р., Дітман Дж. П., Боддінгтон Р.Е., Вудрафф Д.Л., Дрезнер Ц. Питанням оптимізації логістичних процесів за рахунок сучасних інформаційних технологій займалися такі вчені: Грейвс С., МакГініс Л., Пурселл Ф., Ньюман Дж. Серед вітчизняних науковців, слід виділити роботи: Ільченко М., Кот С., Божиновський О., Малярець Л.М, Матвієнко-Біляєва Г.Л., Поліщук Н.В., Крикавський С.В., Ткачова А.В., Василевський О., Піх В., Гудима В., Гладишевський Т., Головач О., Шищенко О.

Серед найбільш популярних сучасних методів оптимізації логістичних задач слід зазначити:

1. Метод використання системи управління ланцюгом постачання (англ. Supplychainmanagement, SCM) [1]
2. Метод системів відстеження (англ. TrackingandTracing) [2]
3. Метод використання Інтернет-речей (англ. Internet of Things, IoT) [3]

Системи управління ланцюгом постачання (англ. supply chain management) - це прикладне програмне забезпечення, метою якого є управління всіма етапами постачання підприємства, автоматизація усіх процесів, а також надання можливості вести контроль над переміщенням товарів. На рисунку 1 зображено принцип дії системи, яка пов'язує і контролює процеси виробництва, логістичних операцій, планування, клієнтський сервіс, фінансові операції і проектування.

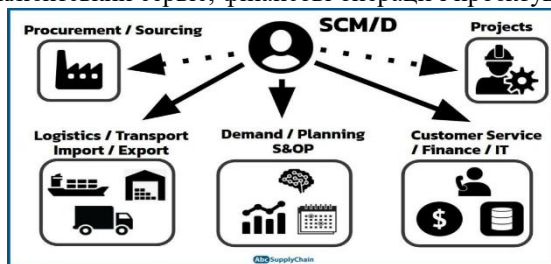


Рис. 1. Загальна схема роботи SCM-системи [4]

Наведена система ділиться на дві підсистеми – SCP (англ. supply chain planning) і SCE (англ. supply chain execution). SCP – це система, що відповідає за планування ланцюгів постачання. В основі цієї системи лежить формування календарних графіків та складання систем розгорнутого планування. SCE – система відстеження і контролю логістичних процесів [1]. Найбільш популярними сервісами, що використовують методи оптимізації SCM, є: Інтернет логістична компанія Transporeon group [5], ABM Inventory [6], JDA Luminate від Blue Yonder [7].

Система відстеження (англ. tracking and tracing) – це система, що поєднує інформаційні системи з системами матеріальних потоків, даючи можливість слідкувати за логістичними процесами у режимі реального часу. В наш час це є надзвичайно важливо, адже через складність і багатогранність багатьох процесів, виникає багато ризиків, а також обставин, які потребують швидких рішень. Основний принцип роботи даної технології лежить у відстеженні місце розташування об'єкта і якщо об'єкт надходить у визначений пункт, система посилає відповідні дані до бази даних. Ці дані містять в собі такі відомості: інформація про попередній пункт, місцезнаходження теперішньої точки і час прибуття. Також може містити дані про подальшу точку, інформацію про товар, інші деталі щодо вантажу. На рисунку 2 зображено загальний процес роботи системи відстеження, де спочатку формуються дані щодо об'єкта матеріального потоку, а далі при досягненні потрібних точок, ці дані оновлюються [2].

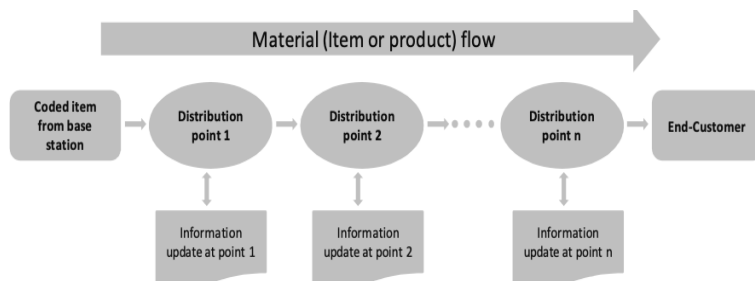


Рис. 2. Загальна схема роботи системи відстеження [2]

Найбільш популярними сервісами для реалізації цього методу оптимізації є: сервіс трекінгу від Ubisolutions [8], Track-Trace [9], Vee technologies [10].

Системи використання Інтернет-речей (Internet of Things) – це системи, які дають можливість об'єднати усі об'єкти у одну мережу, з постійним моніторингом стану, місцеположення і статусу об'єкту. Усі зібрані дані в певну одиницю часу записуються до бази даних, після чого проводиться аналіз отриманої інформації. Отримані дані можуть вказати на причини збоїв роботи, відхилення від норми робочого процесу, а також надати необхідну інформацію для подальшого прогнозу наступних ітерацій логістичних процесів. В результаті, власник виробництва, чи перевізник матиме автоматизовану систему збору даних, буде мати змогу оптимізувати фінансові витрати і отримає підвищений рівень передбачуваності ризиків. Одним з яскравих прикладів використання Інтернет-речей у логістиці є застосування GPS-навігатора, для відстеження місця перебування вантажного автомобіля. Це дає можливість миттєво отримувати інформацію щодо перебування водія для кращого розуміння ситуації, а також зменшує ризики викрадення авто [3]. Прикладами таких сервісів є: Asset Insight [11], IoT BICS [12], KIS.ME [13].

У даному науковому дослідженні було проведено огляд найпопулярніших і найбільш сучасних методів і програмних засобів оптимізації логістичних процесів у галузі вантажних перевезень.

Список використаних джерел

1. Лисак О.І., SCM-системи як засіб автоматизації управління постачанням. Збірник наукових праць Таврійського державного агротехнологічного університету імені Дмитра Моторного. 2022. Вип. 1. С 125-132.

2. Shamsuzzoha, Petri T. Helo. Real-time Tracking and Tracing System: Potentials for the Logistics Network. International Conference on Industrial Engineering and Operations Management.

3. Колешня Я. О., Кравець А. І. Інтернет речей у логістиці. II Міжнародна науково-практична конференція «Бізнес, інновації, менеджмент: проблеми та перспективи». 2021. С. 262-263.

4. What is Supply Chain Management?. [Електронний ресурс] – Режим доступу ресурсу: URL: <https://abcsupplychain.com/what-is-supply-chain/>.

5. Transporeon group official site. [Електронний ресурс] – Режим доступу ресурсу: URL: <https://www.transporeon.com/en/>.

6. ABM Inventory official site. [Електронний ресурс] – Режим доступу ресурсу: URL: <https://abmcloud.com/en/abm-soft/abm-inventory/>.

7. Blue yonder official site. [Електронний ресурс] – Режим доступу ресурсу: URL: <https://blueyonder.com/solutions>.

8. Ubisolutions official site. [Електронний ресурс] – Режим доступу ресурсу: URL: <https://ubisolutions.net/en/solution/assets-tracking-3/>.

9. Track and trace official site. [Електронний ресурс] – Режим доступу ресурсу: URL: <https://www.track-trace.com/>.

10. Vee technologies official site. [Електронний ресурс] – Режим доступу ресурсу: URL: <https://www.veetechnologies.com/>.

11. Asset Insight official site. [Електронний ресурс] – Режим доступу ресурсу: URL: <https://www.a1.digital/iot/solutions/asset-insight/>.

12. IoT BICS official site. [Електронний ресурс] – Режим доступу ресурсу: URL: <https://www.bics.com/>.

13. KIS.ME official site. [Електронний ресурс] – Режим доступу ресурсу: URL: <https://kisme.com/de/>.

УДК 004:42

*Москалик О. С., магістрант,
Левківський В. Л., ст. викладач
Державний університет «Житомирська політехніка»*

ОГЛЯД АЛГОРИТМІВ МАШИННОГО НАВЧАННЯ

У сучасному світі машинне навчання стало невід’ємною частиною нашого життя, воно відіграє важливу роль завдяки своєму широкому застосуванню і потужному впливу на різні сфери діяльності.

Алгоритми машинного навчання натреновані знаходити взаємозв’язки та закономірності в даних. Термін «машинне навчання» часто помилково плутають з поняттям «штучний інтелект» (ШІ), але машинне навчання насправді є підгалуззю ШІ. Термін «машинне навчання», введений американським вченим Артуром Семюелом у 1959 році, визначається як «здатність комп’ютера навчатися без явного програмування» [1].

На рисунку 1 можна побачити наявні алгоритми у машинному навчанні та їх коротку характеристику.

Machine learning models and their training algorithms

Supervised learning	Unsupervised learning	Semi-supervised learning	Reinforcement learning
<p>Data scientists provide input, output and feedback to build model (as the definition).</p> <p>EXAMPLE ALGORITHMS:</p> <p>Linear regressions</p> <ul style="list-style-type: none"> Sales forecasting. Risk assessment. <p>Support vector machines</p> <ul style="list-style-type: none"> Image classification. Financial performance comparison. <p>Decision trees</p> <ul style="list-style-type: none"> Predictive analytics. Pricing. 	<p>Use deep learning to arrive at conclusions and patterns through unlabeled training data.</p> <p>EXAMPLE ALGORITHMS:</p> <p>Apriori</p> <ul style="list-style-type: none"> Sales functions. Word associations. Searcher. <p>K-means clustering</p> <ul style="list-style-type: none"> Performance monitoring. Searcher intent. <p>Artificial neural networks</p> <ul style="list-style-type: none"> Generate new, synthetic data. Data mining and pattern recognition. 	<p>Builds a model through a mix of labeled and unlabeled data, a set of categories, suggestions and example labels.</p> <p>EXAMPLE ALGORITHMS:</p> <p>Generative adversarial networks</p> <ul style="list-style-type: none"> Audio and video manipulation. Data creation. <p>Self-trained Naive Bayes classifier</p> <ul style="list-style-type: none"> Natural language processing. 	<p>Self-interpreting but based on a system of rewards and punishments learned through trial and error, seeking maximum reward.</p> <p>EXAMPLE ALGORITHMS:</p> <p>Q-learning</p> <ul style="list-style-type: none"> Policy creation. Consumption reduction. <p>Model-based value estimation</p> <ul style="list-style-type: none"> Linear tasks. Estimating parameters.

Рис. 1. Алгоритми машинного навчання [1]

У навчанні під наглядом (supervised learning) машина навчається на прикладах. Оператор надає алгоритму машинного навчання відомий набір даних, який включає бажані вхідні та вихідні дані, а алгоритм повинен знайти метод, щоб визначити, як отримати ці вхідні та вихідні дані. У той час, як оператор знає правильні відповіді на завдання, алгоритм виявляє закономірності в даних, вчиться на основі

спостережень і робить прогнози. Алгоритм робить прогнози і коригується оператором, цей процес триває доти, доки алгоритм не досягне високого рівня точності або продуктивності [2].

Напівкероване навчання (semi-supervised) схоже на кероване навчання, але замість цього використовує як мічені, так і немічені дані. Марковані дані – це інформація, яка має значущі теги, щоб алгоритм міг зрозуміти дані, тоді як не марковані дані не мають такої інформації. Використовуючи цю комбінацію алгоритми машинного навчання можуть навчитися маркувати немарковані дані.

Алгоритм некерованого навчання вивчає дані для виявлення закономірностей. Тут немає ключа для відповідей, або людини-оператора, яка б давала вказівки. Замість цього машина визначає кореляції та взаємозв'язки, аналізуючи наявні дані. Алгоритм намагається організувати ці дані певним чином, щоб описати їхню структуру.

Навчання з підкріпленням фокусується на регламентованих процесах навчання, де алгоритм машинного навчання забезпечується набором дій, параметрів і кінцевих значень. Визначивши правила, алгоритм машинного навчання намагається дослідити різні варіанти та можливості, відстежуючи та оцінюючи кожен результат, щоб визначити, який з них є оптимальним. На відміну від інших алгоритмів, навчання з підкріпленням вчить машину методом проб і помилок. Вона вчиться на минулому досвіді і починає адаптувати свій підхід у відповідь на ситуацію, щоб досягти найкращого результату [3].

У підсумку, аналіз показав, що у кожного з цих алгоритмів є свої переваги та недоліки і вибір залежить від конкретної задачі та доступних даних. Зазвичай важливо правильно підібрати тип навчання для конкретного завдання, оскільки це може суттєво вплинути на результати та ефективність моделі машинного навчання.

Список використаних джерел

1. Tucci L., Burns E. What is Machine Learning and How Does It Work? In-Depth Guide. Enterprise AI. [Електронний ресурс] – Режим доступу ресурсу: URL: <https://shorturl.at/vDEI6>.

2. Wakefield K. A guide to the types of machine learning algorithms. [Електронний ресурс] – Режим доступу ресурсу: URL: <https://shorturl.at/dwCL9>.

3. Wong W. StackPath. *StackPath*. [Електронний ресурс] – Режим доступу ресурсу:

URL: <https://www.electronicdesign.com/markets/automotive/article/21804976/whats-the-difference-between-machine-learning-techniques>

УДК 004

Петросян А. Р., аспірант

Державний університет «Житомирська політехніка»

ОРГАНІЗАЦІЯ ТЕСТУВАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДРОНА

Безпілотні повітряні судна (БПС, дрони) становлять важливу частину наукових досліджень у військовій, промисловій та цивільній сферах діяльності: аерофотозйомка та картографування, оперативне отримання інформації про наслідки надзвичайних ситуацій, моніторинг за об'єктами промисловості та природних комплексів, доставка товарів, у розважальних цілях тощо. Помилки, допущені на етапі проектування дрона та розробки його програмного забезпечення (ПЗ), можуть спричинити виникнення аварійних ситуацій або інших непередбачених збоїв у процесі їх експлуатації. У зв'язку з цим постає завдання перевірки надійності програмного забезпечення бортового комп'ютера дрона, що дозволить спростити супровід, модернізацію та оптимізацію програмного забезпечення.

Налагодження та тестування програмного забезпечення дрона є складним завданням. Проблема полягає у складності формування повного набору сигналів датчиків та неможливості створення на реальному дроні позаштатних ситуацій.

Для перевірки надійності ПЗ при розробці, виконують його тестування. За ступенем ізольованості коду існує 4 рівні тестування[1]:

- модульне тестування (unit testing);
- інтеграційне тестування (integration testing);
- системне тестування (system testing);
- приймальне тестування (acceptance testing).

Застосування тестування під час розробки, наприклад, прикладного ПЗ для комп'ютера (software) достатньо, щоб забезпечити необхідний рівень надійності програми, однак для ПЗ вбудованих систем (прошивки, firmware) – ні.

Імітаційне моделювання (симуляція) – метод дослідження, який використовує моделі, що описують процеси реального світу. Використовуючи такі моделі можна провести випробування реальної системи не наражаючи її на небезпеку. До імітаційного моделювання найчастіше вдаються, коли неможливо провести експеримент на реальному об'єкті або необхідно симулювати поведінку реальної системи в часі.

Тест прошивки при симуляції дрона можна виконати у трьох місцях: на хост-комп'ютері, використовуючи компіляцію коду під

вихідну платформу; в емуляторі на хост-комп'ютері, наприклад, QEMU; на реальному контролері дрона, використовуючи крос-компіляцію коду для цільового обладнання.

Перші два варіанти використовуються при виконанні симуляції SIL (Software in the Loop) [2]. Перевага SIL в тому, що його легко організувати, оскільки не потрібно додаткового обладнання, а в нашому випадку – бортового комп'ютера. Вона дозволяє розробникам виконати тестування прошивки на ранніх етапах розробки, ще до того, як воно буде інтегроване в цільове обладнання. Третій варіанти використовуються при виконанні симуляції HIL (Hardware in the Loop) [2]. Симуляція HIL включає використання цільового обладнання, що максимально наближає роботу системи до реальних умов.

Однією з реалізацій імітаційного моделювання у програмуванні є використання mock-об'єктів. Призначення mock-об'єктів полягає в заміні об'єктів, що тестуються у програмному коді, на відлагоджувальні еквівалентні об'єкти. Такий підхід використовується в автопілоті PX4 для імітації датчиків, таких як гіроскоп, акселерометр, магнітометр тощо [3], використовуючи для передачі інформації датчиків послідовний інтерфейс. Недолік такого підходу в тому, що частина коду, яка заміщена mock-об'єктами, не буде протестована або тестування цього коду необхідно організувати окремо.

Для усунення зазначеного недоліку пропонується інформацію датчиків передавати через відповідні інтерфейси бортового контролера дрона, використовуючи окремий блок (рис. 1).

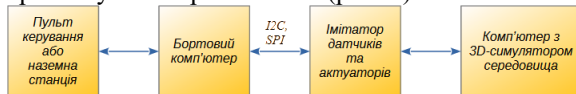


Рис.1. Структурна схема тестування системи

Список використаних джерел

1. Aniche M. Effective Software Testing: A Developer's Guide. Manning Publications Co., 2022. 328 p.
2. Coopmans C., Podhradský M., Hoffer N. Software-and hardware-in-the-loop verification of flight dynamics model and flight control simulation of a fixed-wing unmanned aerial vehicle. 2015 Workshop on Research, Education and Development of Unmanned Aerial Systems (RED-UAS), November 23-25, 2015. Mexico. 2015. С. 115–122.
3. Петросян А.Р., Граф М.С. Архітектура бортового комп'ютера безпілотного повітряного судна. Тези доповідей науково-практичної конференції, 24-25 листопада 2022 року. Київ: «Національний авіаційний університет». 2022. С.24-25.

УДК 004

*Праздніков В. О., асистент,
Розбицький Р. Е., здобувач*

Державний університет «Житомирська політехніка»

ОСОБЛИВОСТІ ТА ЗАСТОСУВАННЯ ГРАФОВИХ БАЗ ДАНИХ

Граф – це математична структура, що включає в себе вершини та ребра, які їх з'єднують. Вершини – об'єкти, ребра – зв'язки між вершинами. Вершини можна уявити як залізниці, а ребра – як колії. Графи широко використовуються для моделювання різноманітних систем, де важливі зв'язки та залежності між елементами. Розділ математики що вивчає властивості графів, називається теорією графів. Графові бази даних – потужний різновид баз даних, що базується на теорії графів. Вони забезпечують ефективне управління даними, які мають складну структуру і взаємозв'язки між собою через свою ключову особливість: зберігання як об'єктів, так і зв'язків між ними.

На сьогодні існує декілька основних галузей використання графових баз даних. Соціальні мережі: графові бази даних ідеально підходять для зберігання та аналізу великих обсягів даних, пов'язаних із соціальними взаємозв'язками. Логістика та транспорт: графові бази даних застосовуються для моделювання та оптимізації транспортних систем, де важливі різноманітні шляхи та взаємозв'язки між вузлами. Біологічні та хімічні дослідження: графові бази даних використовуються для представлення та аналізу генетичних та молекулярних взаємозв'язків у біології та хімії. Однією з найважливіших переваг графових баз даних є швидкий пошук і навігація по графам. Це можливо через те, що пошук по графу набагато швидший за традиційні методи пошуку в таблицях чи колекціях. Також важливим плюсом є гнучкість та масштабованість, можливі через властивості графа.

Найбільшою проблемою графових баз даних є складність в управлінні, пов'язана більшою з комплексністю графа як структури даних в порівнянні з традиційними таблицями. Не менш важливою проблемою є менша популярність.

У порівнянні з іншими типами баз даних, графові програють в популярності. Через це існує менше довідкових та навчальних ресурсів, пов'язаних з ними, а також спеціалістів, що вміють з ними працювати. Проблеми графових баз даних та шляхи їх вирішення активно обговорюються в ряді наукових досліджень та публікацій у галузі баз даних, інформаційних технологій та комп'ютерних наук. Багато з цих досліджень направлені на різні аспекти оптимізації

графових баз даних та представляють нові методи та алгоритми для покращення їх продуктивності та функціональності.

Отже, графові бази даних – це потужний інструмент для моделювання та аналізу складних взаємозв'язків даних. Вони стають все більш важливими в контексті сучасних вимог до зберігання та обробки даних, а також відкривають нові можливості для аналізу складних мережевих структур та дозволяють ефективно працювати з великими обсягами взаємозв'язаних даних.

Список використаних джерел

1. Yoon, Byoung-Ha; Kim, Seon-Kyu; Kim, Seon-Young (March 2017). «Use of Graph Database for the Integration of Heterogeneous Biological Data». *Genomics & Informatics*. 15 (1): 19–27. doi:10.5808/GI.2017.15.1.19.
2. Angles, Renzo; Gutierrez, Claudio (1 Feb 2008). «Survey of graph database models» (PDF). *ACM Computing Surveys*.

УДК 004.78

*Кадькало В. В., магістрант,
Чижмоторя О. В., ст. викладач
Державний університет «Житомирська політехніка»*

ПЕРСПЕКТИВИ ТА ВИКЛИКИ ІНТЕГРАЦІЇ СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ З РІШЕННЯМИ ДЛЯ УПРАВЛІННЯ КОНТЕЙНЕРИЗОВАНИМИ ДОДАТКАМИ

У сучасному світі контейнеризація часто відіграє ключову роль у розробці, розгортанні та управлінні програмними застосунками. Це технологія, яка дозволяє об'єднати застосунки та їх залежності в єдине середовище. Завдяки цьому впровадження контейнеризації може мати позитивний вплив на ефективність та гнучкість програмних рішень при їх розробці, розгортанні чи підтримці. Однак, з розвитком технологій та зростанням обсягів даних, виникають нові потенційні проблеми та виклики, зокрема у сферах оптимізації ресурсів, безпеки та автоматизації процесів. Сучасні системи штучного інтелекту можуть запропонувати рішення що потенційно можуть допомогти у вирішенні таких викликів.

Автоматизація та оптимізація процесів і ресурсів є одними із тих сфер, в яких використання штучного інтелекту може мати значний вплив. За допомогою машинного навчання, можливо реалізувати компоненти системи що здатні аналізувати використання ресурсів та ефективність роботи контейнерів, а також виконувати оптимізацію розподілу навантаження та ресурсів. Це не тільки може значно покращити продуктивність системи, але й значно знизити витрати компаній на інфраструктуру. Наприклад, такі компоненти можуть визначити потребу в масштабування системи, виділяючи необхідні додаткові ресурси для обробки збільшеного навантаження або, навпаки, вивільняти ресурси які не використовуються системою у періоди нижчого навантаження.

Ще однією з сфер в якій використання штучного інтелекту може надати суттєві переваги є безпека в контейнеризованих середовищах. Так системи, які використовують методи штучного інтелекту для аналізу поведінки та виявлення аномалій, можуть надати можливість швидко ідентифікувати потенційні загрози безпеці, такі як вразливості системи або зловмисні дії користувачів, і вживати заходи для їх нейтралізації. Це особливо важливо в умовах зростання кіберзагроз та постійного розвитку різноманітних способів кібератак.

Прогнозування та аналітика також є важливими областями в яких застосування систем штучного інтелекту може суттєво покращити

очікувані результати. При роботі з великими обсягами даних в контейнеризованих середовищах, штучний інтелект може допомогти в аналізі та розумінні тенденцій. Наприклад, аналіз поведінки користувачів та трафіку даних може допомогти в оптимізації розподілу ресурсів та плануванні майбутнього покращення інфраструктури.

Одним з новітніх напрямків в інтеграції штучного інтелекту є використання просунутих чат-ботів. Такий бот може використовуватись для управління та моніторингу контейнеризованих середовищ надаючи користувачеві зручний мовно-орієнтований інтерфейс що може значно спростити взаємодію з системою. Така технологія може полегшити користувацький досвід зробивши управління контейнеризованими середовищами більш доступним та зрозумілим навіть для людей без глибоких технічних знань в даній сфері. Окрім того такі чат-боти можуть бути інтегровані з іншими системами аналітики та моніторингу що дозволить отримувати більш комплексний аналіз стану системи у зручній для людини формі. Таким чином потенційно використання просунутих ІІІ чат-ботів може відкрити нові горизонти в управлінні контейнеризованими додатками, роблячи такі системи надзвичайно інтуїтивними. Однак дуже важливо звертати увагу на аспекти конфіденційності особливо в умовах коли необхідно обробляти чутливі дані.

Незважаючи на численні переваги, інтеграція штучного інтелекту у системи управління контейнеризованими додатками також має свої недоліки та потенційні проблеми. Одним з таких викликів є складність та вартість розробки ефективних рішень що базуються на використанні штучного інтелекту. Також, існують питання приватності, пов'язані з використанням даних.

Враховуючи вищезазначені перспективи та виклики, можна з упевненістю казати про те що інтеграція штучного інтелекту у системи управління контейнеризованими додатками відкриває нові можливості для розвитку ІТ-інфраструктури, роблячи її більш гнучкою, ефективною та безпечною. Однак для повноцінного використання цих переваг необхідно забезпечити ефективне планування, розробку та управління ресурсами, враховуючи потенційні виклики та проблеми що виникають при впровадженні таких систем.

Список використаних джерел

1. M. K. Sharma, A. K. Shukla (2023) «Artificial Intelligence for Containerized Applications: A Survey»

УДК 621.3: 455.63

*Каранет Л. В., магістрант,
Савіцький Р. С., викладач, аспірант
Державний університет «Житомирська політехніка»*

ПЛАТФОРМА ДЛЯ НАВЧАННЯ З ОБМЕЖЕНИМИ МОЖЛИВОСТЯМИ

Сьогоднішній світ навчання і розвитку отримав зміни завдяки технологічним досягненням та інноваціям. Разом із можливостями було отримано і виклики. В країні збільшилась кількість інклюзивних студентів, а платформи для навчання з обмеженими можливостями залишаються недостатньо розробленими та недоступними для вчителів та учнів [1].

Ключовим аспектом вирішення проблем є концепт вебдоступності, що визначає принципи розробки веб-сайтів та веб-додатків, орієнтованих на максимально можливий доступ до них для різних користувачів незалежно від фізичних, когнітивних чи сенсорних обмежень [2]. Заданий підхід стає необхідним для забезпечення інклюзивності та рівності доступу до освіти та інформації.

Вебдоступність стає все важливішою у цифровому світі. Для розробників це означає не лише створення красивого та функціонального вебінтерфейсу, але й забезпечення доступності цього інтерфейсу для всіх користувачів, незалежно від їхніх фізичних, когнітивних чи сенсорних обмежень [3]. Вебдоступність є ключовою для інклюзивності та рівності доступу до інформації та послуг. Ось ключові аспекти вебдоступності з погляду розробника:

- **Знання стандартів вебдоступності.** Знання стандартів вебдоступності, таких як WCAG (Web Content Accessibility Guidelines), є невід'ємною частиною професійної компетентності розробника [4]. WCAG визначає чіткі та конкретні правила та керівництво для створення вебконтенту, який буде доступним для всіх користувачів, включаючи тих, які мають різні обмеження та потреби. Розробник повинен не лише ознайомитися з цими стандартами, але й вміти їх впроваджувати в практиці, забезпечуючи високий рівень доступності свого веб-контенту.

- **Семантична розмітка:** Використання правильної семантичної розмітки є важливим аспектом вебдоступності [5]. Це включає в себе використання правильних HTML-тегів для різних елементів сторінки, що допомагає користувачам з обмеженнями отримувати інформацію зрозуміло та безпечно.

- **Клавішні сполучення та навігація з клавіатури:** Розробники повинні забезпечити, щоб всі функції та елементи на сайті були

доступні для навігації за допомогою клавіатури. Це особливо важливо для людей з обмеженими можливостями, які не можуть використовувати мишу.

• **Альтернативний контент:** Важливо надавати альтернативний контент для мультимедійних елементів, таких як зображення, аудіо та відео [6]. Це дозволяє користувачам з обмеженими можливостями отримувати інформацію, навіть якщо вони не можуть взаємодіяти з вмістом безпосередньо.

• **Тестування з використанням допоміжних технологій.** Тестування з використанням допоміжних технологій, таких як читачі екрану, є необхідним етапом в розробці веб-контенту. Це допомагає переконатися, що весь контент є доступним і зрозумілим для користувачів із різними потребами та обмеженнями.

• **Постійна підтримка та вдосконалення.** Постійна підтримка та вдосконалення вебдоступності є важливим аспектом розробки. Розробники повинні слідкувати за змінами у потребах користувачів і вдосконалювати свій веб-контент відповідно до цих змін [7]. Вироблення та впровадження найновіших технологій та методів є необхідною умовою для забезпечення високого рівня вебдоступності та підтримки різноманітних користувачів [8].

Забезпечення вебдоступності є не тільки питанням етики, але і законодавчо обов'язковим в багатьох країнах. Розробники, які приділяють увагу цьому аспекту, допомагають створити більш доступне та інклюзивне інтернет-середовище для всіх користувачів.

Список використаних джерел

1. Доступність веб-простору: як та для чого [Електронний ресурс] – Режим доступу: <https://ud.org.ua/statti/293-veb-dostupnist>.

2. Веб-доступність. Що варто знати кожному Front-end розробнику і дизайнеру. [Електронний ресурс] – Режим доступу: <https://www.dental.dentplex.com.au/veb-dostupnist%D1%8C-shho-var-to-znati-kozhnomu-front/>

3. Чому вебдоступність – це не примха і як про неї подбати [Електронний ресурс]. – Режим доступу: <https://devzone.org.ua/post/comu-vebdostupnist-ce-ne-primxa-i-iak-pro-neyi-podbati>.

4. WCAG стандарт [Електронний ресурс] – Режим доступу: <https://www.w3.org/WAI/standards-guidelines/wcag/>.

5. Accessibility Checklist for Front-End Developers [Електронний ресурс].– Режим доступу: <https://holistical1y.com/accessibility-checklist-for-front-end-developers/>.

6. Accessibility for Teams [Електронний ресурс] – Режим доступу: <https://accessibility.digital.gov/front-end/getting-started/>.

7. Building Accessible Front-Ends [Електронний ресурс] <https://medium.com/capital-one-tech/building-accessible-front-ends-298c03e5bd86>.

8. A (Short) Guide to Accessibility in Front-End Engineering [Електронний ресурс] – Режим доступу: <https://levelup.gitconnected.com/a-short-guide-to-accessibility-in-front-end-engineering-f7577d00da48>.

УДК 004.92

Марчук Д. К., ст. викладач,

Олексюк О. С., здобувач

Державний університет «Житомирська політехніка»

ПРОБЛЕМИ ТА РІШЕННЯ В ПРОЦЕСІ 3D МОДЕЛЮВАННЯ, UV РОЗГОРТКИ ТА ТЕКСТУРИНГУ

3D моделювання є ключовим аспектом створення віртуальних об'єктів, ігор та візуальних ефектів у різних галузях, включаючи геймдев, архітектуру, кіно та дизайн. Процес створення 3D моделей передбачає ряд складних завдань, включаючи моделювання об'єкта та ретопологію, UV розгортку та текстуринг.

Під час моделювання можуть виникати різні помилки, такі як неправильна топологія (1), дублювання вершин та N-Gon (2), T-вертекси (3), артефакти або розриви в меші (4) (рис. 1).

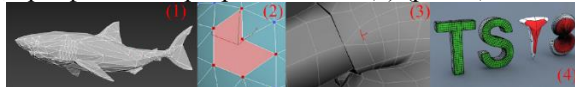


Рис. 1. Помилки моделювання

Створення надто деталізованих моделей може призвести до великої кількості полігонів, що збільшує вагу файлу та знижує продуктивність на обладнанні користувача. Рішення:

- Використати normalmaps, щоб емулювати деталі без додаткових полігонів.
- Видалити невидимі полігони (backfaceculling).
- Використати техніки оптимізації, які дозволяють користуватися LevelofDetail (LOD), тобто різними рівнями деталізації в залежності від відстані об'єкта від камери.

Ретопологія полягає у переробці вже існуючої моделі, зменшенні кількості полігонів та оптимізації топології для покращення продуктивності та якості моделі. Проблеми, що виникають, включають видалення надмірних полігонів без втрати деталей, збереження правильної форми об'єкта та створення топології для анімації.

В процесі ретопології потрібно зменшити кількість полігонів, зберігаючи деталі моделі та форму (рис. 2).



Рис. 2. Помилки ретопології

Можливі варіанти ретопології:

- Використати інструменти ретопології, які автоматично оптимізують полігони.
- Ретопологувати модель вручну для кращого керування топологією.
- Додавання та видалення полігонів де модель при анімації буде згинатися.

UV розгортка полягає в тому, щоб вирівнювати поверхню 3D моделі на плоску текстурну площину. Основною проблемою є мінімізація перекриття та розтягнення текстур на моделі. Рішення:

- Використовувати абсолютне або релятивне UV.
- Використати автоматичні або півавтоматичні методи розгортання, які мінімізують перекриття та розтягнення.
- Вручну корегувати розгортку, де це необхідно, зокрема для основних елементів моделі.

При створенні текстур для моделей можуть виникати проблеми з розміром текстур, роздільною здатністю, кольорами та освітленням. Рішення:

- Використання текстур високої роздільної здатності.
- Коректне налаштування освітлення та колірну корекцію.
- Також, можна використовувати техніки, такі як PBR (PhysicallyBasedRendering) для досягнення реалістичних ефектів.
- Використати текстури з високою роздільною здатністю для ближнього плану та текстури з меншою роздільною здатністю для віддалених об'єктів (мінімізація ваги файлу).
- Застосовувати коректне освітлення та колірну корекцію для досягнення реалістичних ефектів.

3D моделювання, ретопологія, UV розгортка та текстуринг вимагають уваги до деталей та вмінь управляти проблемами, які є важливими етапами при створенні віртуальних об'єктів та ігор. Процес створення моделей може супроводжуватися численними проблемами, але з правильними методами та інструментами їх можна успішно вирішити. Вирішення цих проблем дозволяє створювати якісні 3D об'єкти з реалістичними текстурами, які додають важливий візуальний аспект до проєктів у галузі графіки, дизайну та розваг.

Список використаних джерел

1. What is UV Mapping & Unwrapping? [Електронний ресурс]. – 2023. – Режим доступу до ресурсу: <https://conceptartempire.com/uv-mapping-unwrapping/>

УДК 528.8+007.52

Туз В. І.,

Горелик С. І., к.т.н., доцент

*Національний аерокосмічний університет ім. М. С. Жуковського
«Харківський авіаційний інститут»*

РОЗРОБКА ПОБУДОВИ КАРТОГРАФІЧНОЇ МОДЕЛІ ЗА ДОПОМОГОЮ ШТУЧНОГО ІНТЕЛЕКТУ НА ОСНОВІ ДАНИХ ДЗЗ

У наш час, враховуючи стрімкий розвиток промисловості, інфраструктури та наукового прогресу, виникла необхідність перегляду традиційних підходів до обробки, передачі та архівації даних зондування землі (ДЗЗ). Для досягнення вищого рівня актуалізації, використання штучного інтелекту (АІ) стає невід'ємною частиною сучасних практик в цій області. Це сприяє швидшій та більш точній обробці ДЗЗ, а також удосконаленню алгоритмів передачі та ефективній архівації, що відповідає вимогам динамічного середовища.

Штучний інтелект «АІ» – це галузь науки та технології, присвячена створенню систем і алгоритмів, які здатні виконувати завдання, що потребують інтелектуальних здібностей, властивих людині. Ці здібності включають в себе навчання, аналіз даних, розпізнавання образів, прийняття рішень та багато іншого, схожістю на модель людського мислення. Штучний інтелект «АІ» активно проникає у різні галузі, і геодезія не виняток. Геодезія, наука вимірювання та відображення форми, розмірів та гравітаційного поля Землі, має величезне значення у зйомці та складанні карт. У міру зростання потреби в точних та ефективних геопросторових даних, АІ стає ключовим фактором, пропонуючи інноваційні рішення для подолання проблем, з якими стикаються геодезисти та картографи.

Одне з основних завдань у геодезії – це збирання та обробка великих обсягів даних. Традиційні методи можуть бути трудомісткими та вимагати залучення досвідчених фахівців для ручного збору та аналізу інформації. Однак АІ – інструменти революціонізують цей процес, автоматизуючи збір та обробку даних, що суттєво знижує часові та трудові витрати. Наприклад, алгоритми АІ можуть аналізувати супутникові зображення та автоматично виявляти об'єкти, такі як дороги, будівлі та рослинність, що дозволяє швидше і точно складати карти.

Більш того, АІ може допомогти покращити точність геопросторових даних, ідентифікуючи та виправляючи помилки у існуючих наборах даних. Алгоритми машинного навчання можуть

бути навчені розпізнавати закономірності та аномалії даних, дозволяючи їм виявляти невідповідності та вносити необхідні коригування. Це не тільки підвищує якість геопросторової інформації, але й допомагає запобігати дорогим помилкам, що виникають через ненадійні дані.

Ще однією областю, де AI значно впливає, є сфера дистанційного зондування. Технології дистанційного зондування, такі як ЛІДАР (лазерне сканування) та фотограмметрія, широко використовуються в геодезії для збору даних високої роздільної здатності поверхні Землі. AI може покращити можливості цих технологій, автоматизуючи аналіз даних дистанційного зондування, що дозволяє геодезистам вилучати цінну інформацію ефективніше. Наприклад, алгоритми AI можуть опрацьовувати дані лідару для створення докладних 3D-моделей місцевості та будівель, які можуть застосовуватись у різних галузях, включаючи містобудування, екологічний моніторинг та управління надзвичайними ситуаціями.



Рис. 1. Обробка даних ДЗЗ за допомогою бібліотек AI

На сам кінець, AI доводить свою революційність у галузі геодезії, пропонуючи інноваційні рішення для подолання труднощів, з якими стикаються геодезисти та картографи. Автоматизація збору та обробки даних, покращення точності геопросторової інформації та забезпечення прийняття більш обґрунтованих рішень – все це робить AI ключовим елементом для розуміння та відображення Землі. У міру зростання потреби в точних та ефективних геопросторових даних, впровадження AI в геодезію відіграватиме вирішальну роль у формуванні майбутнього зйомки та складання карт.

Список використаних джерел

1. Artificial Intelligence [Електронний ресурс] – Режим доступу до ресурсу: <https://www.esri.com/ua-ua/artificial-intelligence/overview#ebook>
2. Earth Engine Data Catalog [Електронний ресурс] – Режим доступу до ресурсу: <https://ts2.space/>

УДК 004.42

Бадігон В. О., здобувач,

Левченко А. Ю., к.т.н.

Державний університет «Житомирська політехніка»

РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ В МУЗИЧНІЙ ІНДУСТРІЇ

З розвитком інформаційних технологій створення, дистрибуція та споживання музики стали набагато простішими. Тепер кожен має змогу користуватися програмним забезпеченням для створення аудіоконтенту та платформами для його розповсюдження.

Завдяки здобуткам у галузі розробки програмного забезпечення програмісти можуть створювати потужні програмні продукти для ефективної роботи з аудіофайлами, які задовольняють потреби музикантів та слухачів. Це трудомісткий процес, який вимагає чіткого планування, розуміння основних задач та знань не лише у галузі розробки програмного забезпечення, але й у музичній галузі.

Розробка музичного програмного забезпечення включає в себе наступні вимоги:

- **Широкий інструментарій:** розробники повинні володіти такими мовами програмування як C++, Java, Python or JavaScript, щоб розробляти додатки, які будуть сумісні з різними платформами.

- **Дизайн інтерфейсу (UI) та досвіду користувача (UX):** Зосереджуючись на створенні інтуїтивно зрозумілих та зручних інтерфейсів, які музиканти та продюсери можуть легко використовувати, розробники музичного програмного забезпечення повинні враховувати різноманітні параметри щодо зручності використання.

- **Цифрова обробка звуку:** Розробникам також слід звернути увагу на використання аудіо-бібліотек та API для впровадження функцій, таких як запис аудіо, відтворення, редагування, обробка ефектів та мікшування звуку. Крім того, вони можуть також розробляти віртуальні інструменти, синтезатори та різноманітні аудіо-плагіни.

- **Тестування та виправлення помилок:** Розробники музичного програмного забезпечення повинні проводити ретельне тестування та виправлення помилок своїх програм, щоб забезпечити їх стабільність, продуктивність відсутність помилок. Вони можуть використовувати фреймворки для тестування та інструменти, які автоматизують процес [1].

Музичне програмне забезпечення може мати різне призначення. Існують програми для створення та редагування аудофайлів, плагіни для розширення можливостей програмного забезпечення, платформи для розповсюдження музики та інструменти для аналізу інформації. Розробники беруть безпосередню участь у створенні наступних додатків та інструментів:

- **Цифрові робочі станції звукозапису (DAWs):** DAWs - це програмні застосунки, призначені для запису, редагування та мікшування музики. Вони надають різноманітні інструменти та функції для музикантів, продюсерів і звукорежисерів для створення та обробки аудіодоріжок. Прикладами включають Ableton Live, Pro Tools, Logic Pro та FL Studio [2].

- **Віртуальні інструменти та ефекти:** Програмні інструменти, такі як синтезатори, семплери та drum-машини, дозволяють музикантам створювати музику в цифровому форматі. Розробники створюють віртуальні інструменти та плагіни ефектів, які можна використовувати в межах DAW, розширюючи звукові можливості та підвищуючи творчий потенціал.

- **Стримінгові платформи:** З інтенсифікацією цифрового споживання музики розробка програмного забезпечення відіграла значущу роль у створенні платформ стримінгу музики, таких як Spotify, Apple Music та Deezer.

- **Маркетинг та аналітика:** Програмні платформи допомагають музикантам та студіям звукозапису відстежувати та аналізувати дані, пов'язані з їхньою музикою, такі як кількість програвань, демографічна структура аудиторії та взаємодія в соціальних мережах. Ці уявлення сприяють розробці маркетингових стратегій, прийнятті рішень та стратегічному спрямуванні на конкретні аудиторії [1].

Отже, розробка програмного забезпечення має великий вплив на музичну індустрію. Завдяки розробці інноваційних програмних продуктів музиканти та звукорежисери мають змогу створювати нові рішення у звуковому дизайні, покращуючи досвід слухачів та якість матеріалу.

Список використаних джерел

1. Software Development in the Music Industry [Електронний ресурс] – Режим доступу до ресурсу: <https://www.bocasay.com/software-development-music-industry/>.
2. 10 Best DAW Software in the World Today [Електронний ресурс] – Режим доступу до ресурсу: <https://blog.landr.com/best-daw/>

УДК: 004.89:025.4

*Свінцицька О. М., к.е.н., доцент,
Бордюг Б. Л., магістрант
Державний університет «Житомирська політехніка»*

РОЛЬ ФОРМУВАННЯ ВИМОГ НА РОЗРОБКУ ОНЛАЙН БІБЛІОТЕК В УПРАВЛІННІ ІТ-ПРОЕКТАМИ

Розглядаючи сучасний розвиток онлайн бібліотек, стає зрозуміло, що їхня ефективність не обмежується зовнішнім виглядом або інтерфейсом. Важливою складовою успішності таких платформ є глибина функціональних можливостей, так, як такі проекти мають дуже високу ймовірність провалу, і основною причиною цього є поганий процес розробки вимог. Виявлення вимог і документування є основними і найважливішими етапами життєвого циклу розробки програмного забезпечення. Тому при розробці систем правильне формулювання функціональних вимог набуває першочергового значення.

Загалом, оптимізація процесу розробки онлайн бібліотек полягає в ефективному плануванні, створенні та впровадженні функціональних можливостей, які відповідають потребам користувачів.

Онлайн бібліотеки стали не просто засобом отримання доступу до знань та інформації, але й місцем, де можна знайти різноманітну інформацію з будь-якої точки світу. Тому ключовим фактором стає створення функціоналу, що відповідає потребам користувачів.

Саме функціональні вимоги визначають можливості та функціонал онлайн бібліотек, включаючи пошук, сортування, доступ до ресурсів та інші важливі функції. Недоліки у формулюванні цих вимог можуть призвести до невідповідності очікуванням користувачів, затримок у розробці та інших проблем.

Ці проблеми підкреслюють важливість структурованого та чіткого підходу до формулювання вимог. Аналіз потреб користувачів, докладна документація та активна співпраця з зацікавленими сторонами є ключовими для успішного розвитку онлайн бібліотек.

Для успішного формування функціональних вимог необхідно:

- Ретельно аналізувати потреби користувачів та враховувати їх у формулюванні вимог.
- Докладно документувати всі функціональні вимоги, включаючи усі можливі варіанти використання.
- Активно спілкуватись з користувачами та командою для постійного уточнення вимог та врахування змін у процесі розробки.

Можливо виділити наступні функціональні вимоги для розробки онлайн бібліотек:

- Розширений пошук та фільтрація – можливість пошуку за авторами, назвами книг, темами та ключовими словами.
- Адаптованість до різних пристроїв – забезпечення оптимального відображення та функціональності на різних пристроях (комп'ютери, планшети, мобільні телефони).
- Можливість використання різних браузерів для доступу до бібліотеки.
- Персональні облікові записи – можливість реєстрації та авторизації користувачів для зберігання історії пошуку, списків обраного, позначок та рейтингів.
- Функція порівняння – можливість порівняння книг/ресурсів за різними параметрами (ціна, рейтинг, відгуки тощо).
- Доступ до ресурсів – забезпечення доступу до повного тексту книг або матеріалів з можливістю встановлення обмежень доступу.
- Колекція та обробка даних – можливість створення персональних колекцій книг, складання списків для подальшого вивчення.
- Рекомендації та персоналізація – система рекомендацій на основі історії пошуку та вибору користувача для персонального підбору матеріалів.
- Фідбек та відгуки – можливість залишення відгуків, оцінок, коментарів до книг.

Оскільки розробка онлайн бібліотек потребує глибокого розуміння користувачів та уваги до деталей то формування правильних функціональних вимог є ключовим етапом, оскільки визначає можливості продукту і його придатність для задоволення потреб користувачів. Ефективна бібліотека повинна бути зручною, доступною, адаптованою до сучасних вимог. Врахування поточних тенденцій та потреб користувачів допоможе створити успішний продукт, конкурентоспроможний на ринку.

Список використаних джерел

1. Козак О. Л. Опорний конспект лекцій з курсу «Аналіз вимог до програмного забезпечення» для студентів напрямку підготовки – Програмна інженерія. Тернопіль: 2011. 56 с.
2. Грицюк Ю. І., Немова О. А.. Особливості формулювання вимог до програмного забезпечення. / Національний університет «Львівська політехніка», Львів: 2018. 14 с.

УДК 621.3: 455.63

*Свінцицька О. М., к.е.н., доцент,
Цурукіна Г. А., магістрант,
Іщенко В. В., магістрант*

Державний університет «Житомирська політехніка»

РОЛЬ ЦИФРОВИХ ІНСТРУМЕНТІВ У ВЗАЄМОДІЇ ФАРМАЦЕВТИЧНИХ КОМПАНІЙ З МЕДИЧНИМИ ПРАКТИКАМИ

У сучасному світі фармацевтична галузь динамічно розвивається, а одним з основних аспектів є взаємодія з медичними практиками. Пандемія COVID-19 відіграла кардинальну роль у переосмисленні та переформуванні способів комунікації між цими суб'єктами. Виникнення та широке використання цифрових технологій, зокрема систем управління відносинами з клієнтами (CRM), стало ключовим елементом у цій еволюції. Проаналізуємо вплив та роль цифрових інструментів у взаємодії фармацевтичних компаній із медичними практиками.

Перед пандемією COVID-19 віртуальні візити лікарів були рідкісністю. Однак за даними досліджень, після пандемії віртуальні візити складають 13-17% амбулаторних візитів, що свідчить про зростання їх популярності у 38 разів. Цей феномен став приводом для впровадження цифрових каналів комунікації між фармацевтичними компаніями та медичними практиками.

Одним із засобів удосконалення взаємодії стали системи CRM, такі як Veeva CRM Engage, які дозволяють фармацевтичним представникам оптимізувати взаємодію з лікарями. Ці інструменти стають платформою для швидкого та ефективного реагування на запити медичних практик, забезпечуючи персоналізовані підходи до кожного клієнта.

Однак важливо враховувати змінні очікування лікарів. Їхні вимоги до цифрових інструментів стають все вищими. За звітом Veeva Pulse Field Trends Report, 75% лікарів виразили бажання збільшити кількість цифрових взаємодій з фармацевтичною галуззю, що вимагає постійного удосконалення та розвитку цифрових інструментів в цій сфері.

Впровадження цифрових інструментів, таких як Veeva CRM Engage, стає важливим кроком у розвитку цифрових каналів взаємодії. Ці інструменти допомагають фармацевтичним компаніям забезпечити більш ефективну підтримку медичним практикам, що, у свою чергу, відкриває двері для нових можливостей та стратегій в цій сфері.

Отже цифрові технології відіграють значущу роль у перетворенні комунікаційних стратегій між фармацевтичними компаніями та медичними практиками. Впровадження систем CRM, зокрема Veeva CRM Engage, стає кроком у напрямку більш ефективної та персоналізованої взаємодії, пристосованої до зростаючих очікувань медичних практик. У подальшому, постійний розвиток цифрових інструментів стане ключем до успішної комунікації та співпраці у фармацевтичній галузі.

Список використаних джерел

1. Brenner B. (2018). Transformative Sustainable Business Models in the Light of the Digital Imperative – A Global Business Economics Perspective. *Sustainability*, 10 (12), 4428. Режим доступу: <https://www.mdpi.com/2071-1050/10/12/4428>
2. Forbes Advisor Six Key Benefits a CRM Brings Your Business (2023). Режим доступу: <https://www.forbes.com/advisor/business/software/six-key-benefits-a-crm-brings-your-business/>
3. Customer Lifecycle Management (2023) What It Is & How It Works. / Forbes Advisor. Режим доступу: <https://www.forbes.com/advisor/business/customer-lifecycle-management/>

УДК 004.4

Марчук Д. К., ст. викладач,

Лантвойт К. М., здобувач

Державний університет «Житомирська політехніка»

РОЛЬ DISCONTAINERS В ІГРОВІЙ ІНДУСТРІЇ ТА КОРИСТЬ ЇХ ВИКОРИСТАННЯ В АРХІТЕКТУРІ ПРОЕКТУ

Архітектура коду та побудова правильних залежностей в кодї є одним із найважливіших етапів розробки гри. Залежності класів (компонентів) повинні бути зрозумілими та легко ініціалізованими, щоб інші компоненти мали легкий доступ до компонентів (об'єктів) і чітку структуру з одним місцем ін'єкції залежностей та зв'язків між об'єктами. Рішенням може бути DI Containers (Dependency Injection Container) – контейнер для ін'єкції залежностей, який спрощує та автоматизує впровадження залежностей в об'єкти програми за допомогою деякого контейнера або системи керування контейнерами [1]. На даний момент DI Containers широко використовується в різних сферах розробки програмного забезпечення починаючи з веброзробки і закінчуючи розробкою ігор, тощо.

Проблема розглянута в даному дослідженні – яку роль відіграє DI Containers в ігровій індустрії, коли використовується та є корисним.

DI Containers допомагають надати єдине місце входу ін'єкцій в програмі. Одним із фреймворків що реалізують DI Containers є Zenject, створений для рушія Unity, він дозволяє ефективно управляти залежностями в грі та несе велику функціональну базу. Zenject має велику кількість функцій, методів та класів, що є невеликим мінусом але в той самий момент і плюсом даного фреймворку, так як розширяє його можливостей до великих масштабів. Найбільш часто використовуваними та важливими функціями в є:

- Ін'єкція залежностей надає потужний механізм ін'єкції залежностей, який дозволяє автоматично вставляти залежності в об'єкти під час їх створення
- Контексти для залежностей для визначення які залежності повинні використовуватися певними частинами проекту.
- Керування одиночками (Singeltons) можна виконувати за допомогою Zenject, що робить їх легшими у використанні та управлінні.
- Тестування. Робить тестування зручнішим завдяки заміні реальних залежностей на тестові.
- Масштабованість. Надає змогу підтримувати масштабовані проекти та забезпечує гнучку архітектуру проекту.

І це тільки мала частина можливостей Zenject, але в більшості випадків використовують вище вказані функції так як вони є найбільш актуальними та важливими в розробці ігор. DI широко використовується не тільки в малих проектах, а і у великих проектах та компаніях, так як надає зручні функції в сфері тестування та масштабування, що є дуже важливим під час розробки гри, так як хороше тестування є запорукою успіху проекту і є майже фінальним етапом розробки гри, а масштабування надає змогу реалізувати багато ігрових механік і при цьому мати чітку та зрозумілу архітектуру проекту. Для прикладу можна розглянути використання Zenject під час розробки гри.

Створення зв'язку між InputController та його реалізацією:

```
private void BindDesktop() {
    DesktopInput desktopInput =
    Container.InstantiatePrefabForComponent<DesktopInput>(
        _desktopInput, _desktopInput.transform.position, Quaternion.identity,
        _inputContainer);
    Container.Bind<InputController>().To<DesktopInput>().FromInstance(desktopInput).AsSingle();
}
```

Приклад отримання реалізації:

```
[Inject] public void Construct(
    InputController inputController) {
    _inputController = inputController;
}
```

Приклад швидкої заміни:

```
private void BindHandheld() {
    HandheldInput handheldInput =
    Container.InstantiatePrefabForComponent<HandheldInput>(
        _handheldInput, _handheldInput.transform.position, Quaternion.identity,
        _inputContainer);
    Container.Bind<InputController>().To<HandheldInput>().FromInstance(handheldInput).AsSingle();
}
```

Zenject є важливим та часто використовуваним інструментом під час розробки ігор, він надає змогу чітко визначати залежності між об'єктами, створювати зв'язки та надавати реалізації в потрібних місцях коду, допомагає проводити зручне та гнучке тестування проектів, також сприяє створенню єдиного місця входу.

Список використаних джерел

1. Arora A. Dependency Injection in Unity 3D [Електронний ресурс] / Akshay Arora. – Режим доступу до ресурсу: <https://medium.com/xrpractices/dependency-injection-in-unity-86afabf2cf8d>.

УДК 004.8

*Ясько Н. О., здобувач,
Лисенко М. С., асистент
Державний університет «Житомирська політехніка»*

СПРОЩЕННЯ ПРОЦЕСІВ РОЗВІДКИ ЧЕРЕЗ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ АНАЛІЗУ ОБ'ЄМНИХ ДАНИХ

У наш час військова діяльність стає все складнішою та технологічно вдосконаленою, розвідка, а також розвідувальні операції, набувають актуального значення. Штучний інтелект, завдяки своїм аналітичним та обчислювальним можливостям, відіграє важливу роль у забезпеченні ефективної обробки та аналізу великих обсягів інформації у військовому середовищі. Мета цієї наукової тези полягає в дослідженні застосування штучного інтелекту для удосконалення процесів розвідки та розвідувальних операцій у сучасних військових умовах. ШІ почали використовувати у військовій сфері значно раніше ніж в цивільному житті. Інженери довго працювали над тестуванням алгоритмів, доопрацюванням та навчанням їх виконувати все складніші завдання. Вони домоглися значних успіхів. До прикладу, Армія США активно використовує цю технологію для моделювання бойових ситуацій; у лютому 2023 року Агентство передових оборонних дослідницьких проєктів DARPA успішно протестувало безпілотний вертоліт Black Hawk [1]; в Об'єднаних Арабських Еміратах Корпорація оборонної промисловості Еміратів розробляє невелику пускову установку з розумним безпілотником [2], що самознищується. Одними з вимог до розвідки [2] є безперервність, своєчасність та оперативність. Людський мозок не здатен постійно обробляти велику кількість інформації, яка йому надходить, особливо враховуючи певні фізичні та психологічні чинники такі як: недосип, вигорання та ін. Через це виходять затримки, згодом втрати. Одна з можливих схем того звідки ШІ буде отримувати та обробляти дані може виглядати так (рис. 1).

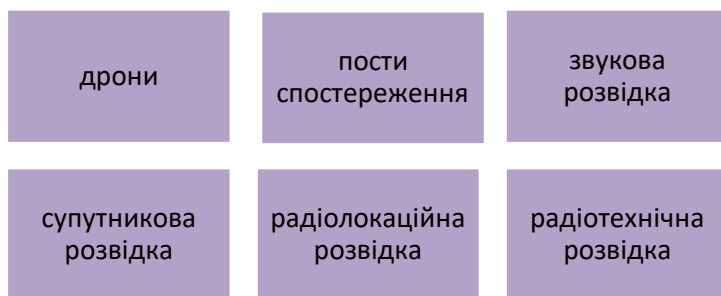


Рис. 1. Джерела інформації

Якщо створити алгоритм та навчити ШІ обробляти ці дані в комплексі, то це оптимізує процес прийняття рішень та усуне такі проблеми:

- пріоритет ураження цілей;
- шляхи поповнення БК;
- прорахування безпечних маршрутів евакуації;
- планування операцій для зменшення втрат особового складу;
- планування майбутніх дій противника.

Українські війська вже активно використовують ШІ у війні з Росією, проте досі велика кількість даних обробляється вручну, що не допустимо враховуючи велику різницю в ресурсах України та країни агресора. ШІ це розв'язання наших проблем, цю сферу потрібно активно розвивати.

Список використаних джерел

1. BlackHawk, розумний безпілотник [Електронний ресурс] – Режим доступу до ресурсу: <https://forklog.com.ua/exclusive/vijna-ta-nejromerezhi-yak-shtuchnyj-intelekt-vykorystovuyut-na-poli-boyu>

2. Вимоги до розвідки [Електронний ресурс] – Режим доступу до ресурсу: <https://tck.pl.ua/wp-content/uploads/2021/02/Viyskova-rozvidka-posibnyk.pdf>

УДК 004

*Кулешов Д. А. здобувач,
Граф М. С., Ph.D*

Державний університет «Житомирська політехніка»

ФАКТОРИ ДЛЯ РОЗРОБКИ КОМП'ЮТЕРНОЇ ГРИ В ЖАНРІ HORROR У ВІРТУАЛЬНІЙ РЕАЛЬНОСТІ

У період зльоту технологічного прогресу та постійного прагнення до новаторства комп'ютерні ігри стають не лише розважальними платформами, але й справжніми імерсивними враженнями. Серед емоційно насичених жанрів вирізняється horror, який, об'єднаний із віртуальною реальністю (англ. virtual reality, VR), перетворює геймерський досвід на захоплюючу подорож у світ страху та напруження. В цьому контексті розробка комп'ютерної гри виявляється цікавим завданням, що сприймає виклик не лише від технічної точки зору, а й з погляду психології гравців.

Метою даного дослідження є розглянути фактори для розробки комп'ютерної гри в жанрі horror з використанням технології віртуальної реальності

Особливості гри та враження від VR

Жанр horror відзначається своєю спроможністю занурити гравця у найглибші рецепторні сфери страху. В поєднанні з віртуальною реальністю, цей жанр виходить на новий рівень, де гравець стає активним учасником жахливого сценарію. Віртуальна реальність дозволяє відчувати кожен звук, поглибитися у кожен тінювий куток та переживати страх, наче це реальність.

Вплив віртуальної реальності на психіку гравця

Важливо враховувати психологічні аспекти впливу гри у жанрі horror на гравців. Віртуальна реальність може спричинити більш сильні емоційні реакції, включаючи страх, тривогу та підвищений пульс. Розробник повинен уважно підходити до створення сценаріїв, збалансовуючи інтенсивність ігрового процесу для забезпечення безпеки гравців.

Специфіка створення жахливої атмосфери за допомогою VR-технологій

Використання VR-технологій вимагає не лише високотехнічних знань, але й тонкої майстерності у створенні жахливої атмосфери. Графічні та звукові ефекти повинні бути високоякісними та реалістичними, щоб максимально поглибити гравця у віртуальний світ страху.

Така розробка гри обіцяє не лише високотехнічну ігрову платформу, але й глибокий емоційний занурений досвід для гравців, де грані між віртуальним та реальним стираються, залишаючи незабутні враження.

Якщо розглядати технічні аспекти розробки такої гри, то можна виділити наступні фактори, що впливають на гравця.

- Використання різних VR-пристроїв

Розробка гри у віртуальній реальності вимагає ретельного вибору VR-пристроїв, які забезпечать оптимальний рівень іммерсії для гравців. Врахування технічних характеристик, таких як роздільна здатність, частота оновлення та ступінь відчуття простору, дозволяє досягти максимального рівня реалістичності та комфорту.

- Графічні та звукові ефекти для підвищення атмосфери

Використання передових графічних та звукових технологій є ключовим аспектом розробки hогog-гри у віртуальній реальності. Відмінна реалізація текстур, світлових ефектів та акустичних аспектів допомагає створити реалістичну та жакливу атмосферу, яка повністю поглиблює гравця у віртуальний світ.

- Програмування реалістичної реакції гри на дії гравця

Ефективне програмування взаємодії гравця з віртуальним середовищем є ключовим етапом розробки. Врахування різних сценаріїв та можливостей взаємодії, таких як фізичні рухи, голосові команди та взаємодія з оточуючими об'єктами, створює неперевершений геймплей, в якому кожен крок гравця впливає на розвиток подій у грі.

Описані технічні аспекти та фактори програмної розробки комп'ютерної гри спрямовані на створення інноваційного та емоційно насиченого віртуального світу, де технічна досконалість поєднується з імерсивністю, надаючи гравцям неповторний досвід жаху у віртуальній реальності.

Список використаних джерел

1. Aestar: Створення VR-ігор. [Електронний ресурс] – Режим доступу до ресурсу:<https://aestar.com.ua/uk/stvorennia-vr-igor/>

2. Психологічна енциклопедія: Віртуальна реальність це. [Електронний ресурс] – Режим доступу до ресурсу:<https://www.psykholoh.com/post/виртуальна-реальность-це>

УДК 004.43

*Гарбич-Мошора О. Р., к.пед.н., доцент,
Городиський Б. І. магістрант*

Дрогобицький державний педагогічний університет імені Івана Франка

ХАРАКТЕРИСТИКИ РЯДКОВИХ ВЕЛИЧИН В JAVASCRIPT

Робота з рядковими величинами є фундаментальною частиною багатьох аспектів сучасної обчислювальної науки і програмування. Вони призначені для представлення та обробки текстової інформації, що є частиною веб-сайтів, мобільних додатків та програм на фронтенді та бекенді. Від обробки текстових даних у веб-розробці до роботи зі структурованими даними в аналітиці, від створення додатків для обробки тексту до підтримки інтернаціоналізації та локалізації, опрацювання рядкових величин важливо для забезпечення правильної функціональності багатьох програм та додатків використовуються практично у всіх аспектах сучасного світу. Розуміння та ефективне володіння опрацюванням рядкових величин є необхідними навичками для розробників та аналітиків, що працюють у різних галузях індустрії і досліджують глибини інформаційних технологій. Рядкові величини є важливою складовою будь-якої мови програмування, і їх використання варіюється у залежності від конкретної мови.

JavaScript є однією з мов програмування, яка широко використовує рядкові дані для взаємодії з користувачем на веб-сторінках, і володіє багатьма потужними інструментами для роботи з рядковими величинами. Перший крок у вивченні JavaScript – це вивчення основ. Студенти повинні розуміти синтаксис мови, структури даних, змінні та операції. Навички роботи зі змінними є важливим етапом, оскільки вони використовуються для зберігання рядкових величин.

Рядкові величини у програмуванні представляють собою складові символи для збереження текстової інформації. Основні характеристики рядкових величин включають [1]:

Послідовність символів: Рядок є послідовністю символів, які можуть включати букви, цифри, символи пунктуації та ймовірності

Незмінність: Рядкові величини в багатьох мовах програмування є незмінними, що означає, що після створення рядка ви не можете змінити його вміст без створення нового рядка.

Індексація: Ви можете отримати доступ до окремих символів у рядку, вказавши їхні індекси у межах рядка, які рахуються з нуля.

Довжина: Рядок має довжину, яка збільшує кількість символів у рядку.

Операції з рядками : Мові програмування надають низку функцій і методів для опрацювання рядків, таких як розділення, пошук, заміна, перетворення реєстру та багато інших.

Регулярні вирази: Рядкові величини можуть бути оброблені за допомогою регулярних виразів, що дозволяє виконувати більш складний пошук і замінювати шаблони в тексті.

Лапки: Рядки можуть бути визначені, використовуючи одинарні (апострофи) або подвійні лапки.

Вбудовані функції: Мова JavaScript і багато інших мов програмування надають вбудовані функції і методи для роботи з рядками, які полегшують оптимізацію.

Методичні особливості вивчення цієї теми включають наступні аспекти [2]:

- **Рядкові літерали**: Студенти повинні навчитися створювати рядкові літерали в одинарних та подвійних лапках та розуміти різницю між ними.

- **Індексація рядків**: Важливо пояснити, як працює індексація рядків, починаючи з 0, та як отримувати доступ до окремих символів рядка.

- **Довжина рядка**: Студенти повинні навчитися використовувати властивість **.length** для визначення довжини рядка.

- **Методи рядків**: JavaScript має велику кількість методів для опрацювання рядків, таких як **split()**, **concat()**, **toUpperCase()**, **toLowerCase()**, **substring()**, **indexOf()**, **replace()** і багато інших. Вивчення та розуміння цих методів є важливою частиною навчання.

- **Регулярні вирази**: Регулярні вирази відкривають широкі можливості для опрацювання рядків. Студенти повинні знати, як створювати та використовувати регулярні вирази.

Розуміння та зміна використання методів роботи з рядковими величинами є критичними для створення високоякісних програм та додатків, які опрацьовують текстову інформацію. Тому розробники повинні активно вдосконалювати свої навички в цій області, щоб стати продуктивними та ефективними у своїй роботі.

Список використаних джерел

1. JavaScript Підручник. Основи веб-програмування. [Електронний ресурс] – Режим доступу до ресурсу: <https://w3schoolsua.github.io/js/index.html#gsc.tab=0>

2. Рядки. [Електронний ресурс] – Режим доступу до ресурсу: <https://uk.javascript.info/string>

УДК 621.3: 455.63

*Oleh Horopashyn., master's student,
Kateryna Kolos, assistant professor
Zhytomyr Polytechnic State University
Silesian University of Technology*

ADAPTATION OF METHODOLOGICAL STRATEGIES TO CHANGES IN SOCIAL AND TECHNOLOGICAL PARADIGMS: NEW REQUIREMENTS AND OPPORTUNITIES

Adapting methodological strategies to the evolving landscape of societal and technological paradigms presents a compelling need in contemporary research.

Shifting societal norms and the rapid advancements in technology impose fresh demands on research methodologies. This necessitates the exploration and development of innovative approaches capable of navigating the complexities of these new landscapes.

Integrating adaptable frameworks that account for societal shifts and technological progressions not only meets the evolving demands but also unlocks new avenues of possibility, offering novel perspectives and enhancing the robustness of research outcomes."

The purpose of the study is the analysis of social and technological changes and the identification of the principles of adaptation of methodological strategies to changes in social and technological paradigms.

Social and technological changes are characterized by:

Societal Changes:

1. Cultural Transformations: Shifts in values, perceptions, and ways of perceiving the surrounding environment impact research approaches. For instance, increased attention to diversity and inclusion may necessitate new methods of analysis and consideration of sociocultural contexts in research.

2. Ethical Demands: The evolution of society also introduces new ethical demands into research work, such as safeguarding data confidentiality and ethical use of technologies in research.

Technological Changes:

1. Artificial Intelligence (AI) and Machine Learning: Expanded capabilities in data analysis and the creation of predictive models both expedite and complicate the research process.

2. Big Data Analysis: The ability to process large volumes of information influences approaches to collecting, processing, and analyzing data in scientific research.

3. Advancements in Communication Technologies: Changes in communication methods and information exchange open new opportunities for collaboration and data collection.

The adaptation of methodological strategies to these changes involves the development of more flexible, multidisciplinary and innovative approaches to scientific research, able to effectively take into account the modern context of society and use new technologies to achieve scientific goals.

The principles of adapting methodological strategies to changes in social and technological paradigms include [1]:

1. Flexibility and Adaptability: Being flexible to adjust research methodologies to evolving societal and technological landscapes.

2. Interdisciplinary Approach: Integrating diverse aspects of change, encompassing social, technological, ethical, and cultural dimensions through an interdisciplinary lens.

3. Experimentation and Innovation: Experimenting with novel methods and innovative tools to enhance the research process.

4. Ethical Considerations: Incorporating ethical perspectives into methodological adaptations, ensuring responsible and ethical research practices.

5. Continuous Learning and Adaptation: Continuously learning about new technologies and social trends to adapt research strategies accordingly for improved outcomes.

Therefore, the adaptation of methodological strategies to changes in social and technological paradigms is an important trend of modern research. This process requires flexibility, adaptability, interdisciplinarity and innovation from scientists. The implementation of adaptive methodological strategies contributes to improving the quality and reliability of research results, increasing their relevance for solving real problems of society, and expanding opportunities for cooperation and interaction between various scientific disciplines and stakeholders.

References

1. Geets V., Golovan V. Adaptation of methodological strategies of organizations in the context of changes in social and technological paradigms. *Economy and society*. 2016. No. 12. P. 132–139.

УДК 004

Kapiton A. M., d.p.s., professor,
Goncharov I. K., education seeker
National University «Yuri Kondratyuk Poltava Polytechnic», Ukraine
Scientific lyceum №3 of Poltava city council, Ukraine

AN INTERPRETED PYTHON LANGUAGE WITH DISTINCTIVE DYNAMIC TYPING

The Python language is most often used to work with machine learning, neural networks and artificial intelligence. It can be used as the main language or to implement individual modules. This makes the language extremely popular among scientists, especially in the fields of exact sciences – physics and mathematics. Dynamic typing - Dynamic typing causes Python to consume more resources than it should, but this is often compensated for by internal caching. We will give several examples of features of the Python language, that distinguish it from competitors. Probably the first difference between Python and other programming languages is the elegance and readability of the code. This allows an untrained person to easily read the code. Below are examples of functions that return the sum of two elements in languages Python and Java.

```
//Java_code
public class SumExample {
    public static int SumNumb (int a, int b) {
        int result = a + b;
        return result;
    }
}

#Python_code
def sum_num (a, b):
    result = a + b
    return result
```

The language developers achieved this simplicity by replacing cumbersome curly braces with colons, which allowed them to write shorter and clearer code. The tab has become a significant symbol, which separates the body of the cycle/function/condition... from the code, which has a different type of hierarchy. Also, the developers decided to abandon the semicolon at the end of each line, which made the code even more readable. In commercial projects, this feature allows you to quickly understand code written by another programmer and continue to support it.

Ease of reading and use is enhanced by the many features and structures contained in Python. Here are some examples of them:

```
#Python_code
a = 4
b = 5
a, b = b, a # Simple change of variable values (swap). Now a = 5, b = 4
squares = [x ** 2 for x in range(1, 6)] # Creating of full list in one line
```

```
square = lambda x: x**2 # Creating anonymous function
my_list = [1, 2, 3]
k, p, g = my_list # Unpacking of list. Now k = 1, p = 2, g = 3
```

These features make Python a powerful and convenient programming language, making development easier and the code more compact and readable. We would also like to say something about the dynamic typing of the language. Although many high-level programming languages have this type of data typing, this factor can be decisive when choosing a main language, distinguishing it from some competitors. Moreover, dynamic typing made it easier for those who chose it as their first programming language, because the student does not have to think at the early stages about what data type to assign to a variable. Also, dynamic typing has other advantages, for example, creating an array whose elements will have different data types (example below).

```
#Python_code
my_list = ["string", 1, True, 3.14, [1, 15, 3]] # This list contains different
data types
```

For example, in C++, to create a list or array with different data types, you need to create separate structures that are inconvenient to fill. Python is among the top five most popular programming languages in the world, according to DOU. It is versatile and can be used to solve tasks on many platforms, including iOS, Android, Windows and server OSes. At the same time, Python has an English-language syntax that significantly simplifies reading and understanding the code. Today, when the computing power of personal computers and servers has become quite high, there is a huge demand for interpreted programming languages. After all, in addition to starting the program itself, it is necessary to start the interpreter, which requires additional resources. Python is just such a language.

References

1. What is the Python programming language? URL: <https://blog.ithillel.ua/ru/articles/yazyk-programmirovaniya-python-s-chego-nachat-i-kuda-dvigatsya>
2. What is Python and where is it used? URL: <https://dan-it.com.ua/blog/python-cto-jeto-za-jazyk-programmirovaniya-i-gde-ego-ispolzujut/>
3. Python: pros and cons of the language, what problems it solves and is it worth studying URL: <https://avada-media.ua/services/python-plyusy-i-minusy-yazyka-kakiye-zadachi-reshayet-i-stoit-li-izuchat/>

УДК 004.4

*Zakharchuk Maksym, a 1st year Master's Student,
Oleksii Chyzhmotria, senior lecturer
Zhytomyr Polytechnic State University*

DESIGNING A WEB-BASED FUZZY LOGIC TESTING SYSTEM

Assessing and evaluating knowledge is an integral part of the educational process. In today's world, web-based systems for testing and evaluating knowledge have gained significant prominence. Integrating fuzzy logic into such systems offers the potential for more precise and flexible assessments [1]. In this article, we will explore the process of designing a web-oriented fuzzy logic testing system, delving into the key considerations, challenges, and best practices to ensure the successful implementation of such a system.

Before embarking on the design process, it is crucial to understand the key considerations that will shape the development of a web-based fuzzy logic testing system [2]:

- **Defining System Objectives:** Clearly defining the objectives and goals of the testing system is paramount. Consider whether the system is designed for formative or summative assessment, diagnostic testing, or skill evaluation.

- **Incorporating Fuzzification and Defuzzification:** The system should incorporate mechanisms for converting crisp input data into fuzzy sets (fuzzification) and interpreting fuzzy results into clear, actionable outcomes (defuzzification).

- **Implementing Adaptive Testing:** Adaptive testing algorithms should be implemented to adjust the difficulty of questions based on a test-taker's previous responses, creating a personalized testing experience.

- **Developing Comprehensive Reporting:** The development of a robust reporting system is vital, which generates detailed performance reports for test-takers and provides insights to educators for improving the learning process.

- **Designing for Scalability:** The system's design should take scalability into account, as it should be capable of handling a growing user base and increased data volumes.

The choice of the technology stack plays a pivotal role in the design and development of the system. Here are some essential components to consider:

- **Front-End Development:** Utilizing web development technologies such as HTML, CSS, and JavaScript is a must. Frameworks like React and Angular can be employed to create dynamic and responsive user interfaces.

- **Back-End Development:** Depending on the project's requirements and the development team's expertise, languages like Python (using frameworks like Django or Flask), Java, PHP, or Ruby on Rails can be considered for the back-end logic.

- **Database Selection:** Opt for a reliable relational database system, such as MySQL or PostgreSQL, to store and manage assessment data.

- **Incorporating Fuzzy Logic Libraries:** Fuzzy logic libraries like Scikit-Fuzzy should be incorporated for implementing fuzzy logic components in the system.

- **Version Control Usage:** Employing version control systems like Git is essential for tracking changes in the codebase and facilitating collaboration among development teams.

User experience is paramount in the success of any web-based system. Ensuring that the system's design and user interface are intuitive, responsive, and accessible across different devices and screen sizes is imperative. Conducting usability testing to gather feedback and making improvements based on user input is recommended.

Thorough testing is critical to ensure the system's reliability and functionality. Automated testing frameworks like Selenium can help create test cases for different system functionalities, enabling comprehensive testing and minimizing the risk of errors.

Selecting a suitable hosting service or cloud platform for deployment, such as AWS, Azure, or Google Cloud, is essential. Ensuring that the system can scale smoothly to accommodate a growing user base and increased data loads is a critical consideration.

Designing a web-based fuzzy logic testing system is a complex yet rewarding undertaking in the field of educational assessment. By addressing the key considerations, selecting an appropriate technology stack, prioritizing user experience, and emphasizing security and scalability, it is possible to create a powerful assessment tool that captures the nuances of knowledge and provides valuable insights for educators and learners alike. Such a system has the potential to revolutionize the assessment process and contribute to more accurate and adaptive learning environments.

References

1. Timothy J. Ross. Fuzzy Logic with Engineering Applications [Text] / T. J. Ross. – New Mexico : Wiley, 2010. – 606 p.
2. Crina Grosan, Ajith Abraham. Intelligent Systems: A Modern Approach [Text] / C. Grosan, A. Abraham. – Berlin : Springer-Verlag Berlin Heidelberg, 2011. – 450 p.

УДК 004:42

*Терещук С. О., ст. викладач,
Дзюбанчук Б. С., здобувач
Державний університет «Житомирська політехніка»*

ОБЪЕСТ POOL ЯК ЗАСІБ ДЛЯ ОПТИМІЗАЦІЇ ПРОЄКТУ

Під час розробки ігор часто зустрічаються моменти, коли нам потрібно створити велику кількість різного типу об'єктів. Все б нічого, але метод, що ми зазвичай використовуємо під час цього, а саме `Instantiate`, охоплює доволі важкі процеси, що часто може значно плинати на оптимізацію.

Задля вирішення даної проблеми було розроблено патерн програмування під назвою Пул об'єктів. Він є ефективним способом для оптимізації ресурсів та підвищення продуктивності програмного забезпечення. Це паттерн створення програмного забезпечення використовує набір ініціалізованих об'єктів, готових до використання (пул), замість їх виділення та знищення за запитом.

Паттерн об'єктного пула створює набір об'єктів, які можуть бути повторно використовувані. Коли потрібен новий об'єкт, його запитують з пула. Якщо попередньо підготовлений об'єкт доступний, він повертається негайно, уникнувши витрат на створення. Якщо в пулу немає об'єктів, створюється і повертається новий. Після використання об'єкта і коли він більше не потрібний, він повертається в пул, що дозволяє його використовувати знову у майбутньому без повторного витратного процесу створення. Важливо враховувати, що після використання і повернення об'єкта існуючі посилання стають недійсними.

У деяких об'єктних пулах ресурси обмежені, тому вказується максимальна кількість об'єктів. Якщо ця кількість досягнута і запитується новий об'єкт, може бути згенеровано виняток або потік буде заблокований до повернення об'єкта до пула.

Одною з основних переваг даного патерну є отримання об'єкта з пула, що відбувається за передбачуваний час, коли створення нових об'єктів (особливо через мережу) може займати чимало часу.

Для його реалізації потрібно мати узагальнюючий клас, що матиме в собі потрібні методи, а саме:

- Ініціалізація пулу;
- Взяття об'єкта з пулу: При потребі у використанні об'єкта, візьміть його із пулу, якщо немає доступного – створіть новий та поверніть, якщо не існують обмежень у кількості об'єктів.

- Повернення об'єкта в пул: Після закінчення використання об'єкта поверніть його назад у пул, де він буде готовий до наступного використання.

```

@ Frequently called  1 usage
private void Attack()
{
    if(Time.time < _nextAttackTime)
        return;

    _nextAttackTime = Time.time + 1.0f / _attackRate;

    Missile missile = _missilePool.Get();

    float flyTime = (transform.position - _target.position).magnitude / _missileSpeed;

    missile.Launch(_launchPoint.position, _target, flyTime, OnReachTarget);

    void OnReachTarget() => _missilePool.Return(missile);
}
    
```

Рис. 1. Лістинг використання пулу у проєкті



Рис. 2. Поведінка об'єктів при використанні пулу у проєкті

Приклад використання наведений на рисунку 1 та 2, де *_missilePool* є завчасно ініціалізований пул з відповідних об'єктів. При атаці замість звичайного створення об'єкту ми отримуємо уже існуючий, звертаючись до пулу. При дотику до цілі, викликається метод, що замість звичайного видалення об'єкту з сцени, повертає його у пул.

Отже, паттерн Object Pool є сильним інструментом для покращення продуктивності програмного продукту, адже він дозволяє отримувати доступ до готових до використання об'єктів, замість створення нового екземпляру, уникнувши витрат на їхнє створення.

Список використаних джерел

1. Object pool pattern [Електронний ресурс] – Режим доступу: https://en.wikipedia.org/wiki/Object_pool_pattern

УДК 004.8

*Maksym S. Sitailo, student,
Andriy V. Morozov, PhD, Associate Professor
Zhytomyr Polytechnic State University*

POPULAR MACHINE LEARNING ALGORITHMS FOR CRYPTOCURRENCY PRICE PREDICTION

Nowadays, machine learning is a popular field of knowledge that helps to resolve different complex problems or find solutions for tasks that cannot be done by any alternative method. Therefore, the mentioned technology is valuable both for scientific research and for practical challenges. Its wide application in different spheres caused the invention and development of different algorithms designed to solve specific practical tasks. However, each method has its own advantages and disadvantages, so it is important to analyze its features and apply the most efficient one based on the goals of our research or the problem that we are trying to solve.

After comparing different neural network models along with traditional technical analysis, researchers discovered that artificial intelligence can identify important features and use them during future price forecasting. This capability allowed neural networks to overperform traditional technical analysis methods demonstrating that machine learning may be more effective for price forecasting task.

The most popular algorithm that is used for solving different regression problems is linear regression. Linear regression determines a linear correlation between a dependent variable and an independent one. The training process involves fine-tuning the parameters of the linear equation to accurately reflect the relationship between these variables. This type of algorithm is used for tackling various tasks. However, using a straight-line model often can lead to excessively conservative forecasts regarding future asset prices.

In addition to linear regression, researchers often analyze the application of ensemble machine learning methods to predict future cryptocurrency prices. Numerous algorithms belong to this category with random forest and XGBoost standing out as notable examples.

Random Forest is a type of ensemble machine learning method that involves the creation of a certain number of decision trees during the model training. The prediction process with this algorithm consists of 2 phases: generating results from each of the created trees and determining the final result through the processing of the obtained data according to the predefined strategy.

XG Boost is an algorithm that is also based on the decision trees, but it has some unique features. Unlike random forest, which relies on an ensemble of trees trained in parallel during the learning process, this algorithm creates sequential trees. Each of these trees learns from the errors of its predecessor. Consequently, it assembles a set of decision trees that have been improved from the mistakes of predecessors during the learning process and this ensemble is used for prediction generation.

Besides the mentioned algorithms, there is a specific type of neural network that was purposely developed to solve issues with the prediction of the data series. It is known as RNN (recurrent neural network). Its main feature is the use sequences of prior data to produce outputs. For example, it can analyze price changes within a specific timeframe and identify possible moments of a trend reversal or confirmation. Application of RNN becomes efficient when extraction and usage of the context from previous data is crucial during the output generation. Conversely, it may be ineffective to analyze long time frames due to the less relevance of the older data. Additionally, using the longer time series can result in reduced sensitivity of the model to the drastic changes in the data. It's a significant drawback during the cryptocurrency price predictions because this type of digital asset tends to be a very volatile.

As a result, LSTM (Long Short-Term Memory) network architecture [1] was developed to overcome the mentioned RNN's disadvantages. It enables analysis of the prior data along with the use of gates. These gates help the model to manage their state in order to control the relevance of the extracted features and patterns. This neural network architecture became widely spread because it allows receiving the benefit of RNN application while eliminating some drawbacks that are inherent to common recurrent neural networks.

So, there are different neural network architectures available for solving diverse tasks including cryptocurrency price predictions. However, it's important to comprehend the specific characteristics of the problems that should be resolved and to use the best methods for that. Forecasting the asset price is a complex task and it is impossible to develop a system that will constantly produce precise forecasts. However, the selection of the most suitable methods enables significant improvement in its performance.

References

1. S. Biswas, M. Pawar. Cryptocurrency price prediction using neural networks and deep learning. 7th International Conference on Advanced Computing and Communication Systems (*ICACCS*). 2021. Vol. 1, P. 408–413.

УДК 004

*Svistelnyk O. S., student,
Zhytomyr Polytechnic State University*

SELECTION AND JUSTIFICATION OF THE ARCHITECTURE FOR THE DEVELOPMENT OF AN ONLINE SERVICE FOR UKRAINIAN LANGUAGE COURSES

In the modern world, the development of online services and applications requires a careful approach to choosing architectural solutions. Regardless of the application, it is important to choose an architecture that optimally meets the needs of users and business. This thesis explores and discusses possible architectural approaches for developing an online service for taking Ukrainian language courses.

The MVC scheme allows you to effectively divide the application components into a model, a view, and a controller, which makes it easier to understand and maintain the code, and speeds up development. The model represents the application data, the view is responsible for displaying information to the user, and the controller processes user requests and interacts with the model and the view. The advantages of this approach are separation of duties, speed of development, and support for simultaneous development by different team members. However, for very simple applications or projects with little functionality, using full MVC may be unnecessary and lead to unnecessary load and increased code complexity. In addition, in some cases, the controller can become a centralized point in the application and overload it from a logical point of view, which can affect the speed and performance of the application.

The MVVM pattern divides the application into a model, a view, and a view-model, where the view-model is responsible for processing data from the model and preparing it for display in the view. This approach uses a declarative approach to programming, which means that the developer describes how the display looks like depending on the data in the view model. The advantages of MVVM are the declarative approach and data binding, which simplifies the development and maintenance of the user interface. However, this approach can lead to an excessive memory load due to the storage of additional view-model objects and create dependence on special frameworks and libraries.

The SPA scheme is an architectural approach in which the entire web application is loaded once, and interaction with the server takes place through asynchronous requests, for example, using AJAX. The entire application code is loaded once during the initial load, and navigation and interaction with the application takes place without a full page reload. This

results in a smoother and faster response to user actions and reduces page load times.

The benefits of the SPA approach include an improved user experience, reduced page loads, reduced server load, and more agile development. However, this approach can lead to a higher client-side load and SEO optimization issues for traditional search engines.

Since our goal is to create an online Ukrainian language course service with an improved user experience close to that of a desktop application, we chose to use the SPA (Single-Page Application) approach. Additionally, the use of RESTful API will allow efficient interaction between the server and client parts of the application, transferring data in JSON format, which is a standard for web applications. This approach will simplify the development and expansion of our service, allowing us to quickly respond to changes and add new functionality.

The following main characteristics and principles of RESTful APIs can be distinguished:

- built around resources, which are usually represented as URLs. Each resource has a unique URL, and clients interact with these resources by making HTTP requests to the corresponding URLs;
- RESTful API uses standard HTTP methods to perform various actions on resources.

The general algorithm of the application using the selected architecture is shown in Fig. 1.

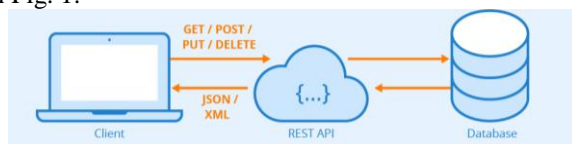


Fig. 1. The general algorithm of the application

After analyzing various architectural approaches, we confirmed that the choice of SPA and RESTful API was optimal for our project and would help us achieve the desired results. This architecture will allow us to create an interactive and convenient service for users, ensure efficient communication between the client and server parts of the application, and quickly adapt to the changing needs of users and the market.

References

1. A. Panchenko, Y. V. Shcherbatyuk. System Analysis and Design of Online Education Systems. Advanced Journal of Education, Science and Technology. 2020. Vol. 2, No. 4. P. 187-194.

УДК 004:42

*Кузьменко О. В., ст. викладач,**Бомблюк М. О., здобувач**Державний університет «Житомирська політехніка»*

WAVE FUNCTION COLLAPSE В РОЗРОБЦІ ІГОР

Wave Function Collapse (WFC) або згортання хвильової функції – концепція, що виникла в квантовій механіці, але знаходить нове застосування в індустрії відеоігор для створення випадкових, але структурованих об’єктів.

Основний принцип WFC полягає в тому, щоб взяти набір можливих патернів або фрагментів та об’єднати їх відповідно до заданих обмежень та вхідних даних.

В контексті ігор цей метод може бути використаний для генерації різноманітних ігрових рівнів, карт, ландшафтів, текстур та архітектурних елементів, забезпечуючи випадковість і одночасно дотримуючись певних правил та обмежень. Це може допомогти створювати унікальні та цікаві геймплейні елементи, необхідні для різноманітності та реіграбельності гри.

Загальний алгоритм процедурної WFC-генерації:

1. Є простір, умовно розбитий на кілька однакових елементів – комірок. Для кожної такої комірки існує кілька модулів, які можна помістити в неї. Ці модулі можуть представляти різні елементи гри, такі як частини карти, блоки ландшафту, об’єкти тощо. Спочатку безліч станів комірок включає всі можливі стани (рис. 1а):

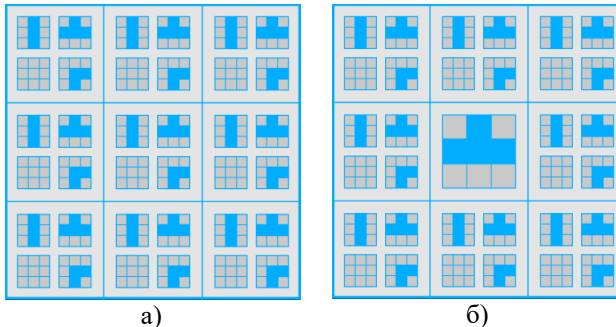


Рис. 1. Приклад ігрового простору:
а) початковий стан алгоритму; б) визначена комірка

2. Далі вибирається випадкова комірка, для якої існує найменша кількість можливих станів (але не менше двох). Всі модулі комірки, за винятком одного, видаляються, а той, що залишився, вважається «визначеним станом» цієї комірки. Спосіб, за допомогою якого цей модуль обиратиметься, може бути довільним (рис. 1б).

3. Тепер слід оновити набір станів кожної з сусідніх комірок: видаляються всі стани, які не поєднуються з модулем, вибраним у попередньому пункті (рис. 2а).

4. Пункти 1-3 повторюються доки не будуть визначені усі потрібні комірки (рис. 2б, 2в).

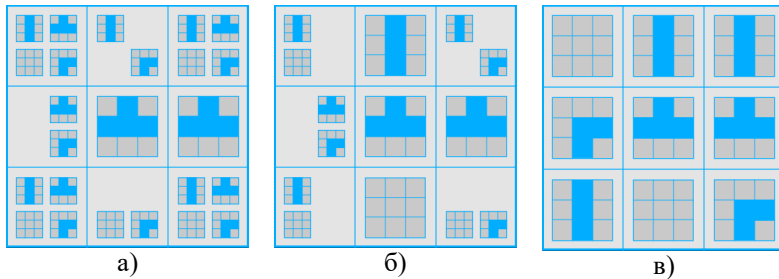


Рис. 2. Етапи алгоритму:

- а) оновлення сусідніх комірок; б) одна із ітерацій алгоритму;
 в) результат алгоритму

Отже, WFC дозволяє випадково генерувати ігрові об'єкти чи карти, при цьому зберігаючи структуру чи відповідність певним правилам. Цей алгоритм має безліч застосувань в розробці ігор, що не тільки дозволяє реалізувати унікальні концепції чи ідеї, а й забезпечити реіграбельність та різноманіття.

Список використаних джерел

1. Wave function collapse. [Електронний ресурс] – Режим доступу: https://en.wikipedia.org/wiki/Wave_function_collapse
2. Wave Function Collapse for procedural generation in Unity. [Електронний ресурс] – Режим доступу: <https://pvs-studio.com/en/blog/posts/csharp/1027/>
3. Generating Worlds With Wave Function Collapse [Електронний ресурс] – Режим доступу: <https://www.proccjam.com/tutorials/wfc/>

УДК 004:42

*Левицький А. А., здобувач,
Левківський В. Л., ст. викладач
Державний університет «Житомирська політехніка»*

ПАТЕРН STATE ЯК ЗАСІБ ДЛЯ СТРУКТУРИЗАЦІЇ ПРОГРАМНОГО КОДУ

Під час розробки комп'ютерної гри розробник може зіштовхнутись з потребою в змінюваному функціоналі об'єктів, наприклад, рух персонажа. Однак чим більше функціоналу в об'єкта, тим складніше буде розробнику додавати нові, адже в такому випадку потрібно переглянути весь програмний код та змінити його задля запобігання неполадок.

Для таких випадків доречно використовувати паттерн стану (State pattern) [1]. Від дозволяє структурувати програмний код, розділивши весь функціонал на окремі логічні блоки, що виконуватимуть свою дію.

Для прикладу, візьмемо програмний код руху персонажа, що дозволяє: стояти (бути в спокої), бігати, стрибати та робити ривок. З патерном всі рухи персонажа будуть окремими класами, в яких виконуватимуться необхідні дії та перевірятимуться умови, при яких стан буде замінюватись на інший. Поточний стан зберігається в класі машини стану (State Machine), а основний клас руху гравця циклічно виконує функціонал стану через єдиний метод машини.

Схема на рисунку 1 візуалізує роботу паттерна.

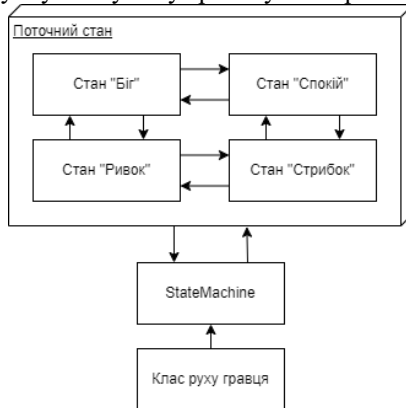


Рис. 1. Схема роботи паттерна

Класи станів є наслідувани від базового класу, що має основні поля та віртуальні методи, які, за потреби функціоналу класу, будуть реалізуватись. Така структура відповідає принципам об'єктно-орієнтованого програмування та допоможе записувати в поле поточного стану машини будь-який створений стан (рис. 2).

Сам клас машини станів, окрім поля поточного стану, має метод його початкової ініціалізації та метод задання поточного стану, який виконує завершення минулого стану та підготовку для роботи наступного (рис. 3).

```

public class PlayerBasicState
{
    Required field
}
class 8
public PlayerBasicState(
    PlayerMovement playerMovement, PlayerMovementStateMachine stateMachine)
}
class 20
public virtual void Enter()
}
class 21
public virtual void Exit()
}
class 22
public virtual void LogicUpdate()
}
class 13
public virtual void PhysicsUpdate()
{
    DoCheck();
}
class 20
public virtual void DoCheck()
}
    
```

Рис. 2. Приклад базового класу стану

```

public class PlayerMovementStateMachine
{
}
class 11
public PlayerBasicState CurrentState { get; private set; }
class 2
public PlayerBasicState PreviousState { get; private set; }
}
class 1
public void Initialize(PlayerBasicState state)
{
    CurrentState = state;
    CurrentState.Enter();
}
}
class 33
public void ChangeState(PlayerBasicState state)
{
    CurrentState.Exit();
    PreviousState = CurrentState;
    CurrentState = state;
    CurrentState.Enter();
}
}
    
```

Рис. 3. Приклад класу машини станів

Перевагою паттерна є:

- спрощення розуміння програмного коду;
- можливість простого додавання або вдосконалення функціоналу.

Однак слід пам'ятати, що будь-який паттерн слід використовувати тоді, коли цього потребує ситуація. State не є виключенням: він не буде доречним, якщо функціонал об'єкта не є великим.

Отже, паттерн State є необхідним інструментом для реалізації комплексного функціоналу об'єктів. З його допомогою можна спростити розуміння програмного коду, легше вдосконалити його в подальшому. Крім того, паттерн дозволяє запобігти виникненню певних можливих конфліктів за допомогою сталій структурі змінюваного функціоналу.

Список використаних джерел

1. State [Електронний ресурс] – Режим доступу: <https://refactoring.guru/design-patterns/state>

УДК 004.4:004.92

*Марчук Г. В., ст. викладач,
Макуховська Д. А., здобувач,
Лімінович І. Д., магістрант*

Державний університет «Житомирська політехніка»

ДОСЛІДЖЕННЯ ПРОБЛЕМ, З ЯКИМИ СТИКАЮТЬСЯ ДИЗАЙНЕРИ РІВНІВ У ПРОЦЕСІ РОЗРОБКИ ГРИ

Левел-дизайнер – це фахівець у галузі розробки ігор, відповідальний за створення та розробку рівнів у відеоіграх. Його робота включає в себе творення ігрових середовищ, визначення геймплейних завдань та розміщення ресурсів для оптимального досвіду гравця.

Основні функції левел-дизайнера: створення ігрового середовища, тобто розміщення ключових об'єктів, які впливають на геймплей, визначення ландшафту та архітектурних елементів рівня; розробка головоломок; місій; завдань у грі. Левел-дизайнер взаємодіє з гейм-дизайнерами, художниками, програмістами для досягнення спільних цілей, володіє комбінацією творчих, аналітичних та технічних навичок для створення захопливих та вирізняючихся рівнів в іграх. Його робота визначає якість геймплейного досвіду та важливо впливає на успіх гри в цілому.

Розробка ігрового рівня – це багатограний процес, під час якого левел-дизайнери стикаються з рядом проблем. Однією з проблем є створення цікавого рівня, який буде захоплюючим для гравців, де дії гравця мають велике значення та стимулюють дослідження. Рішення цієї проблеми: використання великої кількості інтерактивних елементів, складних головоломок та неочікуваних подій, які стимулюють гравців досліджувати рівень. Також розробники часто стикаються з викликом у знаходженні унікальних та захопливих концепцій гри, які забезпечать цікавий геймплей для гравців. У вирішенні цієї проблеми допоможе аналіз популярних ігор, вивчення досвіду гравців та цільової аудиторії. Ще однією проблемою є обмеженість ресурсів та технічних можливостей, що може ускладнювати створення великих та складних рівнів.

При створенні дизайну рівня, встановивши вже готовий ассет може виникнути певна проблема, з якою починаючий левел-дизайнер може зіштовхнутися вперше. Обираючи елемент, наприклад, ялинки, може виникнути помилка, яка сповіщає, що дерево Pine_tree має використовувати шейдер Nature/SoftOcclusion (рис.1).

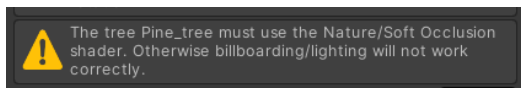


Рис. 1. Зображення помилки

Освітлення не працюватимуть належним чином. Ця помилка вказує, що можливо неправильні текстурні координати, проблеми із світлом та відсутність необхідних властивостей, адже шейдер може вимагати деякі додаткові параметри або властивості, які не були враховані в оригінальному ассеті. Наприклад, на локації ялинки однієї висоти та ширини, що ніяк не підходить гармонійно до дизайну рівня гри (рис. 2).



Рис. 2. Моделі ялинок, які мають один розмір

Для вирішення даних проблем, перше що потрібно зробити, це змінити коефіцієнт вигину моделі ялинки (Blend factory) на 1, також змінити налаштування шейдеру, а також за допомогою графічного редактору можна змінити відтінки кольорів на текстурі, задля того, щоб гармонійно виглядало з іншими елементами на сцені (рис.3).



Рис. 3. Готова локація

Левел-дизайнер відіграє ключову роль у створенні захоплюючих та цікавих рівнів у відеоіграх. Здатність впоратися з рядом складних завдань вимагає не лише теоретичних знань, але й творчого підходу до дизайну та практичних навичок.

Список використаних джерел

1. Fullerton, T., Swain, C., & Hoffman, S. (2004). Game design workshop: A playcentric approach to creating innovative games. Morgan Kaufmann Publishers.

УДК 621.3: 455.63

*Харченко А. В., магістрант,
Левківський В. Л., викладач,
Колос К. Р., д.пед.н., професор
Державний університет «Житомирська політехніка»*

ПРОЦЕДУРНА ГЕНЕРАЦІЯ ІГРОВИХ СВІТІВ

Процедурна генерація є важливим та актуальним елементом у розробці сучасних ігор і віртуальних світів. Цей підхід дозволяє створювати дуже різноманітні та нескінченно ігрові середовища, що змінюються, забезпечуючи унікальний досвід для гравця кожного разу, коли він запускає гру. Важливість процедурної генерації полягає в її здатності створювати величезні, яскраві світи з куточками, які можна досліджувати, зберігаючи при цьому зацікавленість гравця, кидаючи йому виклик. Крім того, цей підхід оптимізує використання ресурсів і дозволяє розробляти ігрові проекти з меншим бюджетом і в коротші терміни. Процедурна генерація продовжує впливати на індустрію розробки ігор і стала важливим інструментом для досягнення варіативності, реалістичності та глибини ігрових світів.

Метою дослідження є аналіз основних алгоритмів і підходів до генерації ігрових світів.

Під час процедурної генерації використовуються різноманітні алгоритми та підходи. Одним з найпоширеніших є використання шуму Перліна. Це тип градієнтного шуму, розроблений Кеном Перліном у 1983 році. Він має багато застосувань, включаючи, але не обмежуючись: процедурне генерування рельєфу, застосування псевдовипадкових змін до змінної та допомога у створенні текстур зображення. Найчастіше він реалізується у двох, трьох або чотирьох вимірах, але може бути визначений для будь-якої кількості вимірів [1].

Іншим доволі популярним алгоритмом є Diamond-Square algorithm або алгоритм «Ромбоподібний Квадрат». Це метод створення карт висот для комп'ютерної графіки. Це кращий алгоритм, ніж тривимірна реалізація алгоритму зміщення середньої точки, яка створює двовимірні пейзажі.

Алгоритм ромбовидного квадрата починається з двовимірного квадратного масиву шириною та висотою $2n + 1$. Для чотирьох кутових точок масиву спочатку потрібно встановити початкові значення. Потім по черзі виконуються кроки ромба та квадрата, доки не буде встановлено всі значення масиву.

Кожне випадкове значення множиться на константу, що відповідає за масштаб, яка зменшується з кожною ітерацією на коефіцієнт 2^{-h} , де

h є значенням від 0,0 до 1,0. Під час квадратних кроків точки, розташовані на краях масиву, матимуть лише три суміжні значення, а не чотири. Існує кілька способів впоратися з цим ускладненням. Найпростішим є взяти середнє лише трьох суміжних значень. Іншим варіантом є «обгортання», беручи четверте значення з іншого боку масиву. При використанні з узгодженими початковими кутовими значеннями цей метод також дозволяє з'єднати згенеровані фрактали без розривів [2].

Ще одним підходом при генерації ігрових світів є використання фракталів. У математиці фрактал – це геометрична фігура, що містить детальну структуру в довільно малих масштабах, зазвичай має фрактальну розмірність, що строго перевищує топологічну розмірність. Багато фракталів виглядають подібними в різних масштабах, як показано на послідовних збільшеннях множини Мандельброта. Ця демонстрація подібних візерунків у дедалі менших масштабах називається самоподібністю, також відомою як розширена симетрія або розгорнута симетрія. Якщо ця реплікація абсолютно однакова в кожному масштабі, як у губки Менгера, форма називається афінною самоподібною. Фрактали відіграють доволі важливу роль у сучасній процедурній генерації ігрових світів, пропонуючи можливість створювати складні та реалістичні ландшафти [3].

Отже, процедурна генерація ігрових світів завжди була важливим елементом ігрової індустрії, а використання різних алгоритмів і підходів демонструє неймовірну силу інновацій у цій галузі. Описані вище алгоритми та методи можуть надати гравцям неймовірно різноманітні та унікальні ігрові світи. Ці підходи допомагають оптимізувати ресурси, покращити процес розробки ігор та розширити можливості створення віртуальних світів з високим рівнем занурення. Використання різних алгоритмів і підходів є важливим кроком в еволюції ігрового дизайну, що дозволяє гравцям насолоджуватися іграми, які пропонують більше свободи, варіативності та реалізму.

Список використаних джерел

1. Perlin Noise: A Procedural Generation Algorithm. Raouf's blog. URL: <https://rtouti.github.io/graphics/perlin-noise-algorithm> .
2. TerrainGeneration – Diamond Square Algorithm. Daniel Beard's Programming Blog. URL: <https://danielbeard.wordpress.com/2010/08/07/terrain-generation-and-smoothing/>.
3. The Mandelbrot Set – Fractals – Mathigon. Mathigon. URL: <https://uk.mathigon.org/course/fractals/mandelbrot>.

УДК 004.4

*Ячменьова С. О., здобувач,
Марчук Г. В., ст. викладач
Державний університет «Житомирська політехніка»*

ВИКОРИСТАННЯ РОЗУМНИХ ПОКАЖЧИКІВ В C++

На сьогоднішній день одним із ефективних способів роботи з великою кількістю інформації в C++ є використання розумних покажчиків (Smart pointer), що розширюють функціональні можливості звичайного покажчика задля усунення проблем при роботі з пам'яттю, зокрема випадків спроби подвійного звільнення її комірок, тощо. Задля реалізації розумних покажчиків є необхідним створення абстрактного класу, який буде імітувати роботу звичайного покажчика, тому важливо зазначити.

Покажником є будь-яка змінна, яка містить адресу іншої в пам'яті і визначається як похідний тип даних. За видами використання розрізняють три види покажчиків: керовані покажчики (managed pointers), некеровані покажчики (unmanaged pointers), некеровані покажчики на функції (unmanaged function pointers) [1].

Традиційні або звичайні покажчики C++ є некерованими покажчиками, які вказують на об'єкти в нерегульованому об'ємі пам'яті, що виділяється для виконання програми [1]. Основними підвидами звичайних покажчиків є: покажчики на ціле і дійсне значення, на масив, символи, функції і структури, подвійні, нульові, постійні покажчики а також покажчики порожнечі і на константу [2].

У випадку, коли використання звичайного покажчика є недостатнім для вирішення програмних проблем застосовують розумні покажчики - класи, імітуючи роботу вказівника і розширюючи його можливості. Розрізняють три основних види розумних покажчиків: унікальний (unique), частковий (shared), слабкий (weak) [3].

Unique_ptr – це розумний покажчик, який володіє та керує іншим об'єктом через вказівник і позбавляється цього об'єкта, коли unique_ptr виходить за межі видимості [4]. Покажчик оголошується в C++ в просторі імен std за звернення std::unique_ptr.

```
unique_ptr<int> p1(new int(25));  
int* p2=p1.get();  
cout<<"*p1 = " << *p1 << endl << "*p2 = " << *p2 << endl;
```

Один з розумних покажчиків, який може вказувати на об'єкт, який вже має покажчика називається shared_ptr, оголошується в C++ в просторі імен std за звернення std::shared_ptr. Коли видаляється або перезаписується останній shared_ptr, то об'єкт знищується, а його

пам'ять звільняється [5].

```
shared_ptr<float> p3(new float(2.8f));
shared_ptr<float> p5 = p3;
cout << "*p3 = " << *p3 << endl << "*p5= " << *p5 << endl;
```

Розумний покажчик, який містить не володіючи ("слабке") посилання на об'єкт називають `weak_ptr`, викликають у `std` в `C++` за допомогою звернення `std::shared_ptr`. Цей вказівник потрібно перетворити на `shared_ptr`, щоб отримати доступ до об'єкта [6].

```
weak_ptr<int> p6;
shared_ptr<int> p7(new int(5));
p6 = p7;
cout << "p6 " << *p6.lock().get() << endl;
```

Отже, використання розумних покажчиків в `C++` - це поширена практика у сучасному світі, яка полегшує процес роботи з пам'яттю. Подальші дослідження будуть спрямовані на вдосконалення існуючих методів використання розумних вказівників.

Список використаних джерел

1. Покажчики. Частина 1. Загальні поняття. Типи покажчиків. Керовані та некеровані покажчики. Покажчики на функцію. Приклади використання [Електронний ресурс] // Bestprogish, BestBlog. – 2017. – Режим доступу до ресурсу: <https://www.bestprog.net/uk/2017/03/21/покажчики-частина-1-загальні-поняття/>.
2. C Pointers. [Електронний ресурс] – Режим доступу до ресурсу: <https://www.geeksforgeeks.org/c-pointers/>.
3. Розумні покажчики. Класи покажчиків `unique_ptr`, `shared_ptr`, `weak_ptr`. [Електронний ресурс] // Bestprogish, BestBlog. – 2017. – Режим доступу до ресурсу: https://www.bestprog.net/uk/2022/04/10/c-smart-pointers-pointer-classes-unique_ptr-shared_ptr-weak_ptr-ua/.
4. `std::unique_ptr`. [Електронний ресурс] // cppreference.com. – 2023. – Режим доступу до ресурсу: https://en.cppreference.com/w/cpp/memory/unique_ptr.
5. `std::shared_ptr`. [Електронний ресурс] // cppreference.com. – 2023. – Режим доступу до ресурсу: https://en.cppreference.com/w/cpp/memory/shared_ptr.
6. `std::weak_ptr`. [Електронний ресурс] // cppreference.com. – 2023. – Режим доступу до ресурсу: https://en.cppreference.com/w/cpp/memory/weak_ptr.

УДК 004

*Білецький Є. В., здобувач,
Петросян Р. В., ст. викладач
Державний університет «Житомирська політехніка»*

ВИКОРИСТАННЯ БЛОКЧЕЙНУ ДЛЯ ЗАХИСТУ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

Інтелектуальна власність є важливим активом у сучасному світі для багатьох людей та компаній. З розвитком цифрового світу збільшується обсяг обміну інформацією та пропорційно зростає ризик порушень прав на інтелектуальну власність. У цьому контексті технологія блокчейн може відігравати ключову роль у захисті прав власності та управлінні інтелектуальною власністю.

Блокчейн – це розподілена база даних, яка зберігає інформацію в децентралізованій мережі, тобто зберігається на декількох вузлах (комп'ютерах) мережі, утворюючи послідовні блоки даних, які взаємодіють між собою. Кожен блок містить інформацію та вказівник на попередній блок, утворюючи ланцюг [1].

Блокчейн може зіграти важливу роль для захисту інтелектуальної власності, тому що дана технологія використовує децентралізований реєстр та немає доступу для змін і надає прозорість інформації про інтелектуальну власність. Кожен об'єкт інтелектуальної власності може бути представлений у вигляді цифрового токена, який зберігається в блокчейні, що дозволить створити цифровий слід до кожного об'єкту, а це дозволить стежити за його власником, транзакціями та змінами власності [2].

Також використання блокчейну може облегшити процес ліцензування чи патентування, тому що процес буде автоматизовано за допомогою смарт-контрактів, тобто програм, які будуть автоматизовано виконувати процес ліцензування чи патентування при виконанні визначених вимог [3].

Блокчейн також може слугувати ефективним інструментом для перепродажу інтелектуальної власності, так як на сьогоднішній час є багато випадків коли у стартапів, винахідників та компаній у яких просто викрадали чи обманювали при покупці їх інновацій та ідей. Наприклад, у 2014 році німецька компанія Art+Com подала позов проти Google, звинувачуючи її у крадіжці технології для створення Google Earth [4]. Art+Com стверджували, що вони розробили цю технологію ще в 1994 році, а Google використала її без дозволу. Однак Google зміг відстояти свою позицію в суді і Art+Com не отримала

жодної компенсації. Блокчейн міг б допомогти вирішити цю проблему, забезпечивши прозорість та безпеку процесу як патентування, так і перепродажу інтелектуальної власності, тому що всі дії було б записано в єдиному місці, де також знаходилась би інформація про власника, про дату створення об'єкту інтелектуальної власності тощо. При необхідності доказів усі сліди в системі може переглянути кожен бажаючий і не може бути змінено зацікавленими сторонами.

Блокчейн зможе винахідників заохотити до нових інновацій, за допомоги створення екосистеми, в якій інноватори та творці зможуть безпечно обмінюватися ідеями та розробками, знаючи, що їх права будуть належним чином захищені. Все це може заохотити співпрацю та прискорити процес інновацій.

Надивлячись на те на скільки блокчейн ефективний та як він може використовуватися для захисту інтелектуальної власності, на разі йому ще треба подолати декілька проблем, які дозволили би його ефективно використовувати для захисту інтелектуальної власності. Перша проблема пов'язана з розробленням стандарту, щоб забезпечити сумісність різних систем та платформ. Друга проблема пов'язана з вирішенням юридичного питання, щодо того чи будуть токенизовані об'єкти інтелектуальної власності вважатися об'єктами інтелектуальної власності в правовому сенсі.

Коли всі проблеми будуть подолані, то блокчейн стане важливим інструментом для захисту інтелектуальної власності. Його використання може принести численні переваги для власників прав на інтелектуальної власності, інноваторів та компаній.

Список використаних джерел

1. What is blockchain technology? How does it work?. URL: <https://cointelegraph.com/learn/how-does-blockchain-work-everything-there-is-to-know> (date of access: 12.11.2023).
2. Blockchain for Protecting Intellectual Property. URL: <https://simbachain.com/blog/blockchain-for-protecting-intellectual-property> (date of access: 12.11.2023).
3. What are smart contracts on blockchain?. URL: <https://www.ibm.com/topics/smart-contracts> (date of access: 12.11.2023).
4. Art+Com Vs Google Case: What Every Inventor Should Know About Patent Rights. URL: <https://www.tekedia.com/artcom-vs-google-case-what-every-inventor-should-know-about-patent-rights/> (date of access: 12.11.2023).

УДК 004

*Райковський В. А., здобувач,
Петросян Р. В., ст. викладач*

Державний університет «Житомирська політехніка»

ОСОБЛИВОСТІ ВИКОРИСТАННЯ МІКРОКОНТРОЛЕРІВ У БЕЗПІЛОТНИХ ПОВІТРЯНИХ СУДНАХ

Мікроконтролер – це мінікомп'ютер, що в своїй будові на одній мікросхемі містить: процесор, пам'ять та периферійні пристрої. Сукупність мікроконтролера та додаткових елементів являють собою мініатюрні пристрої, основною задачею яких є виконання певних функцій у складі більш складного компонента [1].

Ці на перший погляд незначні пристрої, створюють реальність навколо нас та значно спрощують життя. Вони використовуються в наших авто (система GPS, подушки безпеки та антиблокувальна система гальмування ABS тощо); офісних приладах, медичних пристроях тощо.

Варто розглянути одну з вузько-направлених галузей інженерії, існування якої без мікроконтролерів є майже неможливим – галузь конструювання безпілотних повітряних суден (БПС) / дронів.

Дрон – це літаючі роботи, які розрізняють за цивільним та військовим призначенням. Вони використовуються у різних сферах, наприклад, сільському господарстві для моніторингу, зрошення та оброблення полів. Їх використовують в логістиці для доставки вантажів. Застосування дронів у військових цілях це не майбутнє, а сьогодення, саме ці пристрої відіграли важливу роль у відбитті наступу агресора на початку повномасштабного вторгнення росії в Україну.

На даній момент в дронах використовується вдосконалена система керування польотом, яка забезпечує надійність, стабільність та функціональність пристрою, система працює на основі ряду датчиків, які забезпечують більшу точність у керуванні [2]. Центром такої системи є контролер польоту на базі мікроконтролера, який відповідає за керування траєкторією польоту дрона на основі аналізу датчиків, які надають інформацію про положення пристрою в повітрі. Таким чином контролер польоту являє собою сукупність пристроїв: датчики, двигуни, мікроконтролер тощо.

В даному випадку основна задача мікроконтролера це аналіз даних, зібраних датчиками (гіроскоп, акселерометр, барометр, GPS тощо), та керування двигунами [2, 3]. Також він забезпечує отримання та обробку даних від пульта дистанційного керування або наземної

станції та здійснює управління інтерфейсом пристрою відеоспостереження. Однак обробка відео не здійснюється, тому що мікроконтролер не може обробляти відеопотоки у реальному часі.

Останнім часом істотно зросла розробка гетерогенних процесорів (це багатоядерні процесори, у яких ядра виконані з різною архітектурою), наприклад, відомі процесори M1 і M2 від Apple. Проте інші виробники також не стоять на місці. Подібні процесори стали випускати виробники чіпів для відеокamer, наприклад китайська компанія Fuzhou Rockchip Electronics випустила процесори серії RV11xx [4]. Особливістю даного процесора в тому, що, крім ARM-ядра, до складу входить мікроконтролер. Це означає, що використовуючи мікроконтролер можна виконувати керування БПС, а використовуючи сам процесор – обробку відеопотоку. Також до складу процесора входить нейронний блок обробки інформації, тому також можна задіяти штучний інтелект для обробки даних. Використовуючи такі процесори, можна обробку даних перенести з наземних станцій безпосередньо в БПС, роблячи їх суттєво функціональнішими (рис. 1).

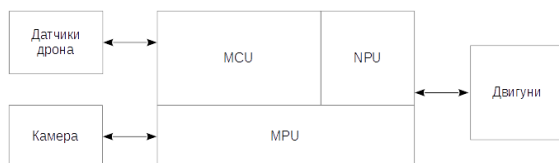


Рис. 1. Структура дрона з обробкою відеопотока на базі процесора RV1126

Використання мікроконтролерів в БПС спричинило суттєвий поштовх в розвитку конструювання цих пристроїв, забезпечивши більшу технологічність, точність та якість польоту.

Список використаних джерел

1. Zappa F. Microcontrollers. Hardware and Firmware for 8-bit and 32-bit devices. Società Editrice Esculapio, 2020.
2. Drone Technology: Future Trends and Practical Applications. / Mohanty S. N. et al. (ed.). John Wiley & Sons, 2023.
3. Петросян А.Р., Граф М.С., Петросян Р.В. Алгоритм фільтрації даних інерціальної навігаційної системи на базі нейронної мережі. Тези доповідей XIII Міжнародної науково-технічної конференції «Інформаційно-комп'ютерні технології», м. Житомир, 30-31 березня 2023р. Житомир: Житомирська політехніка, 2023. С.113 – 114 .
4. .Rockchips. URL: <https://www.rock-chips.com/a/en/> (date of access: 10.11.2023).

УДК 004

*Валецький М. С., здобувач,
Граф М. С., Ph.D*

Державний університет «Житомирська політехніка»

АНАЛІЗ СУЧАСНИХ ТЕНДЕНЦІЙ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ПРИ РОЗРОБЦІ ІНФОРМАЦІЙНИХ СИСТЕМ

Вступ. Для того щоб зрозуміти сучасні тенденції у розробці інформаційних систем, потрібно спочатку розібратись у самому понятті «Інформаційна система». Відповідно до визначення в книзі «Інформаційні системи та технології» авторства Леонарда М.Джессупа та Джозефа Валланті, інформаційна система – це «система, яка забезпечує збір, зберігання, обробку, передачу та використання інформації для вирішення завдань або вирішення проблем» [1]. А за визначенням Національного інституту стандартів та технологій, який знаходиться у Сполучених Штатах Америки, це – «система обробки інформації, включаючи обладнання, програмне забезпечення, комунікаційні, робочі, інформаційні та забезпечувальні системи, а також людей, які використовують, управляють, контролюють та обслуговують інформацію» [2].

Мета дослідження. Проаналізувати сучасні тенденції розробки інформаційних систем.

Виклад основного матеріалу. Якщо проаналізувати обидва ці визначення, то можна виділити наступні пункти, які є визначними для інформаційних систем: 1) Збір інформації; 2) Обробка та зберігання зібраної інформації; 3) Використання обробленої інформації;

Перед тим як перейти до безпосередніх тенденцій у розробці інформаційних систем, потрібно зрозуміти загальні тенденції у світі інформаційних технологій (ІТ). Очевидно, що темою номер один, на даний момент, є штучний інтелект (далі ШІ). Його стрімкий розвиток спричинив справжній бум серед всього людства. Це зачепило навіть тих людей, які аж ніяк не пов'язані з ІТ. Також варто зазначити, що не всі люди тепло прийняли такий стрімкий розвиток ШІ, одні ставляться з обережністю до нього, та притримуються поглядів теоретика та фізика Стівена Хокінга, який казав: «Розвиток повної штучної інтелектуальної системи може означати кінець людської раси» [3]. Інші ж, не цураються його використовувати і переконані що за ним майбутнє.

Сундар Пічаї, генеральний директор Google та Alphabet, дуже влучно сказав: «Штучний інтелект дійсно може змінити світ. Я вірю, що величезні можливості, які він нам принесе, будуть домінуючим фактором в майбутньому» [4]. Автори поділяють висловлену думку Сундара Пічаї: людству потрібно вчитися на помилках, адже історія циклічна. Як відомо, у XIX столітті набув популярності рух «лудитів» – це обітники, які виражали опозицію та стурбованість через впровадження машин та верстатів на виробництвах. Цей рух виявився неефективним у заваді технологічному прогресу, і з часом втратив свою активність.

Дослідженням впливу ШІ займалися і українські компанії. Так, найбільша ІТ-компанія України SoftServe зараз займається розвитком власної ШІ-лабораторії GenAI [5]. Згідно дослідженню компанії, ефективність роботи команд, які використовують у своїй роботі ШІ підвищилась на 40%. Результати дослідження за вересень 2023 показано на рис.1.

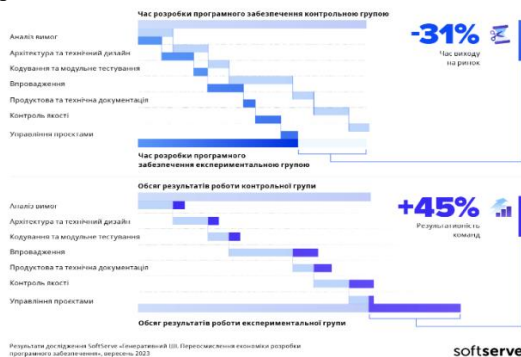


Рис. 1. Результати дослідження SoftServe «Генеративний ШІ». Переосмислення економіки розробки програмного забезпечення» [6]

Наступний графік видання Forbes (рис. 2), демонструє прогноз прибутків, які можуть в майбутньому отримувати корпорації при використанні ШІ.

Це означає, що все більше й більше компаній будуть зацікавлені в запровадженні ШІ. Його використання привносить лише переваги, та включає в себе й інші тенденції, які були популярні ще рік тому, а саме: Інтернет речей (IoT) – з розвитком Web 3.0, різні ШІ можуть взаємодіяти між собою, незалежно від пристрою; Обробка великих даних (Big Data); Автономність архітектури; Використання хмарних технологій та ін.

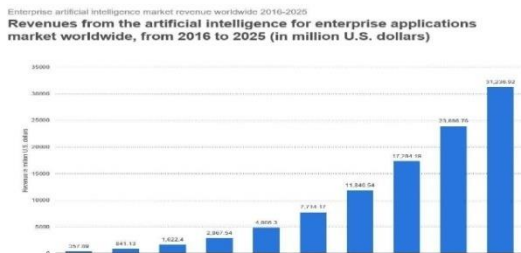


Рис. 2. Прогноз прибутків, згідно видання Forbes [5]

Висновки. Отож, основною тенденцією у розробці інформаційних систем стане впровадження ШІ. Адже в наш час, масиви інформації тільки збільшуються, збирати та обробляти інформацію стає все важче. Саме тут на допомогу може прийти ШІ.

Список використаних джерел

1. Leonard M. Jessup, Joseph S. Valacich, Information systems today, Prentice Hall, 2002, том 1, вип.1, с. 3-17.

2. Національний інститут стандартів і технологій (NIST) [Електронний ресурс]. Режим доступу: <https://www.nist.gov/information-technology>.

3. Сайт BBC Ukrainian. Хокінг, Ш. (2014). Штучний інтелект може стати "кінцем людства" [Електронний ресурс]. Режим доступу: https://www.bbc.com/ukrainian/science/2014/12/141202_hawking_artificial_intelligence_ozh.

4. Сайт Укрінформ. Глава Google вважає створення глобальних рамок для штучного інтелекту спільною відповідальністю держав [Електронний ресурс]. Режим доступу: <https://www.ukrinform.ua/rubric-technology/3788167-glava-google-vvazae-stvorennia-globalnih-ramok-dla-si-spilnou-vidpovidalnistu-derzav.html>.

5. Сайт Forbes.ua. Спільний проект з NVIDIA: галюцинації щі вплив на ринок праці. Інтерв'ю про штучний інтелект з Володимиром Карповим, R&D директором найбільшої ІТ-компанії "SoftServe" [Електронний ресурс]. Режим доступу: <https://forbes.ua/innovations/spilnyy-proekt-z-nvidia-galyutsinatsii-shi-vpliv-na-rinok-pratsi-intervyu-pro-shtuchniy-intelekt-iz-volodimirom-karpovim-rampd-direktorom-naybilshoi-it-kompanii-softserve-15112023-17263>

6. Statista. Worldwide Artificial Intelligence for Enterprise Applications [Електронний ресурс]. Режим доступу: <https://www.statista.com/statistics/607612/worldwide-artificial-intelligence-for-enterprise-applications/>

УДК 531.7

*Чалій О. В., аспірант
Київський авіаційний інститут*

СИСТЕМИ КЕРУВАННЯ КООРДИНАТНО-ВИМІРЮВАЛЬНИХ МАШИН

Система управління КВМ забезпечує функцію оперативної взаємодії між різними компонентами машини, такими як приводи, датчики переміщень, зондувальні системи і периферійні пристрої. За типом систем управління КВМ, що використовуються, можуть бути класифіковані на наступні групи:

- КВМ з ручним керуванням;
- КВМ з прямим комп'ютерним керуванням;
- КВМ, пов'язані з CAD/CAM системами (також мають пряме комп'ютерне керування).

Назва першого типу (з ручним керуванням) говорить сама за себе. У разі прямого комп'ютерного управління комп'ютер відповідає за переміщення рухомих частин машини, зчитування даних датчиків переміщень та обмін даними. При цьому для переміщення рухомих частин машини застосовуються різні стратегії управління, а саме:

- Позиційне управління;
- контурне керування;
- Векторне управління.

У разі позиційного управління цільове положення рухомого компонента визначається трьома координатами точки. Компонент рухається у напрямку цього положення з керованими швидкістю/прискоренням, поки досягне заданої точки. У цьому режимі керування спочатку переміщається компонент, що має найкоротшу відстань до заданої координати.

При використанні контурного керування можливі два відмінні один від одного режими: керування по розімкнутому контуру і керування по замкнутому контуру. У першому випадку зондувальна система переміщається в кінцеве положення по визначеній траєкторії із заданою швидкістю. При цьому рух завжди відстежується комп'ютером. Цей тип управління використовується, коли виконуються вимірювання геометричних елементів відомої форми. У разі керування по замкнутому контуру (адаптивного керування) вимірювальна головка переміщається в кінцеве положення по одній або двох осях з вибраною швидкістю. Якщо форма вимірюваного елемента змінюється, адаптивне керування гарантує підтримку

контакту вимірювального наконечника з поверхнею деталі. Цей тип керування використовується для сканування невизначених геометричних елементів (номінальна форма яких невідома).

Зазвичай сканування із розімкненим контуром управління швидше, ніж сканування із замкнутим контуром керування при одній і тій же точності, оскільки не потребує тривалого зворотного зв'язку з контролером. Однією з тактик програмування може бути створення заданого шляху елемента невідомої форми шляхом його початкового вимірювання в режимі сканування із замкнутим управлінням. Це може заощадити час, коли необхідно виміряти більш як одну деталь з однаковим елементом невідомої геометричної форми.

При використанні векторного управління досягається найкоротший шлях (рух прямої лінії) між початковими і кінцевими положеннями вимірювальної головки. В даному випадку вимірювальна головка переміщається в кінцеве положення одночасно по всіх трьох осях з оптимізованою швидкістю. Крім векторного позиціонування при даному типі управління, можливий векторний вимір. Це дуже важливо для швидких і відтворюваних вимірювань, коли вони виконуються для отворів з похилими осями та криволінійних поверхонь. Векторне керування також використовується для визначення розташування поверхонь вільної форми [1].

Додаткові завдання, які виконує система управління, включають у себе:

- спеціальні команди управління (наприклад, вибір режиму ручного чи прямого комп'ютерного управління чи режиму управління та команд для вимірювальної системи);
- різні завдання контролю, які охоплюють, наприклад, відстеження заданих положень; положень зупинки рухомих вузлів та виявлення можливих зіткнень.

У координатно-вимірювальних машинах останнього покоління вищезазначені завдання вирішуються за допомогою модульних мікропроцесорних систем керування. Ці багатопроцесорні модульні системи, в яких окремі мікропроцесори з'єднані внутрішньою шиною даних, виконують різні завдання, такі як збір інформації від датчиків переміщень, управління вимірювальною головою і приводною системою, а також передачу даних в комп'ютер, включаючи периферійні пристрої (рис. 1). Вони дозволяють значно відключити комп'ютер КВМ від завдань процесу управління. Комп'ютеру КВМ зазвичай залишаються тільки високорівневі завдання відправки вимірювальних команд (виміряти елемент 1, виміряти елемент 2 і т.д.),

обчислювальної обробки вимірних даних і генерації звітів, що підвищує продуктивність вимірювань. Для машин із системами температурної компенсації окремі мікропроцесори зазвичай виконують корекцію вимірних даних перед їх відправкою на обчислювальну обробку комп'ютер КВМ [2].

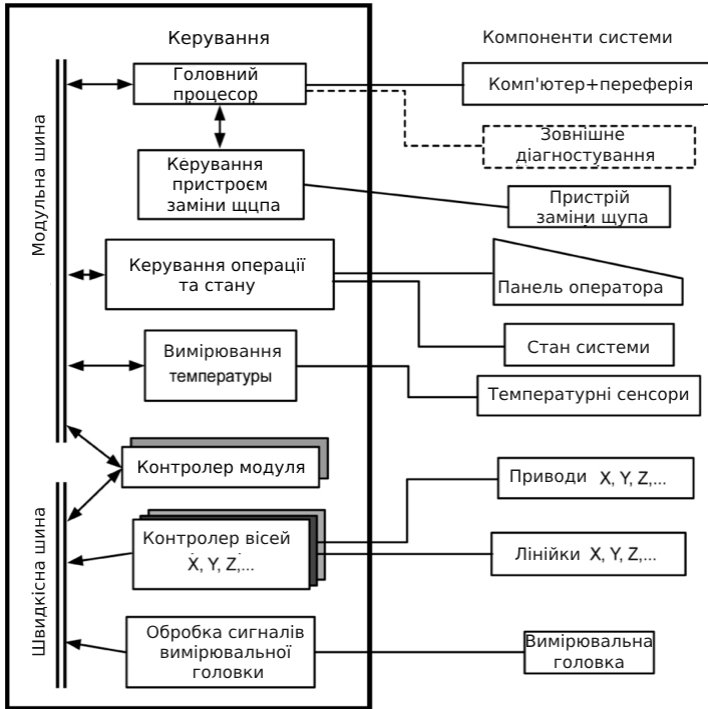


Рис. 1. Модульна багатопроцесорна система

Список використаних джерел

1. Mantel M. R. Coordinate Measuring Machines: Modern Inspection Tool in Manufacturing: thesis submitted in partial fulfillment of requirements for degree master of science in manufacturing systems engineering / M.R. Mantel. – Newark: New Jersey Institute of Technology, 1993. – 102 p.
2. Kolomiets L.V. Measuring systems of coordinate moving of measuring robots / L.V. Kolomiets, Y.P. Leschenko // Safety in Aviation and Space Technologies: proceedings V world congress – Aviation in the XXI-st century. – Kyiv, NAU, 2012. – P. 1.9.22-1.9.25.

УДК 004.8

*Дешков М. Ю., здобувач,
Марчук Г. В., ст. викладач*

Державний університет «Житомирська політехніка»

НАПРЯМКИ ВИКОРИСТАННЯ НЕЙРОННИХ МЕРЕЖ ПРИ ОБРОБЦІ ПРИРОДНОЇ МОВИ

Вступ. Останні досягнення в галузі нейромережових технологій відкрили велику кількість перспектив у сфері опрацювання природної мови (англ. Natural Language Processing, далі NLP). Мережі, що спеціалізуються на аналізі та обробці мовленнєвої інформації – являють собою універсальний інструмент, що спрощує та пришвидшує роботу сотень систем та технологій напряму пов’язаних з цим [1].

Загалом, сучасні нейронні мережі дають змогу створювати моделі, з покращеними якість адаптації до мовленнєвих особливостей і контекстів, забезпечуючи більш точний і граматично правильний переклад з однієї мови на іншу, якщо проводити порівняння з більш ранніми моделями, наприклад такими як перцептрон [2].

Мета дослідження. Отже, метою даного дослідження є провести опис напрямів використання нейронних мереж, що спеціалізуються на обробці природної мови.

Виклад основного матеріалу. Декілька ключових напрямків використання нейронних мереж для обробки природної мови:

1. Найбільш поширене застосування – це автоматичний переклад текстів між різними мовами. Завдяки процесу глибокого навчання, сучасні системи, побудовані на нейронних мережах, можуть забезпечувати високу точність перекладу. Саме з перекладу тексту, в 1940-х роках, почав своє існування напрямок обробки природної мови [3]. Подальший розвиток така модель була застосована в таких продуктах як “DeepL”, “OpenNMT” та “GoogleTranslator” [4].

2. Опрацювання аудіо. Це охоплює такі завдання як класифікація тексту, виявлення емоцій, поєднання текстів тощо. Серед найвідоміших на даний момент продуктів можна назвати такі системи: “Google’sWaveNet”, “DeepSpeech” – для генерації природної мови, та “EmoReact” для розпізнавання емоцій в аудіо.

3. Голосові асистенти широко використовуються для обслуговування клієнтів та персоналізованої взаємодії з користувачами. Вони можуть розпізнавати мову, інтерпретувати її та надавати користувачеві відповідь в потрібному вигляді. З відомих, “Amazon Alexa”, “Microsoft Cortana”, “Apple Siri”, “Google Assistant”.

4. Автоматичне генерування субтитрів для фільмів, переклад діалогів різними мовами. З популярних сервісів які використовують цю технологію: “GoogleCloudVideoAPI”, “IBMWatson”, “Netflix”.

5. Допомога при створенні адаптивних системи навчання, перекладаючи чи озвучуючи навчальні матеріали. Серед популярних платформ та додатків можна виділити “Duolingo” та “Coursera”.

6. Автоматичний переклад медичних записів, консультацій і документів. Серед систем які використовують подібний метод: “Lilt for Healthcare”, “Sensely”.

7. Туризм, готельний бізнес, сфера обслуговування. Скрізь, де необхідна комунікація з клієнтом для коректного та швидкого надання послуг. Наприклад це можуть бути консьерж-боти. А в Японії вже існують ресторани, де персоналом є роботи.

8. Інтеграція з соціальними мережами: автоматичний переклад постів і коментарів у соціальних мережах. Наприклад, мережа Meta–використовує нейронну мережу для автоматичного перекладу постів. Варто також відокремити потенціал реалізації подібних систем для допомоги людям з обмеженими можливостями. Створення не лише усних інструментів перекладу, а й візуальних чи тактильних, що зможуть правильно форматувати аудіо – значно спростить взаємодію з такими людьми.

Висновки. Описано напрями використання нейронних мереж для обробки природньої мови. Останнім часом стало розвинуто набуло використання нейронних мереж при автоматичному перекладі, візуальному розпізнаванні. Це дозволяє поліпшення комунікації людей, які спілкуються на різних мовах.

Список використаних джерел

1. Machine Translation With Natural Language Processing: A Strategy for Artificial Intelligence JUN 9, 2023 | AI AND MACHINE TRANSLATION.; <https://www.betranslated.com/blog/machine-translation-natural-language-processing/>.

2. Вікіпедія. Перцептрон. Електронний ресурс: <https://uk.wikipedia.org/wiki/Перцептрон>.

3. Обробка природньої мови. Електронний ресурс: https://www.wikidata.uk-ua.nina.az/Обробка_природньої_мови.html.

4. Exploring DeepL for Machine Translation: How It Works, and How Accurate It Is. Електронний ресурс: <https://phrase.com/blog/posts/deep/>.

УДК 621.3: 455.63

*Смульський Д. З., магістрант,
Левківський В. Л., ст. викладач,
Колос К. Р., д.пед.н., професор
Державний університет «Житомирська політехніка»*

ІГРОВІ ДОДАТКИ У НАВЧАЛЬНОМУ ПРОЦЕСІ

Вступ. Сучасні технології докорінно змінюють обличчя освіти, надаючи їй нові грані завдяки інноваційним ігровим додаткам, які активно використовуються для вивчення різних предметів, зокрема історії. Ці додатки не лише передають інформацію, але й перетворюють навчальний процес, переносячи учнів у захоплюючий віртуальний світ, де вони можуть інтерактивно вивчати предмет.

Постановка завдання. Провести аналіз використання ігрових додатків у навчальному процесі.

Основний матеріал. Ігрові технології, які застосовуються під навчання, виявляються не просто засобом передачі знань, але й каталізатором активного та ефективного навчання. Одним з найважливіших елементів успішного функціонування ігрових додатків є алгоритми обробки інформації. Ці алгоритми відіграють ключову роль у підтримці точності, стабільності та ефективності навчального процесу в ігрових середовищах. Ефективні алгоритми мають здатність адаптуватися до різних стилів навчання та унікальних особливостей кожного учня. Це досягається завдяки різним завданням та гнучкому рівню складності, які можуть бути налаштовані для відповідності потребам кожного учасника навчального процесу. Важливою характеристикою є інтерактивність: можливість співпраці між учнями, ігрові елементи та можливість виконання завдань разом для зміцнення знань. Мотивація, важливий аспект, що підтримує досягнення результатів та поглиблює інтерес до вивчення історії, також є результатом впливу цих алгоритмів. Вони сприяють створенню захоплюючого та цікавого навчального середовища, де процес вивчення історії перетворюється на динамічний та ефективний, завдяки вдосконаленим алгоритмам обробки інформації. Такі алгоритми є не тільки важливим елементом успішності ігрових додатків для вивчення історії, але і гарантують якість освіти, створюючи доступне середовище для різних типів навчальних потреб та стилів навчання [2]. Поєднання технічної досконалості та педагогічної ефективності алгоритмів обробки інформації у таких додатках відкриває безмежні можливості для розвитку освіти,

викликаючи захоплення учнів історією через захопливі ігрові технології. Ігрові додатки в наш час займають в освіті важливе місце, адже технології не стоять на одному місці, постійно розвиваючись у геометричній прогресії. Більшості учням було б значно цікавіше вивчати той чи інший предмет завдяки грі ніж за шкільними підручниками. Іграм властиві характеристики, що дають підставу розглядати їх як засіб навчання. Порівняння компонентів навчальної й ігрової діяльності переконує в наявності подібності між ними, тому що засоби здійснення навчальної й ігрової діяльності, по суті, ідентичні, оскільки навчальна задача – це не що інше, як модель проблемної ситуації, а імітаційне моделювання в грі – це спосіб формулювання завдання. Крім того, ефективність навчання збільшується за рахунок того, що учні одержують інформацію в той момент, коли вона їм потрібна, вони у будь-який час можуть повернутися і продивитись раніше пройдене та запросити підказку у комп'ютера. Саме комп'ютерне навчання у позааудиторному середовищі несе в собі величезний мотиваційний потенціал і відповідає принципам індивідуалізації навчання [1].

Висновки. Отже, ігрові додатки для вивчення історії на сьогоднішній день стали не лише інструментом передачі знань, а й потужним стимулом до активного та поглибленого освоєння історичних фактів. Вони є ключовим чинником залучення учнів до процесу навчання, створюючи цікаві та захопливі ігрові віртуальні світи, де історія стає живою та доступною. Додатки цього типу відкривають необмежені можливості в удосконаленні навчальних програм. Їхня технічна складність поєднується з педагогічною ефективністю, що робить процес вивчення історії захопливим для різних типів учнів. Враховуючи різноманітність методів навчання, індивідуальні особливості та потреби кожного учня, ці додатки надають персоналізований підхід до освіти. Такі інноваційні рішення у світі освіти не лише допомагають збагатити навчальний процес, але й стимулюють інтерес до вивчення історії.

Список використаних джерел

1. Басов В. В., Сергіна С. В. Комп'ютерні ігри у навчальному процесі : thesis. 2008. URL: <http://repository.kpi.kharkov.ua/handle/KhPI-Press/39679>
2. Моряк П. А. Технічні засоби обробки інформації. Львів, 1977. 111 с.

Секція 4 СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ТЕЛЕКОМУНІКАЦІЯХ ТА БІОМЕДИЦИНІ

УДК 535.37; 621.317

*Яненко О. П., д.т.н., професор,
Шевченко К. Л., д.т.н., професор,
Клочко Т. Р., к.т.н., доцент*

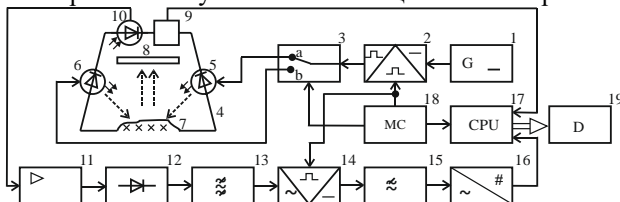
*Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»*

ВИСОКОЧУТЛИВИЙ ВИМІРЮВАЧ ЛЮМІНЕСЦЕНТНОГО ВИПРОМІНЮВАННЯ

Фотолюмінісцентні процеси і апаратура для вимірювання їх параметрів представляють достатньо складну галузь фотометрії. В той же час використання фотолюмінесценції є перспективним для діагностики стану біологічних тканин, дослідження матеріалів в медицині, харчовій та хімічній промисловості [1, 2]. Використання цих методів підвищує ефективність медико-діагностичних досліджень, однак на ринку відсутня проста та доступна апаратура для їх проведення, що обумовлює актуальність розробки.

Авторами [3] запропонований фотометричний вимірювач інтенсивності люмінесцентного випромінювання звикористанням комутаційно-модуляційного перетворення оптичного інформаційного сигналу. Для опромінення досліджуваного об'єкта використовуються світлодіоди ультрафіолетового (УФ) та інфрачервоного (ІЧ) діапазонів. Випромінювання УФ діапазону забезпечує дослідження поверхневих шарів біологічної тканини, а ІЧ сигнали – глибинних.

На рисунку представлена функціональна схема розробленого авторами вимірювача потужності люмінесцентного випромінювання.



Вимірювач працює наступним чином. Спочатку проводиться вимірювання потужності люмінесценції при збудженні УФ сигналом. Для цього ключ 3 сигналом з мікроконтролера 18 встановлюють в

положення a , періодично подаючи на УФ світлодіод 5 напругу з модулятора 2. Це призводить до періодичної модуляції світлового потоку, що опромінює об'єкт дослідження 7. При цьому формується модульований відгук сигналу люмінесценції.

За один період модуляції на фотодіод 10 поступають два сигнали:

$$\begin{cases} \phi_1(t) = K_v \phi_o(t) + \phi_w(t) \\ \phi_2(t) = \phi_w(t) \end{cases},$$

де $\phi_o(t)$ – опромінюючий сигнал світлодіода 5; K_v – коефіцієнт енергетичного виходу люмінесценції; $\phi_w(t)$ – сигнал шумів, наводок та інших завод на вході фотодіода 10.

Відповідно, на навантаженні фотодіода 10 виділяється напруга:

$$U_1 = S_1(K_v I_o + I_w) R_n = S_1(U_o + U_w),$$

$$U_2 = S_1 I_w R_n = S_1 U_w,$$

де S_1 – крутість перетворення фотодетектора 10; I_o, I_w – струми, які відповідають амплітуді люмінесцентного випромінювання U_o та шумових завод U_w ; R_n – опір навантаження фотодетектора 10.

Після підсилення (11), квадратичногодетектування (12), смугової фільтрації за частотою комутації (13), синхронного детектування (14) на виході вимірювального каналу компенсуються шуми, а фільтром нижніх частот 15 виділяється напруга, яка пропорційна потужності люмінесцентного випромінювання:

$$U_5 = \frac{1}{2} S_2 U_3 (U_1 - U_2)^2 = \frac{1}{2} S_2 (K_v U_o + U_w - U_w)^2 = 0,5 S_2 K_v U_o^2 U_4 \approx P_o,$$

де S_2 – сумарний коефіцієнт перетворення вимірювального каналу.

Отримане значення потужності випромінювання перетворюється АЦП 16 в код і подається на пристрій реєстрації сигналів. Дослідження люмінесцентного відгуку в ІЧ діапазоні виконується аналогічно при перемиканні ключа 3 в положення b і роботі світлодіода 6.

З кінцевого рівняння видно, що шуми каналу перетворення не впливають на результат вимірювання, що дозволяє на 1...2 порядки збільшити чутливість вимірювача, а відповідно і його точність.

Список використаних джерел

4. Shimomura, Osamu. Bioluminescence: chemical principles and methods. WorldScientific, 2006. ISBN 9812568018, 9789812568014.

5. Aubin Fleissand Karen S. Sarkisyan. A brief review of bioluminescent systems (2019) Архівна копія від 27.12.2020 на WaybackMachine. CurrGenet. 2019; 65(4): 877-882. PMID 30850867.

6. Вимірювач потужності люмінесцентного випромінювання. Патент України на корисну модель № 143355 Бюл. №15 від 10.08.2020 р.

УДК 621.396.24

*Андреев О. В., к.т.н, доцент,
Нестеренко К. О., магістрант,
Лециньський Ю. І., магістрант*

Державний університет «Житомирська політехніка»

ОСОБЛИВОСТІ ПЕРЕДАВАННЯ ЦИФРОВИХ ДАНИХ З ВИКОРИСТАННЯМ БЕЗДРОТОВИХ ТЕХНОЛОГІЙ

В наш час розвиток систем передачі команд управління на відстань є надзвичайно важливим. Аспекти безпеки та швидкість передавання команд також мають суттєве значення. Сьогодні безпілотні літальні апарати (БПЛА) знаходять все більше застосувань у різних сферах людської діяльності. Якщо раніше вони використовувалися переважно для військових цілей, то на сьогоднішній день вони є потребою й у цивільних галузях, таких як сільське господарство та спостереження за дикими тваринами, тощо. Тому для при експлуатації БПЛА надзвичайно актуальним є визначення та дослідження можливостей та параметрів в контексті використання певних технологій, зокрема технологій LoRa та DVB-T2.

Технології LoRa та DVB-T2 – це можливість бездротового зв'язку на відносно великих відстанях, які працюють на радіочастотах до 1 ГГц. У своїй основі, LoRa використовує для розширення спектру сигналу модуляцію ChirpSpreadSpectrum, що дозволяє підвищити стійкість радіосигналу як до ненавмисних, так і до навмисних перешкод. Під час передавання цифрових даних відбувається адаптивна зміна бази радіосигналу з метою забезпечення необхідної якості зв'язку. Це досягається за рахунок зміни тривалості символу, що залежить від коефіцієнту розширення спектру радіосигналу, який фактично визначає розрядність символу даних, що передається за час тривалості символу. Крім адаптивної зміни швидкості передачі даних передбачається також зміна потужності передавача для кожного окремого пристрою індивідуально задля забезпечення заданої якості передавання даних і економного використання автономних джерел живлення. При цьому змінюється і дальність дії радіолінії. Тому при побудові бездротової радіолінії важливо мати методіку розрахунку дальності передавання пакетів даних з визначеною швидкістю.

На якість передавання цифрових даних за стандартами LoRa та DVB-T2 впливає ряд факторів. Втрати корисного сигналу при розповсюдженні від передавача до приймача на відстань R складаються з втрат у вільному просторі та втрат, що обумовлені

специфічними умовами поширення радіохвиль. Багатопроменивий характер поширення радіохвиль, утворення тінювих зон, багаторазове відбиття і розсіювання радіохвиль, при розповсюдженні в умовах міського середовища, породжує явище міжсимвольної інтерференції при передачі цифрових даних.

Спотворення сигналу, що обумовлені міжсимвольною інтерференцією, можуть викликати погіршення якості передачі цифрової інформації. Крім того мають місце втрати сигналу при розповсюдженні в атмосфері і через не ідеальність приймально-передавального тракту. Для оцінки сумарних втрат сигналу в радіолінії LoRa та DVB-T2 запропоновано використання моделі розповсюдження радіохвиль Окамура–Хата, згідно з якою втрати в місті розраховуються за виразом:

$$L_{50/місто} = 69,55 + 26,16 \lg(f_{[MGz]}) - 13,83 \lg(h_B) - a(h_M) + (44,9 - 6,55 \lg(h_B)) \cdot \lg(R_{[км]}),$$

де $a(h_M)$ – поправочний коефіцієнт.

Для малого та середнього міста цей коефіцієнт визначається наступним чином:

$$a(h_M) = (1,11 \lg(f_{[MGz]}) - 0,7)h_M - (1,56 \lg(f_{[MGz]}) - 0,8).$$

Втрати в передмісті:

$$L_{50/передмістя} = L_{50/місто} - 2 \left(\lg \left(\frac{f_{[МГц]}}{28} \right) \right)^2 - 5,4.$$

Втрати в сільській місцевості:

$$L_{50/село} = L_{50/місто} - 4,78(\lg(f_{[МГц]}))^2 + 18,33 \lg(f_{[МГц]}) - 40,94.$$

Для визначення рівня потужності сигналу на вході приймача радіолінії запропоновано використовувати максимально можливе значення послаблення радіосигналу. Наводяться орієнтовні значення запасу на завмирання сигналу при побудові зони дії радіоліній.

Список використаних джерел

1. Які відмінності між LoRa та LoRaWAN. <https://www.mokosmart.com/uk/lora-and-lorawan/>
2. Що таке технологія LoRa – Поглиблений посібник 2023. <https://www.mokosmart.com/uk/lora-technology/>
3. Howaredronescontrolledandaperated? <https://ts2.space/en/how-are-drones-controlled-and-operated/>

273УДК 621.3: 455.63

*Сторожук І. М., магістрант,
Коренівська О. Л., к.т.н., доцент
Державний університет «Житомирська політехніка»*

ВИЗНАЧЕННЯ ЕФЕКТИВНОСТІ ГЕМОДІАЛІЗУ ТА ГЕМОДІАФІЛЬТРАЦІЇ ПРИ НИРКОВІЙ НЕДОСТАТНОСТІ

Наразі в світі спостерігається щорічне зростання хронічних захворювань нирок, серед яких значну кількість займає хронічна ниркова недостатність, що є серйозним фактором загрози здоров'ю та життю населення. Класичним методом очищення організму від токсинів та надлишку рідини при цьому є гемодіаліз. Дослідження ефективності гемодіалізу важливо для пошуку способів поліпшення процедури, забезпечення найвищого ступеня безпеки і комфорту для пацієнтів, а також оптимізації витрат медичних ресурсів на проведення гемодіалізу. Враховуючи постійний розвиток медичних технологій та важливість гемодіалізу для великої кількості людей, дослідження у цій області є актуальними і можуть сприяти подальшому вдосконаленню методів лікування та догляду за хворими з хронічною нирковою недостатністю.

Гемодіаліз [1] – це один із способів замісної ниркової терапії, за допомогою якого проводиться видалення кінцевих продуктів метаболізму – креатиніну та сечовини, а також вільної води. Метод заснований на принципі дифузії та конвекції речовин з малою та середньою молекулярною масою через напівпроникну мембрану, що дозволяє видалити з крові токсичні речовини та продукти метаболізму.

Швидкість руху речовин через мембрану залежить від наступних факторів: різниці в концентрації; величини пор мембрани; поверхні мембрани; величини молекули речовини; часу експозиції; температури і заряду мембрани. При цьому, якщо концентрація речовини по обидві сторони мембрани вирівнюються, то дифузія повністю припиняється.

На практиці застосовують такі мембрани, через які вільно дифундує вода і електроліти, гірше низькомолекулярні метаболіти, дуже погано середньо молекулярні токсини (ММ 500 – 5000 дальтон). Навпаки, повністю не проникають білки і великомолекулярні фракції, що дозволяє підтримувати онкотичний тиск крові і інші фізіологічні процеси.

Гемодіафільтрація (ГДФ) – це один з апаратних методів очищення крові, який відрізняється від традиційного гемодіалізу тим, що поєднує в собі два принципи – дифузію та конвекцію. Тоді як гемодіаліз відбувається тільки за рахунок дифузії і дозволяє виводити переважно

низькомолекулярні сполуки. Конвективний процес заснований на ультрафільтрації великої кількості води з плазми крові крізь напівпроникну мембрану і дозволяє виводити середні та великі молекули. Тому гемодіафільтрація дозволяє очищати більший об'єм крові від більшого спектру токсинів, а обсяг втраченої рідини заміщується стерильним розчином, який готує апарат.

Лікування методом ГДФ-онлайн має ряд переваг для пацієнтів:

- Стабілізація артеріального тиску під час процедури (зменшення епізодів низького тиску під час гемодіалізу).

- Крайній контроль анемії, підвищення рівню гемоглобіну, зниження доз еритропоєтинів та потреби в гемотрансфузіях.

Через підвищену ефективність діалізу при застосуванні методу ГДФ також зростає якість лікування:

збільшується Kt/V,

краще видаляються середньо-молекулярні токсини,

знижується ризик серцево-судинних ускладнень через крайній контроль артеріального тиску і анемії.

Задачею дослідження було визначити ефективність гемодіалізу та гемодіафільтрації, порівняти яка з процедур краще та довести твердження [2], що у результаті постійного лікування методом ГДФ, зменшується кількість госпіталізацій та смертності серед пацієнтів на діалізі.

Для визначення ефективності та розрахунку Kt/V були проведені дослідження на базі відділення гемодіалізу Житомирської обласної лікарні ім. О.Ф. Гербачевського Житомирської обласної ради. Індекси, що застосовуються для кількісної оцінки ефективності процедур гемодіалізу та гемодіафільтрації залежать від концентрації сечовини в пробах крові до та після процедур. Тому були взяті проби крові у контрольних груп пацієнтів на початку процедури та після. У пацієнтів застосовувалася стандартна програма діалізу – три рази на тиждень по 4 години.

Список використаних джерел

1. Надання медичної допомоги хворим на хронічну хворобу нирок у стадії, які лікуються гемодіалізом. Адаптована клінічна настанова, заснована на доказах. [Електронний ресурс]. Режим доступу: https://dec.gov.ua/wp-content/uploads/2019/11/2016_89_akn_xxn.pdf

2. High-Efficiency Postdilution Online Hemodiafiltration Reduces All-Cause Mortality in Hemodialysis Patients /Maduell, Francisco; Moreso Francese; Ramos Rosa /JournaloftheAmericanSocietyofNephrology, 2013, 24(3) : p 487-497.

УДК 621.37

**Ципоренко В. В., к.т.н., доцент,
Мельниченко О. В., магістрант**
Державний університет «Житомирська політехніка»

ДОСЛІДЖЕННЯ КОМБІНОВАНОЇ МЕРЕЖІ ВІДЕОСПОСТЕРЕЖЕННЯ ТЦ ОЛДІ

Проектування та операційна діяльність великих торгових комплексів вимагають впровадження складних систем для гарантування безпеки відвідувачів та персоналу, а також для збереження майна підприємства. Однією з центральних компонентів таких систем є мережа відеоспостереження.

Для створення бездротової мережі для IP-камер у 5 ГГц діапазоні потрібно подвоїти кількість точок доступу. На підставі розрахунків, знаємо, яка швидкість передачі даних необхідна для нашої мережі для повного набору IP-камер у системі відеоспостереження. Але за умови обмеженої кількості IP-камер у нашому розпорядженні, ми можемо встановити нашу мережу на стандарті 2.4 ГГц. Всі роутери випромінюють сигнал на частоті 2412 МГц із вихідною потужністю 20 дБм, користуючись антеною, яка має підсилення 6 дБі.

Усі точки доступу були розташовані так, щоб гарантувати мінімальний рівень сигналу не нижче -59 дБм. Ця конфігурація дозволяє забезпечити стабільну передачу даних на швидкості приблизно 55 Мбіт/с, що вже більш ніж достатньо для ефективної роботи системи відеоспостереження. Максимальна швидкість передачі даних в системі становить 38,3 Мбіт/с при використанні високоєфективного кодека H.264 та відмінного стиснення відео.

При роботі з мережами 802.11 часто виникають проблеми, пов'язані з підвищеним навантаженням на мережу та якістю надання послуг зв'язку та інформації. Це обумовлено значною кількістю активних користувачів, які підключені до однієї точки доступу, а також численними користувачами, які використовують послуги передачі потокового відео, такі як відеокамери. Навіть в рамках однієї будівлі можуть виникати проблеми через насиченість бездротового середовища.

Відповідно до теоретичних досліджень, щодо основних показників якості камер, було зроблено висновок, що всі ці характеристики взаємозалежні, і не існує єдиного визначального параметра, що визначав би їх якість.

Важливо відзначити, що діапазон 5 ГГц має свої переваги порівняно зі старішим стандартом. Він дозволяє з'єднувати більше

пристроїв без втрати якості сигналу і має значно вищу максимальну швидкість та пропускну здатність для мережі. Це досягається завдяки розширенню ширини каналу до 80 МГц, а її можна подвоїти за потреби. Проте є одна суттєва негативна риса.

З аналізу показників моделювання покриття можна зробити висновок, що для нашого об'єкта площа ефективної області покриття та стійкість до перешкод для стандарту 5 ГГц принаймні вдвічі менша, ніж для стандарту 2.4 ГГц.

В роботі було проведено дослідження комбінованої мережі відеоспостереження ТЦ ОЛДІ. Мережа відео нагляду складається із двох частин: система зовнішнього відео нагляду та внутрішнього. Аналізуючи результати наших досліджень параметрів відеокамер, можна прийти до висновку, що аналогові камери втрачають актуальність через численні переваги, які пропонують IP-камери. Зокрема, до цих переваг входить легший доступ до інформації, вища роздільна здатність та підтримка новітніх технологій. Єдиний плюс аналогових камер полягає у їх більш доступній ціні.

Під час аналізу зон покриття радіоканалу в системах зовнішнього відеоспостереження ми можемо прийти до висновку, що для ефективної реалізації системи відеонагляду з використанням передових технологій в основному обирається діапазон частот 2.4 ГГц через його оптимальний радіус дії та стійкість до різних видів перешкод. Хоча цей діапазон має меншу пропускну здатність, але її вистачає для систем відеоспостереження, в яких використовуються камери з невеликою роздільною здатністю. Якщо з'явиться необхідність, можна побудувати більш щільну мережу та перейти на стандарт 5 ГГц, який має більшу пропускну здатність і може витримати більше навантаження.

Мережа внутрішнього відеонагляду забезпечує спостереження за персоналом та відвідувачами всередині приміщення торговельного центру. Передача даних здійснюється через виту пару з використанням Ethernet. Керування потоками даних здійснюється за рахунок використання відеореєстраторів, а архівування – дискового накопичувача. Відео зберігається протягом 14 діб.

Список використаних джерел

1. Ковтун О. І. Бездротові мережі з використанням стандартів ZigBee, Bluetooth, Wi-Fi / О. І. Ковтун, В. Л. Плєскач, О. П. Ткаліч // Радіоелектронні і комп'ютерні системи. – 2016. – № 4. – С. 42–47.
2. План ТРЦ “ОЛДІ”. Інтернет ресурс: <https://oldi.center/schema-oldi>

УДК 621.37

*Дубина О. Ф., к.т.н., доцент,
Коваль Д. В., к.т.н.,
Коваль М. В., здобувач*

Державний університет «Житомирська політехніка»

АНТЕННИЙ ТРЕКЕР БЕЗПЛОТНОГО ЛІТАЛЬНОГО АПАРАТУ FPV

Сьогодні в Україні та у світі в цілому спостерігається стрімкий розвиток безпілотних систем, зокрема безпілотних авіаційних комплексів (БпАК).

Розвиток БпАК відбувається в тому числі й за рахунок вдосконалення їх наземної складової. Використання наземних спрямованих антен командної радіолінії та відеолінку дозволяє суттєво збільшити дальність радіозв'язку з дроном.

Разом з тим, постає задача орієнтування спрямованих антен у напрямку безпілота (антенний трекінг).

Вирішення вказаної задачі передбачає попередньо визначення кутових координат безпілотного літального апарату (БпЛА). Визначення кутових координат БпЛА можливе декількома шляхами:

1. Активне пеленгування.
2. Пасивне пеленгування за випроміненням сигналу відеолінку, або радіотелеметрії.
3. Розрахунок кутових координат з відомих географічних координат БпЛА та наземного пункту керування, у разі наявності на борту навігаційного модуля GPS та передавача телеметрії, а також навігаційного модуля GPS та приймача радіотелеметрії на пункті приймання.

Пасивне пеленгування дрону є апаратно більш виправданим та найбільш універсальним рішенням.

Серед відомих пасивних методів пеленгування для розв'язання вказаної задачі обґрунтовано метод порівняння амплітуд сигналів відеолінку, враховуючи особливості побудови наземного приймача. Наземний приймач радіосигналу відеолінку, як правило є двоканальним (діверсіті) пристроєм, що має виводи вимірних рівнів потужності прийнятих сигналів (RSSI) в кожному з двох приймальних каналів. RSSI в даному випадку пропорційні напрузі 0...5 В на цих виводах.

Використання RSSI у схемі пеленгації з порівнянням амплітуд дозволяє визначити кутову координату, наприклад, азимут дрона, відносно спостерігача на землі. Далі азимут передається на пристрій

керування азимутальним сервоприводом опорно-поворотної платформи.

Як пристрій керування обґрунтовано вибір плати прототипування ArduinoUno. Напруги, що пропорційні RSSI в кожному з двох приймальних каналів подаються на два канали АЦП плати Arduino Uno. Отримані цифрові значення RSSI порівнюються та виробляється сигнал керування, що передається на сервопривод з вбудованого в Arduino Uno генератора сигналу з широтно-імпульсною модуляцією.

Антенна система, що закріплена на платформі, складається з двох приймальних антен, взаємне розміщення яких відповідає вимогам побудови пеленгатора за методом порівняння амплітуд – суміщені фазові та рознесені горизонтально на ширину діаграми спрямованості амплітудні центри.

Вибір типу приймальних антен залежить від виду поляризації, характеристик спрямованості, забезпечення робочого діапазону частот. До таких антен можуть бути віднесені спіральні, директорні, патч-антени.

Для побудови антенної системи антенного трекера FPV-БпЛА обґрунтовано вибір фабричних приймальних патч-антен, що задовольняють вказані вище вимоги. Крім того, патч-антені властива міцність та компактність конструкції, що дає додаткові переваги їх використання в складі мобільного наземного пункту керування в польових умовах.

Слід відмітити, що наведена структура антенного трекера актуальна для роботи на дальностях до дрона, що суттєво перевищують висоту його польоту.

Для менших дальностей необхідно додати кутомісцевий канал пеленгації, що не відрізняється ані апаратно, ані програмно від азимутального. Це дозволить організувати трекінг FPV-БпЛА у всій верхній полусфері на любых доступних до пеленгації дальностях дії БпЛА.

Список використаних джерел

1. M. Hassanalian Classifications, applications and design challenges of drones: A review / M. Hassanalian, A. Abdelkefi // Progressin Aerospace Sciences. – 2017. – №91. – с. 99 -131.

2. Антени і пристрої НВЧ / Н. Т. Бова, Г. Б. Резніков. – 2-е вид., перероб. и доп. – К.: Вища школа, 1982. – 278 с.

3. Банков С. Е., Грибанов А. Н., Курушин А. А. Електродинамічне моделювання антенних та НВЧ структур з використанням ФЕКО. – К., One-Book, 2013. – 423 с.

УДК 621.37

*Дубина О. Ф., к.т.н., доцент,
Коваль Д. В., к.т.н.,
Латко І. І., здобувач*

Державний університет «Житомирська політехніка»

ШИРОКОДІАПАЗОННИЙ СИНТЕЗАТОР ЧАСТОТИ НА ADF4351

Сучасний радіоелектронний пристрій сьогодні часто має мікроконтролерне управління. Мікроконтролер, в свою чергу, діє за закладеною мікропрограмою (прошивкою). Тому програмне забезпечення мікроконтролера часто впливає на властивості, технічні параметри та функціонал радіоелектронного пристрою в цілому.

Яскравим представником сучасних широкодіапазонних гібридних синтезаторів частоти є ADF43515, рис. 1, що реалізований у вигляді інтегральної мікросхеми з 32 виводами. Діапазон робочих частот синтезатора – 35...4400 МГц.



Рис. 1. Синтезатор частоти ADF43515

Для зручності розробника ADF4351 розміщують на платі прототипування – модуль, що обладнаний необхідними інтерфейсними та високочастотним роз'ємами, задавальним кварцовим генератором, стабілізатором живлення.

Як пристрій керування для ADF4351 обґрунтовано вибір плати ArduinoUNO, оскільки програмо-апаратна платформа Arduino містить широкий набір електронних компонентів та пристроїв, що супроводжуються бібліотеками та прикладами програм їх використання. Пристрій керування виконує такі основні задачі:

1. Надання можливості обирати параметри сигналу через інтерфейс користувача.

2. Формування на основі параметрів сигналу коду керування синтезатором.

3. Передача сформованого коду синтезатору для отримання з його виходу сигналу з необхідними користувачу параметрами.

Вибір інтерфейсу користувача синтезатора полягає у виборі пристрою відображення параметрів сигналу, що генерується, а також пристрою введення користувачем необхідних параметрів сигналу. Серед пристроїв відображення (сегментний дисплей, графічний LCDдисплей, символнийLCDдисплей) виправдане використання символного LCD дисплею, враховуючи його сумісність з продуктами екосистеми Arduino – наявність програмних бібліотек, низьку вартість. Серед пристроїв введення (клавіатура, енкодер) обрано клавіатуру, що змонтована на одній платі з символним LCD дисплеєм.

Таким чином, структура синтезатора частоти на ADF4351 складена з плати прототипування, плати управління Arduino UNO, модуля інтерфейсу користувача на базі LCD дисплею з клавіатурою (LCD keypadshield), а також програмного забезпечення мікроконтролера плати Arduino UNO для керування синтезатором.

Параметри живлення плати прототипування ADF4351 дозволяють використати як джерело – плату ArduinoUno, що, в свою чергу має універсальний порт живлення 6-20 В, або 5 В через порт USB-A.

Експериментальні дослідження показали, що потужність на виході синтезатора частоти змінюється від 5 до 2 dBmв діапазоні 40...2700 МГц, що корелюється з теорією та демонструє можливість практичного використання створеного макету синтезатора, принаймні у дослідженому діапазоні частот.

Список використаних джерел

1. Фесіч В.П. Прямий цифровий синтез (DDS) в системах керування ультразвуковими резонансними приводами. – Київ: Вісник Національного технічного університету України "КПІ" Серія – Радіотехніка. Радіоапаратобудування. – 2012. – №48.

2. В. Макаренко, Б. Паращак. Універсальний широкосмуговий синтезатор частоти збудованим ГУН // Електронні компоненти системи: – 2009. – №4 – Київ: VD MAIS.

3.Mixed-signalanddigital signalprocessingICs | AnalogDevices. URL: <https://www.analog.com/media/en/technical-documentation/data-sheets/adf4351.pdf>.

УДК 621.37:621.391

*Опанасюк К. С., магістрант,
Ципоренко В. Г., к.т.н., доцент
Державний університет «Житомирська політехніка»*

СИСТЕМА ПОПЕРЕДЖЕННЯ ТЕХНОГЕННИХ АВАРІЙ

Актуальною задачею забезпечення контролю якості лікарської сировини впродовж усього її життєвого циклу є створення відповідних систем комплексного моніторингу мікроклімату. Існуючі системи моніторингу мікроклімату вирішують тільки локальні задачі контролю та регулювання на окремих етапах життєвого циклу лікарської сировини, а саме: вирощування або виробництва сировини, збору та попереднього її перероблення, підготовки до транспортування, транспортування та зберігання в складських приміщеннях перед остаточним переробленням, зберігання в торгових приміщеннях та на базах, доставки до споживача тощо.

Визначено, що вимірювання і регулювання мікрокліматичних показників на фармацевтичних підприємствах має кілька цілей:

- забезпечення оптимальних умов при розробці, виготовленні та зберіганні препаратів для імунізації;
- створення сприятливого середовища для життєдіяльності і роботи людей, дотримання вимог охорони праці;
- підтримання справної і ефективної роботи обладнання.

Показано, що основні вимоги до системи моніторингу лікарської сировини наступні:

- система моніторингу повинна забезпечувати необхідну точність вимірювання;
- система повинна бути гнучкою, здатною до нарощування і збільшення контрольованих параметрів;
- система повинна бути оснащена звуковою (світловою) сигналізацією;
- повинна бути система автоматичного архівування вимірних значень;
- отримані дані вимірювань повинні бути надійно захищені;
- можливість віддалених сигналізацій про порушення умов зберігання та контролю за вимірюваними параметрами.

Враховуючи сукупність особливостей вказаних вимог, запропонована мобільна розподілена система комплексного моніторингу лікарської сировини, що охоплює всі основні етапи її життєвого циклу. Одним з основних параметрів сучасних систем

телекомунікацій є наявність надійного та недорогого каналу зв'язку, що забезпечує технологія LoRa [1].

Дослідження показали, що технологія модуляції LoRa (LongRange) являє собою метод модуляції, який забезпечує велику дальність зв'язку (зону покриття), ніж інші конкуруючі з ним методи. Метод ґрунтується на технології модуляції з розширеним спектром і варіацією лінійної частотної модуляції (ChirpSpreadSpectrum, CSS) з інтегрованою прямою корекцією помилок (ForwardErrorCorrection, FEC).

Технологія LoRa дозволяє виконувати демодуляцію сигналів з рівнем на 19,5 дБ нижче рівня шумів, при тому, що для правильної демодуляції більшості системам з частотною маніпуляцією (FrequencyShiftKeying, FSK) необхідна потужність як мінімум на 8 –10 дБ вище рівня шумів [2].

Переваги технології LoRa: велика дальність роботи, низька ціна обладнання, низька потужність, стандартизація, велика ємність мережі.

Авторами запропоновано два варіанти топології системи моніторингу: кільцева та вузлова з можливістю програмного її трансформування. Перевагами запропонованої системи є: низька ціна обладнання, використання неліцензованого діапазону частот, низьке енергоспоживання, великий радіус дії та високі мобільність і швидкодія.

Виконано дослідження завадостійкості запропонованої системи і її вплив на дальність дії. Запропоновано цифровий алгоритм вагового оброблення LoRa-символів, що покращує достовірність прийому до 50%.

Показано, що при демодуляції сигналів LoRa використовується комбінована частотна та широтно-імпульсна багаторівнева маніпуляція, яку доцільно реалізовувати на основі цифрової адаптивної узгодженої фільтрації.

Запропонований алгоритм оброблення LoRa-символів забезпечує максимум співвідношення завадостійкість/швидкодія. Виконано імітаційне моделювання роботи системи та отримані характеристики її завадостійкості і швидкодії для різних режимів прийому.

Список використаних джерел

1. Laveyne J. Application of LoRaWAN for Smart Metering: An Experimental Verification / J. Laveyne, G. Van Eetvelde, L. Vandeveldel. // International Journal of Contemporary ENERGY. – 2018. – №1.
2. Wu Mengdi. Wireless communication technologies in Internet of Things (IOT) / Wu Mengdi. – University of Vaasa: Vaasa, 2016.

УДК 615.47

*Борисевич О. Р., магістрант,
Коломієць Р. О., к.т.н., доцент,
Манойлов В. П., д.т.н., професор
Державний університет «Житомирська політехніка»*

АНАЛІЗ МОЖЛИВОСТІ ПЕРЕДАЧІ МЕДИЧНИХ ДАНИХ ІСНУЮЧИМИ ПРОГРАМНО – АПАРАТНИМИ ЗАСОБИМИ

При організації передачі даних від медичного діагностичного обладнання виникає ряд технічних проблем, пов'язаних з високими вимогами, що пред'являються до якості передаваної інформації.

Ці проблеми можна розділити на три основні групи:

1. Проблема отримання діагностично адекватного зображення для подальшої діагностики, аналізу та зберігання.
2. Проблема спряження діагностичного обладнання із системами передачі інформації.
3. Проблема передачі отриманої інформації «віддаленим» користувачам.

Ключові слова: зображення, системи передачі інформації, аналіз і зберігання інформації.

Перша проблема пов'язана в першу чергу з психологією виховання спеціалістів – лікарями результатів отриманих від медичних діагностичних установ, тобто вони частіше всього не підготовлені до роботи з альтернативними варіантами надання медичної допомоги, такими як, наприклад, зображення на моніторі персонального комп'ютера. Зв'язок із цією інформацією, з якою передбачається працювати на персональних комп'ютерах, має бути наданий у «приватному» для спеціалістів вигляді.

Крім того, програма обробки інформації повинна бути простою у використанні та інтуїтивно зрозумілою, що дозволить скоротити час адаптації та забезпечити швидку можливість переходу до роботи з новими методами надання медичних даних [1, 2].

Друга проблема пов'язана з тим, що не існує єдиного стандарту формату надання та зберігання медичних даних. Фірми-розробники медичного обладнання базуються на власних стандартах, які закриті, часто несумісні з аналогічними системами інших фірм, і можуть змінюватися в подальших розробках і модифікаціях вже існуючого обладнання.

Попити стандартизації форматів зберігання та відображення медичних даних привели до виявлення кількох стандартів, найбільш

відомим з яких є DICOM3, але які всі загальні дані не отримані. Виходячи із всього вище сказаного, можна констатувати, що кожна медична діагностична установка вимагає індивідуального підходу для забезпечення можливості передачі інформації.

Також існує ряд проблем, що виникають при спробах забезпечення високої якості передачі медичної інформації, пов'язаних з тим, що сучасні програмно-апаратні засоби неспеціалізовані для передачі даних подібного роду. Це накладає певні вимоги до підбору обладнання для передачі інформації з медичної діагностичної апаратури на персональні електронно-обчислювальні машини.

Спеціалізованих (стандартних) програмних засобів, призначених для обробки медичної інформації (вироблених) на персональних електронно-обчислювальних машинах на даний момент практично не існує.

Використання програми загального призначення, для роботи з медичними даними, практично неможливо. Це пов'язано з тим, що потрібен високий рівень спеціальної підготовки спеціалістів – лікарів, і вимоги, що пред'являються до персональної електронно-обчислювальної машини, для встановлення програми такого класу, невиправдано високі, що практично неможливо через невиправдано високі матеріальні і часові витрати.

Третя проблема пов'язана з обмеженнями, накладеними на передану інформацію, сучасними засобами зв'язку. Медичні дані (зображення, звук, відео) неможливо передавати в «реальному часі» за сучасними каналами зв'язку, з тим якістю, яке потрібно для задовільної роботи спеціаліста.

Об'єми інформації вимагають розробки спеціальних алгоритмів згортання даних і вироблення нових методів передачі інформації.

Список використаних джерел

1. The transfer Approach for assessing the transferability of systematic review findings. [Електронний ресурс] Heather Munthe-Kaas, Heid Nokleby, Simon Lewin & Claire Glenton – 2020. – Режим доступу до ресурсу:

<https://bmcmedresmethodol.biomedcentral.com/articles/10.1186/s12874-019-0834-5>

2. European committee for standardization. Telemedicine in the United States: An Introduction for Students and Residents. [Електронний ресурс] Maryam A Hyder 1 Author OrcidImage; Junaid Razzak 2 Author Orcid Image. Режим доступу до ресурсу: <https://www.jmir.org/2020/11/e20839/>

УДК 621.396.6

*Чухов В. В., к.т.н., доцент,
Павицький О. Ю., магістрант
Державний університет «Житомирська політехніка»*

ДОСЛІДЖЕННЯ ЛОГОПЕРІОДИЧНОЇ АНТЕНИ З НЕСТАНДАРТНИМ КРОКОМ ВІБРАТОРІВ

Антенні у сучасному світі відіграють надзвичайно важливу роль у забезпеченні бездротового зв'язку, радіолокації, супутникового зв'язку та багатьох інших сферах. Вдосконалення їх характеристик та розширення смуги робочих частот стають актуальними завданнями для науковців і інженерів, які розробляють антени.

Логоперіодичні антени (ЛПА) стали об'єктом інтенсивних досліджень у зусиллях досягти більшої продуктивності та ефективності антенних систем. Однак залежно від конкретних завдань та потреб, може бути необхідним модифікувати їхню конфігурацію, включаючи зміну кроку вібраторів.

При збільшенні швидкості передачі даних по радіоканалу підвищуються вимоги до смуги пропускання антен. Звідси важлива вимога, що висувається до антен – це сталість електричних характеристик у заданій смузі частот, що може досягатися за рахунок застосування частотно-незалежних антен. Антена з логарифмічною періодичною структурою найчастіше реалізована як антенна решітка, що складається з паралельних вібраторів, підключених до двопровідної лінії живлення з переполусовкою точок живлення вібраторів (рис. 1). ЛПА працюють у діапазонах декаметрових, метрових, дециметрових і навіть у сантиметрових діапазонах хвиль.

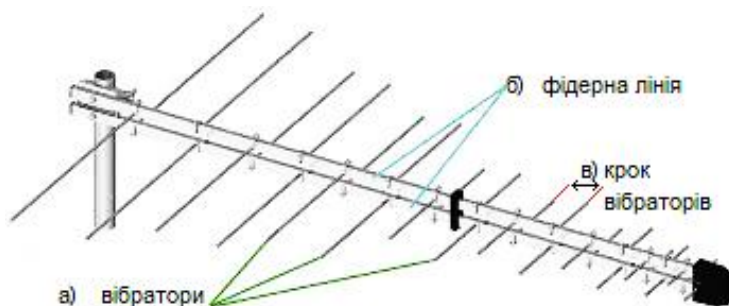


Рис. 1. Будова логоперіодичної антени

Кожен тип антен має свої технічні показники, у тому числі вони є в логоперіодичних антен. Такі характеристики як коефіцієнт стоячої хвилі (КСХ), смуга пропускання, резонансна частота визначаються формою та розмірами вібратора та іншими елементами антени [1, 2]. Таким чином, можна вважати, що вібратор є головною частиною дротової антени.

У результаті дослідження, потенційно очікується, що зміна кроку мультивібратора, (відстані між сусідніми вібраторами, рис. 1, в) у логоперіодичній антені впливатиме на її характеристики у різних аспектах. Зокрема, передбачається розширення смуги пропускання антени, що може бути корисним у випадках, де необхідна широкосмуговість. Зміна кроку також може змінювати діаграму напрямленості антени, зробивши її ширше або вужчою залежно від конкретних параметрів та конфігурації антени. Зміни у параметрах вібратора можуть зробити антену більш або менш чутливою до поляризації сигналу. Регулювання кроку дозволяє досягти більших значень амплітудного та фазового діапазонів, що є важливим для деяких застосувань, зокрема в антенних решітках. Зміна кроку може вплинути на фізичні розміри антени, що важливо у випадках обмеженого простору для її розміщення.

Вплив зміни кроку мультивібратора на антену визначатиметься конкретною геометрією та конфігурацією логоперіодичної антени, а також конкретними параметрами системи, в якій вона використовується.

Моделювання цих ефектів за допомогою програм для аналізу антен може надати докладніші відомості щодо конкретного впливу на параметри інтересів.

У сучасних умовах результати досліджень можуть бути використані для поліпшення функціональності існуючих та розроблених засобів зв'язку. Особливо це актуально в областях, де важлива простота конструкції, замість використання масивної площини зі збереженням апертури антени, наприклад, у переносних чи літальних апаратах.

Список використаних джерел

1. Constantine A. Balanis. Antenna Theory: Analysis and Design / Constantine A. Balanis., 2005.
2. Mailloux R. J. Phased Array Antenna Handbook. Artech House / Mailloux R. J., 2005.
3. Log-periodic antenna [Електронний ресурс] – Режим доступу до ресурсу: https://www.wikiwand.com/en/Log-periodic_antenna

УДК 004.021.7:614.2:005.8

*Свінцицька О. М., к.е.н., доцент,
Мяновська М. В., магістрант*

Державний університет «Житомирська політехніка»

РОЛЬ СТРАТЕГІЙ УПРАВЛІННЯ РИЗИКАМИ В ЗАБЕЗПЕЧЕННІ УСПІХУ ПРОЕКТІВ В ГАЛУЗІ ТЕЛЕМЕДИЦИНИ

У сучасному світі інформаційні технології швидко розвиваються і змінюють різні аспекти нашого життя. Телемедицина, використовуючи ці технології та Інтернет, революціонізує надання медичної допомоги та консультацій на відстані. Проекти в сфері телемедицини є вкрай важливими, але вимагають специфічного підходу до управління ризиками для забезпечення їх успішного впровадження.

Для забезпечення успішності проектів у сфері телемедицини потрібна висока увага і обережність, оскільки ця галузь об'єднує два важливі аспекти: медицину та інформаційні технології. Реалізація таких проектів супроводжується значною технічною складністю та великими ризиками, пов'язаними з якістю медичних послуг та безпекою пацієнтів.

Ризики у проектах телемедицини можуть виникати з різноманітних джерел, такі як дефекти в програмному забезпеченні та обладнанні, а також кібербезпекові загрози, що ставлять під загрозу конфіденційність пацієнтських даних. Додатково важливі фактори включають законодавчі обмеження, вимоги до якості медичних послуг і інші аспекти, які роблять проекти телемедицини складними та вразливими перед різними видами ризиків. Це підкреслює необхідність уважного управління ризиками у проектах телемедицини, оскільки можливі неуспіхи чи негативні наслідки можуть серйозно вплинути на пацієнтів та медичні організації. І тут ключову роль відіграють стратегії управління ризиками. Адже правильно розроблені та застосовані стратегії дозволяють досягти кількох важливих цілей:

1. Покращення планування. Ретельне і детальне планування підвищує ймовірність успіху інших процесів управління ризиками [1].

2. Зменшення фінансових витрат: Ефективне управління ризиками дозволяє уникнути недоцільних витрат і зберегти грошові ресурси для інших важливих аспектів проекту.

3. Підвищення якості та точності проекту: Зменшення ризиків сприяє покращенню якості медичних послуг та точності діагностики, що є ключовим для задоволеності пацієнтів та репутації проекту в галузі телемедицини.

4. Зменшення втрат часу: Своєчасне реагування на потенційні проблеми допомагає уникнути непередбачуваних затримок та мінімізує втрати часу, що може призвести до серйозних фінансових та графічних ускладнень.

Після розуміння важливості управління ризиками слід навести кілька конкретних стратегій управління ризиками, які можуть бути застосовані в телемедицині для їх успішного впровадження:

1. Проведення всебічного аналізу та оцінки ризиків ще до початку реалізації проекту, що включає дослідження можливих технічних проблем, аналіз кібербезпекових загроз, визначення вимог до якості медичних послуг та урахування законодавчих обмежень. Такий підхід сприяє розробці ефективного плану управління ризиками ще на етапі старту проекту.

2. Створення докладного реєстру ризиків, в якому вказані всі identified ризики, їх характеристики та можливі наслідки. Регулярне оновлення цього реєстру дозволяє ефективно виявляти нові ризики та вчасно реагувати на зміни.

3. Регулярне оновлення та вдосконалення програмного забезпечення та обладнання для усунення можливих технічних неполадок та врахування нових вимог до якості послуг.

4. Укладання страхових полісів для покриття можливих фінансових збитків, пов'язаних з ризиками в проекті. Це може включати страхування від кіберзагроз, технічних збоїв та інших негараздів.

5. Запровадження системи постійного моніторингу та оновлення стратегій управління ризиками відповідно до змін у технологічному та регуляторному середовищі.

Шлях до успішної імплементації телемедицинських проектів вимагає глибокого розуміння ризиків та виважених стратегій для їх подолання. Отже, управління ризиками та використання різноманітних механізмів, звичайно, не гарантує 100% успіху [2]. З огляду на складність та важливість таких ініціатив, правильне управління ризиками стає невід'ємною складовою їх успішної реалізації.

Список використаних джерел

1. Скопенко Н.С., Євсєєв І.В., Москаленко В.О. Управління ризиками в проектному менеджменті. Інвестиції: практика і досвід. – 2013. – №24. – с. 41 – 42.

2. Журан О. А. Управління ризиками в ІТ-проектах / О. А. Журан, М. Г. Глава // Project Program, Portfolio p3 Management : перша Міжнарод. наук.-практ. конф. : тези доп., м. Одеса, 16-17 груд. 2016 р. / Одес. нац. політехн. ун-т. – Одеса, 2016. – Т. 2. – с. 46-48.

621.396.6

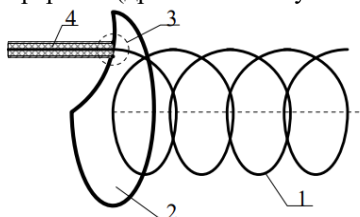
**Чухов В. В., к.т.н., доцент,
Ожегов І. Є., магістрант**

Державний університет «Житомирська політехніка»

ДОСЛІДЖЕННЯ СПІРАЛЬНОЇ АНТЕНИ ДЛЯ ПОПЕРЕЧНОГО ВИПРОМІНЮВАННЯ

Спіральні антени, як важливий елемент частотно-незалежних антен, привертають увагу науковців та інженерів завдяки своїй здатності працювати в широкому діапазоні частот зі стабільними характеристиками випромінювання та поляризації.

За конструктивними особливостями спіральні антени поділяються на декілька груп: еліптичні, циліндричні (рис. 1), конічні, плоскі (рис.2), комбіновані структури, антени з провідника з постійним або змінним поперечним перерізом (дротова або смужкова структура).



1 – спіраль; 2 – екран; 3 – точка підключення до лінії живлення; 4 – коаксіал.

Рис. 1. Будова циліндричної спіральної антени

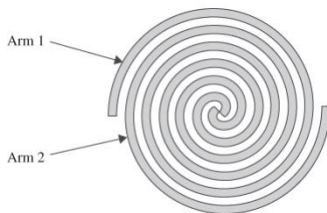


Рис. 2. Приклад плоскої спіральної антени

Геометрія цих антен визначається габаритами основи спіралі, що може мати поперечний переріз у вигляді еліпса або кола. В залежності від співвідношення піввісей еліпса спіральні антени можуть мати різні форми – від циліндричних до плоских. Крім того, спіральні антени можуть бути однозахідні, багатозахідні або складатися в антенні решітки.

Головними перевагами спіральних антен є:

- можливість створення поля випромінювання з поляризацією відлінійної до кругової;
- можливість забезпечити необхідні характеристики випромінювання і вхідні характеристики антени за рахунок зміни геометричних параметрів спіралі;
- простота і надійність конструкції;
- відносно невеликі габаритні розміри антени;
- на основі циліндричних, конічних, напівсферичних спіральних антен можуть бути виконані комбіновані структури (сфероциліндричні, циліндроконічні і т.д.);
- можливість без використання великих екранів забезпечити відносно низький рівень бічного і заднього випромінювання (менше $-15 \dots -10$ дБ в робочому діапазоні частот);
- можливість хорошого узгодження з живильним фідером в широкій смузі частот.

Важливим аспектом дослідження спіральних антен є аналіз поздовжнього та поперечного випромінювання, які визначають напрямкові характеристики антени та ефективність випромінюваного поля. Поздовжнє випромінювання, що випромінюється вздовж осі спіралі, та поперечне випромінювання, що розповсюджується перпендикулярно до осі, визначаються геометричними параметрами спіральної структури та її фізичними властивостями.

У межах цієї роботи буде виконано детальний аналіз впливу геометричних параметрів спіральних антен на поперечне випромінювання. За допомогою комп'ютерного моделювання у MATLAB будуть створені моделі антен з різними кількостями оборотів та різним кроком спіралі. Далі ці моделі будуть використані для аналізу радіаційних патернів і поляризації, що дозволить визначити оптимальні параметри для різних застосувань.

Експериментальна частина включатиме виготовлення антенних прототипів та їхнє тестування, щоб порівняти отримані дані з результатами симуляції. Це дасть можливість визначити найефективніші конструкції для практичного використання.

Список використаних джерел

1. Luo Q., Gao S., Zhu F. Circularly Polarized Antennas. Wiley & Sons, Incorporated, John, 2013.
2. Balanis C. A. Antenna Theory: Analysis and Design. Wiley & Sons, Incorporated, John, 2016.

УДК 621.3: 455.63

Макарик Ю. С., магістрант

Державний університет «Житомирська політехніка»

ДОСЛІДЖЕННЯ МОЖЛИВОСТІ ЗАСТОСУВАННЯ РАДІОМОДУЛІВ NRF24L01 У СЕНСОРНІЙ МЕРЕЖІ

Сенсорна мережа – це інтегрована система розподілених сенсорних вузлів, що взаємодіють між собою та іншими мережами для ефективного обміну запитаннями, обробки, передачі та представлення інформації, отриманої від об'єктів реального фізичного світу.

Мета цієї системи полягає в тому, щоб систематизувати інформацію та реагувати на неї з врахуванням контексту. Структурно, сенсорна мережа включає в себе не лише сенсори, актуатори, і комунікаційні вузли, але й встановлює зв'язок з іншими мережами для комплексного аналізу та обробки даних.

Основне призначення сенсорної мережі полягає в контролі та моніторингу параметрів фізичних середовищ та об'єктів, а також у випадках потреби – управлінні ними.

Зона покриття сенсорної мережі може розширюватися від кількох метрів до кількох кілометрів завдяки вмінню передавати повідомлення від одного вузла до іншого через інтерфейс сусідніх вузлів, що забезпечує оптимальний маршрут для руху інформаційних потоків.

Однією з унікальних характеристик сенсорних мереж є їх здатність ретранслювати повідомлення ланцюжком від одного вузла до іншого. Це дозволяє забезпечити передачу інформації через сусідні вузли у разі виходу з ладу одного з елементів мережі, зберігаючи високу якість передачі даних.

Зв'язок в сенсорних мережах, зазвичай, реалізується за допомогою бездротових технологій, таких як радіо, інфрачервоне випромінювання або оптичні сигнали. Однак основним обмеженням такого зв'язку є вимога прямої видимості між відправником та отримувачем.

Максимальна відстань взаємодії між вузлами бездротової системи залежить від ряду факторів, включаючи робочу частоту, вихідну потужність передавача, характеристики антен, чутливість приймача, а також перешкоди, переміщення об'єктів і навіть атмосферні умови. Безумовно, важливим аспектом створення бездротових систем є вибір частотного діапазону.

Використання смуг частот ISM (промислові, наукові та медичні цілі) є одним з популярних варіантів радіозв'язку, оскільки вони

доступні без ліцензій у більшості країн і дозволяють впровадження енергозберігаючих стратегій у сенсорних мережах.

У конкретній роботі розглядається можливість застосування радіомодулів nRF24L01, рис. 1, для створення бездротової сенсорної мережі. Зазначений модуль має 125 частотних каналів у діапазоні ISM від 2,4 ГГц до 2,525 ГГц з кроком 1 МГц. Один канал може обслуговувати одночасну роботу 7 пристроїв (1 приймач і 6 передавачів) з різними адресами.



Рис. 1. Вигляд радіомодулів nRF24L01

Модуль використовує передавач із GFSK модуляцією та максимальною вихідною потужністю 0 дБм, а також антену із коефіцієнтом підсилення 2 дБм, що забезпечує зв'язок на відстань до 100 метрів при чутливості приймача -82 дБм.

Модуль підключається до мікроконтролера сенсорного вузла за допомогою інтерфейсу SPI, забезпечуючи максимальну швидкість передачі до 2 Мбіт/с. Використання послідовного периферійного інтерфейсу (SPI) дозволяє синхронний обмін даними між мікроконтролером та підключеними пристроями.

У цілому, функціональні можливості радіомодуля NRF24L01 дозволяють ефективно організовувати бездротову сенсорну мережу без потреби в Інтернет-підключенні, забезпечуючи надійний обмін даними між різними вузлами мережі.

Список використаних джерел

1. Dargie W.; Poellabauer C. Fundamentals of wireless sensor networks: theory and practice. John Wiley and Sons. 2010. pp. 168–183, 191–192.
2. Ullo Silvia Liberata; Sinha G. R. Advances in Smart Environment Monitoring Systems Using IoT and Sensors. Інтернет ресурс: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7309034/>
3. nRF24L01+ - Single Chip 2.4GHz Transceiver. Інтернет ресурс: https://www.sparkfun.com/datasheets/Components/SMD/nRF24L01Pluss_Preliminary_Product_Specification_v1_0.pdf

УДК 621.3: 455.63

Грищенко Н. О., ст. викладач

Державний університет «Житомирська політехніка»

ВИМІРЮВАННЯ ТЕМПЕРАТУРИ З ВИКОРИСТАННЯМ УЛЬТРАЗВУКОВОГО ДАТЧИКА ВИМІРУ ВІДСТАНІ HC-SR04

У сучасному науковому світі фізика займає одне із провідних місць та урізноманітнює методи вимірювання величин. Наприклад, для вимірювання температури існують такі методи: об'ємний, манометричний, терморезисторний (метод термоопору), термоелектричний, пірометричний та ультразвуковий.

Ультразвук – пружні звукові коливання високої частоти. Людське вухо сприймає поширюються в середовищі пружні хвилі частотою приблизно до 16-20 кГц; коливання з більш високою частотою є ультразвук (за межею чутності). Зазвичай ультразвуковим діапазоном вважають смугу частот від 20000 до мільярда Гц. Звукові коливання з більш високою частотою називають гіперзвуком. У рідинах і твердих тілах звукові коливання можуть досягати 1000 ГГц. Поняття «ультразвук» придбало в даний час більш широкий зміст, ніж просто позначення високочастотної частини спектра акустичних хвиль. З ним пов'язані цілі області сучасної фізики, промислової технології, інформаційної та вимірювальної техніки, медицини та біології.

Випромінювачі ультразвуку можна поділити на дві великі групи. До першої відносяться випромінювачі-генератори; коливання у них збуджуються через наявність перешкод на шляху постійного потоку – струменя газу або рідини. Друга група випромінювачів – електроакустичні перетворювачі, вони перетворюють вже задані коливання електричної напруги або струму в механічне коливання твердого тіла, яке і випромінює в навколишнє середовище акустичні хвилі. Широке поширення ультразвукових методів обумовлено появою нових надійних засобів випромінювання та прийому акустичних хвиль, з одного боку, забезпечили можливість істотного підвищення випромінюваної ультразвукової потужності та збільшення чутливості при прийомі слабких сигналів, а з іншого – дозволили просунути верхню межу діапазону випромінюваних і прийнятих хвиль в область гіперзвукових частот.

Ультразвуковий датчик HC-SR04 може бути використаний для вимірювання відстані між датчиком і до перешкоди, в діапазоні від 2 до 400 см, причому межа точності може досягати до 3 мм. Модуль включає ультразвуковий передавач, приймач і вузол контролю. На

покази датчика практично не впливають сонячне випромінювання і електромагнітні шуми. При використанні ультразвукового датчика для вимірювання температури, необхідно врахувати вплив температури на швидкість поширення ультразвукових хвиль. Для компенсації впливу температури необхідно провести калібрування ультразвукового датчика з використанням відомих значень температури та відстані. Вимірювання температури з використанням ультразвукового датчика може бути корисним для вимірювання температури у важкодоступних місцях або у випадках, коли інші методи вимірювання недоступні. При використанні ультразвукового датчика для вимірювання температури, необхідно враховувати його обмежену точність і можливість помилки, пов'язані з шумом вимірювання та іншими факторами.

Також точність датчика залежить ще від декількох факторів:

- Температури і вологості повітря;
- Відстані від об'єкта;
- Розташування щодо датчика;
- Якості виконання елементів модуля датчика.

В основу принципу дії будь-якого ультразвукового датчика закладено явище відображення акустичних хвиль, що поширюються в повітрі. Як відомо, швидкість поширення звуку в повітрі залежить від властивостей цього самого повітря.

Датчики, випускаючи хвилі і заміряючи час до їх повернення, не знають, в якому саме середовищі вони будуть поширюватися і використовують для розрахунків середню величину. Саме через ці фактори в реальних умовах датчик HC-SR04, може давати недостовірну інформацію. Саме цей метод вимірювання температури не є самим простим та ефективним, але входить у різновид. Ультразвуковий метод вимірювання температури може бути додатковим засобом контролю, але необхідно провести додаткові дослідження для підтвердження його точності та надійності.

Список використаних джерел

1. Зорко Є.В. Метод підвищення точності перетворювачів для ультразвукової діагностики / Є.В. Зорко, Т.Р. Клочко // Погляд у майбутнє приладобудування: 11 Всеукраїнська науково-практична конференція студентів та аспірантів, м. Київ, 15 – 16 травня 2018 р. – НТУУ «КПІ». – 2018. – с. 344 –347.

2. М. Гоцацюк, Нейт Сілвер. Сигнал і шум. Чому більшість прогнозів виявляються хибними. 2018 р. – с. 544.

3. В. Д. Дідух, Ю. А. Рудяк, О. А. Багрій-Заяць Біологічна фізика з фізичними методами аналізу. Навчальний посібник. / Тернопіль 2021 р. – с. 305.

УДК 621.3:455.63

Кушнірук В. Л., магістрант

Державний університет «Житомирська політехніка»

ДОСЛІДЖЕННЯ ДИСТАНЦІЙНОЇ СИСТЕМИ МОНІТОРИНГУ ЯКОСТІ ПОВІТРЯ У ПРИМІЩЕННІ

Розвиток науки та техніки, а також зростання обсягів промислового виробництва призвели до збільшення рівня забруднення навколишнього середовища, зокрема атмосферного повітря, що негативно впливає на здоров'я людей. Тому в сучасному світі велика увага приділяється контролю за якістю повітря. Один із ключових аспектів впливу на здоров'я студентів у навчальних закладах полягає в дотриманні санітарно-гігієнічних стандартів мікроклімату, таких як температура, вологість повітря, концентрація вуглекислого газу та рівень легких аероіонів.

Підвищення температури призводить до значного збільшення виливання поту, що призводить до стрімкого порушення водно-сольового обміну та зміни інших параметрів крові. Це може викликати згущення крові, збільшення частоти пульсу та артеріального тиску. Висока температура негативно впливає особливо при підвищеній вологості, оскільки це обмежує тепловіддачу від тіла людини і викликає зміни в обміні речовин, роботі серцево-судинної та дихальної систем, а також впливає на центральну та периферійну нервову системи. Подібні фізіологічні зміни відбуваються й при впливі низьких температур, які викликають звуження судин м'язів та шкіри, зменшення пульсу та збільшення об'єму дихання і споживання кисню. Усі ці зміни впливають на працездатність, концентрацію уваги, сприйняття інформації та можуть призвести до захворювань.

Система дистанційного моніторингу стану повітря у приміщенні може бути ефективно побудована за допомогою технології Інтернету речей (IoT). Для забезпечення взаємодії між Інтернет-речами та користувачем, цілеспрямовано можна використовувати сервер із застосуванням посередницької платформи даних. Ця платформа здійснюватиме наступні функції:

- Прийом повідомлень від Інтернет-речей та їх передача користувачам: сервер отримує дані від датчиків, які спостерігає за станом повітря в приміщенні, і передає цю інформацію користувачам через визначений інтерфейс.

- Зберігання прийнятої інформації та обробка: Отримані дані зберігаються на сервері, що дозволяє їх подальшу обробку. Це може

включати аналіз та візуалізацію даних, виявлення аномалій чи змін в показниках повітря.

- Забезпечення інтерфейсу користувача: Посередницька платформа також надає інтерфейс, який дозволяє користувачам взаємодіяти з системою. Це може включати перегляд поточних показників, отримання сповіщень про стан повітря та виконання дій для покращення якості повітря в приміщенні.

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

У роботі проводяться дослідження точності вимірів температури та вологості повітря у приміщенні, а також концентрації вуглецево-водневих сполук. Відображення результатів здійснюватиметься за допомогою веб ресурсу «thingspeak», а також передбачається віддалена передача даних на сервер в форматі HTML в режимі реального часу. Для роботи Інтернет-речей, які можуть збирати різну інформацію та поширювати її по комунікаційних мережах, використовуються недорогі модулі Wi-Fi – ESP32 та ESP8266, та датчики DHT11 та MQ-2. Збирання даних від датчиків та передавання контрольованих параметрів на сервер запропоновано здійснювати через пристрій-шлюз на базі мікроконтролера ESP8266, який надає точку доступу до мережі Інтернет.

Під час дослідження дистанційної системи моніторингу якості повітря у приміщенні, будуть використані обрахунки та аналізи температури, вологості, концентрації CO₂, яка буде визначатися у значеннях ppm. Наводяться результати розрахунку температури, вологості та середньої концентрації окремих забруднюючих речовин за певний період часу у різних приміщеннях.

Список використаних джерел

1. Мікроклімат виробничих приміщень та його вплив на організм працівника. [Електронна публікація]. Режим доступу – <https://oppb.com.ua/news/mikroklimat-vyrobnychyh-prymishchen-ta-yogo-vplyv-na-organizm-pracivnyka>

2. CO₂ у приміщеннях. На що впливає діоксид вуглецю у повітрі та як зменшити його рівень. [Електронна публікація]. Режим доступу – <https://aerostar.ua/ua/news/novosti/co2-u-primischennjah-na-scho-vplivae-dioksid-vuglecju-u-povitri-ta-jak-zmenschiti-jogo-riven.html>

3. Carbon Monoxide Levels Chart. [Електронна публікація]. Режим доступу – <https://www.co2meter.com/blogs/news/carbon-monoxide-levels-chart>

УДК 681.5.08

*Вознюк С. І., магістрант,
Коренівська О. Л., ктн, доцент
Державний університет «Житомирська політехніка»*

СИСТЕМА ДИСТАНЦІЙНОГО КЕРУВАННЯ МІКРОКЛІМАТОМ

Приміщення відіграє важливу роль в житті людини. Його особливістю є не лише здатність стабілізувати умови в середині, на відміну від зовнішнього середовища, де погода змінюється щогодини, але й можливість ефективно стабілізувати такі фізичні параметри, як:

- ✓ температура повітря у приміщенні;
- ✓ вологість повітря у приміщенні;
- ✓ атмосферний тиск;
- ✓ концентрація вуглекислого газу у повітрі;
- ✓ концентрація озону у приміщенні.

Мікроклімат – це поєднання фізичних параметрів, які впливають на обмін теплової енергії людини з навколишнім її середовищем. Необхідність отримання інформації про поточний стан мікроклімату будівлі виникає при контролі умов праці, виробництва та зберігання продукції в приміщеннях.

В нас час, розвиток зробив великий крок вперед, тому традиційний підхід до моніторингу кліматичних параметрів стає неефективним, а враховуючи низьке споживання енергії сучасних автономних систем, ще й економічно не вигідним. Набагато вигідніше побудувати систему, яка зможе в режимі реального часу швидко реагувати на зміну показників, ніж витратити власні сили та час, щоб самостійно контролювати та регулювати ці показники. До того ж ручний моніторинг не позбавлений впливу людського фактору.

Для автоматизації мікроклімату в приміщенні, необхідно побудувати систему, що дозволить не просто визначати основні параметри повітря, але й регулювати ці показники для підтримання комфортних умов проживання, праці, а також підтримці справності певного обладнання та зберігання певних видів продуктів. Узагальнюючи дані нормативних документів можна зробити висновки по параметрам мікроклімату в приміщеннях різного типу:

- температура повітря у навчальних кабінетах, лабораторіях, аудиторіях повинна бути 18-20 °С; 20 – 23 °С для житлових кімнат,
- вологість повітря – 40 – 60%;
- концентрація вуглекислого газу – 400 – 600 ppm;

Наразі актуальність даної системи важко оцінити, бо вони можуть застосовуватися в багатьох сферах таких як:

- ✓ освіта;
- ✓ медицина
- ✓ виробництво;
- ✓ сфера послуг;
- ✓ аграрна промисловість.

Технічна реалізація системи складається з трьох основних складових, таких як:

- система збору інформації, яка складається з сенсорів параметрів мікроклімату, систему збору, первинної обробки інформації з датчиків, засобу бездротової передачі інформації на центральний сервер;

- система порівняння реальних показників з встановленими нормами. Керуючим елементом в системі виступає мікроконтролер, який зчитує показники з датчиків, обробляє та, при необхідності, вмикає відповідні прилади, а також передає дані користувачеві.

- системи керування параметрами мікроклімату, для можливості автоматичного регулювання параметрів мікроклімату, що складається з приладів, що здатні впливати на показники, та повертати їх до норми.

Керування та налаштування здійснюється безпроводним шляхом. Для цього використовується технологія Wi-Fi. Це дозволяє легко та ефективно ввести пристрій в експлуатацію.

Характеристики Wi-Fi стандарту IEEE 802.11n:

- Частота передачі в діапазонах 2.4 і 5 ГГц;
- Максимальна швидкість передачі 600 Мб/с;
- Швидкість передачі 100 Мб/с;
- Пропускна здатність 20/40 МГц;
- Дальність дії 75 м.

Список використаних джерел

1. Питання дистанційного керування мікрокліматом закритих приміщень. [Електронна публікація]. Режим доступу – <https://conf.ztu.edu.ua/wp-content/uploads/2023/02/257.pdf>

2. Про затвердження Державних санітарних правил та норм «Підприємства вугільної промисловості». [Електронна публікація] https://ips.ligazakon.net/document/view/reg7819?an=1291&ed=2002_1213

3. Методи реалізації програмно-апаратного комплексу, для керування параметрами мікроклімату. [Електронна публікація]. Режим доступу – <https://academconf.com/article/194>

УДК 528.8

*Долматова М. С., магістрант,
Горелик С. І., к.т.н., доцент
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»*

ВИКОРИСТАННЯ ДАНИХ ДЗЗ ДЛЯ АНАЛІЗУ ШТОРМОВИХ НАГОНІВ

Дистанційне зондування є ефективним інструментом для вивчення та моніторингу штормових нагонів. Воно дозволяє отримувати інформацію про різні параметри атмосфери та поверхні Землі, що є корисним для прогнозування та вивчення таких непогодних явищ.

Одним із основних методів дистанційного зондування є використання супутникових даних. Метеорологічні супутники спостерігають за атмосферою Землі, збираючи інформацію про характеристики хмар, температуру, вологість і тиск. Ці дані дозволяють фахівцям прогнозувати інтенсивність та рух штормових нагонів.

Ще одним корисним інструментом дистанційного зондування є системи радіолокації. Вони дозволяють виміряти висоту морської поверхні з високою точністю та деталізацією. Це дозволяє відстежувати зміни рівня моря, включаючи припливи та штормові нагони, які можуть бути пов'язані з сильними вітрами та повеннями. За допомогою даного методу було побудовано геоінформаційну модель поверхні води на Землі (рис.1). [1]

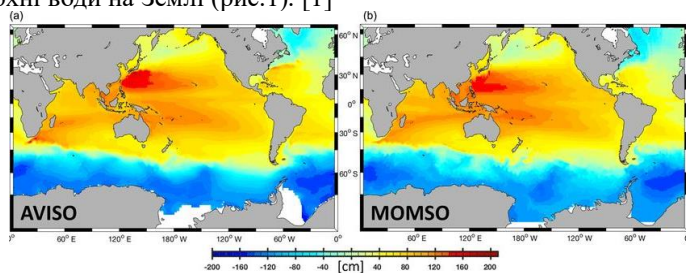


Рис. 1. Середня кліматологічна висота поверхні моря (в см)

Штормовий нагін води – це нетипове підняття рівня моря, викликане сильними вітрами та низьким тиском, внаслідок шторму, що виштовхує воду у бік суші. Штормові нагони зазвичай вважаються найбільш руйнівними подіями під час ураганів, і особливо дорого обходяться, якщо вони трапляються у густонаселених містах.

Використання даних ДЗЗ може бути дуже цінним при оцінці потенційних загроз, пов'язаних із штормовими нагонами, та визначенні вразливих областей. Такі дані дозволяють виявляти та моніторити штормові нагони на великих територіях. За допомогою супутників та інших дистанційних засобів можна отримати оглядову інформацію про масштаб та інтенсивність штормів, а також їх просторовий розподіл.

Використовуючи дані ДЗЗ у поєднанні з іншими метеорологічними даними, можна розробити моделі та прогнози штормових нагонів. Це дозволяє оцінити потенційні загрози і попередити населення про наближення штормів.

Аналіз даних ДЗЗ дозволяє виявити вразливі області, схильні до штормових нагонів. Наприклад, аналіз висоти затоплення та зміни морського рівня за допомогою даних ДЗЗ може допомогти визначити прибережні райони, які найбільш схильні до повеней (рис.2).

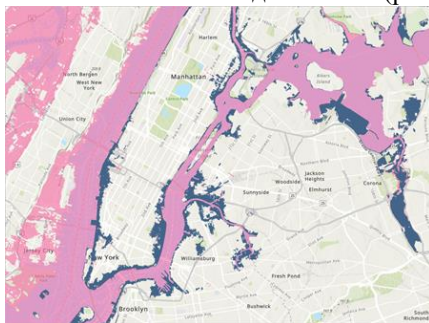


Рис. 2. Аналіз даних ДЗЗ для виявлення загроз на прибережній території під час штормових нагонів

Знаючи, яку загрозу несуть штормові нагони, можна готуватись до них заздалегідь. Розробляти та оптимізувати плани захисних заходів та евакуації. Це дозволяє мінімізувати потенційні збитки як матеріальні, так і людські втрати.

Загалом використання даних ДЗЗ в аналізі штормових нагонів дає можливість більш точної оцінки потенційних загроз та сприяє розробці ефективних стратегій управління та запобігання негативним наслідкам штормових подій.

Список використаних джерел

1. MOMSO 1.0 – an eddying Southern Ocean model configuration – Heiner Dietze, Ulrike Lötjen, and Julia Getzlaff – 27 с.
2. Storm surgemap URL: <https://learn.arcgis.com/en/projects/map-hurricane-storm-surges/>

УДК 347.426.3+528.8

*Стародубцева В. В., магістрант,
Горелик С. І., к.т.н., доцент
Національний аерокосмічний університет ім. М. С. Жуковського
«Харківський авіаційний інститут»*

ЗБИТКИ ВІД ВІЙСЬКОВОЇ ДІЯЛЬНОСТІ ЛІСГОСПАМ ХАРКІВСЬКОЇ ОБЛАСТІ ЗА ДАНИМИ ДЗЗ

Лісовий фонд є важливою складовою природного та економічного потенціалу регіонів, проте військова діяльність може значною мірою вплинути на стан та ефективність лісгосподарського сектору. Дослідження розглядає проблему збитків, завданих лісам Харківської області під час воєнних конфліктів, зокрема визначаючи розмір та характер зруйнувань за допомогою супутникових знімків. За останні роки, в умовах нестабільної ситуації в регіоні, розуміння впливу військових дій на лісові ресурси набуває великої актуальності для розробки стратегій відновлення та збереження екосистеми. Цей дослід спрямований на використання сучасних технологій супутникового моніторингу для об'єктивного визначення масштабів збитків та розробки ефективних заходів з відновлення лісового фонду Харківської області.

Таблиця 1

Площа лісів, які опинилися в зоні військових дій та на тимчасово окупованій території Харківської області, га, тис. м.

ХАРКІВСЬКА ОБЛАСТЬ	126906,1	31924,96
ДП "Жовтневий лісгосп"	4317,1	1026,26
ДП "Балаклійський лісгосп"	10132	2073,43
ДП "Вовчанський лісгосп"	26053,7	7237,45
ДП "Куп'янський лісгосп"	30975	7179,9
ДП "Гусятинський лісгосп"	110,4	31,07
ДП "Ізюмський лісгосп"	29386	7354,52
ДП "Харківська лісова науково-дослідна станція"	9792,5	2426,76
ДП "Чугуєво-Бабчанський лісгосп"	16139,4	4595,57

Важливим аспектом аналізу є визначення впливу військової діяльності на різноманіття видів, густоту лісового покриву. Переважаючі форми збитків можуть включати в себе загибель дерев, втрату придатності для лісового господарства та зміни в якості ґрунтового покриву. Аналіз таких аспектів дозволить визначити екологічні та економічні наслідки військових конфліктів для лісового сектору. Супутникові знімки відіграють важливу роль у дослідженні цих аспектів. Технології обробки та аналізу супутникових даних надають можливість деталізовано вивчати зміни у лісовому покриві, визначати розміри та розподіл зруйнувань.



Рис. 1. Супутникові знімки лісів Харківської області

Для виконання дослідження збитків від військової діяльності лісгосподарствам Харківської області застосовано комплексний методологічний підхід. Перший етап включає в себе вибір та обробку супутникових знімків, з їх подальшим аналізом. Для цього обрані відомі супутникові платформи з високою роздільною здатністю, що дозволяє детально вивчати лісові території та виявляти можливі пошкодження.

Другий етап включає в себе розробку методології для оцінки збитків, враховуючи різноманітність можливих ефектів від військових подій на лісові екосистеми. Зазначена методологія враховує параметри, такі як ступінь лісового покриття, густина деревостану, та інші фактори, що визначають стан лісових ресурсів.

На третьому етапі виконується аналіз супутникових знімків під час військових подій. Основна увага спрямована на виявлення зон збитків та пошкоджень, а також на класифікацію цих збитків за типами та обсягами. Використання сучасних технологій аналізу даних дозволяє здійснити точну ідентифікацію пошкоджених ділянок.

Четвертий етап включає в себе кількісну оцінку збитків, враховуючи розміри областей з пошкодженнями та види втрат, які вони завдали лісовим ресурсам. Результати цього етапу нададуть унікальний інформаційний матеріал для подальшого вивчення та аналізу. Застосована методологія, дозволить об'єктивно визначити масштаби та ступінь впливу військових конфліктів на лісові ресурси Харківської області.

Список використаних джерел

1. Аналіз площ ПЗФ в Україні в розрізі адміністративно-територіальних одиниць за 2022 рік. Міністерство захисту довкілля та природних ресурсів України. URL: <https://mepr.gov.ua/news/37155>.

2. Армія Inform. Побачити війну немов на долоні: інтерактивна мапа боїв deepstatemap.live. Армія Inform. – 2022. URL: <https://armyinform.com.ua/2022/06/22/pobachyty-vijnu-nemov-na-doloni-interaktyvna-mapa-boyiv-deepstatemap-live/>.

УДК 623.48

*Мілевський О.В., Ph.D,
Манойлов В.П., д.т.н., професор
Державний університет «Житомирська політехніка»*

МЕТОДИ ТА ПІДХОДИ ТЕХНІЧНОГО ОБСЛУГОВУВАННЯ СИСТЕМ ТА ОБЛАДНАННЯ

Сучасне виробництво продукції неможливе без використання засобів праці, які задіяні у виробництві тривалий час. До таких засобів відносяться устаткування. Устаткування – сукупний термін, який включає в себе машини, агрегати, механізми, вузли, а також апарати, колони, установки, технологічні лінії, електротехнічні та теплотехнічні об'єкти, мережі, технологічні, IoT та інші пристрої, які використовуються при виробництві продукції та виконують ті чи інші технологічні функції. Сучасні вимоги до роботи обладнання, машин, систем, підприємств, корпорацій і т.д. є надвисокі. Конкурентна боротьба призводить до мінімізації простоїв обладнання, підвищення швидкостей, зменшення обслуговуючого персоналу, ускладнення алгоритмів взаємодії всередині процесів.

Метод планово-профілактичного обслуговування (PM - Preventive maintenance) – найбільш розповсюджений на сьогодні, оскільки забезпечує довготривале та якісне обслуговування обладнання, поступово витісняється методом прогнозованого стану (PHM - Prognostic health monitoring) в зв'язку з низкою недоліків, які відіграють все суттєвішу роль в PM. Основні недоліки PM-методу – відносно часті зупинки обладнання для обслуговування, заміна деталей, у яких ще достатній ресурс для роботи. PM-метод має використовуватись лише в тому випадку, коли ресурс усіх деталей та механізмів приблизно однаковий, або кратний найменшому ресурсу. Така ситуація дуже рідкісна, тому PM-метод застосовується все рідше.

Ще більш ранній, коригуючий метод (CM – Corrective maintenance) – був витиснутий PM, але також має свою сферу застосування – в найпростіших системах, де час простою обладнання та аварія об'єкта не відіграють великого значення. Обладнання працює до аварійної зупинки й лише після зупинки проводяться корегуючі дії та обслуговування.

Новий підхід мав взяти всі переваги з існуючих методів та не мати їх недоліків. Такий підхід отримав назву методу прогнозованого стану (PHM). Обладнання сигналізує про необхідність обслуговування лише у випадку потреби обслуговування; при цьому йде обслуговування лише того модуля або об'єктів, стан котрих почав погіршуватись й

система контролю вбачає необхідність втручання. Метод РНМ виник в авіакосмічній галузі в 1990-х роках та поступово розповсюдився на найбільш відповідальні системи – системи гальм високошвидкісних потягів, управління гвинтокрилами, ударними винищувачами і т.п.

2000-і роки характерні використанням РНМ методу великими промисловими корпораціями, в першу чергу котрі виробляють складні та надскладні машини – потужні турбокомпресори, вітрильні електростанції, гідроелектростанції, системи військового призначення і т.п. Кожен рік алгоритми та можливості РНМ покращуються. Вивчення світового досвіду та робота з впровадження РНМ методу в скляній промисловості – тема подальшого дослідження. На сьогоднішній день відомо три основних підходи прогнозування.

В основі фізичного підходу (Physics based – PB) – побудова фізичної моделі і аналізування даних. Незаперечною перевагою PB є інтуїтивне прогнозування результатів, а також можливість копіювати розроблену модель на інші системи та конструкції.

Підхід, котрий базується на даних (Data driven – DD) – збирають, аналізують дані, що були зібрані в поточному та попередньому періоді (називаються навчальними даними) для визначення характеристик. Перевага даного методу: універсальність алгоритмів (готових пакетів) для обробки даних. Недоліки: необхідна велика кількість даних для обробки, результати можуть суперечити здоровому глузду (якщо не задіяні фізичні знання).

Гбридний підхід (Hybrid approach – HA) має на меті об'єднати переваги як фізичних (PB), так і тих що базуються на даних (DD), для поліпшення можливостей прогнозування.

Компанія General Electric стверджує, що підвищення ефективності на 1 % зможе принести 276 мільярдів доларів в п'яти основних галузях промисловості. Підвищення ефективності безпосередньо пов'язане з технічним обслуговуванням, тому впровадження РНМ-методу є пріоритетним для кожної галузі та системи.

Список використаних джерел

1. Котлярова В.Г. Сучасний підхід до організації підтримки працездатності устаткування на промисловому підприємстві [Електронний ресурс]. – Режим доступу:

http://www.economy.nayka.com.ua/pdf/4_2020/82.pdf

2. Аксютенко І.С., Аксютенко П.С. Технології та засоби організації системи технічного обслуговування [Електронний ресурс]. – Режим доступу:

https://www.researchgate.net/publication/356887866_Tehnologii_ta_zasobi_organizacii_sistemi_tehnicnogo_obslugovuvanna/link/61b15ba54d7ff64f05368d28/download

УДК 621.397.63

Дзюба М. В., Ph.D,

Нікітчук Т. М., к.т.н., доцент

Державний університет «Житомирська політехніка»

МЕТОДИКА ІНТЕГРАЦІЇ ДАНИХ ГІБРИДНИХ СИСТЕМ ОХОРОНИ З ІОТ ТЕХНОЛОГІЯМИ «РОЗУМНОГО БУДИНКУ»

Розумні будинки і системи охорони з використанням Інтернету Речей (IoT) стали популярними в останні роки, завдяки своєму потенціалу для забезпечення безпеки та зручності для мешканців. Проте інтеграція гібридних систем охорони IoT з розумними будинками вимагає ретельного узгодження та обробки даних для забезпечення ефективної реакції на різні події та ситуації.

Впровадження Інтернету речей відбувається не в глобальних масштабах, а всередині компаній. Складність впровадження полягає в тому, що жоден виробник не має в своєму складі закінченого рішення, що включає всі компоненти. Необхідно використання великої кількості систем від різних виробників і від їх правильного підбору та інтеграції залежить те, наскільки точно реалізоване рішення буде відповідати завданням і вимогам конкурентного середовища.

Першим кроком до інтеграції є визначення вимог до системи. Це включає в себе ідентифікацію меж і функцій гібридної системи охорони IoT та розумного будинку. Детальне розгляд цих вимог дозволяє визначити, які дані потрібно збирати та як вони повинні бути оброблені.

Для ефективної інтеграції систем важливо вибрати відповідні протоколи зв'язку. Зазвичай, використовуються стандартні протоколи, такі як MQTT, CoAP, або HTTP, які забезпечують можливість обміну даними між різними пристроями та системами. При цьому слід враховувати енергоефективність та безпеку обраного протоколу.

Дані, зібрані від датчиків і систем безпеки, повинні бути оброблені перед подальшим використанням. Це включає в себе фільтрацію, агрегацію, аналіз та зберігання даних. Обробка даних допомагає виявити аномалії та події, що потребують уваги.

Приклади практичного застосування:

- Система безпеки розумного будинку

Припустимо, що система безпеки розумного будинку включає в себе датчики відкривання дверей і вікон, камери відеоспостереження та сенсори диму.

Ці дані можуть бути інтегровані з системою охорони IoT, яка має датчики руху та відеоспостереження в реальному часі. Комбінування цих даних дозволяє виявити небажану активність в будинку та відразу сповістити власника.

- *Енергоефективність*

Гібридні системи охорони IoT також можуть використовуватися для підвищення енергоефективності розумного будинку. Наприклад, вони можуть автоматично вимикати світло та обігрівачі, коли нікого немає в приміщенні, зберігаючи енергію.

Енергоефективність є ключовим аспектом при розгляді інтеграції гібридних систем охорони Інтернету Речей (IoT) з технологіями «розумного будинку». Враховуючи, що багато розумних будинків мають різні системи автоматизації, які споживають електроенергію, такі як освітлення, опалення, кондиціонування повітря, електроприлади тощо, оптимізація споживання енергії може виявитися дуже важливою.

Висновок

Інтеграція гібридних систем охорони IoT з розумними будинками вимагає комплексного підходу, включаючи визначення вимог, вибір протоколів зв'язку та обробку даних. Правильна інтеграція дозволяє підвищити безпеку та комфорт для мешканців розумних будинків і зробити їх більш енергоефективними.

Загальний результат інтеграції полягає в зменшенні споживання енергії та витрат, збільшенні комфорту для мешканців та зниженні викидів в атмосферу. Це важливий крок у напрямку більш сталого та зеленого житла, і в майбутньому він може мати значний вплив на забезпечення енергоефективності та стійкості будівельних об'єктів

Список використаних джерел

1. Права розумного будинку. [Електронний ресурс]. – Режим доступу: <https://legalitgroup.com/prava-rozumnogo-budyunku/>

2. Кращі системи «Розумний будинок» по виробниках 2023 року [Електронний ресурс]. – Режим доступу:

<https://vencon.ua/ua/articles/rejting-sistem-umnyy-dom-proizvoditelyam>

3. Інтернет речей та сектор охоронної сигналізації. [Електронний ресурс]. – Режим доступу:

<https://worldvision.com.ua/internet-veshchey-i-sektor-okhrannoy-signalizatsii/>

УДК 621.391.8

*Сімчук А. Р., Ph. D.,
Нікітчук Т. М., к.т.н., доцент,
Марцева Л. А., д.пед.н., професор
Державний університет «Житомирська політехніка»*

ПРОБЛЕМИ ПЕРЕДАЧІ ТА ОБРОБКИ МЕДИЧНИХ СИГНАЛІВ У ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Передача та обробка медичних сигналів у телекомунікаційних системах є складним завданням, яке пов'язане з низкою проблем.

Однією з основних проблем є чутливість медичних сигналів до шуму. Медичні сигнали часто мають низьку амплітуду та високу частоту, що робить їх вразливими до шуму, який може спотворити сигнал і ускладнити його аналіз.

Іншою проблемою є необхідність забезпечення безпеки. Медичні сигнали часто містять конфіденційну інформацію, таку як дані про пацієнтів, що вимагає від телекомунікаційних систем забезпечення високого рівня безпеки.

Ще однією проблемою є необхідність забезпечення стабільності. Медичні сигнали часто є критичними для життєдіяльності пацієнта, тому телекомунікаційні системи повинні забезпечувати стабільну передачу та обробку сигналів навіть у несприятливих умовах, таких як перебої в електроживленні або слабкий сигнал.

Ось деякі конкретні приклади проблем, які можуть виникнути при передачі та обробці медичних сигналів у телекомунікаційних системах:

- Шум може спотворити медичні сигнали, що може призвести до помилок у діагнозі або лікуванні. Наприклад, шум може призвести до того, що серцебиття буде інтерпретовано як аритмія.
- Перешкоди можуть заважати передачі медичних сигналів, що може призвести до їх втрати або спотворення. Наприклад, перешкоди можуть виникнути внаслідок електромагнітного випромінювання від інших пристроїв.
- Затримки можуть виникнути при передачі медичних сигналів, що може призвести до затримки в обробці сигналів. Наприклад, затримка може призвести до того, що лікар не зможе вчасно реагувати на зміну стану пацієнта.
- Втрата пакетів може призвести до того, що частина медичних сигналів буде втрачена. Наприклад, втрата пакетів може призвести до того, що лікар не зможе отримати повні дані про стан пацієнта.

Для вирішення цих проблем розробляються нові методи та технології передачі та обробки медичних сигналів. Ці методи та технології спрямовані на підвищення точності, надійності та безпеки передачі та обробки медичних сигналів.

В роботі зазначаються методи та технології, які використовуються для вирішення проблем передачі та обробки медичних сигналів у телекомунікаційних системах, зокрема

- Шумоподавлення – метод, який використовується для зменшення впливу шуму на медичні сигнали.
- Корекція помилок – метод, який використовується для виявлення та виправлення помилок, які можуть виникнути при передачі медичних сигналів.
- Компресія – метод, який використовується для зменшення розміру медичних сигналів для їх ефективнішої передачі.
- Мультиплексування – метод, який використовується для передачі декількох медичних сигналів по одному каналу.
- Захист інформації – метод, який використовується для захисту конфіденційної інформації, яка міститься в медичних сигналах.

Розробка ефективних методів та технологій передачі та обробки медичних сигналів у телекомунікаційних системах є важливим завданням, яке сприятиме покращенню якості медичної допомоги.

Список використаних джерел

1. Coiera E. Guide to medical informatics, the Internet and telemedicine. – Chapman and Hall Medical, 2020. – 376 p
2. Jor Rodrigues. Health Information Systems: Concepts, Methodologies, Tools and Applications. – USA: IGI Global, 2019. – 1140p.
3. Сергеев-Горчинський О.О. Методи та моделі підвищення завадостійкості інформаційно-телекомунікаційних систем медичного призначення/ Дисертація на здобуття наукового ступеня кандидата технічних наук, 05.12.02 – телекомунікаційні системи та мережі. – Київ, НТУУ «Київський політехнічний інститут», 2016. – 174 с.
4. Кошева Л.О. Стандарти передачі медичної інформації в телемедичних системах / Л.О. Кошева, О.С. Корпан, Є.О. Павлов Інформаційні технології в медицині. Системи обробки інформації. – Випуск 2 (109). – 2017. С. 255-258.

УДК 621.397

*Твардовський Ю. В., магістрант,
Нікітчук С. М., магістрант,
Коренівська О. Л., к.т.н., доцент,
Коротун О. В., к.пед.н.*

Державний університет «Житомирська політехніка»

ОГЛЯД ТЕХНОЛОГІЙ РОЗУМНОГО БУДИНКУ

Системи «Розумний будинок» – це перспективний напрямок розвитку технологій. Вони можуть забезпечити комфорт, безпеку та енергоефективність житла.

Популярність систем «Розумний будинок» зростає з кожним роком завдяки кільком факторам:

- Покращення технологічної грамотності населення. Люди стають більш знайомі з новими технологіями та готові використовувати їх для покращення свого життя.

- Зниження вартості обладнання. Системи «Розумний будинок» стають більш доступними для широкого кола споживачів.

Системи «Розумний будинок» можуть виконувати широкий спектр функцій, включаючи:

- Автоматичне керування освітленням, опаленням, кондиціонуванням та іншими системами, що дозволяє економити енергію та створювати комфортний мікроклімат у будинку.

- Безпека. Системи «Розумний будинок» можуть використовуватися для контролю доступу, відеоспостереження та сигналізації.

- Комфорт. Системи «Розумний будинок» можуть дозволяти керувати пристроями та системами в будинку за допомогою голосу або смартфона.

У Західній Європі, а також в США, Канаді та інших розвинених країнах, такі програмно-апаратні комплекси активно використовуються не тільки забезпеченими людьми, але і тими, хто в силу своїх фізичних особливостей не може повноцінно жити і самостійно вести свій побут.

Сучасний ринок пропонує величезний вибір технічних пристроїв для автоматизації житла, тому порівняння системи «Розумний будинок» актуальна тема для багатьох.

Для зручності можна виділити основні критерії оцінювання таких систем. Наприклад, це можуть бути наступні моменти:

- стандартні складові частини комплексу і можливість масштабування (тобто додавання обладнання для розширення функціоналу);
- порядок підключення системних елементів між собою (дротовий бездротовий);
- спосіб управління (через ПК, смартфон, панель управління);
- канали зв'язку з користувачем (Інтернет, GSM, радіоканал);
- дальність роботи сигналу (чим показник більший, тим краще);
- вартість;
- виробник і багато іншого.

Згідно літературних джерел, першу позицію займає вітчизняна система Ajax, другу – BroadLink, третю – Fibaro, четверту – Orvibo, п'яту – Xiaomi. Звісно, це опосередкований рейтинг, але він був сформований згідно переваг та недоліків кожного із брендів.

Основними складовими системи безпеки є датчики руху, присутності, вібрації, розбиття скла, відкриття вікон чи дверей, відеоспостереження, відеодомофони та відеоокуляри, електронні замки (розумні замки, смартлоки) і модулі керування воротами, сирени. Ці пристрої дозволяють сконструювати оптимальну систему безпеки, від порівняно простої до достатньо складної.

Отже, проведено детальний огляд існуючих технологій побудови системи «Розумний будинок». Проаналізовано основні аспекти безпеки системи та в подальшому буде спроектована система розумного будинку, яка передбачає в собі використання різного виду датчиків та модулів, таких як датчик відстані, Bluetooth-модуль, датчик руху, двоканальне реле, ArduinoUno, ArduinoNano, GSM-модуль, RFID-мітки, освітлення.

Список використаних джерел

1. Права розумного будинку. [Електронний ресурс]. – Режим доступу: <https://legalitygroup.com/prava-rozumnogo-budynku/>
2. Кращі системи «Розумний будинок» по виробниках 2023 року [Електронний ресурс]. – Режим доступу: <https://vencon.ua/ua/articles/rejting-sistem-umnyy-dom-proizvoditelyam>
3. Інтернет речей та сектор охоронної сигналізації. [Електронний ресурс]. – Режим доступу: <https://worldvision.com.ua/internet-veshchey-i-sektor-okhrannoy-signalizatsii/>

УДК 621.397.63

Коренівська О. Л., магістрант

Державний університет «Житомирська політехніка»

МЕТОДИ ПРОГНОЗУВАННЯ РОЗВИТКУ ЦУКРОВОГО ДІАБЕТУ

Актуальність досліджень щодо прогнозування цукрового діабету залишаються надзвичайно важливими у сфері медичних наук і громадського здоров'я. Це обумовлено наступними аспектами:

1. **Зростання поширеності:** Щороку спостерігається значний приріст випадків цукрового діабету як в Україні, так і світі.

2. **Серйозні наслідки для здоров'я:** Цукровий діабет призводить до численних ускладнень, таких як серцево-судинні захворювання, проблеми з очима, нирками та іншими органами та є значним фактором ризику смертності населення.

3. **Інновації в терапії, індивідуалізована медицина:** Сучасні дослідження спрямовані на розробку нових методів лікування та контролю цукрового діабету, враховуючи індивідуалізований підхід до лікування кожного пацієнта.

4. **Економічний вплив:** Вплив цукрового діабету на економіку є значним через високі витрати на лікування та втрату продуктивності працівників.

Раннє виявлення розвитку цукрового діабету дає змогу почати лікування на ранніх стадіях та у багатьох випадках, при корекції способу життя та лікування, можна підтримувати легкий перебіг цього захворювання або навіть позбутися його. Це можливо зробити завдяки вивченню та розробці методів прогнозування наявності цукрового діабету у пацієнтів на основі аналізу розширених масивів клінічних та біохімічних даних. З урахуванням зростаючого розуміння ролі генетичних, клінічних та лабораторних факторів у розвитку цього захворювання, визначення точних та невідкладних методів прогнозування може слугувати ключовим інструментом для ранньої діагностики та ефективного управління хворобою.

Для визначення хворий пацієнт чи ні, можна скористатися допомогою різних методів, включаючи медичні та статистичні підходи. Ось деякі з них:

1. Машинне навчання:

Класифікаційні моделі: Використовуються для розділення пацієнтів на групи, такі як «хворий» чи «здоровий». Популярні алгоритми включають Random Forest, Support Vector Machines, та нейронні мережі.

Логістична регресія: Використовується для моделювання ймовірності того, що пацієнт належить до конкретного класу.

2. **Аналіз великих даних:** Використовується для обробки та аналізу великих обсягів клінічних даних для виявлення патернів, трендів та зв'язків.

3. **Дерева прийняття рішень:** Використовуються для визначення кроків прийняття рішень на основі клінічних параметрів.

4. **Аналіз чутливості та специфічності:** Використовується для визначення ефективності діагностичних тестів та алгоритмів.

5. **Порогові значення та криві ROC:** Визначення оптимальних порогів для класифікації на основі чутливості та специфічності.

6. **Аналіз виживання:** Використовується для аналізу часу до виникнення подій, таких як виявлення хвороби.

7. **Аналіз природної мови (NLP):** Використовується для обробки та розуміння текстової інформації у медичних записах.

8. **Байєсівські методи:** Використовуються для оцінювання ймовірностей виникнення конкретних станів на основі апріорних та спостережуваних даних.

9. **Аналіз групових відмінностей:** Використовується для визначення, чи є статистично значущі різниці між групами.

Ці методи можуть використовуватися окремо або комбінуватися для створення комплексних моделей, які допомагають визначати стан здоров'я пацієнтів на основі клінічних даних.

Для нашого дослідження були використані відкриті клінічні дані, включаючи результати аналізів крові, сечі, інформацію про спосіб життя, анамнез захворювань пацієнтів.

Масивні об'єми даних були піддані статистичному аналізу (описова статистика, регресійний аналіз, кореляційний аналіз, аналіз дисперсії (ANOVA), множинне порівняння) для визначення зв'язків та патернів, що вказують на ризик розвитку цукрового діабету.

Застосовані методи прогнозування можуть стати основою для створення інструментів ранньої діагностики цукрового діабету, що дозволить ефективно втручання та управління хворобою. Розроблені програми обробки даних та прогнозування можуть бути інтегрованими у медичні інформаційні системи та застосовуватися для оцінки наявності розвитку цукрового діабету у пацієнтів.

Список використаних джерел

1. Сучасні технології обробки й аналізу медичних даних/ О.В. Гойко. – Медична інформатика та інженерія. №4, 2009. – С. 39-44.

Секція 5 ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ В ОСВІТІ

УДК 378.018.43

*Гарбич-Мошора О. Р., к.пед.н., доцент,
Варварич Р. І., магістрант*

Дрогобицький державний педагогічний університет імені Івана Франка

ДИСТАНЦІЙНЕ НАВЧАННЯ В УМОВАХ ВІЙСЬКОВОГО СТАНУ

У сучасній епосі розвитку освіти, науки та технологій особливо актуальною стає проблема дистанційного навчання, як унікального процесу здобуття знань, навичок та умінь за допомогою інформаційно-комунікаційних технологій. Швидкий технологічний розвиток вимагає від освітніх систем адаптуватися до нових умов і забезпечити учнів необхідними навичками для успішного функціонування в сучасному світі.

В умовах військового стану дистанційне навчання вирішує низку проблем, які виникли в освітній системі України. Важливо зауважити, що успішне впровадження цієї форми навчання в освітній процес вимагає взаємодії батьків, учнів та педагогічних працівників, а також підтримки з боку держави. Дистанцій ненавчання особливо актуальне в період воєнного стану з ряду причин:

Безпека та здоров'я: Дистанційне навчання дозволяє уникнути фізичного зближення учнів та вчителів, забезпечуючи безпеку і здоров'я під час кризових ситуацій, таких як військовий конфлікт.

Гнучкість та адаптивність: В умовах воєнного стану можуть виникнути непередбачені властивості, які вимагають швидкого реагування та адаптації. Дистанційна освіта є гнучким інструментом, який можна швидко впровадити.

Збереження навчального процесу: Дистанційне навчання дозволяє зберегти навчальний процес у важливий період, коли традиційна форма навчання може бути ускладненою або неможливою.

Доступність для віддалених регіонів: У період війни можна виникнути потребу в забезпеченні освітніх можливостей для людей, які знаходяться в зоні конфлікту або віддалених районах. Дистанційне навчання робить це можливим.

Комунальна інфраструктура: Умови воєнного конфлікту можуть призвести до пошкодження або втрати комунальної інфраструктури, у

тому числі навчальних закладів. Дистанційна освіта дозволяє уникнути прямих залежностей від фізичних приміщень.

Залучення учнів у навчання: Дистанційне навчання може стати способом залучення учнів до навчального процесу у важких умовах, забезпечуючи можливість отримати освіту, не знаходячись у безпеці.

Ефективне використання технологій: За допомогою сучасних технологій інформаційно-комунікаційної сфери можна забезпечити ефективне проведення дистанційного навчання під час воєнного стану.

Характерною особливістю дистанційного навчання є розподіл відповідальності між учасниками навчального процесу, що призводить до збільшення обсягу обов'язків для батьків. Саме на батьків покладається відповідальність за забезпечення належних та безпечних умов навчання для дитини, забезпечення технічними засобами, забезпечення доступу до Інтернету, підключення до синхронних занять та інше.

Навчання в період війни вимагає важливого врахування різноманітних аспектів, щоб забезпечити безпеку та ефективність навчального процесу, а саме:

Фізична безпека: Забезпечте фізичну безпеку учнів, вчителів та персоналу, враховуючи ризики та заходи безпеки.

Психологічне здоров'я: Слід звернути увагу на психологічне здоров'я учасників освітнього процесу в умовах воєнного стресу. Надання психологічної підтримки може бути ключовим аспектом.

Технологічна інфраструктура: Перегляньте, що інфраструктура для дистанційного навчання доступна та надійна.

Навчання онлайн: Розгляньте можливості використання онлайн-платформи для навчання в разі обмеженого доступу до фізичних приміщень.

Онлайн-спілкування: Забезпечте можливість соціальної взаємодії між учнями та вчителями через онлайн-засоби для підтримки позитивного соціального середовища.

Педагогічна підтримка: Надайте педагогічну підтримку вчителям, допомагаючи їм адаптуватися до нових умов та вимог.

Пристосування матеріалів: Пристосуйте навчальні матеріали до поточної ситуації, можливо, враховуючи вплив воєнного конфлікту на контекст уроків.

Інформування та залучення: Активно інформуйте та залучайте батьків до навчального процесу, надаючи їм зрозумілу інформацію та забезпечуючи можливість поділитися власними спостереженнями та питаннями.

Враховуючи ці аспекти, освітні заклади можуть максимально ефективно впроваджувати навчання в умовах військового конфлікту, забезпечуючи безпеку та здоров'я всіх учасників.

УДК 004.8

*Ковтун В. В., магістрант,
Чижмоторя О. В., ст. викладач
Державний університет «Житомирська політехніка»*

РОЗРОБКА ІНТЕЛЕКТУАЛЬНОЇ ОСВІТНЬОЇ ПЛАТФОРМИ З ІНДИВІДУАЛЬНО АДАПТИВНИМИ НАВЧАЛЬНИМИ ПЛАНАМИ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ

У сучасному світі зростає вимога до індивідуалізації навчання, оскільки кожен учень має унікальні потреби, і різний темп навчання. Традиційні освітні системи не завжди в змозі забезпечити оптимальний розвиток кожного учня. Однак, засоби штучного інтелекту можуть революціонізувати освіту, надаючи індивідуально адаптивний підхід до навчання.

Проведений аналіз існуючих освітніх платформ виявив, що багато з них обмежені в наданні персоналізованої освіти. Більшість з них засновані на стандартних навчальних програмах та не здатні адаптуватись до потреб кожного учня. Однак, розвиток технологій штучного інтелекту дозволяє створювати інтелектуальні освітні платформи з адаптивними навчальними планами [1].

Штучний інтелект може використовуватись у багатьох аспектах освіти. Він може аналізувати поведінку та прогрес учнів, здійснювати прогнозування їхніх навчальних потреб, а також рекомендувати персоналізовані навчальні матеріали та методи. Алгоритми машинного навчання дозволяють виявляти індивідуальні сильні сторони та слабкі місця учнів, що допомагає розробити оптимальний навчальний план для кожного.

Розробка інтелектуальної освітньої платформи є комплексним завданням. Вона включає визначення архітектури системи, розробку інтерфейсу користувача, збір та обробку даних, використання алгоритмів машинного навчання для аналізу та інтерпретації даних, а також розробку модулів інтеграції з існуючими освітніми системами.

Edlearn, організація, що базується в Сієтлі, розробила адаптивну освітню платформу, яку можна використовувати для створення персоналізованих навчальних програм за допомогою машинного навчання з метою оптимізації часу навчання кожного учня. Команда Edlearn зазначає, що їх інструмент формує процес навчання, використовуючи велику кількість дрібних і непомітних компонентів, щоб проаналізувати, що саме заважає навчальній ефективності учня. Потім, як репетитор, інструмент допомагає учню заповнити прогалини в знаннях перед початком вивчення нового матеріалу.

При розробці інтелектуальної освітньої платформи велика увага приділяється питанням безпеки та конфіденційності. Система має гарантувати захист особистих даних учнів і їхнє використання лише для

навчальних цілей. Також забезпечується стійкість системи до можливих кібератак та несанкціонованого доступу.

Окрім розробки, важливо провести етап тестування платформи. Це дозволяє перевірити функціональність, ефективність та якість роботи системи. Контрольні групи учнів можуть використовуватись для порівняння ефективності платформи з традиційними методами навчання [1].

Успішна розробка інтелектуальної освітньої платформи з індивідуально адаптивними навчальними планами може відкрити шлях до її впровадження в освітні заклади. Поступове впровадження платформи у загальну освітню систему може сприяти підвищенню якості навчання та розвитку потенціалу кожного учня.

Поява нових доступних форм і засобів комунікації між викладачем та студентом розширює можливості підвищення рівня адаптивності в освітньому процесі [2]. Ці нові можливості дозволяють оперативно вносити зміни як у поданні навчального матеріалу, так і у формах та методах освітнього процесу, враховуючи персональні потреби кожного учня. Проте на сьогоднішній день більшість навчального контенту для адаптивного навчання характеризується обмеженим рівнем зворотного зв'язку між персональними потребами учня та адаптацією навчання до цих потреб. Зазвичай цей зв'язок базується на аналізі процесу вивчення матеріалу учнем, результатів тестових завдань та деяких суб'єктивних факторів, не враховуючи повністю ситуаційний контекст процесу навчання та індивідуальні особливості та характеристики учня. Сучасні адаптивні технології дозволяють глибше визначати ситуаційний стан процесу навчання та індивідуальні особливості та характеристики учня.

Підсумовуючи, розробка інтелектуальної освітньої платформи з індивідуально адаптивними навчальними планами є актуальним та перспективним напрямом розвитку освіти. Впровадження штучного інтелекту в освітній процес допоможе забезпечити більш ефективне та персоналізоване навчання, що сприятиме зростанню знань та навичок кожного учня. Для успішної реалізації цього проекту необхідно подолати технічні, етичні та соціальні виклики, але можливість покращення освіти заслуговує нашої уваги та зусиль.

Список використаних джерел

1. Мар'єнко М.В., Шишкіна М.П., Коновал О.А. Методологічні засади формування хмаро орієнтованих систем відкритої науки у закладах вищої педагогічної освіти. Інформаційні технології і засоби навчання, 2022,89(3), с. 209–232. Режим доступу: <https://doi.org/10.33407/itlt.v89i3.4981>.

2. Awasthi S., Soni Y. Empowering Education System with Artificial Intelligence: Opportunities and Challenges. Shodh Samagam, 2023, 6 (1) [http://www.shodhsamagam.com/admin/uploads/Empowering%20Education%20System%](http://www.shodhsamagam.com/admin/uploads/Empowering%20Education%20System%20)

УДК 004.8

*Ковтун В. В., магістрант,
Первалова А.Д., магістрант,
Чижмотря О. В., ст. викладач*

Державний університет «Житомирська політехніка»

ШТУЧНИЙ ІНТЕЛЕКТ В ОСВІТІ

Сучасне суспільство все більше стає залежним від передових технологій, що включає не лише використання Інтернету чи потужних смартфонів. Кожен раз, коли ми переглядаємо новини в Instagram, використовуємо пошук у Google, отримуємо рекомендації від AliExpress або замовляємо поїздку в Uber, ми використовуємо штучний інтелект (ШІ). Він проник в усі сфери нашого життя, і сфера освіти не є виключенням.

Штучний інтелект (ШІ) визначається як здатність цифрового комп'ютера чи робота керувати завданнями, які зазвичай виконувалися людиною або виконувати їх. Яскравим прикладом ШІ є роботи-гуманоїди, які можуть діяти самостійно, аналізуючи оточуюче середовище за допомогою різних сенсорів руху та світла.

Використання штучного інтелекту в освіті активно досліджується як в українських, так і в іноземних джерелах. У дослідженні розглядаються можливості використання штучного інтелекту для автоматизації комунікаційних і інформативних завдань. Це дозволяє освітнім установам зменшити час, потрібний для виконання цих завдань, і тим самим надати викладачам можливість більше часу приділяти роботі зі студентами.

Штучний інтелект здатний обробити набагато більше інформації, ніж людина. Це означає, що він може виконувати завдання швидше і точніше [1]. Деякі розробники освітнього програмного забезпечення використовують ці переваги для створення програм, які автоматично адаптуються до індивідуальних особливостей кожного учня. Наприклад, компанія Enlearn розробила освітню платформу, що використовує машинне навчання для створення персоналізованих навчальних планів, що сприяють ефективнішому освоєнню матеріалу для кожного учня [2].

Важливо пам'ятати, що ШІ представляє собою не просто об'єкт, а складну галузь наукових досліджень, яка включає багато піддисциплін, кожна з яких має власну історію, сферу знань та темпи розвитку. Розуміння цього є ключовим при оцінці можливого впливу ШІ на освіту. Освіта є основою формування особистості та прогресу

суспільства. З цієї причини не дивно, що уряди багатьох країн зростаюче зацікавлені у використанні ШІ, оскільки його впровадження сприяє удосконаленню навчального процесу [2].

Викладач витрачає значну кількість часу на оцінку домашніх завдань та тестів. ШІ може втрутитися та ефективно вирішити ці завдання, одночасно надаючи рекомендації щодо поліпшення навчання. Навіть оцінюючи тести з різними варіантами, машини наближаються до здатності оцінити письмові відповіді. Оскільки ШІ допомагає автоматизувати адміністративні завдання, це дозволяє вчителям віддати більше уваги індивідуальним розмовам з кожним студентом. Важливо також, що ШІ володіє великим потенціалом для вдосконалення процесів реєстрації та вступу.

Незважаючи на значний потенціал, використання штучного інтелекту має свої обмеження. Ефективність застосування залежить від обсягу наявних даних, які описують навчальні приклади. У сфері освіти, де немає місця для помилок, необхідно аналізувати різні сценарії, які можуть вплинути на навчальний процес. Освітні установи повинні розглянути можливі заходи для захисту особистих даних учнів [2].

Штучний інтелект в освіті використовується для виконання різноманітних завдань, включаючи інформаційні, комунікаційні та навчальні. Однією з ключових технологій у цьому контексті є використання чатботів. При цьому важливо приділяти особливу увагу безпеці обробки інформації, коли використовуються технології штучного інтелекту, зокрема чат-боти.

Якщо країна йде в ногу зі світовими тенденціями, то слід зауважити, що персоналізація стає загально визнаною. Головною перевагою штучного інтелекту є можливість навчити виконувати довгий перелік завдань у більш простий та цікавий спосіб. Але, на нашу думку, незважаючи на значні переваги штучного інтелекту у сфері освіти, не можна стверджувати, що він може абсолютно замінити викладачів. Так, ШІ може допомогти та полегшити їхню працю, але ніколи не може стати повноцінним їхнім заміником.

Список використаних джерел

1. Ушакова. І. О. Підходи до створення інтелектуальних чат-ботів / І. О. Ушакова // Системи обробки інформації. – 2019. – Випуск 2 (157). – С. 76 – 83.

2. 5 ways AI is changing the education industry. [Electroni cresource] – Access mode: <https://elearningindustry.com/ai-is-changing-theeducation-industry-5-ways>.

Отже, запропоноване рішення вирізняє три ролі користувача:

Адміністратор – інженер з охорони праці через інтерфейс повинен мати можливість редагувати, додавати дані, користуватися всіма функціями системи.

Викладач – штатний працівник підприємства або особа, що працює за сумісництвом і залучається до викладацької діяльності. Має можливість переглядати інформацію з організації навчального процесу в навчальних групах; виконувати дії щодо створення навчально-методичного забезпечення, а також змінювати його; створювати тести для перевірки знань учнів у тестовій формі та переглядати результати проведеного тестування.

Слухач – штатний працівник підприємства, який направлений на навчання з питань охорони праці. Він має можливість отримати інформацію про навчальний процес, ознайомлюватись з навчальними матеріалами та проходити тестування за напрямком навчання. Слухач має можливість проходити навчання у декількох групах одночасно.

Функціональні вимоги: можливість авторизації користувачів (реєстрацію здійснює безпосередньо адміністратор); валідація введених даних; модифікація введених даних; віображення результатів виконаної процедури; можливість збереження інформації.

Реалізацію рішення заплановано створити у вигляді десктопного додатку, оскільки він є менш вартісний у порівнянні з веб-додатком. Він може працювати автономно без приєднання до мережі Інтернет. Це гарантує безпеку даних та високу продуктивність. Документообіг відділу охорони праці здійснюється у паперовому вигляді, у цьому випадку перевага буде надана десктопним версіям додатків, які мають доступ до всіх пристроїв, як під'єднані до комп'ютеру, і без проблем інтегруються з принтерами, сканерами і іншими периферійними пристроями.

Після ретельного вивчення характеристик і можливостей систем управління базами даних було обрано PostgreSQL. Вибір обґрунтований тим, що йому PostgreSQL притаманно управління паралельним доступом за допомогою багатoversійності (Multiversion concurrency control, MVCC). Це вдосконалена функція бази даних, яка створює дублікати записів для безпечного одночасного читання та оновлення тих самих даних. Таким чином, кілька користувачів можуть одночасно читати і змінювати ті самі дані без шкоди для їх цілісності.

Отже, обрана модель дозволить оперативно отримати інформацію про підготовку і навчання співробітників для прийняття ефективних управлінських рішень та покращити планування та здійснення з роботи охорони праці в цілому.

Список використаних джерел

1. Getting Started with PostgreSQL. [Electronic resource] – Access mode: <https://www.postgresqltutorial.com/postgresql-getting-started/>.

УДК 372.8+004.9

Антоненко Є.Д.
Криворізький державний педагогічний університет
Мінтій І. С., к.пед.н., доцент,
с.н.с. відділу відкритих освітньо-наукових систем
Інститут цифровізації освіти НАПН України

ВИКОРИСТАННЯ ОНЛАЙН-РЕДАКТОРА CANVA В ОСВІТІ

В умовах стрімкого розвитку цифрового середовища та переходу до дистанційної форми, як навчання, так і роботи, стає необхідністю вміння використовувати сучасні інструменти для створення презентацій. Реальність вимагає від нас використання потужних засобів, щоб надати презентаційним матеріалам новий рівень зрозумілості та привабливості.

Наразі існує безліч редакторів, які можна використовувати для створення презентацій, але багато з них мають свої обмеження. Наприклад, вони можуть ускладнювати створення сучасних, динамічних презентацій з аудіосупроводом чи застосуванням цікавих дизайнерських шаблонів. Однак існує ефективний вихід із цієї ситуації – використання онлайн-сервісу Canva. Цей інструмент не лише забезпечує відмінну якість та креативність створених матеріалів, але й дозволяє уникнути типових обмежень, що зазвичай супроводжують інші редактори. З Canva можна легко створювати сучасні, динамічні презентації з власним озвучуванням та захопливим дизайном, що робить його ідеальним інструментом для задоволення високих вимог освітніх ресурсів у цифрову епоху. До того ж, ресурс «Canva для навчання» є безкоштовним для вчителів і їхніх учнів, які відповідають вимогам, а також доступний у всіх країнах світу без винятку» [1].

Мета: огляд можливостей онлайн-редактора презентація Canva.

Аудіосупровід. Canva дозволяє не лише візуально збагачувати презентації, але й надає можливість здійснити її аудіосупровід (рис. 1). Це стає особливо корисним у освітньому процесі, коли необхідно пояснити складний матеріал, а умови дистанційного навчання та постійних тривог створюють виклик для звичайного уроку. За допомогою Canva вчителі можуть легко і швидко створювати зрозумілі пояснення, роблячи навчальний процес більш ефективним та цікавим.

Спільна робота. Онлайн-платформа Canva відкриває безліч можливостей для колективної роботи в режимі реального часу. Учні можуть легко співпрацювати та об'єднувати свої зусилля, щоб

створювати інноваційні проекти. Це особливо актуально в умовах дистанційного навчання [2].

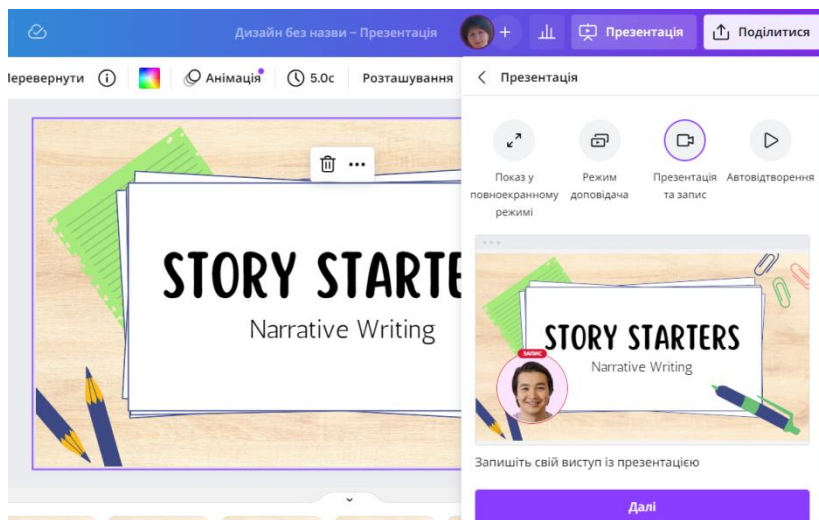


Рис. 1. Додавання аудіосупроводу до презентації Canva

Великий вибір шаблонів. В цьому редакторі наявний величезний вибір різних креативних і вже готових шаблонів для будь-яких типів проектів, що дозволяє користувачам швидко розпочати роботу, обираючи стиль, який найкраще відповідає їхнім потребам (рис. 2). Сучасні дизайни презентацій надихають студентів та учнів використовувати цей інструмент для створення своїх проектів з освітніми цілями, сприяючи представленню матеріалу у творчому та привабливому форматі.

Інтеграція з іншими сервісами. Canva також надає можливість взаємодії з різноманітними веб-ресурсами та сервісами. Інтеграція з популярними платформами, такими як WordPress, Instagram та Facebook, розширює можливості використання створених матеріалів. Підтримка платформи для зберігання файлів Dropbox, а також можливість вставляти елементи з Giphy та інших сервісів робить Canva універсальним інструментом для створення та редагування контенту.

Наявність мобільного додатку. Завдяки своєму мобільному додатку для планшетів та смартфонів Canva робить творчість доступною навіть в дорозі чи поза офісом, дозволяючи користувачам

редагувати та створювати графічний контент в будь-який час та в будь-якому місці легко з будь-якого додатку.

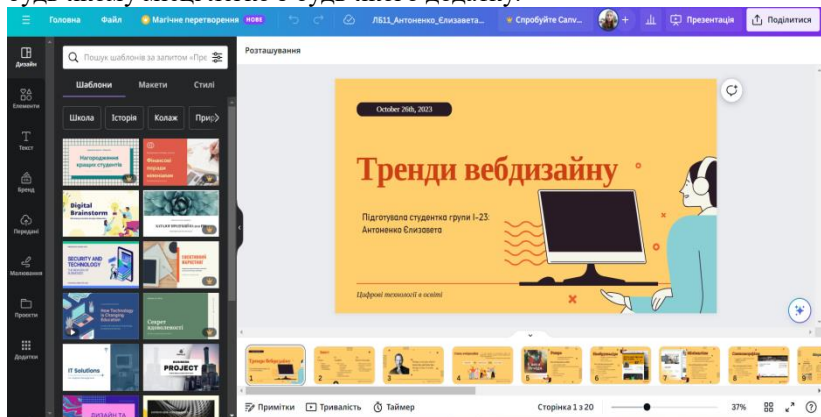


Рис. 2. Інтерфейс онлайн-сервісу Canva

Інтеграція з іншими сервісами. Canva також надає можливість взаємодії з різноманітними веб-ресурсами та сервісами. Інтеграція з популярними платформами, такими як WordPress, Instagram та Facebook, розширює можливості використання створених матеріалів. Підтримка платформи для зберігання файлів Dropbox, а також можливість вставляти елементи з Giphy та інших сервісів робить Canva універсальним інструментом для створення та редагування контенту.

Інтуїтивно зрозумілий інтерфейс. Легкість у використанні редактору із-за простого інтерфейсу, що дозволяє користувачам швидко освоювати програму. На рис. 2 показано, наскільки просто використовувати всі необхідні елементи для створення презентацій. Відсутність складних меню та легка навігація роблять Canva доступним навіть для тих, хто тільки починає працювати з графічним редактором.

«Магічне перетворення». Команда розробників Canva постійно працює над розширенням можливостей цього сервісу. Так, один з оновлених інструментів надає можливість конвертувати презентації в інші формати і змінювати їхній розмір (рис. 3), зокрема перетворювати у текстові документи – анотації, дописи для блогів або тексти пісень та ін.

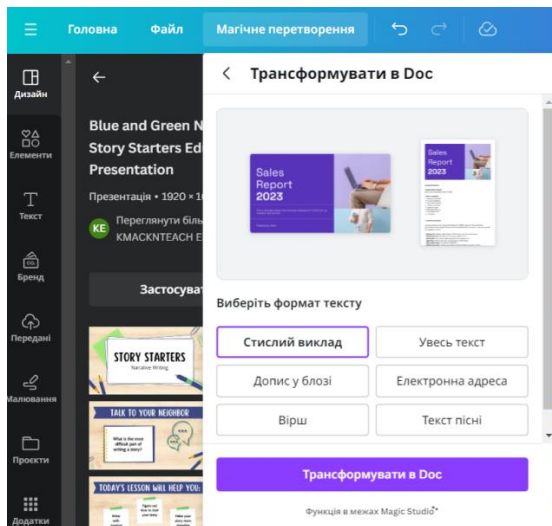


Рис. 3. Інструмент «Магічне перетворення» в Canva

Висновки. Canva є потужним та універсальним інструментом, який не лише полегшує процес створення презентацій, але й перетворює його в творчий та захопливий досвід. Можливість здійснювати аудіосупровід презентацій робить його надзвичайно цінним для освітнього процесу, а особливо – для дистанційної/комбінованої форми навчання. Великий вибір шаблонів надає можливість користувачам швидко розпочати роботу, а креативні дизайни стимулюють студентів та учнів використовувати Canva для своїх проєктів. Можливість колективної роботи в режимі реального часу та інтеграція з іншими платформами розширюють можливості співпраці та використання матеріалів. Легкість у використанні та мобільний додаток роблять Canva доступним для всіх, незалежно від рівня вмінь у графічному дизайні. У цілому Canva є важливим інструментом для творчого та ефективного створення візуального контенту в будь-яких умовах.

Список використаної літератури

1. Умови участі | Canva для навчання. URL: https://www.canva.com/uk_ua/osvita/umovy-uchasti/
2. Ресурси для навчання в Інтернеті. URL: https://www.canva.com/uk_ua/osvita/dystantsiina-osvita/

Секція 6
ЦИФРОВА ОБРОБКА СИГНАЛІВ В
АВТОМАТИЗОВАНИХ ТА ІНФОРМАЦІЙНО-
ВИМІРЮВАЛЬНИХ СИСТЕМАХ

УДК 621.3

*Бугайов М. В., к.т.н., с.д., ЗННДВ НЦ
Житомирський військовий інститут імені С.П. Корольова*

ОЦІНЮВАННЯ ЧАСТОТНИХ ПАРАМЕТРІВ СИГНАЛІВ У
ПАНОРАМНИХ СИСТЕМАХ РАДІОМОНІТОРИНГУ

У сучасних умовах для ведення радіомоніторингу все частіше використовують панорамні аналізатори спектра. Це зумовлено розширенням смуг роботи радіоелектронних засобів та ускладненням частотно-часової структури сигналів. Основними параметрами сигналів для їх попередньої селекції є несуча частота та ширина спектра (смуги). Для оцінювання частотних параметрів сигналів доцільно використовувати відліки енергетичного спектра.

У результаті оброблення ділянки радіочастотного спектра отримують значення меж частотних каналів та значення спектральних відліків. Причому межі каналів у відліках k_{min} та k_{max} визначено в результаті порогового оброблення на рівні близькому до рівня шуму. Для довжини вікна аналізу N при частоті дискретизації F_s значення оцінки несучої частоти можна отримати за таким виразом:

$$f_0 = F_s (k_{max} + k_{min}) / (2N), \quad (1)$$

а значення ширини спектра розрахувати за такою формулою:

$$\Delta f = F_s (k_{max} - k_{min}) / N. \quad (2)$$

Це найбільш простий на інтуїтивно зрозумілий спосіб отримання оцінок частотних параметрів. У [1] для вимірювання ширини зайнятої смуги частот рекомендовано використовувати метод $\beta\%$ та метод вимірювання "х-дБ". Для застосування першого способу роздільна здатність за частотою повинна бути не гірше 0,03 від ширини спектра сигналу, а відношення сигнал-шум (ВСШ) повинно бути не гірше 30 дБ. Для другого методу обирається опорний рівень, як правило 0 дБ. Метод $\beta\%$ доцільно застосовувати для оцінювання ширини

спектра цифрових сигналів при низьких значеннях ВСШ. У випадках наявності перешкод більш прийнятним буде метод “х-дБ”. При цьому для отримання надійних оцінок значень ширини смуги спектр сигналу повинен містити 100-200 спектральних відліків [2].

У [3] для оцінювання частотних параметрів сигналів використовують значення спектральної щільності потужності сигналів. З урахуванням значень відліків енергетичного спектра P_{xx} сигналу його центральну частоту запропоновано розраховувати за таким виразом:

$$f_0 = \frac{F_s}{EN} \sum_{i=k_{min}}^{k_{max}} iP_{xx}[i], \quad (3)$$

де E – енергія сигналу.

Відповідно ширину спектра сигналу (ефективну) можна розрахувати таким чином:

$$\Delta f = \frac{F_s}{EN} \sqrt{\sum_{i=k_{min}}^{k_{max}} i^2 P_{xx}^2[i]}. \quad (4)$$

Отримані відповідно до виразу (4) оцінки будуть відрізнятися від ширини смуги сигналу на рівні шуму і залежатимуть від форми спектра. Це створює передумови до селекції сигналів із використанням статистик від спектральних відліків.

У ході експериментальних досліджень при аналізі смуги частот 933-953 МГц було встановлено, що отримані за виразами (3) – (4) оцінки значень частотних параметрів мають в середньому (за 20 сигналами) у 2 рази меншу дисперсію, ніж за виразами (1) – (2).

Через мінливість шуму при невисоких значеннях ВСШ кожна реалізація спектра сигналу буде представлена різною кількістю частотних відліків, що призведе до коливань значень частотних параметрів. Тому для отримання надійних оцінок центральної частоти та ширини смуги сигналу необхідно проводити додаткову обробку послідовностей отриманих значень параметрів.

Список використаних джерел

1. Recommendation ITU-R SM. 443 – Bandwidth measurement at monitoring stations.
2. Handbook spectrum monitoring. ITU Radio communication Bureau 2011 678 p.
3. Cook C. E., Bernfeld M. Radar Signals: An Introduction to Theory and Applications. Artech House, Inc.: Norwood, MA, USA, 1993.

УДК 621.3

*Бугайов М. В., к.т.н., с.д., ЗННДВ НЦ,
Поздняков В. В., ад'юнкт
Житомирський військовий інститут імені С. П. Корольова*

МАТЕМАТИЧНА МОДЕЛЬ АКУСТИЧНИХ СИГНАЛІВ СИСТЕМИ АКУСТИЧНОГО МОНІТОРИНГУ ПОВІТРЯНОГО ПРОСТОРУ

Удосконалення методів одночасного виявлення, розпізнавання та визначення координат декількох засобів повітряного нападу (ЗПН) за їх акустичними сигналами (АС) є одним з перспективних напрямків розвитку системи акустичного моніторингу повітряного простору. Для виявлення, розділення, розпізнавання та локалізації ЗПН за їх АС необхідно розробити модель прийнятого сигналу, за параметрами якої можна вирішити дане завдання.

У шумові силовій установці БпЛА, що містить поршневий двигун повітряного охолодження за відсутності у вихлопному тракті двигуна глушника, визначальним джерелом зовнішнього шуму є поршневий двигун [1]. Іншим джерелом шуму є повітряний гвинт. Акустичний шум утворюється в результаті силовій взаємодії лопатей гвинта з навколишнім середовищем у процесі створення тяги і при витісненні повітря з фіксованого об'єму середовища лопатями. До точки спостереження будуть доходити імпульси, що викликані проходженням кожної лопаті, що збурює повітря. Оскільки гвинт обертається з визначеною частотою, і в шумі будуть існувати гармоніки [2]. Сумарний рівень шуму силовій установці БпЛА визначається, здебільшого, першими 10-ма гармоніками шуму двигуна і першими 5-ма гармоніками шуму обертання гвинта [1]. Ширококутовий низькочастотний аеродинамічний шум корпусу планера виникає в результаті обтікання повітрям поверхні БпЛА та тиску, що створюється підйомною силою крила.

Таким чином, АС БпЛА є сумою гармонік, що кратні частоті обертання ротора двигуна а також інших високо- і низькочастотних ширококутових складових. З огляду на частотний склад такого сигналу можна провести його аналіз та ідентифікувати конкретний тип джерела звуку.

Амплітуда АС залежить від багатьох факторів: температури та вологості повітря, сили і напрямку вітру, наявності опадів, тощо. Тобто вона є нестійким та неінформативним параметром. Частота конкретної гармоніки прийнятого АС залежить від швидкості руху

джерела звуку та напрямку його польоту (ракурсу відносно точки прийому) при фіксованому режимі роботи силової установки. Фаза прийнятого АС залежить від напрямку на джерело звуку та відстані від нього до точки спостереження. Пропонується розпізнавати АС від декількох джерел звуку аналізуючи частоти гармонічного сигналу на окремих мікрофонах акустичного датчика в точці прийому. Модель гармонічного сигналу $S_{I\theta}$ (де I – індекс джерела звуку, θ – індекс гармоніки виділеної для аналізу) на вході одного мікрофона на частоті f_0 можемо подати у вигляді:

$$S_{I\theta}(t) = A_{I\theta} \sin \left(2\pi f_0 t + 2\pi \frac{V_1(t)\alpha_1(t)}{\lambda_{I\theta}} t + 2\pi \frac{R_1(t)}{\lambda_{I\theta}} \right), \quad (1)$$

де $A_{I\theta}$ – амплітуда гармоніки АС; $\frac{V(t)\alpha(t)}{\lambda}$ – зсув частоти, який залежить від швидкості $V(t)$ джерела звуку та ракурсу його польоту відносно точки спостереження $\alpha(t)$; $2\pi \frac{R(t)}{\lambda}$ – набіг фази зумовлений зміною відстані до джерела звуку; λ – довжина хвилі АС. Тоді гармонічна складова АС одного джерела звуку може бути записана у вигляді суми N компонент:

$$S_1(t) = \sum_{i=1}^N S_{1i}(t), \quad (2)$$

а сигнальна суміш $X_1(t)$ на вході одного мікрофона акустичного датчика може бути записана у такому виді:

$$X_1(t) = \sum_{i=1}^M S_i(t) + n(t), \quad (3)$$

де $S_i(t)$ – АС одного джерела звуку; M – кількість джерел звуку; $n(t)$ – шумова складова, яка включає в себе ширококутну складову АС, шум навколишнього середовища, внутрішній шум акустичного датчика.

Список використаних джерел

1. Даник Ю.Г., Пулеско І.В., Бугайов М.В. Виявлення безпілотних літальних апаратів на основі аналізу акустичних та радіолокаційних сигналів // Вісник ЖДТУ. 2014. № 4 (71). С.71-80
2. Бугайов М.В. Алгоритм виявлення акустичних сигналів безпілотних літальних апаратів // Вісник ЖДТУ. 2015. № 3(74). С. 46-53.

УДК 621: 317

*Вакарюк Я. А., магістрант,
Лугових О. О., старший викладач
Державний університет «Житомирська політехніка»*

КОМП'ЮТЕРИЗОВАНА СИСТЕМА ВИМІРЮВАННЯ ЄМНОСТІ ТА ІНДУКТИВНОСТІ КОМПОНЕНТІВ ЕЛЕКТРОННИХ СХЕМ

Розвиток електроніки та сучасних технологій вимагає високофункціональних та точних методів вимірювання та контролю параметрів електронних компонентів. Справжній прогрес у цьому напрямку можливий завдяки впровадженню комп'ютеризованих систем вимірювання та контролю, які забезпечують не лише точність, але й автоматизацію цих процесів. В сучасних електронних схемах особливо важливими є параметри ємності та індуктивності компонентів. Зміни в їхніх значеннях можуть впливати на працездатність та ефективність електронних пристроїв. Таким чином, виникає потреба у вдосконалених методах вимірювання та контролю цих параметрів.

Об'єкт дослідження – компоненти електронних схем, зокрема, їхні ємнісні та індуктивні характеристики.

Предмет дослідження – комп'ютеризована система вимірювання та контролю ємності та індуктивності компонентів електронних схем.

Наукова новизна полягатиме в розробці та впровадженні комп'ютеризованої системи, яка буде вирішувати актуальні завдання вимірювання та контролю ємності та індуктивності компонентів електронних схем.

Практичне значення роботи полягатиме в покращенні точності, швидкості та автоматизації процесів, пов'язаних із вимірюванням та контролем параметрів електронних компонентів.

Розроблена система може знайти застосування в промисловості, дослідницьких лабораторіях та інших галузях, де важливо забезпечити високу точність вимірювань та ефективний контроль параметрів електронних компонентів.

Для створення системи була побудована структурна схема комп'ютеризованої системи вимірювання та контролю ємності та індуктивності компонентів електронних схем (рис.1), яка складається з наступних елементів мікроконтролер PIC16F1936 для управління пристроєм вимірювання; акумулятор для живлення пристрою; стабілізатор напруги для стабілізації напруги; реле для вибору режиму

вимірювання ємності чи індуктивності; роз'єму Х2, Х3 куди підключаються щупи для вимірювання; перемикач включення чи виключення живлення; кнопка скидання даних використовується для обнуління, тобто повернення до початкових даних; дисплей для виведення результату вимірювання ємності чи індуктивності; кварцовий резонатор видає електричний імпульс з частотою 32 МГц на вхід мікроконтролера для обробки показів, інформації та обчислення по програмі.



Рис. 1. Структурна схема

Вимірювач індуктивності та ємності є вимірювачем частоти, що має у складі генератор коливачів, який генерує коливання і вимірює величини L або C , після чого обчислюється кінцевий результат. Похибка частоти становить 1 Гц. Лічильник працює на основі математичних рівнянь.

Список використаних джерел

1. Мікропроцесорні пристрої: навч. посібник для студентів зі спец-ті «Електроніка» / Т.О. Терещенко, В.А. Тодоренко, Л.М. Батрак, Ю.С. Ямненко. – К.: Кафедра, 2017. – 244 с.
2. Методи і засоби вимірювань електричних та неелектричних величин: навчальний посібник / Д.М. Нестерчук, С.О. Квітка, С.В. Галько. – Мелітополь: Видавничо-поліграфічний центр «Люкс», 2017. – 206 с.
3. Основи метрології та вимірвальної техніки. Навчальний підручник / За заг. ред. Н.А. Яремчук. – К: Видавництво «Політехніка», 2012. – 266 с.

УДК 621: 317

*Вовк В. В., магістрант,
Лугових О. О., старший викладач
Державний університет «Житомирська політехніка»*

КОМП'ЮТЕРИЗОВАНА ІНФОРМАЦІЙНО- ВИМІРЮВАЛЬНА СИСТЕМА КОНТРОЛЮ ПАРАМЕТРІВ ПАПЕРУ

Папір – найпоширеніший у світі матеріал, без нього неможливо уявити наше життя: документи, книги, журнали, гроші, упаковка, санітарно-гігієнічні вироби та багато іншого. Виробництво паперу – процес складний та безперервний, трудомісткий та ресурсозатратний.

Паперова промисловість сьогодні має багато викликів: глобалізація загострює конкуренцію, цифровізація виборює першість серед носіїв інформації, ціни на енергоресурси зростають, екологічні вимоги посилюються.

Щоб зберегти виробництво, потрібні: заощадливі технології, стабільність на кожній стадії виготовлення продукту, наочність виконання технологічних операцій, їх повна простежуваність.

Основними факторами, що дозволяють сучасному підприємству залишатися конкурентоспроможними, є ціна та якість продукції. Роль нецінових факторів зростає. Тому кожне підприємство приділяє особливу увагу якості продукції на всіх стадіях виробництва. Ефективна система контролю дає змогу своєчасно впливати на рівень якості продукції, попереджувати, а також усувати можливі недоліки, і в умовах безперервного виробництва уникнути зайвих втрат.

Високих показників можна досягнути лише за допомогою часткової передачі функцій обслуговуючого персоналу системам вимірювання та автоматичного регулювання.

В результаті скорочення участі людини в технологічному процесі, зменшується кількість помилок, підвищується ефективність роботи підприємства. Як результат – отримання продукції високої якості при низькій собівартості.

Одним із способів вирішення такої задачі є встановлення на виробництві комп'ютеризованої інформаційно-вимірювальної системи контролю параметрів паперу, яку виробники такого обладнання називають автоматичною системою контролю якості (QCS). Комплексна QCS може складатися зі сканерів та датчиків, встановлених у різних точках переробної машини. Отримані дані візуалізуються в єдиній системі відображення.

Основна задача полягає в удосконаленні QCS для більш узгодженої роботи, покращення виробництва, посилення контролю якості, зменшення кількості відходів продукції, енергозбереження та зниження витрат.

Для виконання задачі пропонується забезпечити додатковий проміжний контроль вологості та температури в мокрій частині переробної машини, за допомогою якого будуть удосконалені режими роботи переробної машини, внесені зміни в технологічні карти кожного виду продукції, завдяки чому буде забезпечена стабільна робота сушильної частини, а коливання вологості готової продукції будуть мінімальними.

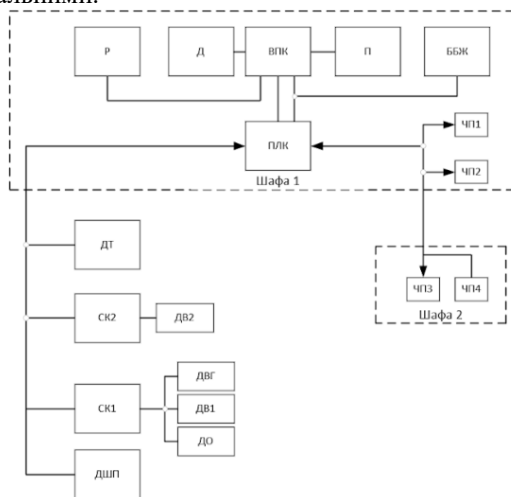


Рис. 1. Структурна схема

Складові структурної схеми наступні: Р – роутер; Д – Дисплей; ВПК – виробничий персональний комп’ютер; П – принтер; ББЖ – безперебійний блок живлення; ПЛК – програмований логічний контролер; ЧП1-ЧП4 – частотні перетворювачі; ДТ – датчик температури; СК1-СК2 – сканери; ДВ1-ДВ2 – датчики вологості; ДВГ – датчик ваги; ДО – датчик обриву; ДШП – датчик швидкості паперу.

Окремі елементи схеми є доповненням до існуючого варіанту, а саме:

Датчик температури (ДТ) – призначений для вимірювання температури під ковпаком сушильної частини ПРМ.

Сканер (СК2) – рама на якій буде встановлений датчик для вимірювання вологості після пресової частини ПРМ (ДВ2).

Частотні перетворювачі (ЧП2, ЧП3) – пристрої які застосовуються для зміни електричного струму. Частотний перетворювач забезпечує плавний пуск і зупинку двигунів, а також дозволяє змінювати напрям їх обертання.

Програмований логічний контролер (ПЛК) – електронний пристрій, який використовується для автоматизації технологічних процесів. ПЛК є центральною ланкою системи контролю якості.

Модульна конструкція дозволяє надалі нарощувати систему, вимірювати інші технологічні параметри, коригувати дані вимірювань.

Існуюча QCS включає в себе сканер на основі модульної платформи автоматизації ComCore від компанії Voith (Німеччина). Модульність дозволяє легко інтегрувати QCS в існуючі системи автоматизації та надає чітку інформацію виробнику паперу.

Простий у використанні інтерфейс користувача забезпечує прямий доступ і оптимізацію профілів параметрів якості.

Додаткове вимірювання вологості в процесі виготовлення паперу після пресової частини ПРМ забезпечує оптимальне сушіння для досягнення цільових показників якості продукції. Це також дозволяє виробнику паперу оптимізувати споживання енергії для зменшення витрат або збільшити швидкість виробництва для досягнення виробничих цілей.

Підвищення якості та стабільності готової продукції зменшує кількість відходів виробництва і претензій від замовника.

Список використаних джерел

1. Voith Quality Control System (QCS) On Quality | Voith [Електронний ресурс]. – Режим доступу: <https://voith.com/corpen/products-services/automation-digital-solutions/onquality.html>

2. Paper Machine Quality Control Systems – Volume 1: Measurement Systems and Product Variability [Електронний ресурс]. – Режим доступу: <https://imisrise.tappi.org/TAPPI/Products/01/R/0101R328.aspx>.

3. Борисова Л.В. Автоматизовані системи управління технологічного процесу в хімічних виробництвах. Курс лекцій, Харків, НУЦЗУ, 2015, 99 стор.

4. Діордієв В.Т. Засоби автоматизації електротехнічних комплексів: навчальний посібник / В.Т. Діордієв, А.О. Кашкар'юв, С.В. Дубініна, Г.В. Новіков. – Мелітополь: ФОП Однорог Т.В., 2020. – 220 с.

УДК 621: 317

*Лугових О. О., ст. викладач,
Уляницький В. П., магістрант
Державний університет «Житомирська політехніка»*

КОМП'ЮТЕРИЗОВАНА СИСТЕМА ВНУТРИШНЬОСХЕМНИХ ВИМІРЮВАНЬ ОПОРУ

У радіоконструюванні потрібно виміряти малі опори. Для цього застосовується міліометр. Крім того, одне з основних призначень описуваного приладу – внутрішньо схемний пошук місць короткого замикання під час ремонту радіоапаратури шляхом визначення ділянки з мінімальним опором.

На ринку вимірвальної техніки існує багато готових технічних рішень міліометрів, але вони відчутно дорого коштують на відміну наведеної в роботі вимірвальної системи. Натомість розроблена вимірвальна система майже ні в чому не буде поступатися готовому приладу.

Розробка цієї системи є досить актуальною тому що вимірювання низького опору широко використовується в галузі виробництва компонентів: резисторів, котушки індуктивності, трансформаторів, провідники, напівпровідники.

Дана система буде вимірювати низький опір і також зможе знаходити коротко замкнуті ділянки електричних ланцюгів радіоприладів, що дає змогу ремонтувати прилад без випаювання тих чи інших елементів.

Вимірювання низького опору виконується з багатьох причин, включаючи, але не обмежуючись, тестування безпеки, продуктивності та якості.

Виробники електричних компонентів, таких як резистори, котушки індуктивності та дроселі, усі повинні перевірити, чи відповідає їхня продукція зазначеним допускам, закінченню виробничої лінії та перевірі контролю якості.

Для виробника кабелю опір мідних проводів, які вони виготовляють, має надзвичайне значення. З точки зору безпеки, якщо опір дроту занадто високий, це свідчить про недостатню подачу міді, що знижує здатність кабелю пропускати струм. Якщо опір занадто низький, виробник занадто щедрий на діаметр кабелю, використовуючи більше міді, ніж йому потрібно, що може бути дуже дорогим у довгостроковій перспективі.

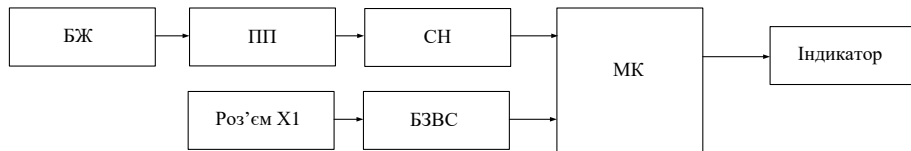


Рис. 1. Структурна схема

Схема складається з наступних елементів:

- Мікроконтролеру для управління пристроєм вимірювання;
- Підвищуючий перетворювач напруги;
- Стабілізатора напруги;
- Роз'єм X1 для щупів щупів;
- Блок задання вимірюючого струму;
- Індикатор для виведення результату вимірювання опору;
- Блок живлення.

Вимірне значення було отримано непрямым методом за формулою (1):

$$R_x = \frac{N \times R_0}{1023 \times K_{op} - N} \quad (1)$$

де $R_0 = R_6 + R_1$, K_{op} – коефіцієнт посилення (КП), N – величина відліку АЦП. Як видно з формули, результат не залежить від напруги живлення (при його рівності з напругою, що подається на R_6) і взагалі не залежить від активних елементів.

В результаті, дана схема забезпечує більш високу точність вимірювань, ніж при використанні активного джерела струму.

Список використаних джерел

1. Методи і засоби вимірювань електричних та неелектричних величин: навчальний посібник / Д.М. Нестерчук, С.О. Квітка, С.В. Галько. – Мелітополь: Видавничо-поліграфічний центр «Люкс», 2017. – 206 с.

2. Build Your Own Low-Resistance Meter [Електронний ресурс]. – Режим доступу: <https://www.allaboutcircuits.com/projects/build-your-own-low-resistance-meter>.

УДК 621.317

*Подчашинський Ю. О., д.т.н., професор,
Гагін А. В., магістрант,
Чепюк Л. О., к.т.н., доцент
Державний університет «Житомирська політехніка»*

КОМП'ЮТЕРИЗОВАНА ІНФОРМАЦІЙНО- ВИМІРЮВАЛЬНА СИСТЕМА ДЛЯ ВИЗНАЧЕННЯ ТА КОНТРОЛЮ ПАРАМЕТРІВ ВИРОБНИЦТВА ХАРЧОВИХ СОУСІВ

Технологічна схема процесу виробництва харчових соусів (на прикладі соєвого соусу) наведена на рис. 1.

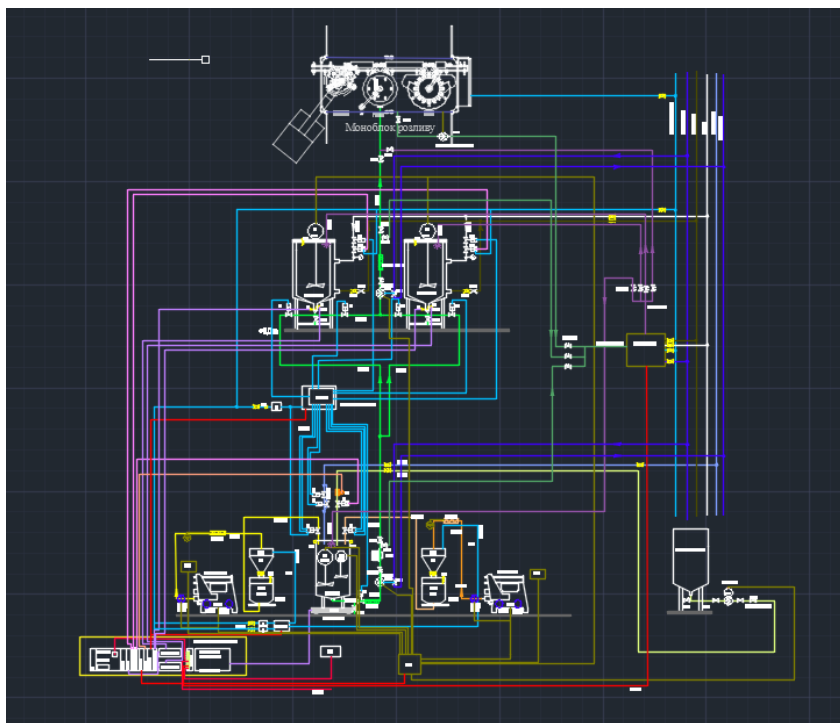


Рис. 1. Технологічна схема процесу виробництва харчових соусів

Апаратна частина системи побудована на базі обладнання фірми Siemens: PLC: Siemens Simatic S7, HMI Simatic Comfort Panel 10 "Touch, Вагова система складається з модуля PLC Siemens SIWAREXWP321, тензодавачів METTLERLEDO, «Weighing module SWB505 Multi Mount». Витратомір Sitrans FMMagflo Mag 1100 Food +Mag6000.

Процес виробництва складається з наступних стадій: дозування компонентів, змішування, пастеризація, перекачування суміші, фасування. В процесі виробництва соєвих соусів необхідно контролювати наступні параметри технологічного процесу:

1. Дозування води (грубо/точно, вагова система), оцту (витратомір), цукру, солі, сої, інших (1-4) компонентів.

2. Швидкість перемішування – для автоматичного і ручного режиму.

3. Час перемішування.

4. Температуру пастеризації.

Система має можливість записувати вагу кожного з компонентів в архів з датою та часом а також загальну вагу замісу.

Вимоги до точності дозування компонентів наведено в таблиці 1.

Таблиця 1

Похибки дозування компонентів

Маса, кг	Границя допустимої похибки, кг	
	При повірці	При експлуатації
$10 \leq m \leq 200$	$\pm 0,25$	$\pm 0,50$
$250 < m \leq 1000$	$\pm 0,50$	$\pm 1,0$
$1000 < m \leq 1500$	$\pm 0,75$	$\pm 1,50$

Похибки вимірювання витрат: 0,1% від дозованого продукту

Список використаних джерел

1. «Soy Sauce» How Products Are Made. Advameg, Inc. 2018, [Електронний ресурс]. – Режим доступу:

<http://www.madehow.com/Volume-3/Soy-Sauce.html>.

2. Recent progress and advances in soysauce production technologies: A review Soumaya Sassi, Wan Abd Al Qadr Imad Wan-Mohtar, Nazzatush Shimar Jamaludin, Zul Pnam Firstpublished: 26 July 2021 <https://doi.org/10.1111/jfpp.15799>

3. Офіційний сайт Siemens. [Електронний ресурс]. – Режим доступу: <https://www.siemens.com/ua/uk/produktu/>

УДК 621.3: 455.63

*Подчашинський Ю. О., д.т.н., професор,
Чепюк Л. О., к.т.н., доцент,
Криворучко М. Г., магістрант
Державний університет «Житомирська політехніка»*

ОГЛЯД МЕТОДІВ ВИМІРЮВАННЯ КУТОВОЇ ШВИДКОСТІ

На сьогоднішній день існують різноманітні засоби вимірювання частоти обертання об'єкта відносно статичної осі протягом визначеного інтервалу часу. Основні методи вимірювання кутової швидкості є механічний, електромагнітний та оптичний.

Механічні методи вимірювання кутової швидкості ґрунтуються на принципах роботи центр обіжних тахометрів та гіроскопів з двома ступенями свободи.

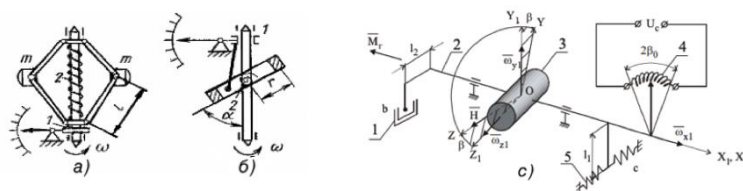


Рис. 1. Види тахометрів

a – конічний тахометр; *б* – кільцевий тахометр,
с – гіроскоп з 2-ма ступенями свободи

Центробіжні тахометри поділяються на конічні (рис. 1а) та кільцеві (рис. 1б) типи. У кільцевому тахометрі кутова швидкість визначається за рухом нахилоного кільця, яке утримується пружиною під час обертання. У конічному тахометрі вантажі на шарнірах розходяться під дією відцентрових сил, стискаючи пружину і переміщуючи муфту вздовж осі.

Гіроскоп з двома ступенями (рис. 1с) працює за принципом виникнення гіроскопічного моменту під час обертання, який змушує гіроскоп відхилитися від його початкового положення. Це призводить до деформації пружин, які створюють протилежний момент. Коли ці моменти урівноважуються, гіроскоп залишається на певному куті, і це положення використовується для вимірювання кутової швидкості за допомогою потенціометрів.

Методи вимірювання кутової швидкості, які використовують електромагнітні принципи, ґрунтуються на функціонуванні магнітоіндукційних тахометрів та MEMS-гіроскопів.

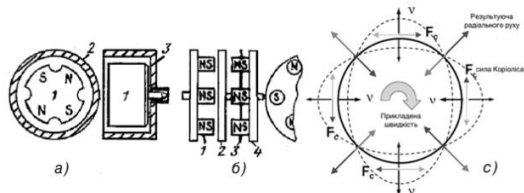


Рис. 2. Тахометри
a – з циліндром; *б* – диском, *с* – MEMS-гіроскоп

У цих типах тахометрів використовується принцип електромагнітної індукції, що базується на захопленні провідного тіла (циліндра або диска) рухливим постійним магнітом, внаслідок чого виникають індуквані струми у провідному тілі, які взаємодіють з магнітним полем постійного магніту, що призводить до сили, яка утримує провідне тіло. Вимірювання кутової швидкості обертання вала здійснюється шляхом оцінки цієї сили та маси провідного тіла.

Імпульсний метод вимірювання кутової швидкості в MEMS-гіроскопі заснований на сприйнятті радіального руху. Вісім приводів, розташованих навколо кільця, забезпечують два типи сигналів: первинні, що керують вібрацією, і вторинні, що реєструють радіальний рух. Демодуляція сигналів у вторинних перетворювачах дає дані про кутову швидкість обертання гіроскопа.

Оптичний метод використовує компоненти, такі як світлодіодне джерело світла та фотодетектори. Під час обертання вала світловий промінь направляється на оптичну шкалу з прозорими та непрозорими областями. Фотодетектори реєструють зміни у світловому потоці, який відбивається від шкали, і перетворюють їх на електричні сигнали.

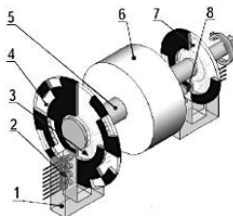


Рис. 3. Оптичний енкадер

Шляхом аналізу цих змін фотодетектори визначають кутове положення або швидкість обертання вала. Роздільна здатність оптичного енкодера залежить від кількості та розподілу прозорих і непрозорих областей на оптичній шкалі.

Ще одним варіантом оптичного методу вимірювання кутової швидкості є лазерний гіроскоп, що базується на оптичному резонаторі, який містить відбиваючі елементи (такі як дзеркала чи призми), утворюючи шлях для світла в певній конфігурації.

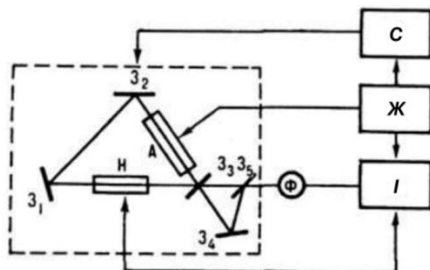


Рис. 4 Лазерний гіроскоп

Зміна часу, необхідного світлу для його обходу, залежить від швидкості обертання та напрямку руху. Рух гіроскопа змінює час, необхідний світлу для проходження по контуру, що призводить до зміни частоти світлових хвиль.

Коли гіроскоп обертається, зміна швидкості світла через резонатор призводить до зміни частоти світлових хвиль. Ця зміна частоти використовується для визначення кутової швидкості обертання.

Список використаних джерел

1. Gyroscope Technology and Applications: A Review in the Industrial Perspective [Текст] / V.M.N. Passaro, A. Cuccovillo, L. Vaiani, M. DeCarlo, C. E. Campanella // Sensors. – 2017. – Vol. 17, Iss. 10. – P. 2287. – DOI: 10.3390/s17102287.
2. Метрологічне забезпечення тахометричних вимірвальних перетворювачів: монографія / В. О. Поджаренко, В. М. Севастьянов, В. П. Осадчий. – Вінниця : ВНТУ, 2009. – 148 с.
3. Інтелектуальні оптоелектронні сенсори кута: схемотехнічні та програмно-алгоритмічні методи синтезу: Монографія / М.І. Паламар, А. В. Чайковський; ТНТУ ім. І. Пулюя. – Тернопіль: вид-во "Джура", 2015. – 144 с.

УДК 621.317

*Подчашинський Ю. О., д.т.н., професор,
Магалецький Я. В., магістрант,
Ченюк Л. О., к.т.н., доцент*

Державний університет «Житомирська політехніка»

ОЦІНКА ПРОДУКТИВНОСТІ МІКРОПРОЦЕСОРНОЇ СИСТЕМИ ДЛЯ ВИМІРЮВАННЯ МЕХАНІЧНИХ ПАРАМЕТРІВ ЕЛЕКТРОДВИГУНІВ

Заявками на обслуговування в системі для вимірювання механічних параметрів електродвигунів є вимірювальна інформація, що надходить на обробку з виходу ємнісного датчика сили в частоту f_D . Частота проходження запускаючих імпульсів на вході аналого-цифрового перетворювача:

$$f_{3П} = (nZk) / k_0,$$

де n – частота обертання приводного двигуна; Z – число градацій модулятора датчика кута; k – кількість вимірювань на одному кутовому положенні ротора; k_0 – коефіцієнт переліку лічильника ЛТО програмованого таймера частотного вимірювального каналу.

Період, проходження імпульсів ЗП, що генеруються апаратними засобами:

$$T_0^{A3} = k_0 \cdot 60 / nZk.$$

Максимальний час, необхідний для одержання одного вимірюного значення програмними засобами:

$$T_0^{ПЗ} = T_B + T_n^{обр} + T_{ви\check{e}}.$$

Час вимірювання T_B мікропроцесорного засобу

$$T_B = T_{обм} + T_{АЦП},$$

де $T_{обм}$ – час обміну інформацією між аналоговим вимірювальним каналом і центральним процесором МПС; $T_{АЦП}$ – час перетворення аналого-цифрового перетворювача.

Час попередньої обробки $T_n^{обр}$ необхідний для перетворення вимірювальної інформації до подання чисел у МПС.

Час обробки інформації визначається з раніше розглянутого алгоритму вимірювання пускового моменту:

$$T_{обр} = \sum Q_{ui} + \sum \Delta Q_{oi} + (\sum \bar{Q}_{ui} - \sum \Delta \bar{Q}_{oi}) / k + (360\alpha) / Z + WR_{озн}.$$

де $\sum Q_{ui}$ і $\sum \Delta Q_{oi}$ – час виконання операції підсумовування відповідно вимірних значень Q_{ui} і силу опору ΔQ_o ; $(360\alpha)/Z$ – час виконання операції визначення дійсного значення кута повороту; $WR_{озп}$ – час, необхідний для запису одного з дійсних значень в ОЗП; $(\sum \bar{Q}_{ui} - \sum \Delta \bar{Q}_{oi})/k$ – час виконання операції визначення дійсного значення пускового моменту.

$T_{n\bar{вв}}$ – час тривалості циклу обміну пристрою введення-виведення і центрального процесора; N – кількість вимірювань за один оберт приводного двигуна; b – кількість байт в одному рядку таблиці результатів вимірювання.

Таким чином, час, необхідний для одержання одного вимірюного значення пускового моменту складає:

$$T_o^{nc} = T_{обм} + T_{АЦП} + \sum Q_{ui} + \sum \Delta Q_{ci} + (\sum \bar{Q}_{ui} - \sum \Delta \bar{Q}_{ci})/k + \frac{360\alpha}{Z} + T_{n\bar{вв}} N b + T_n^{обп} + WR_{озп}$$

Якщо умова $T_o^{nc} \leq T_o^{AC}$ може бути виконана, то можливий режим реального часу. В противному разі необхідно: вибрати центральний процесор МПС з великою швидкодією; процес вимірювання і обробки інформації поділити, на першому етапі виміряти і запам'ятати усі значення в ОЗП, а на другому – обчислити і вивести результати. Є можливість виконати оцінювальний розрахунок параметрів T_o^{AC} і T_o^{nc} . Період імпульсів, що генеруються АЗ (при цьому параметри системи приблизно можна прийняти: $k_0=5$; $Z=2500$; $n=14$ об/хв; $k=16$): $T_o^{AC} = k_0 \cdot 60/nZk$. Після цього потрібно вибрати мікропроцесор, який би задовольнив вищезгаданим умовам.

Список використаних джерел

1. Подчашинський Ю.О., Магалецький Я.В. Інформаційно-вимірювальна система визначення пускового моменту двигуна з цифровою обробкою сигналів. Тези XIII Міжнародної науково-технічної конференції «Інформаційно-комп'ютерні технології», 30–31 березня 2023 р. Житомир : «Житомирська політехніка», 2023. С. 162-163.

2. Коваленко І. О., Магалецький Я. В. Мікропроцесорна система вимірювання пускового моменту електродвигунів. Вісник Житомирського державного технологічного університету. Серія «Технічні науки». 2005. № 4(35). С. 56-60.

УДК 621.317

*Подчашинський Ю. О., д.т.н., професор,
Радзівський Б. В., магістрант,
Чепюк Л. О., к.т.н., доцент*

Державний університет «Житомирська політехніка»

АЛГОРИТМІЧНЕ ЗАБЕЗПЕЧЕННЯ КОМП'ЮТЕРИЗОВАНОЇ СИСТЕМИ ДЛЯ ВИМІРЮВАННЯ ТА КОНТРОЛЮ ЯКОСТІ НАФТОПРОДУКТІВ

В процесі контролю якості нафтопродуктів необхідно визначати їх фізико-хімічні показники з метою порівняння до стандарту або технічних умов на даний продукт.

Лінія вимірювання показників якості призначена для отримання та видачі інформації за такими технологічними параметрами нафтопродукту, як тиск та температура нафти; щільність; відсотковий вміст вологи в нафтопродукті. Відбір проб може здійснюватися автоматично або у ручному режимі.

Вхідний нафтопровід блоку приєднується до щільного пробовідбірного пристрою (ПВП), що знаходиться на вхідному колекторі установки.

На вході в блок передбачено пристрій, що перемішує – статичний змішувач для створення однорідності середовища. Витрату нафти через блок забезпечує регулюючий клапан.

Розроблено комп'ютеризовану систему для вимірювання та контролю якості нафтопродуктів. Основними елементами системи є датчики та програмований логічний контролер.

Похибка вимірювального каналу 0,2 %.

Діапазон вимірювання щільності 0,5 ... 1 г/см³;

Точність вимірювання щільності – $\pm 0,2$ %;

Діапазон вимірювання температури 0... 100 °С;

Точність вимірювання температури $\pm 0,2$ %.

Розроблена система може застосовуватись у системах контролю, управління та збору даних на різних нафтопереробних підприємствах. Дана система дозволить збільшити продуктивність, підвищити точність та надійність вимірів, скоротити кількість аварій. Область застосування: нафтогазова та хімічна галузі.

Блок-схема алгоритму роботи комп'ютеризованої системи для вимірювання та контролю якості нафтопродуктів наведено на рис. 1.



Рис. 1. Блок-схема алгоритму роботи комп'ютеризованої системи для вимірювання та контролю якості нафтопродуктів

Список використаних джерел

1. Інструкція з контролювання якості нафти і нафтопродуктів на підприємствах і організаціях України [Електронний ресурс]. – Режим доступу: zakononline.com.ua/documents/show/278054___278119.

2. Подчашинський Ю.О., Чепюк Л.О., Омельчук І.А., Радзієвський Б.В. Комп'ютеризована система для вимірювання та контролю якості нафтопродуктів. Тези V Всеукраїнської науково-технічної конференції «Комп'ютерні технології: інновації, проблеми, рішення», 01-02 грудня 2022 р. – Житомир : «Житомирська політехніка», 2022. С. 342-344.

Секція 7
КОМП'ЮТЕРНО-ІНТЕГРОВАНІ ТЕХНОЛОГІЇ.
ПРИЛАДОБУДУВАННЯ

УДК 64.52

*Мельник М.М., магістрант,
Підтиченко О.В., к.т.н.*

Державний університет «Житомирська політехніка»

**ЛАБОРАТОРНА УСТАНОВКА АВТОМАТИЗОВАНОЇ
СИСТЕМИ КЕРУВАННЯ ТЕМПЕРАТУРОЮ НА ОСНОВІ
ПЛАТФОРМИ ARDUINO**

Задача керування температурою виконується у величезній множині виробничих процесів, починаючи від виготовлення хлібобулочних та кондитерських виробів, будівельних матеріалів, сушіння деревини, закінчуючи реалізацією задач керування мікрокліматом побутових та промислових приміщень.

Дослідження процесів керування температурою технічних та технологічних об'єктів, вибір законів керування, визначення показників якості систем керування тощо є важливими задачами, які виконуються при розробці систем керування, вміння виконувати їх є важливою частиною навчання майбутніх фахівців. Все це потребує наявності відповідного лабораторного обладнання (навчальних лабораторних стендів), що демонструють роботу відповідних процесів керування, в тому числі такого поширеного процесу, як керування температурою. Тому створення навчальних стендів та лабораторних установок для навчання майбутніх фахівців, проведення різного роду досліджень в межах освітнього процесу є завжди актуальною задачею. В роботі проаналізовано декілька технологічних процесів, що передбачають температурну дію на продукцію в межах певних конструкцій, де розміщується продукція. Моделлю таких просторових конструкцій може служити лабораторна термошафа, на якій можна досліджувати процеси, аналогічні тим, що відбуваються в промислових масштабах.

Все сказане визначило мету роботи, якою є розробка та побудова лабораторного стенду керування температурою у термошафі на основі апаратно-програмної мікропроцесорної платформи Arduino, що дозволяє виконувати дослідження процесів керування температурою для навчальних цілей. Для досягнення поставленої мети було виконано аналіз ряду технологічних процесів, що передбачають керування

температурою, виконано підбір елементної бази, розроблено структурну схему керування лабораторною установкою (рис.1), що надає загальне розуміння будови системи.

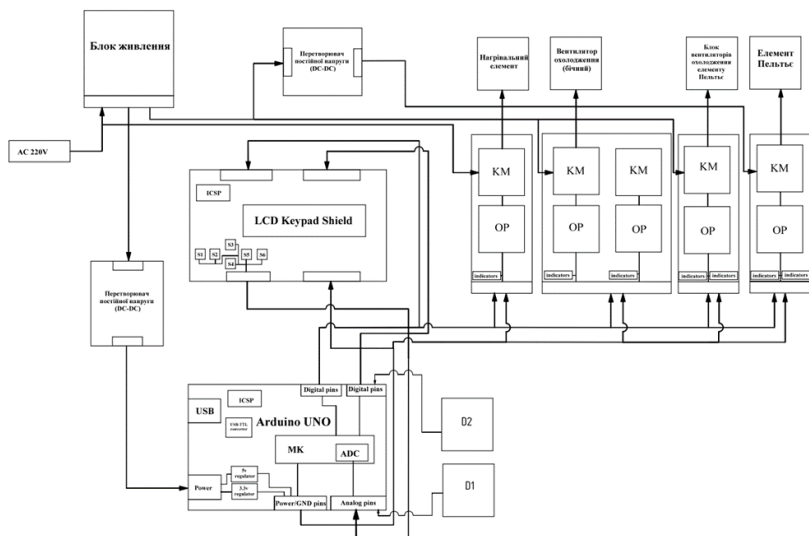


Рис. 1. Структурна схема системи керування лабораторної установки керування температурою у термошафі

Для реалізації розробки обрано модульну мікропроцесорну платформу Arduino, підібрано модулі та розроблено електричну принципову схему системи керування, алгоритмічне та програмне забезпечення для процесорного модуля. Для введення значень параметрів та спостереження за процесом функціонування передбачено пульт керування. Установка реалізує керування в чотирьох режимах за релейним законом та в двох – за пропорційним.

Установка може бути використана для навчальних та дослідницьких цілей, дозволяє досліджувати перехідні процеси, вплив параметрів законів керування на показники якості в різних режимах керування, вивчати методи ідентифікації об'єктів керування тощо.

Список використаних джерел

1. Температурний датчик водонепроникний DS18B20: [Електронний ресурс] – Режим доступу: <https://arduino.ua/prod414-temperaturnii-datchik-vodonepronicamii-ds18b20>.
2. LCD Keypad Shield 1602: [Електронний ресурс] – Режим доступу: <https://arduino.ua/prod235-lcd-keypad-shield>.

УДК 681.1

*Шавурський Ю.О., к.т.н., доцент
Державний університет «Житомирська політехніка»*

МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ТЕРМОАНЕМОМЕТРИЧНОГО ВИТРАТОМІРА ДЛЯ ВИМІРЮВАННЯ ВИТРАТИ АВТОМОБІЛЬНОГО ДИЗЕЛЬНОГО ПАЛИВА З ІНДУКЦІЙНИМ НАГРІВАЛЬНИМ КОНТУРОМ

Термоанемометричні витратоміри для вимірювання витрат потоку палива є актуальними на теперішній час, так як мають високу точність вимірювання. Ці витратоміри широко досліджувалися в різних сферах його використання і в даній конференції буде досліджено на основі вимірювання витрат автомобільного палива з деякими відмінностями від класичного ТАВ з контактним нагрівачем. Витрата палива – це виклик для кожного водія, в тому числі для підприємств, які мають великі власні автопарки, так як ціни на пальне у світі щороку підіймаються. Тому для контролю витрати палива і ефективнішого використання транспортних засобів було прийнято рішення використовувати термоанемометричний витратомір з індукційними нагрівальними елементами на вимірювальній ділянці трубопроводу.

Нагрівання теплоносія в ТАВ відбувається рівномірно – перепад температур в системі не більше 1 °С. Тобто локальні перегріву, здатні призвести до займання, відсутні, що робить такий вид нагрівання пожегобезпечним. Точність вимірювання витрат можна досягнути саме за рахунок інерційних складових, в даному випадку це за рахунок індукційного нагрівача. За рахунок енергоефективності індукційного нагрівача ця система перетворює до 90% витраченої енергії на корисне тепло, тоді як ефективність контактних нагрівальних елементів становить до 60%. Продуктивність, а саме швидкість нагрівання можна змінювати за рахунок індукційного процесу. Менш ніж за секунду тепло почне миттєво обгортати трубопровід і передавати тепло до палива, нагріваючи його за короткий проміжок часу. Крім того, сам цикл нагрівання можна контролювати через контролер управління, що дозволяє повністю автоматизувати процес разом з датчиками потоку палива.

Пристрій індукційного нагріву по суті включає: джерело електричного живлення, що включає, як правило, генератор середньої або високої частоти, перетворювач, що дозволяє створювати електричні струми з потрібною частотою, адаптаційний

трансформатор, необхідний для регулювання напруги і батареї конденсаторів, нагрівальний індуктор, навантаження, що підлягає нагріванню, система охолодження індуктора та інших компонентів живлення, органи управління та керування. Структурна схема робота ТАВ з індукційним нагрівачем має наступний вигляд, рис. 1.

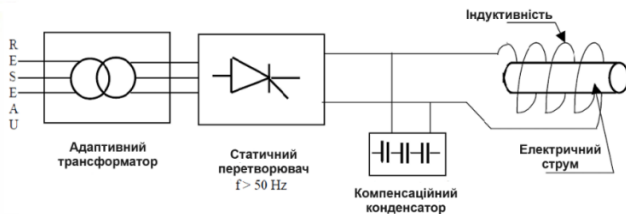


Рис. 1. Структурна схема ТАВ з індукційним нагрівачем

Математична модель описується диференціальним рівнянням з частковими похідними, які описують електромагнітні та теплові явища систем, для двовимірного циліндричного випадку, які можна описати наступним виразом:

$$\frac{\partial}{\partial z} \left(\frac{v}{r} \frac{\partial A}{\partial z} \right) + \frac{\partial}{\partial r} \left(\frac{v}{r} \frac{\partial A}{\partial r} \right) - Jw \frac{\sigma}{r} A = -J(1)$$

Перевагою цього нагрівального елемента є підвищення точності за рахунок інерційності нагрівання палива в трубопроводі з недопусканням його перегріву, так як сам індукційний елемент працює безконтактним методом. Недоліком даного методу є саме вартість індукційного нагрівача з повним комплектом його підключення до генератора середньої або високої частоти, а також перетворювальні елементи.

Проведене моделювання дослідного зразка витратоміра палива диференціальним методом вимірювання показали, що рівень вихідного сигналу достатній для проведення вимірювань витрати палива в широкому діапазоні значень. Загалом отримані результати важливі для проектування, виробництва та оптимізації витратомірів палива.

Список використаних джерел

1. Безвесільна О.М., Шавурский Ю.О. Високоточний термоанемометричний витратомір з цифровою обробкою вимірювальної інформації. Матеріали Всеукраїнська НПК присвячена Дню науки, Житомир, 2014. с. 98-99.

2. Chaboudez C., Clain S., Glardon R., Rappaz J., Swierkosz M., Touzani R., Numerical modeling in induction heating of long workpieces, IEEE Trans. Magn., Vol. 30, No. 6, pp. 5028-5037, Nov. 1994.

УДК 681.5

*М'янівський В. М., магістрант,
Гуменюк А. А., к.т.н., доцент
Державний університет «Житомирська політехніка»*

АВТОМАТИЗОВАНА СИСТЕМА КОНТРОЛЮ ТА РЕЄСТРАЦІЙ ВІБРАЦІЙ ПРИ ЗЕМЛЕТРУСІ

Землетрус є непередбачуваним і неминучим природним явищем, що часто завдає шкоди життю та майну людей. Ми не можемо з цим боротися, але можемо розпізнавати загрозу заздалегідь, використовуючи технології, які можуть захистити нас і нашу промисловість.

Однією із очевидних сфер, де необхідно передбачити землетрус – є промислові і житлові об'єкти в районах з частими і можливими сейсмічними поштовхами. Варто додати, що під час землетрусу, окрім природної катастрофи, як наслідок, може виникнути наступна техногенна. Тож проблема інформування про можливість настання землетрусу є дуже важливою і актуальною.

Існуючі аналоги, які фіксують вібрації, за допомогою вбудованих реле, здатні вимикати різні промислові прилади, такі як газові труби, печі для плавки металів. Пропонується використати прилад, який призначений для побутового користування та моніторингу наявності вібрації.

Метою розробки є автоматизована система контролю та реєстрації вібрацій при землетрусі, яка фіксуватиме вібрації та після обробки даних попереджуватиме про землетрус.

Завдання, які постали під час дослідження, є:

- розробка технічного завдання;
- аналіз існуючих систем контролю та реєстрації вібрацій при землетрусі;
- обґрунтування та вибір складових системи;
- розробка структурної, функціональної та принципової схем;
- побудова алгоритму системи та написання програми;
- побудова друкованої плати;
- розрахунок показників надійності системи.

Актуальність даної теми полягає в тому, що розроблювана система використовується для контролю та реєстрації вібрації при землетрусі, що дозволить запобігти катастрофі завдяки своєчасному інформуванню.

Призначенням та областю застосування даної розробки є:

автоматизована система, яка повинна контролювати, реєструвати вібрацій при землетрусі та виводити повідомлення про землетрус.

Областю застосування також є використання в промисловості і житлових об'єктах в районах з частими і можливими сейсмічними поштовхами.

Умови експлуатації:

- температура навколишнього середовища від 0 °С до + 50 °С.
- відносна вологість до 80 % при температурі + 25 °С;
- атмосферний тиск 600-800 мм рт. ст.;
- хімічно активні компоненти присутні;
- вібрація, тряска, удари присутні;
- характер роботи безперервний;
- напруга живлення – 5В.

Під час проведених досліджень в Державному університеті «Житомирська політехніка» було розроблено структурну схему, на базі якої були вибрані всі необхідні комплектуючі. Розроблено функціональну схему. Розроблено схему електричну принципову та друковану плату відповідно. Розроблений алгоритм роботи системи та написана програма для даної системи.

Розроблена система має ряд переваг, серед яких: дешевизна, простота та легкість обслуговування. Але можливий ряд подальших модернізацій, таких як:

- підвищення звукової та світлової індикації для оповіщення більшої кількості населення;
- безпроводну передачу оповіщення на смартфон;
- реалізацію автоматичного відключення інших систем при явній загрозі землетрусу.

Список використаних джерел

1. Дуднікава І. І. Безпека життєдіяльності: навч. посібник – К.: Вид-во Європ. ун-ту, 2003. – 268 с.
2. R. Carter, P. Duffey, S. Bachorski, M. Kagi, H. Havlicsek. Weighted Least-Squares Based Control for a Four Axis Gimbal Set / Proceedings of SPIE. – 2010. – Vol. 7663. – P. 1–12

УДК 681.5

*Кашиуренко Б. О., магістрант,
Гуменюк А. А., к.т.н., доцент
Державний університет «Житомирська політехніка»*

АВТОМАТИЗОВАНА СИСТЕМА УПРАВЛІННЯ ВАНТАЖНОЮ ПЛАТФОРМОЮ З ВИКОРИСТАННЯМ МАШИННОГО НАВЧАННЯ

Сучасний розвиток технологій та автоматизації транспортних та логістичних процесів вимагає нових підходів до управління вантажними платформами, які стають все більшими та складнішими. Автоматизовані системи управління здійснюють збільшення продуктивності та зниження ризиків у різних галузях їх застосування. Тому сучасні науковці перебувають в постійному пошуку способів автоматизації та оптимізації управління цими платформами. Однією з ключових інноваційних технологій, що революціонізує управління вантажними платформами, є машинне навчання.

Машинне навчання – це галузь штучного інтелекту, яка дозволяє системам аналізувати дані та вчитися на основі досвіду [1]. У контексті автоматизованих систем управління вантажними платформами, машинне навчання використовується для аналізу даних про вантаж, дорожні умови, трафік та інші фактори з метою прийняття оптимальних рішень.

Система управління вантажною платформою, де машинне навчання відіграє ключову роль в аналізі даних та прийнятті рішень для оптимізації роботи платформи має у своєму складі сенсори та датчики (такі як gps, акселерометри, камери, радары, термометри тощо), які передають дані для початку роботи. Далі отримані дані передаються до центральної системи, що включає в себе алгоритми машинного навчання та базу даних для зберігання історичних даних, з метою обробки, аналізу, прийняття рішень та керування платформою, яке відповідає за фізичне керування платформою, включаючи керування двигунами, рульовими системами, гальмами тощо.

Для спілкування з оператором або користувачем системи створюється візуальний інтерфейс, який відображає дані та стан платформи. Крім того, система може взаємодіяти з іншими транспортними засобами, інфраструктурою доріг, а також з центральними системами управління трафіком.

Дані про роботу системи використовуються для вивчення, оптимізації та вдосконалення алгоритмів машинного навчання, що

дозволяє системі покращувати свою продуктивність та адаптуватися до змінних умов.

Використання алгоритмів машинного навчання відкриває широкий ряд можливостей для покращення управління вантажними платформами. По-перше, воно дозволяє платформам прогнозувати навантаження, розподіляти вантаж оптимальним чином та планувати маршрути. Це призводить до зменшення витрат пального, покращення продуктивності та зниження часу доставки.

По-друге, машинне навчання дозволяє системі в реальному часі аналізувати дорожні умови, виявляти перешкоди та небезпеки на дорозі. Це допомагає уникнути аварій та збитків, забезпечуючи вищий рівень безпеки для вантажів, автівок та людей.

Крім того, системи управління, побудовані на основі машинного навчання, можуть навчатися на основі досвіду та адаптуватися до змінних умов, таких як зміни в погоді, трафіку та типах вантажу, що робить їх більш гнучкими та надійними.

Використання машинного навчання сприяє зменшенню потреби в людському втручанні у процес управління вантажною платформою, забезпечуючи більшу стійкість та надійність операцій, при цьому знижуючи рівень небезпеки та шкоди для життя та здоров'я людини.

Застосування машинного навчання в системах управління вантажними платформами призводить до зменшення витрат на обслуговування, підтримку та паливо, що сприяє ефективнішому використанню ресурсів і сталому покращенню показників.

Автоматизовані системи управління вантажними платформами з використанням машинного навчання представляють собою потужний інструмент для підвищення ефективності, безпеки та стійкості в транспортній та логістичній галузі. Вони дозволяють оптимізувати управління вантажними платформами, знижувати ризики та ефективно використовувати ресурси. Машинне навчання відкриває нові можливості для інновацій та постійного покращення у цій галузі, що робить його однією з ключових сфер розвитку в транспортній та логістичній індустріях.

Список використаних джерел

1. Григоров О.В., Аніщенко Г.О., Стрижак В.В., Петренко Н.О., Турчин О.В., Окунь А.О., Пономарьов О.Е. (2022). Artificial intelligence. Machine learning. Vehicle and Electronics. Innovative Technologies, (15), 17–27. [Електронний ресурс] – Режим доступу: <https://doi.org/10.30977/VEIT.2226-9266.2019.15.0.17>.

УДК 528.8

*Дубель М. В., магістрант,
Кириченко О. М., магістрант,
Кравчук А. Р., PhD, ст. викладач
Державний університет «Житомирська політехніка»*

АВТОМАТИЗОВАНА СИСТЕМА ВИЯВЛЕННЯ ПОЖЕЖ

Сьогодні застосування БПЛА є необхідним з точки зору забезпечення безпеки та економії витрат (у порівняння, наприклад, з застосуванням гелікоптерів чи літаків). Розроблені безпілотні літальні апарати можуть бути включені до складу сил і засобів з ліквідації надзвичайних ситуацій, а також можуть виявитися вкрай корисними, а часом й незамінними, при проведенні пошуково-рятувальних операцій на суші і на морі. При цьому є можливість оперативної заміни програмного забезпечення для реалізації різних задач одним й тим БПЛА (розпізнавання різних об'єктів) – наприклад, після роботи з пошуку уражених об'єктів та визначення їхніх координат перехід до пошуку груп людей, які необхідно знайти та врятувати.

Пожежі є серйозною загрозою для людського життя, навколишнього середовища та майна. Ефективний моніторинг наявності пожеж та потенційних джерел їх займання стає важливою складовою системи безпеки та збереження ресурсів. У зв'язку з цим, розробка і вдосконалення систем моніторингу пожеж має велике значення для сучасного суспільства.

Дані дослідження присвячені аналізу існуючих технічних рішень у галузі моніторингу пожеж та розробці нових підходів до використання безпілотних літальних апаратів (БПЛА) для виявлення та відстеження пожеж. У ході дослідження були проведені аналізи електричних принципів, функціональних характеристик та структурних аспектів систем моніторингу пожеж.

Одним із головних завдань цієї роботи було вивчення можливостей використання БПЛА у якості засобу моніторингу пожеж та визначення галузей, в яких цей підхід може бути особливо ефективним. Дослідження включало в себе аналіз характеристик БПЛА, їх технічних можливостей та вимог до сенсорів для виявлення пожеж. Крім того, у роботі були створені прототипи моделей для вивчення можливостей та переваг використання БПЛА у сфері моніторингу пожеж. Ці прототипи дозволили провести детальні дослідження щодо точності та надійності виявлення пожеж за допомогою безпілотних літальних апаратів.

В даній роботі також буде розглянуто, яким чином використання БПЛА може полегшити відстежування пожеж та зменшити ймовірність їх появи, сприяючи ранньому виявленню та швидкому реагуванню на пожежні загрози.

Отже, ця робота має на меті внести важливий внесок у розвиток систем моніторингу пожеж, використовуючи передові технології БПЛА та надійшовши до розуміння їх потенціалу у забезпеченні безпеки та збереженні навколишнього середовища.

Науковцями Державного університету «Житомирська політехніка» було розроблено автоматизовану систему управління моніторингу пожеж, та їх ймовірного займання на базі БПЛА. Проведений аналіз існуючих технічних рішень. Також були розглянуті сфери використання БПЛА. Розглянуто, яким чином використовувати БПЛА в якості моніторингу пожеж.

Були розроблені та створені наступні схеми: структурна, функціональна, електрична принципова та алгоритм роботи системи. Було визначено, що питання використання БПЛА в якості моніторингу потрібно розвивати та розглядати в подальшому.

Список використаних джерел

1. Ткачук А.Г., Коваль А.В., Гуменюк А.А., Богдановський М.В. Автоматизована система моніторингу наявності шкідливих та вибухонебезпечних газів на основі міні безпілотних літальних апаратів: монографія з грифом Державного університету «Житомирська політехніка». Житомир : «Житомирська політехніка», 2021. 145 с.

2. Ткачук А.Г., Безвесільна О.М., Добржанський О.О., Гуменюк А. А., Янчук В.М. Налаштування польотного контролера та системи стабілізації безпілотного літального апарата із системою моніторингу наявності пожеж та витоків теплової енергії на борту. Науковий журнал «Технічна інженерія». 2022. №2 (90). С. 59-69.

3. Гуменюк Р.П., Гуменюк А.А., Ткачук А.Г. Побудова систем зв'язку безпілотних літальних апаратів для передачі інформації на великі відстані. Тези Всеукраїнської науково-практичної online конференції аспірантів, молодих учених та студентів, присвяченої Дню науки, 15-19 травня 2023 року. Житомир: «Житомирська політехніка», 2023. С.116-117.

4. Ткачук Д.Ю., Ткачук А.Г., Кравчук А.Р., Неведров М.О. Моніторинг пожеж з використанням алгоритмів YOLO. Тези Всеукраїнської науково-практичної online конференції аспірантів, молодих учених та студентів, присвяченої Дню науки, 15-19 травня 2023 року. Житомир: «Житомирська політехніка», 2023. С.121.

УДК 681.5

*Стрельченко І. М., магістрант,
Ткачук А. Г., к.т.н., доцент
Державний університет «Житомирська політехніка»*

АВТОМАТИЗОВАНА СИСТЕМА УПРАВЛІННЯ ПРОЦЕСОМ ДОЗУВАННЯ КОМПОНЕНТІВ МАРГАРИНУ

Маргарина промисловість – одна з галузей масложирової промисловості, покликана організувати вироблення твердих харчових жирів в основному з рослинних олій з добавкою деякої кількості тваринних жирів. Вона за складом і властивостями багато в чому перевершує вершкове масло, наприклад за змістом поліненасичених жирних кислот, також званих есенціальними (не заміної) які є важливим компонентом і надають лікувальну профілактичну дію для організму людини.

Маргарин – продукт на основі рослинних олій, води, емульгаторів з додаванням ароматизаторів. Маргарин широко використовується в якості інгредієнту для приготування багатьох блюд. Він являє собою фізико – хімічну систему, один з основних компонентів якої – вода (дисперсна фаза) – розподіляється в іншому – маслі (дисперсійне середовище) у вигляді найдрібніших часток, утворюючи емульсію типу «вода в маслі».

Процес виробництва маргарину на ряді ділянок вимагає дозування компонентів – при надходженні жирів з масло-зливної станції до рафінаційного цеху, при приготуванні сумішей жирів, додаванні маргарину та харчових жирів за певним рецептом.

Автоматизація виробництва є найважливішим чинником прискорення науково-технічного прогресу у виробництві продуктів харчування. Подальші розвиток промисловості вимагає створення автоматизованого обладнання, автоматизованих ліній, технологічних процесів.

Актуальність даної теми полягає в проведенні автоматизації технологічного процесу виготовлення маргарину на етапі дозування та змішування компонентів шляхом розробки системи керування на основі промислової автоматики – програмованих логічних контролерів та панелей візуалізації.

Для досягнення поставленої мети виконано ряд задач:

– проаналізовано технологію виробництва, визначити об'єкта автоматизації;

- визначено керовані параметри, розробити функціональну схему автоматизації;
- обрано необхідні елементи автоматики, розроблено структурну схему системи керування;
- розроблено алгоритмічне забезпечення контролера системи керування.

Система управління призначена для реалізації наступних функцій:

- 1) автоматичне дозування жирових і водно-молочних компонентів на вагах відповідно до рецептури;
- 2) можливість зберігання та редагування всіх необхідних рецептур продукції;
- 3) автоматична перекачування компонентів, відміряних згідно з рецептом, з ваг на підготовчі змішувачі, автоматична циркуляція (емульгування) і перекачування продукту в робочий бак;
- 4) можливість виконання всіх операцій в покрововому (при натисканні на кнопку операції) і в ручному режимах;
- 5) можливість проведення миття лінії в ручному режимі;
- 6) оперативний контроль процесу приготування маргарину з екранів робочих станцій за допомогою реалізованих у кольоровому виконанні фрагментів мнемосхем технологічного процесу;
- 7) аварійна сигналізація при виході технологічних параметрів за нижні і верхні межі встановлених технологічних та аварійних меж;
- 8) фасування продукції в контейнери на фасувальній машині в автоматичному режимі і можливість роботи в ручному режимі;
- 9) збереження звітів по вазі.

Основними цілі створення даної системи управління є:

- підвищення якості продукції;
- підвищення точності дозування відповідно до рецептури;
- підвищення точності наповнення контейнерів на фасувальній машині;
- підвищення продуктивності ліній приготування та фасування маргарину;
- зниження матеріальних витрат за рахунок підвищення оперативності і точності управління.

Список використаних джерел

1. ДСТУ 4465:2017 «Маргарин. Загальні технічні умови.». Вид офіц. Київ: ДП «УкрНДНЦ». 2016. [Чинний від 2016-07-01]. 51 с.
2. Демидов І.М. Споживчі властивості харчових жирових продуктів / Демидов І.М., Тимченко В.К. – Харків: НТУ «ХПІ». 2004. 172 с

УДК 623.746

*Онуфрійчук О. С., магістрант,
Ткачук А. Г., к.т.н., доцент,
Добржанський О. О., к.т.н, доцент
Державний університет «Житомирська політехніка»*

РАДИОКЕРОВАНІЙ FPV БПЛА З МОЖЛИВОСТЯМИ ВЕРТИКАЛЬНОГО ЗЛЕТУ ТА ПРИЗЕМЛЕННЯ

У сучасному світі на допомогу людині все частіше і частіше приходять роботи та роботизовані механізми, які дозволяють виконувати роботу в складних або навіть небезпечних умовах праці, дозволяють заощаджувати ресурси та скорочувати час на виконання тих чи інших задач.

Один з напрямків, який дуже швидко розвивається і набуває великої популярності та розповсюдженості є БПЛА (безпілотні літальні апарати). БПЛА дозволяють отримувати доступ до важкодоступних або небезпечних місць, наприклад, для збору інформації, розвідки, надання допомоги в надзвичайних ситуаціях, доставки товарів та багатьох інших сфер. БПЛА можна використовувати для вирішення бізнес задач таких як фото, відео зйомка, моніторинг певних робочих процесів, доставка товарів. Можна використовувати для досліджень таких як, наприклад, моніторингу навколишнього середовища, вивчення погодних умов, геологічних формувань, вивчення поведінки тварин тощо.

БПЛА можна класифікувати за різними критеріями, такими як розмір, призначення, характеристики та технічні можливості:

- мікро- і міні-дрони: Це невеликі безпілотні апарати, які можуть мати розмір від декількох сантиметрів до декількох метрів;

- мультироторні дрони: БПЛА, які складаються з багатьох пропелерів із короткими роторами, таких як квадрокоптери, гексакоптери або октокоптери. Вони мають високу маневреність і здатні стояти на місці у повітрі;

- фіксованоспрямовані дрони: мають жорстку конструкцію і рухаються вперед за допомогою крил або гвинтів;

- вертольотоподібні дрони: мають кілька роторів, що надає їм здатність до вертикального зльоту та посадки, а також політ уперед.

Авторами пропонується розробити проєкт БПЛА з використанням технологій FPV (First Person View) та системи вертикального злету та приземлення VTOL (Vertical Take Off and Landing).

Зазвичай, система FPV складається з камери, яка знаходиться на БПЛА, передавача зображення та приймача, який може бути підключений до відеогарнітури або екрана. Оператор може отримувати зображення з камери в реальному часі, що дозволяє керувати апаратом більш точно та реагувати на будь-які зміни. Система VTOL робить БПЛА більш гнучкими і здатними працювати в обмежених просторових умовах, таких як міські або недоступні території, де немає довгих злітно-посадкових смуг. Ця технологія стає все більш важливою для розвитку безпілотних систем у різних галузях, від комерційного використання до військових додатків.

До розробки та реалізації БПЛА будуть входити наступні етапи:

1. Визначення та формалізація вимог до БПЛА. Описання цілей та задач для яких буде використовуватись БПЛА, опис вимог щодо максимальної швидкості, дальності польоту, маси, вантажопідйомності, тривалості польоту тощо.

2. Розробка концепції побудови БПЛА. Розробка концептуального дизайну БПЛА, створення 3Д моделі. Прорахунок та визначення форми несучого каркасу, розміру та форми крил, конфігурація фюзеляжу та хвостової частини, розробка вертикальних злітно-посадкових пристроїв, тощо.

3. Розробка електронної схеми, що включає в себе електронну плату керування, пристрій для збору даних та передачі їх на землю, а також компоненти для стабілізації та керування польотом літака.

4. Компоненти БПЛА. Збір та виготовлення всіх необхідних компонентів для складання БПЛА, включаючи елементи корпусу БПЛА, електронні компоненти та необхідне додаткове обладнання.

5. Підготовку та налаштування програмного забезпечення для БПЛА та збору інформації з ПК або мобільного пристрою, що дозволяє пілотувати на відстані та зручному для пілота місці, що збільшує комфорт і безпеку пілотування.

Список використаних джерел

1. Готов В. М., Фис М. М. та ін. Застосування БПЛА у військовій справі та аерозніманні. Львівська політехніка. 2022. 196 с.

2. Ткачук А.Г., Безвесільна О.М., Добржанський О.О., Гуменюк А. А., Янчук В.М. Налаштування польотного контролера та системи стабілізації безпілотного літального апарата із системою моніторингу наявності пожеж та витоків теплової енергії на борту. Науковий журнал «Технічна інженерія». 2022. №2 (90). С. 59-69.

3. Ткачук А.Г., Коваль А.В., Гуменюк А.А., Крижанівська І.В., Левчук В.О. Експериментальні дослідження автоматизованої системи моніторингу наявності шкідливих та вибухонебезпечних газів на базі БПЛА. Науковий журнал «Технічна інженерія». 2021. № 2(88). С. 55-62.

УДК 681.5

*Самойленко Б. Ю., магістрант,
Крижанівська І. В., к.т.н., доцент
Державний університет «Житомирська політехніка»*

ЕЛЕКТРОННІ СИСТЕМИ РОЗУМНОГО БУДИНКУ З ПІДВИЩЕНОЮ ЕФЕКТИВНІСТЮ

Розумний будинок – це концепція, що передбачає використання різноманітних технологій для автоматизації та оптимізації різних аспектів побутового життя в будинку. Основна мета полягає у створенні комфортного, ефективного та безпечного життєвого простору для мешканців.

Ключові аспекти концепції «розумного будинку»:

1. Автоматизація побутових процесів: використання систем автоматизації для управління освітленням, опаленням, кондиціюванням повітря, водопостачанням та іншими елементами життєвого середовища. Це може включати в себе сенсори, програмні рішення та зв'язок з мережею Інтернет речей (IoT).

2. Розумні пристрої та домашні системи – використання різноманітних розумних пристроїв, таких як розумні термостати, домашні асистенти (наприклад, голосові асистенти), системи безпеки з відеоспостереженням, замки з можливістю віддаленого управління.

3. Енергоефективність: використання технологій для збереження енергії, таких як сонячні батареї для виробництва електроенергії, енергоефективні освітлювальні системи та інші рішення для зменшення споживання енергії.

4. Інтеграція інформаційних технологій: застосування різноманітних програмних рішень та платформ для керування різними аспектами життя в будинку через смартфони, планшети або інші пристрої (рис. 2).

5. Забезпечення безпеки та захисту даних – це заходи безпеки, які включають в себе захист від потенційних кіберзагроз та забезпечення захисту особистих даних.

Ці концепції та технології постійно розвиваються, щоб забезпечити власникам будинків більше зручності, ефективності та безпеки у повсякденному житті.

Ці системи розумного будинку спрямовані на оптимізацію споживання ресурсів, забезпечення комфорту, безпеки та зниження витрат на утримання будинку, що робить життя в такому будинку більш зручним та ефективним.



Рис. 1. Керування «розумним будинком» з телефона

Економія ресурсів у розумному будинку є однією з ключових переваг цієї технології. Ось деякі способи, які сприяють ефективному використанню ресурсів:

1. Енергоефективність:

- автоматизація освітлення: використання сенсорів руху або світлових датчиків для автоматичного увімкнення та вимкнення освітлення в приміщенні в залежності від присутності людей.

- регулювання температури.

- використання сонячних батарей.

2. Управління водою:

- ефективне поливання: використання систем автоматичного поливу, які регулюють час та кількість використовуваної води відповідно до погодних умов і потреб рослин.

- виявлення витоків: встановлення датчиків витоків води, які швидко виявляють проблеми та зменшують втрати води.

3. Управління відходами: роздільний збір відходів, а саме, автоматизовані системи роздільного збору відходів для ефективної переробки та використання вторинних матеріалів.

4. Оптимізація ресурсів через IoT: використання мережі IoT для збору та аналізу даних щодо споживання ресурсів з метою оптимізації процесів.

Список використаних джерел

1. Чижевська М. А. Параметри інформаційної системи “Розумний будинок”. Наукові записки Державного університету телекомунікацій, № 4(56). 2019. С. 61-67.

УДК 681.1

*Палій О. О., магістрант,
Бондарчук В. М., ст. викладач,
Ткачук Д. Ю., асистентка*

Державний університет «Житомирська політехніка»

АВТОМАТИЗОВАНА СИСТЕМА ВИЛОВУ ПТАХІВ

Сьогодні важливим питанням є вилов птахів та контроль міграцій під час їх весняних та осінніх перельотів вздовж узбережжя морських акваторій, великих річок та водойм. Також, важливим аспектом є ефективний відлов домашніх птахів. У місцях зі значними скупченням птахів можливо розглядати встановлення спеціалізованих пасток для їх ефективного вилову. Проведення відлову та систематичний моніторинг міграції птахів сприяє контролю над розповсюдженням захворювань, що передаються через птахів.

Системи відловлювання птахів повинні бути спроектовані та використовуватися з урахуванням принципів гуманного ставлення, щоб не завдати шкоди життєдіяльності та здоров'ю птахів. Ретельне проектування та ефективна експлуатація таких систем не лише забезпечать ефективний відлов птахів, але й дозволять здійснювати максимально деталізований контроль та моніторинг міграції птахів.

У сучасному арсеналі інструментів для відлову птахів використовуються пастки у формі кліток, тобто механічні (рис.1 (а)), де приманкою є їжа. Також використовуються звукові приманки (рис.1. (б)), сприяючи приваблюванню птахів, які потім виловлюються за допомогою спеціальних сіток. Тому існує необхідність автоматизації цього процесу, де приманка та пастка інтегруються в єдиний механізм.



Рис. 1. Інструменти вилову птахів

Принцип дії механічних пасток ґрунтується на порушенні рівноваги конструкції внаслідок втручання птаха, що викликає активацію пускового механізму. Втручання може приймати дві форми: спроба птаха дістати приманку з пастки (приманкові), або зачеплення птаха сторожовою ниткою під час його руху (нитяні). Іноді птаха привчають до пастки, надаючи йому їжу та відпускаючи. За принципом дії виділяють механічно-утримуючі, ударні, давлячі, защемлюючі, здригаючі, поранюючі та інші типи механічних пасток, включаючи самостріли. Механічні пастки широко використовуються в контексті розвитку товарного хутового промислу.

Хоч деякі з цих методів є ефективними, але, нажаль, не є гуманними, тому науковцями Державного університету «Житомирська політехніка» було розроблено автоматизовану систему вилову птахів за використанням звукової приманки та пастки.

Автоматизована система відловлювання птахів розроблена з метою виконання ряду функцій, які включають:

1. Включення/виключення системи – робота системи за потреби;
2. Індикація при включенні системи – зелений світлодіод для маркування роботи системи.
3. Вибір мелодії для відтворення – в залежності від птаха, обирається звук.
4. Відтворення запису мелодії птахів – модуль звукового сигналу для приманки птахів.
5. Виявлення птаха в клітці – датчик руху для виявлення присутності птаха в клітці.
6. Зачинення клітки при наявності птаха – мотор для автоматичного зачинення клітки, якщо система виявляє присутність птаха.

Використання звукової приманки, датчика руху та мотора забезпечує ефективну роботу системи. Система автоматично реагує на присутність птаха, забезпечуючи його безпечний відлов. Результати роботи системи будуть корисні для вчених, які займаються вивченням міграції птахів та їх хворобами.

Список використаних джерел

1. Соколова Н.О., Белов А.С. Розробка програмного забезпечення IoT-системи на апаратній платформі Arduino. Applied questions of mathematical modelling, 3(2.1), 2020, 251-259. [Електронний ресурс] – Режим доступу: <https://doi.org/10.32782/KNTU2618-0340/2020.3.2-1.23>

УДК 681.5

*Дмитрук А. А., магістрант,
Турчук Д. О., магістрант,
Ткачук А. Г., к.т.н., доцент*

Державний університет «Житомирська політехніка»

СИСТЕМА АВТОМАТИЗОВАНОГО ТЕПЛОПОСТАЧАННЯ ЖИТЛОВОГО БУДИНКУ

Системи автоматизованого теплопостачання житлових будинків – це комплекс інженерних рішень, спрямованих на ефективне забезпечення опалення, гарячої води та кліматичного комфорту для мешканців. Використання ефективних опалювальних систем, таких як конвектори, підлогове опалення або радіатори з можливістю регулювання температури для кожної зони.

Встановлення систем "розумного будинку" для керування температурою, забезпечення комфорту та оптимізації енергоспоживання. Це може включати сенсори температури, програмне забезпечення для керування опаленням та кондиціонуванням.

Інтеграція сонячних колекторів для обігріву води або системи сонячних батарей для електропостачання для зменшення залежності від традиційних джерел енергії. Розробка системи, що дозволяє регулювати споживання енергії в залежності від піків навантаження або часу доби, що сприяє зниженню витрат.

Використання сучасних систем розподілу тепла, таких як системи з використанням теплових насосів чи гідрогеотермальні системи.

Застосування систем моніторингу, що дозволяють відслідковувати споживання енергії та ефективність системи, а також оптимізувати роботу системи для максимальної продуктивності та енергоефективності.

Науковцями Державного університету «Житомирська політехніка» було розроблено один з варіантів універсальної автоматизованої системи теплопостачання жилого будинку, яка може працювати у зв'язці як з газовим, так і з електричним котлом.

Автоматизована система теплопостачання повинна контролювати температуру та тиск в системі.

Було розроблено функціональну і принципову схему системи теплопостачання. Обрані комплектуючі для коректної роботи системи, а також розроблений алгоритм роботи.

Умови експлуатації:

- Температура навколишнього середовища від -35°C до $+90^{\circ}\text{C}$.
- Відсутність хімічно-активних компонентів.
- Відсутність ударів, тряски, екстремальних умов.
- Обов'язкове технічне обслуговування один раз на рік.
- Забезпечення безперебійної подачі електроенергії.

Технічні параметри системи.

Система повинна забезпечити наступні умови:

- Забезпечення комфортної температури на об'єкті;
- Аналіз отриманих даних та діагностика системи;
- Вмикання/вимикання циркуляційних насосів;
- Спрацювання звукової та світлової сигналізації при критичних

помилках роботи системи;

- Вивід значень на дисплей.
- Включення/виключення системи.

Вимоги до конструктивного оформлення:

Елементи системи управління: контролер, датчики тиску та температури, циркуляційні насоси, автоматичні запорно-регулюючі клапани, 3-х ходовий електричний клапан, блок живлення, кнопки для активації процесів, дисплей, сигналізація світлова та звукова. Мінімальне напрацювання на відмову системи складає не менше 26280 годин або 3 роки, при дотриманні сервісного обслуговування компонентів системи.

Список використаних джерел

1. Кирилович В.А., Покляченко О.В. Інноваційний підхід щодо побудови гібридних теплогенеруючих систем для побутових споживачів. Тези Всеукраїнської науково-практичної online конференції аспірантів, молодих учених та студентів, присвяченої Дню науки, 15-19 травня 2023 року. Житомир: «Житомирська політехніка», 2023. С. 74.

2. Матвійчук І.В., Покляченко О.В., Добржанський О.О. Огляд апаратної частини схеми стенду для дослідження примусового переносу енергії в системі повітря-повітря. Тези Всеукраїнської науково-практичної online конференції аспірантів, молодих учених та студентів, присвяченої Дню науки, 16-20, 26 травня 2022 року. Житомир: «Житомирська політехніка», 2022. С.48-49.

3. Добржанський О.О., Ткачук А.Г., Покляченко О.В. Розробка алгоритму функціонування системи керування рухомою роботизованою платформою для вимірювання теплових показників об'єктів дистанційно з використанням пульта. Журнал «Наука і техніка сьогодні». 2023. №9 (23). С. 569-582.

УДК 623.746

*Шапран Д. Я., магістрант,
Добржанський О. О., к.т.н, доцент,
Ткачук А. Г., к.т.н., доцент*

Державний університет «Житомирська політехніка»

СИСТЕМА АВТОМАТИЧНОГО СТЕЖЕННЯ ЗА ОБ'ЄКТАМИ НА ОСНОВІ ОБРОБКИ ДАНИХ ВІДЕОПОТОКУ

Сьогодні обробка відеоданих займає центральне місце в багатьох сферах життя, включаючи безпеку, транспорт та рекламу. Системи автоматичного стеження за об'єктами на основі обробки даних відеопотоку відіграють ключову роль у поліпшенні точності, ефективності та надійності таких систем. Метою роботи є розглянути основні аспекти розробки та застосування системи автоматичного стеження за об'єктами на основі обробки даних відеопотоку.

Система автоматичного стеження за об'єктами – це комплекс технологій та алгоритмів, які дозволяють виявляти, слідкувати та ідентифікувати об'єкти у відеопотоці. Вона базується на аналізі руху, виокремленні об'єктів та визначенні їх розташування у часі. Система може бути реалізована з використанням комп'ютерного зору, машинного навчання та глибинного навчання.

Ключові аспекти системи автоматичного стеження:

1. Детектування об'єктів: відеопотік аналізується з метою виявлення об'єктів на зображенні. Це може включати визначення розміру, форми, контуру або особливих особливостей, щоб визначити об'єкти для подальшого стеження.

2. Відстеження руху: після виявлення об'єкта система відстежує його рух по відеопотоці.

3. Аналіз поведінки: в деяких системах відбувається аналіз поведінки об'єктів, наприклад, передбачення траєкторій руху, розпізнавання змін поведінки або інші параметри, що вказують на певні дії.

4. Системи відбору сцен: деякі системи можуть відбирати або підкреслювати певні сцени або об'єкти для подальшого аналізу або спеціального втручання.

5. Використання машинного навчання: застосування алгоритмів машинного навчання, таких як нейронні мережі, для покращення точності відстеження та розпізнавання об'єктів у відеопотоці.

6. Застосування в різних сферах: застосовується в багатьох галузях, від відеоспостереження та безпеки до автономних автомобілів та виробництва.

Виявлення руху дозволяє відрізнити динамічні об'єкти від статичного фону. Виокремлення об'єктів з відеопотоку залежить від особливостей об'єктів та умов освітлення. Для точного визначення розташування об'єктів можуть використовуватись алгоритми, які враховують їхні траєкторії та зміни розміру.

Система автоматичного стеження за об'єктами повинна бути здатна аналізувати та валідувати дані, що надходять з відеопотоку. Це включає в себе виявлення шуму та аномалій, розпізнавання рухів та прогнозування траєкторій об'єктів. Точність, чутливість та швидкодія системи є важливими критеріями для її ефективності та надійності.

Системи автоматичного стеження за об'єктами на основі обробки даних відеопотоку є потужним інструментом, який сприяє покращенню точності, ефективності та надійності різноманітних систем. Розробка та застосування таких систем має великий потенціал у багатьох сферах життя, і дослідження в цьому напрямку є актуальним і перспективним.

Список використаних джерел

1. Павлюк Д.Ю., Добржанський О.О. Сегментація зображення для визначення об'єкта. / Тези Всеукраїнської науково-практичної on-line конференції здобувачів вищої освіти і молодих учених, присвяченої Дню науки, 11-15 травня 2020 року. Житомир : «Житомирська політехніка», 2020. С. 213.

2. Добржанський О.О., Лівіцький М.М. Застосування сучасних систем технічного зору для аналізу роботи промислових систем. / Тези II-ї Міжнародної науково-технічної конференції «Комп'ютерні технології: інновації, проблеми, рішення – 2017», 17–19 жовтня 2017 р. – Житомир: Вид. О.О. Євенок, 2017. – С. 146–147.

3. Добржанський О.О., Павлюк Д.Ю. Галузь використання технології ідентифікації руки. / Збірник тез доповідей II Всеукраїнської науково-практичної інтернет-конференції здобувачів вищої освіти і молодих учених «Інформаційно-комп'ютерні технології: стан, досягнення та перспективи розвитку», 14-15 листопада 2019 р. Житомир: Житомирська політехніка, 2019. С. 84-85.

4. Ткачук Д.Ю., Ткачук А.Г. Порівняння методів виявлення малих об'єктів за допомогою систем комп'ютерного зору на YOLO та SSD. / Тези доповідей XIII Міжнародної науково-технічної конференції «Інформаційно-комп'ютерні технології – 2023», 30-31 березня 2023 року. Житомир : «Житомирська політехніка», 2023. С.190-191.

УДК 681.5

*Безбородов Є. Ю., магістрант,
Янчук В. М., к.т.н., доцент,
Ткачук А. Г., к.т.н., доцент*

Державний університет «Житомирська політехніка»

АВТОМАТИЗОВАНА СИСТЕМА КЕРУВАННЯ ПРОЦЕСОМ ВИПІКАННЯ ХЛІБА У ТУПИКОВІЙ ПЕЧІ

Сучасні технології та автоматичні системи не лише полегшують та прискорюють процес приготування хліба, але й забезпечують однорідність якості продукції, виключаючи помилки та забезпечуючи відповідність стандартам безпеки та якості. Від використання точних рецептур до автоматичного контролю температури та часу випікання – автоматизація у сфері хлібопекарства переосмислює традиційні методи виробництва та відкриває нові горизонти у світі хліба.

У харчовій промисловості використовуються складні та трудомісткі технології, які потребують автоматизації. І сьогодні без сучасних систем автоматичного регулювання, які вловлюють напрям до зміни параметрів таких як температура в камері печі і відповідності керуючою роботою пальника, в печі не вдалося би стабільно підтримувати на заданому рівні температуру в камерах, що в свою чергу призводить до виробництва продукції з непотрібним якісним показником.

Нині на підприємствах існують такі хлібопекарські печі, де відсутні автоматизовані засоби контролю подачі повітряно-газової суміші в пальник, а керування температурою відбувається в ручну. Хлібопекарські печі можна класифікувати за різними критеріями, такими як принцип роботи, розмір, використання палива та функціональні можливості. Ось кілька типів хлібопекарських печей:

- піч з конвекційним нагрівом: використовує принцип конвекції, де повітря прогрівається та циркулює для рівномірного нагрівання продуктів. Забезпечує рівномірне печення та швидке приготування;

- піч зі спрямованим нагрівом: має спрямоване нагрівання зверху або знизу, що дозволяє контролювати температуру для різних типів хліба та випічки;

- піч з ротаційним пекарським листом: використовуються для автоматичного обертання хліба під час приготування для забезпечення рівномірного прожарювання;

- тунельні печі;
- вертикальні печі.

Тупикова піч, відома також як тунельна піч, є типом хлібопекарської печі, яка використовується для багатосерійного виробництва хліба, випічки, печива та інших хлібних виробів. Тупикова піч зазвичай має прямокутну форму, у якій продукти рухаються від входу до виходу через тунель. Вона оснащена конвеєрною системою, яка переміщує випічку через піч, що дозволяє пекарям ефективно керувати часом пекарня, температурою та іншими параметрами приготування. Вони зазвичай оснащені системами автоматичного контролю, які дозволяють регулювати температуру, швидкість конвеєра та інші параметри під час пекарського процесу.

Мета – автоматизація керування потужністю топки, витратами повітряно-газової суміші та контроль температури в зонах печі.

Для досягнення поставленої мети вирішено наступні задачі:

- розроблено структурну схему системи керування потужністю топки та витратами повітряно-газової суміші;
- розроблено функціональну схему системи керування потужністю топки та витратами повітряно-газової суміші;
- розроблено функціональну схему системи керування температурою у зонах печі.

Науковцями Державного університету «Житомирська політехніка» була розроблена автоматизована система керування процесом випічки хліба, зокрема керування потужністю топки, витратами газової суміші та регулювання температури у зонах печі. Було проведено вибір засобів автоматизації з конкретним підбором датчиків, витратомірів, клапанів, ЦАП та вибором регуляторів.

Список використаних джерел

1. Беспалюк Д. С., Підтиченко О. В. Автоматизована система управління піччю для випікання хлібобулочних виробів. / Тези доповідей V Всеукраїнської науково-технічної конференції «Комп'ютерні технології: інновації, проблеми, рішення», м. Житомир, 01–02 грудня 2022р. Житомир: Житомирська політехніка, 2022. С.389-390.

2. Дубченко К.О., Крижанівська І.В., Ткачук А.Г. Автоматизація технологічного процесу виготовлення хлібного квасу. / Збірник тез доповідей Всеукраїнської науково-практичної on-line конференції здобувачів вищої освіти і молодих учених, присвяченої Дню науки, 15-17 травня 2019 р. Житомир: ЖДТУ, 2019. С. 20.

3. Гвоздев О.В., Ялпачик О.В., Олексієнко В.О. Машини та обладнання хлібопекарського виробництва: Підручник, Мелітополь: ТОВ «Видавничий будинок», 2010. 317 с.

ЗМІСТ

**Секція 1. МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ТА РОЗРОБКА
ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ**

Чухов В.В., Варганова Д.О., Ващенко А.І.	Аналіз методів сортування масивів, порівняння швидкодій	3
Полоневич Д.В., Вакалюк Т.А.	Аналіз можливостей кросплатформового набору інструментів GTK при створенні відеоредактора	5
Блоха Я.С., Петросян Р.В.	PWA як один із сучасних підходів для створення мобільних застосунків	9
Гаманюк І.А., Петросян Р.В.	Особливості мови програмування rust	11
Болотіна В.В., Субчак Ю.Ю.	Оптимізація веб-додатків з використанням асинхронного програмування в JavaScript	13
Бондаренко А.В.	Дослідження UX на різних етапах циклу проектування	15
Варганова Д.О., Свістельник О.С., Локтікова Т.М.	Дослідження принципів побудови та проектування веборієнтованої системи трансферного ринку футболістів	17
Вакалюк Т.А., Власенко О.В., Василенко М.К.	Аналіз методів розпізнавання номерних знаків	19
Жовноватюк Р.М., Варшавський П.В.	Створення бази веб-орієнтирів у системі IP-геолокації	22
Яконюк А.В., Сугоняк І.І.	Автоматизовані системи контролю та моніторингу громадського транспорту	24
Андрєєв С.М., Шостак А.В.	Оцінка однорідності вибірок випадкових чисел платформи .Net	26
Огінський Є.В., Антонюк Д.С.	Метод Монте-Карло у моделюванні процесів управління персональними фінансами	28
Ожго Ю.А., Дацюк Д.В.	Round Robin Tournament алгоритм для генерації розкладу спортивної ліги	30

Хіміч В.О., Чижмотря О.В.	Аналіз форматів файлів для поширення за стосунків для ОС Android	33
Коренівська О.Л., Коротун О.В., Франчук В.О.	Гнучка система реєстрації в мобільному банкінгу за допомогою Server-Side Rendering (SSR)	35
Шануріна Д.С.	Сучасні методи дослідження UX	37
Чос А.С., Терещук С.О.	Алгоритми Ханойської вежі: аналіз та оптимізація в контексті розв'язання комбінаторних проблем	39
Кравченко С.М., Горбачевська Д.А.	Особливості юзабіліті тестування	41
Кравченко С.М., Ігнатов О.С.	Користувачький і клієнтський досвід: аспекти взаємодії з компанією	43
Кравченко С.М., Предчук Т.В.	Згортовка нейронна мережа для розпізнавання об'єктів	45
Кравченко С.М., Чуприна В.А.	Штучний інтелект для дослідження UX	48
Петришин А.О.	Шаблони сканування тексту	50
Кравченко С.М., Предчук Т.В.	Пошук зображень за допомогою комп'ютерного зору	52
Лобанчикова Н.М., Захаров Д.М.	Особливості розробки веб-систем для планування та організації процесу навчання	54
Плечистий Д.Д., Войтюк О.В.	Багатозалежні зв'язки у рекурсивній структурі фронтенд додатку	56
Секція 2. КОМП'ЮТЕРНА ІНЖЕНЕРІЯ ТА КІБЕРБЕЗПЕКА		
Котенко В.М., Пархомчук О.Ю.	Інтегрована система охоронно - пожежної сигналізації	58
Humeniuk I., Lahodnyi O., Kosheva I.	Information encryption method is based on a combination of cryptographic and steganographic properties of algorithms	60
Ячменьова С.О., Шелуха О.О.	Методи захисту Wi-Fi мереж від спуфінгу	62
Магурін О.О., Шелуха О.О.	Інфраструктура як код, хмарна інтеграція та нові тенденції	64
Дячук О.Ю., Єфіменко А.А.	Аналіз основних методів захисту комп'ютерних мереж	66

Goncharov M.	Modern frontend architectures analysis	70
Капітон А.М., Прокудін А.Ю.	Кібербезпека в епоху цифрової трансформації	72
Трокоз Є.М., Таргонський О.В.	Сучасні інструменти та технології соціальної інженерії	74
Трокоз Є.М., Сірик А.Ю.	Застосування безпечних API для обміну даними: методи та технології	76
Болотіна В.В., Адамчук Р. С.	Захист даних у веб-додатках створених за допомогою мови програмування Javascript	78
Поліщук С.М.	Аналіз вразливості браузера Google Chrome та необхідність додаткового захисту конфіденційних даних на вебсайтах	80
Поліщук С.М.	Passkeys – сучасна технологія аутифікації без пароля	83
Бродський Ю.Б., Сябрук М.О.	Роль соціальних мереж в забезпеченні кібербезпеки	86
Миколайчук В. В., Сфіменко А. А.	Дослідження методів підвищення відмовостійкості інформаційної системи на базі кластеру Kubernetes на прикладі Linux кластеру Azure Kubernetes Service	88
Матвеев К.І., Бродський Ю.Б.	Система моніторингу та управління теплопостачанням на основі концепції ІоТ	92
Кушнір І.В., Бродський Ю.Б.	Технологія захисту корпоративної мережі на основі системи виявлення та запобігання вторгнень Suricata	94
Мельник Р.І.	Використання блокчейн-технологій для забезпечення безпеки даних та автентифікації в онлайн-сервісах	96
Марчук Г.В., Сфіменко Д.А.	Дослідження особливостей форматів та типів даних сучасних компіляторів	98
Супруненко К.О., Шелуха О.О.	Перспективи та проблеми інтеграції квантових технологій у сучасні системи кіберзахисту	100

Луцевич М.О., Бродський Ю. Б.	Роль та вплив загального регламенту з захисту даних (GDPR) у сучасному цифровому світі	102
Чуприна В.А., Бродський Ю.Б.	Штучний інтелект у системі прийняття рішень	104
Ульяницький М.А., Бродський Ю. Б.	Підсистема захисту клієнт-серверної мережі від кібератак	106
Анчис А. О., Бродський Ю. Б.	Технологія захисту кінцевих вузлів	108
Добровольський Д.В., Бродський Ю.Б.	Захист ІТ-інфраструктури в умовах хмарних технологій	110
Бродський Ю.Б., Рудюк Б.М.	Підвищення ефективності та рівня безпеки корпоративної мережі на базі технології Cisco DMVPN	112
Умінський І.О., Бродський Ю.Б.	Оптимізація ефективності та забезпечення високого рівня безпеки корпоративної мережі за допомогою реалізації технології OpenVPN	114
Хоменко В.Р., Бродський Ю.Б.	Балансування навантаження та безпека: роль PFSense у високодоступних мережах	116
Головня О. С., Магурін О. О., Дехтяр М. С.	Добір віртуалізаційного програмного забезпечення для прототипу хмарної мережної інфраструктури	118
Ищук К.О., Покотило О.А., Щур Н.О.	Дослідження функціоналу, ефективності та безпеки криптографічних бібліотек у середовищі Javascript	120
Драчевський Н.В., Покотило О.А., Щур Н.О.	Застосування алгоритмів хешування для захисту паролів у програмах на мові Python	122
Пірог О.В.	Стандарти верифікації безпеки мобільних додатків	124
Колощук М.С., Дячук О.Ю.	LI-FI: технологія бездротового зв'язку через світло	127
Сушко Р.М., Пірог О.В.	Забезпечення кібербезпеки пристроїв на базі ОС Android	130

Ковальчук І.В., Бродський Ю.Б.	Міжмережевий екран нового покоління palo alto networks як новий підхід до захисту корпоративних мереж організацій	132
Герус В.А.	Хакерські угруповання	134

Секція 3. ІНФОРМАЦІЙНІ СИСТЕМИ ТА ТЕХНОЛОГІЇ

Мельник Р.І.	Автоматизоване тестування та якість програмного забезпечення: розробка методів для виявлення та усунення помилок в програмах	139
Стельмах А.О., Левківський В.Л.	Алгоритми взаємодії в інформаційних системах	141
Граф М. С., Райковський В. А.	Алгоритми оптимізації даних	143
Паламарчук М.П., Граф М.С., Колос К. Р.	Алгоритми синхронізації процесів в онлайн грі	145
Москалик О.С., Левківський В. Л., Колос К.Р.	Аналіз алгоритмів машинного навчання	147
Єфремов Ю. М., Павлішин М.С.	Аналіз причин використання мікросервісної архітектури в сучасних програмних рішеннях	149
Єфремов Ю. М., Павлішин М.С.	Аналіз тенденцій розвитку ринку музичних стрімінгових сервісів	151
Марчук Г.В., Дяченко В.В.	Важливість візуальної частини ігор	153
Коваленко Я.П.	Вибір архітектури програмного забезпечення	156
Кадькало В.В., Чижмотря О.В., Кузьменко О.В.	Використання методів машинного навчання для аналізу фінансових ринків	158
Штиль М.Р., Фуріхата Д.В.	Використання технології AI Upscaling у відеоіграх	160
Гайдай І.Я., Граф М.С.	Використання фреймворку Android Jetpack для спрощеного створення мобільних додатків	163

Горопашин О.С., Колос К.Р.	Використання штучного інтелекту та машинного навчання для оптимізації методів наукових досліджень	165
Фуріхата Д.В.	Генеративні моделі нейронних мереж	167
Варганова Д.О., Кушнір Н.О., Москаль М.В.	Генерація зображень за допомогою штучного інтелекту	169
Вольних І.В., Концидайло А.М.	Генерація тестових даних за допомогою штучного інтелекту для Restful API	171
Горницький О.В.	Дослідження психоемоційного стану розробників інтернет-магазину	174
Олексійчук М.В., Чижмотря О. В.	Етичні проблеми розвитку і використання технологій машинного навчання та NLP та підходи до їх вирішення	176
Байло О.В., Левченко А. Ю.	Застосунок GAEA: аналіз застосування алгоритмів в сучасних ІТ-системах	178
Карапет Б.В., Савіцький Р.С.	Знаходження відмінностей при порівнянні зображень з дрону, знаходження потенційної цілі	180
Венгловська Ю.В., Марчук Г.В., Колос К.Р.	Ідеальні лабіринти та алгоритми їх створення	183
Пількевич І.А., Гордієнко Ю.О., Мірошніченко С.І.	Методика автоматичного визначення осередку сейсмічної події трикомпонентною сейсмічною станцією	186
Менес Ю.В., Марчук Г.В., Колос К.Р.	Методологічні основи використання кольорів у інформаційно-комунікаційних технологіях	188
Марчук Г.В., Кірій Д.О.	Механіки та дизайн рівнів в жанрах «Metroidvania» та «Souls-Like»	192
Хіміч В.О., Чижмотря О.В.	Минуле, теперішнє та майбутнє способів розробки користувацьких інтерфейсів для ОС Android	195
Єфремов Ю.М., Крискун С.І.	Обґрунтування вибору інструментальних засобів для розробки веб-сайту	197

Крискун С.І.	Комп'ютерні технології: інновації, проблеми, рішення	198
Болотіна В.В. Панібратець О.Д.	Обробка зображень засобами Adobe Photoshop з використанням штучного інтелекту	199
Багрій В.В., Граф М.С.	Огляд методів та програмних засобів для оптимізації логістичних процесів у вантажних перевезеннях	201
Москалик О.С., Левківський В. Л.	Огляд алгоритмів машинного навчання	205
Петросян А. Р.	Організація тестування програмного забезпечення дрона	207
Праздніков В.О., Розбицький Р.Е.	Особливості та застосування графових баз даних	209
Кадькало В.В., Чижмотря О.В.	Перспективи та виклики інтеграції систем штучного інтелекту з рішеннями для управління контейнеризованими додатками	211
Карапет Л.В., Савіцький Р.С.	Платформа для навчання з обмеженими можливостями	213
Марчук Д.К., Олексюк О.С.	Проблеми та рішення в процесі 3D моделювання, UV розгортки та текстуригу	215
Туз В. І. Горелик. С.І.	Розробка побудови картографічної моделі за допомогою штучного інтелекту на основі даних ДЗЗ	217
Бадігон В.О., Левченко А.Ю.	Розробка програмного забезпечення в музичній індустрії	219
Свінцицька О.М., Бордюг Б.Л.	Роль формування вимог на розробку онлайн бібліотек в управлінні ІТ-проектами	221
Свінцицька О.М., Цурукіна Г.А., Іщенко В.В.	Роль цифрових інструментів у взаємодії фармацевтичних компаній з медичними практиками	223
Марчук Д.К., Лантвойт К. М.	Роль Discontainers в ігровій індустрії та користь їх використання в архітектурі проекту	225

Ясько Н.О., Лисенко М.С.	Спрощення процесів розвідки через використання штучного інтелекту для аналізу об'ємних даних	227
Кулешов Д.А., Граф М.С.	Фактори для розробки комп'ютерної гри в жанрі Horror у віртуальній реальності	229
Гарбич-Мошора О.Р., Городиський Б.І.	Характеристики рядкових величин в Javascript	231
Oleh Horopashyn, Kateryna Kolos	Adaptation of methodological strategies to changes in social and technological paradigms: new requirements and opportunities	233
Карітон А.М., Goncharov І.К.	An interpreted python language with distinctive dynamic typing	235
Zakharchuk Maksym, Oleksii Chyzhmotria	Designing a web-based fuzzy logic testing system	237
Терещук С.О., Дзюбанчук Б.С.	Object pool як засіб для оптимізації проекту	239
Maksym S. Sitailo, Andriy V. Morozov	Popular machine learning algorithms for cryptocurrency price prediction	241
Svistelnik O.S.	Selection and justification of the architecture for the development of an online service for ukrainian language courses	243
Кузьменко О.В., Бомблюк М.О.	Wave function collapse в розробці ігор	245
Левицький А.А., Левківський В.Л.	Патерн state як засіб для структуризації програмного коду	247
Марчук Г.В., Макуховська Д.А., Лімінович І.Д.	Дослідження проблем, з якими стикаються дизайнери рівнів у процесі розробки гри	249
Харченко А. В., Левківський В. Л., Колос К. Р.	Процедурна генерація ігрових світів	251
Ячменьова С.О., Марчук Г.В.	Використання розумних покажчиків в C++	253
Білецький С. В., Петросян Р. В.	Використання блокчейну для захисту інтелектуальної власності	255

Райковський В. А., Петросян Р. В.	Особливості використання мікроконтролерів у безпілотних повітряних суднах	257
Валецький М.С., Граф М.С.	Аналіз сучасних тенденцій використання штучного інтелекту при розробці інформаційних систем	259
Чалій О. В.	Системи керування координатно- вимірювальних машин	262
Дешков М.Ю., Марчук Г.В.	Напрямки використання нейронних мереж при обробці природної мови	265
Смутьський Д.З., Левківський В.Л., Колос К. Р.	Ігрові додатки у навчальному процесі	267

Секція 4. СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ТЕЛЕКОМУНІКАЦІЯХ ТА БІМЕДИЦИНІ

Шевченко К.Л., Яненко О.П., Клочко Т.Р.	Високочутливий вимірювач люмінесцентного випромінювання	269
Нестеренко К.О., Лещинський Ю.І., Андрєв О.В.	Особливості передавання цифрових даних з використанням бездротових технологій	271
Сторожук І.М., Коренівська О.Л.	Визначення ефективності гемодіалізу та гемодіафільтрації при хронічній нирковій недостатності	273
Ципоренко В.В., Мельниченко О.В.	Дослідження комбінованої мережі відео спостереження ТЦ ОЛДІ	275
Дубина О.Ф., Коваль М.В., Коваль Д.В.	Антенний трекер безпілотного літального апарату FPV	277
Дубина О.Ф., Коваль Д.В., Латко І.І.	Широкодіапазонний синтезатор частоти на ADF4351	279
Опанасюк К.С., Ципоренко В.Г.	Система попередження техногенних аварій	281
Борисевич О.Р., Коломієць Р.О., Манойлов В.П.	Аналіз можливості передачі медичних даних існуючими програмно – апаратними засобами	283

Чухов В.В., Павицький О.Ю.	Дослідження логоперіодичної антени з нестандартним кроком вібраторів	285
Свінцицька О.М., Мяновська М.В.	Роль стратегій управління ризиками в забезпеченні успіху проектів в галузі телемедицини	287
Чухов В.В., Ожегов І.Є.	Дослідження спіральної антени для поперечного випромінювання	289
Макарик Ю.С.	Дослідження можливості застосування радіомодулів NRF24L01 у сенсорній мережі	291
Грищенко Н.О.	Вимірювання температури з використанням ультразвукового датчика виміру відстані HC-SR04	293
Кушнірук В.Л.	Дослідження дистанційної системи моніторингу якості повітря у приміщенні	295
Вознюк С.І., Коренівська О.Л.	Система дистанційного керування мікрокліматом	297
Долматова М.С., Горелик С.І.	Використання даних ДЗЗ для аналізу штормових нагонів	299
Стародубцева В.В., Горелик С.І.	Збитки від військової діяльності лісгоспам Харківської області за даними ДЗЗ	301
Мілевський О.В., Манойлов В.П.	Методи та підходи технічного обслуговування систем та обладнання	303
Дзюба М.В., Нікітчук Т.М.	Методика інтеграції даних гібридних систем охорони з IoT технологіями «розумного будинку»	305
Сімчук А.Р., Нікітчук Т.М., Марцева Л.А.	Проблеми передачі та обробки медичних сигналів у телекомунікаційних системах	307
Твардовський Ю. В., Нікітчук С. М., Коренівська О. Л., Коротун О.В.	Огляд технологій розумного будинку	309
Коренівська О.Л.	Методи прогнозування розвитку цукрового діабету	311

Секція 5. ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ В ОСВІТІ

Гарбич-Мошора О.Р., Варварич Р.І.	Дистанційне навчання в умовах військового стану	313
Ковтун В.В., Чижмотря О.В.	Розробка інтелектуальної освітньої платформи з індивідуально адаптивними навчальними планами на основі штучного інтелекту	315
Ковтун В.В., Передалова А.Д., Чижмотря О.В.	Штучний інтелект в освіті	317
Козирева Т.А., Передалова А.Д., Чижмотря О.В.	Моделювання інформаційної системи для навчання з питань охорони праці	319
Антоненко Є.Д., Мінтій І.С.	Використання онлайн-редактора Canva в освіті	321

Секція 6. ЦИФРОВА ОБРОБКА СИГНАЛІВ В АВТОМАТИЗОВАНИХ ТА ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНИХ СИСТЕМАХ

Бугайов М.В.	Оцінювання частотних параметрів сигналів у панорамних системах радіомоніторингу	325
Бугайов М.В., Поздняков В.В.	Математична модель акустичних сигналів системи акустичного моніторингу повітряного простору	327
Вакарюк Я.А., Лугових О.О.	Комп'ютеризована система вимірювання ємності та індуктивності компонентів електронних схем	329
Вовк В. В., Лугових О.О.	Комп'ютеризована інформаційно- вимірювальна система контролю параметрів паперу	331
Лугових О.О., Уляницький В.П.	Комп'ютеризована система внутришньосхемних вимірювань опору	334
Подчашинський Ю.О., Гагін А.В., Чешок Л.О.,	Комп'ютеризована інформаційно- вимірювальна система для визначення та контролю параметрів виробництва харчових соусів	336

Подчашинський Ю.О., Чепок Л.О., Криворучко М.Г.	Огляд методів вимірювання кутової швидкості	338
Подчашинський Ю.О., Магалецький Я.В., Чепок Л.О.	Оцінка продуктивності мікропроцесорної системи для вимірювання механічних параметрів електродвигунів	341
Подчашинський Ю.О., Радзівський Б.В., Чепок Л.О.	Алгоритмічне забезпечення комп'ютеризованої системи для вимірювання та контролю якості нафтопродуктів	343

Секція 7. КОМП'ЮТЕРНО-ІНТЕГРОВАНІ ТЕХНОЛОГІЇ. ПРИЛАДОБУДУВАННЯ

Мельник М.М. Підтиченко О.В.	Лабораторна установка автоматизованої системи керування температурою на основі платформи Arduino	345
Шавурський Ю.О.	Математичне моделювання термоанемометричного витратоміра для вимірювання витрати автомобільного дизельного палива з індукційним нагрівальним контуром	347
М'янівський В.М., Гуменюк А.А.	Автоматизована система контролю та реєстрацій вібрацій при землетрусі	349
Кашпуренко Б.О., Гуменюк А.А.	Автоматизована система управління вантажною платформою з використанням машинного навчання	351
Дубель М.В., Кириченко О.М., Кравчук А.Р.	Автоматизована система виявлення пожеж	353
Стрельченко І.М., Ткачук А.Г.	Автоматизована система управління процесом дозування компонентів маргарину	355
Онуфрійчук О.С., Ткачук А.Г., Добржанський О.О.	Радіокерований FPV БПЛА з можливостями вертикального злету та приземлення	357
Самойленко Б.Ю., Крижанівська І.В.	Електронні системи розумного будинку з підвищеною ефективністю	359

Палій О.О., Бондарчук В.М., Ткачук Д.Ю.	Автоматизована система вилову птахів	361
Дмитрук А.А., Турчук Д.О., Ткачук А.Г.	Система автоматизованого теплопостачання житлового будинку	363
Шапран Д.Я., Добржанський О.О., Ткачук А.Г.	Система автоматичного стеження за об'єктами на основі обробки даних відеопотоку	365
Безбородов Є.Ю., Янчук В.М., Ткачук А.Г.	Автоматизована система керування процесом випікання хліба у тупиковій печі	367

Наукове видання

**Тези VI Всеукраїнської науково-технічної
конференції «Комп'ютерні технології:
інновації, проблеми, рішення»**

Житомир, 29-30 листопада 2023 р.

Відповідальний за випуск:

О.Л. Коренівська