Міністерство освіти і науки України,
ДНУ «Інститут модернізації змісту освіти»,
Національний технічний університет України «Київський політехнічний інститут ім. Ігоря Сікорського»,
Інститут кібернетики ім. В.М. Глушкова НАН України,
Інститут телекомунікацій і глобального інформаційного простору НАН України,
Інститут цифровізації освіти НАПН України,
Житомирський державний університет імені Івана Франка,
Житомирський військовий інститут імені С.П. Корольова,
Черкаський державний технологічний університет,
Вінницький національний технічний університет,
Опольська політехніка (Республіка Польща),
Варшавський технологічний університет (Республіка Польща),
Технологічний університет Лулео (Королівство Швеція),
Технічний університет (Чеська Республіка),
Технічний університет (Республіка Болгарія),
Університет країни Басків (Королівство Іспанія),
Віденський технічний університет (Республіка Австрія),
ADA University (Азербайджан)

ТЕЗИ ДОПОВІДЕЙ

XV Міжнародної науково-технічної конференції

Інформаційно-комп'ютерні технології

м. Житомир, 28-29 березня 2025 р.

Житомир
2025

УДК 004
Т11

Рекомендовано до друку Вченою радою Державного університету «Житомирська політехніка» (протокол № 6 від 24.03.2025 р.)

Тези XV Міжнародної науково-технічної конференції
Т11 «Інформаційно-комп'ютерні технології», м. Житомир, 28-29 березня 2025 р. – Житомир: Житомирська політехніка, 2025. – 352 с.
ISBN 978-966-683-698-7

Представлено доповіді учасників XV Міжнародної 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

ISBN 978-966-683-698-7

Наукове видання

Тези XV Міжнародної науково-технічної конференції «Інформаційно-комп'ютерні технології», Житомир, 28-29 березня 2025 р.

Відповідальний за випуск В.В. Болотіна

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

Секція 1
МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ТА РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

УДК 621.313

Бевз С.В., к.т.н., доцент, інженер відділення КЗ ІОЦ
Бурбело С.М., к.т.н., начальник відділення ПІЗ ІОЦ
Житомирський військовий інститут імені С.П. Корольова

АВТОМАТИЗАЦІЯ МЕТОДОЛОГІЇ РІВНОВАЖНОГО БАЛАНСУВАННЯ У РОЗРАХУНКАХ УСТАЛЕНОГО РЕЖИМУ ЕЛЕКТРИЧНОЇ МЕРЕЖІ

Актуальність сучасних засобів розрахункових процесів в енергетичних системах зростає у зв'язку з повсюдним запровадженням нових обчислювальних алгоритмів та сучасних методів, які дозволяють підвищити ефективність та точність розрахунків. В [1] нами було запропоновано використання нового методу рівноважного балансування для розрахунку усталеного режиму електричної мережі, який на відміну від існуючого традиційного підходу [2], дозволяє виконати розрахунок без вибору балансуючого вузла, у цьому разі наявний небаланс розподіляється рівномірно між усіма вузлами схеми.

Узагальнене рівняння стану відповідно до запропонованої методології набуде вигляду:

$$\begin{bmatrix} Ms \\ N * Zs \end{bmatrix} * \begin{bmatrix} I \\ Ig \end{bmatrix} = \begin{bmatrix} J \\ N \cdot Es \end{bmatrix},$$

де Ms та $Zs = diag(\{Z;1\})$ – доповнені за пропонованою методологією матриці інцидентності та матриця опорів віток:

$$Ms = \{M;1\} = \begin{pmatrix} M_{11} & \dots & M_{1m} & 1 \\ M_{21} & \dots & M_{2m} & 1 \\ \dots & \dots & \dots & 1 \\ M_{n1} & \dots & M_{nm} & 1 \end{pmatrix}, \; Zs = diag \begin{pmatrix} Z_1 \\ \dots \\ Zm \\ 1 \end{pmatrix} = \begin{pmatrix} Z_1 & 0 & 0 & 0 \\ 0 & \dots & 0 & 0 \\ 0 & 0 & Z_m & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

Ig – значення балансуючого струму, що дорівнює нулю при відсутності небалансу спожитої та генерованої потужності.

Розраховані за даною методологією значення струмів у вітках дорівнюють середньому арифметичному значенню струмів I_k, $k = \overline{1,n}$, визначених за класичним методом розрахунку з різними балансуючими вузлами [3]: $Is = \sum_{k=1}^{n} I_k \Big/ n$.

Модель розрахунку усталеного режиму за методологією рівноважного балансування проілюстрована на рис. 1 включає в себе функції та підпрограми мовою Python, а також бібліотеки numpy.

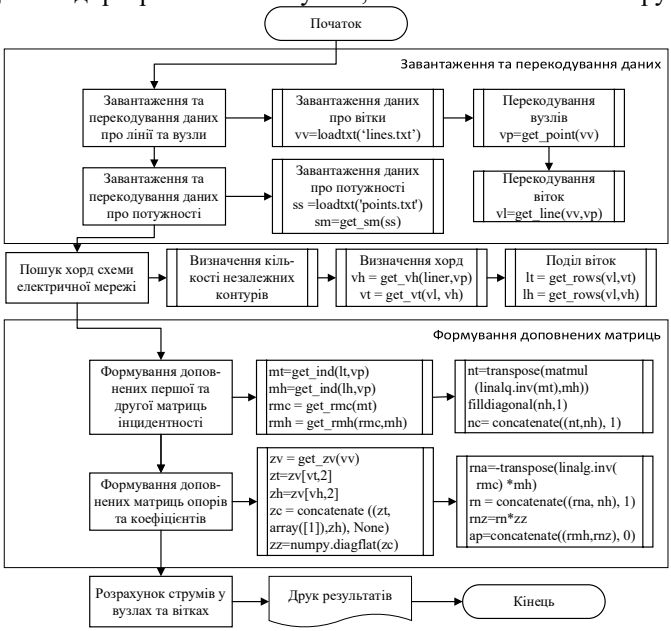


Рис. 1. Модель розрахунку усталеного режиму

На відміну від класичних підходів дана модель включає доповнення матриць інцидентності, діагональних матриць опорів та коефіцієнтів рівняння, а також розрахунок доповненого вектору струмів у вітках.

Висновок: в роботі розроблено засоби автоматизації методології рівноважного балансування для розрахунків усталеного режиму електричної мережі в програмному середовищі Python.

Список використаних джерел:

1. Бевз С. В., Бурбело С.М., Войтко В.В. Метод рівноважного балансування та автоматизація розрахунків усталеного режиму електричної мережі. Збірник наукових праць НУК. 2020. № 4 (482). С. 36-44. DOI: https://doi.org/10.15589/znp2020.4(482).5.

2. Кириленко О.В., Сегеда М.С., Буткевич О.Ф. Математичне моделювання в електроенергетиці : Підручник. Львів : НУ «Львівська політехніка», 2010, 608 с.

3. Бурбело М. Й., Бевз С. В., Кравець О. М. Математичні задачі електроенергетики : практикум. Вінниця : ВНТУ, 2021, 127 с.

УДК 004.7

Basystyi Ivan, master's student,
Vakaliuk Tetiana, Dr. Sc., prof.,
Chyzhmotria Oleksii, Senior Lecture
Zhytomyr Polytechnic State University

USE OF THE INTERNET OF THINGS IN LOGISTICS

Almost every day, we use various tag trackers and other devices that are integral components of the Internet of Things (IoT). These devices, which include smart tags, sensors, and connected gadgets, have become an essential part of our daily lives, often without us even realizing it. From tracking the location of personal items like keys and luggage to monitoring the health of equipment in factories, the reach of IoT is vast and growing.

For example, in the logistics sector, businesses rely heavily on IoT-enabled devices to track shipments' real-time movement, manage inventory, and monitor environmental conditions such as temperature and humidity during transport [1].

The first thing that comes to mind is vehicle location tracking, which allows you to monitor their movement online. This opportunity dramatically facilitates vehicle management and increases the efficiency of logistics operations. Through GPS trackers and sensors, IoT allows businesses to constantly receive up-to-date information about the location of vehicles, the status of their routes, and even the technical condition of vehicles in real time [2].

This can significantly improve transportation planning and organization, as companies can optimize routes, reduce fuel consumption, avoid traffic jams, and avoid unforeseen situations that could affect delivery times. In addition, constant monitoring allows for a quick response to technical problems or accidents, which helps to reduce downtime and mitigate risks.

Another example is using sensors to monitor temperature and pressure, which is especially important for transporting sensitive goods such as food, medicine, or chemicals. Thanks to IoT sensors that can be integrated into packaging or vehicles, companies can continuously monitor transportation conditions in real-time and receive alerts for deviations from established norms.

For example, when transporting vaccines or frozen foods, even slight temperature changes can lead to a loss of quality or safety. Thanks to temperature sensors that send data in real-time, companies can instantly detect problems, such as if the temperature in a container has dropped or risen beyond the permissible range. This allows them to take prompt action to remedy the situation, prevent losses, and ensure the safety of the cargo [3].

A promising option for improving the efficiency of cargo transportation is using smart containers, which allow for remote monitoring of cargo during transportation.

These containers are equipped with sensors that monitor important parameters such as temperature, humidity, pressure, or fill level, which allows for appropriate conditions for different types of cargo.

This technology provides real-time monitoring and integration with other logistics systems, which automates the management of transportation processes and reduces the risks associated with deviations in transportation conditions [4].

Integrating IoT technologies into logistics significantly increases the efficiency and transparency of processes, allowing for the creation of detailed reports that are an important tool for managers to make informed decisions. This data facilitates the planning process and allows you to respond to unforeseen situations while transporting goods quickly.

In addition, online transport monitoring ensures a higher level of safety for both drivers and cargo, as potential problems or violations of transportation conditions can be detected in time. Such transparency in the company's operations increases its internal efficiency and builds trust from customers and partners, which is an important factor for successful cooperation in a competitive environment.

Thus, IoT technologies are an important step in developing modern logistics, opening up new opportunities for process optimization and increasing the competitiveness of companies [5].

References:

1. Friess P., Vermesan O. Internet of Things Applications - from Research and Innovation to Market Deployment. River Publishers, 2022. 372 p.

2. Kaplan E., Hegarty C. Understanding Gps/Gnss Principles (Gnss Technology and Applications Series). Artech House Publishers, 2017. 1016 p.

3. Smart Sensors for Industrial Internet of Things: Challenges, Solutions and Applications / P. L. Mehta et al. Springer International Publishing AG, 2022. 534 p.

4. Supply Chain 4. 0: Improving Supply Chains with Analytics and Industry 4. 0 Technologies / M. Bourlakis et al. Kogan Page, Limited, 2020. 288 p.

5. Kern J., Sullivan M. Digital Transformation of Logistics: Demystifying Impacts of the Fourth Industrial Revolutio., 2021. 480 p.

УДК 004.738.5

Госало А.О., магістрант
Вакалюк Т.А., д-р пед.наук, професор,
Власенко О.В., ст. викладач
Державний університет «Житомирська політехніка»

ДОСЛІДЖЕННЯ ВПЛИВУ МЕТОДІВ ОПТИМІЗАЦІЇ НА ШВИДКІСТЬ ЗАВАНТАЖЕННЯ ВЕБСТОРІНОК

Процес оптимізації вебсторінок є фундаментальним для вдосконалення функціонування будь-якого інтернет-проєкту в сучасному цифровому середовищі. Тому знайдення нових моделей, методів та технологій оптимізації є доволі актуальною задачею.

В умовах постійно зростаючих користувацьких вимог до швидкодії онлайн-сервісів та підвищення конкуренції на ринку веб-рішень, питання ефективного завантаження сторінок набуває критичного значення для комерційного успіху та утримання аудиторії.

Численні дослідження демонструють, що навіть незначні затримки у відображенні контенту можуть призвести до суттєвого збільшення показника відмов і зниження конверсії [1].

Для вимірювання швидкості завантаження застосовуються кілька ключових метрик. TTFB визначає інтервал між надсиланням запиту до серверу та отриманням першого байту інформації, включаючи етапи перенаправлення, DNS-пошуку та TLS-узгодження. Оптимальне значення цього показника не має перевищувати 2-3 секунди [2].

FID відображає проміжок від моменту першої користувацької взаємодії з елементами сайту до реакції браузера, який не повинен перевищувати 1 секунду.

FCP вимірює час до появи на екрані першого контентного елементу (тексту чи зображення) з рекомендованим показником до 1.8 секунди.

LCP фіксує момент, коли основна частина видимого контенту стає доступною користувачеві, з еталонним значенням до 2.5 секунд.

Серед факторів, що найбільше впливають на швидкодію, виділяють: загальний обсяг сторінки, частоту серверних запитів, чутливість реагування та тривалість рендерингу в браузері.

Найпоширеніші проблеми продуктивності включають використання нестиснених медіафайлів, нехтування кешуванням, надлишкове застосування зовнішніх скриптів та неефективний програмний код.

Для прискорення завантаження вебсторінок можна використати низку методів оптимізації. Браузерне кешування дозволяє зберігати локально часто використовувані файли та мультимедійний контент, суттєво зменшуючи час відгуку серверу.

Оптимізація зображень передбачає правильний вибір формату файлів, їх компресію та адаптацію розмірів відповідно до потреб інтерфейсу. Для цього ефективно використовуються такі інструменти як TinyPNG, ImageOptim та Adobe Photoshop.

Мініфікація коду полягає у видаленні зайвих пробілів, коментарів та символів з файлів CSS, JavaScript та HTML. Ліниве завантаження забезпечує відтермінування завантаження зображень та медіаресурсів до моменту їхньої видимості в інтерфейсі, що зменшує обсяг початкового завантаження та покращує користувацький досвід, хоча вимагає обережності через потенційні проблеми з SEO [3].

Асинхронне завантаження уможливлює паралельне отримання ресурсів без блокування процесу рендерингу сторінки, що істотно прискорює її відображення.

Мережі доставки контенту (CDN) реалізують географічно розподілену інфраструктуру для оптимізації розповсюдження даних кінцевим користувачам.

Використання CDN дозволяє скоротити час завантаження через кешування вмісту, зменшити мережеві затримки та знизити навантаження на основний сервер, що особливо корисно для відвідувачів, віддалених від вихідного серверу.

Підсумовуючи, оптимізація продуктивності вебресурсів має першорядне значення для підвищення швидкості та ефективності завантаження сторінок.

Для досягнення оптимальних результатів слід комбінувати різноманітні методи оптимізації, регулярно контролювати функціональність та продуктивність, а також відслідковувати нові технологічні рішення, оскільки сфера оптимізації постійно розвивається.

Застосування описаних підходів дозволить суттєво покращити якість взаємодії користувачів з вебресурсом та підвищити його загальну ефективність.

Список використаних джерел:

1. Захарчук В. І. Методи оптимізації та комп'ютерні технології : навч. посіб. Луцьк : РВВ Луцького НТУ, 2017. 140 с.

2. Ладієв Л. Р. Методи оптимізації та пошуку оптимальних рішень : навч. посіб. Київ : КПІ ім. Ігоря Сікорського, 2023. 124 с.

3. Основні метрики швидкості завантаження сайту: TTFB, FCP, LCP та інші. URL: http://surl.li/elcloz (дата звернення: 17.03.2025).

УДК 004.42

Садовий Я.С., аспірант,
Воротніков В.В., д.т.н., доцент
Державний університет «Житомирська політехніка»

ДОСЛІДЖЕННЯ ОПТИМІЗАЦІЇ ПРОЦЕСУ ПОДІЛУ НА СЕГМЕНТИ ДЛЯ ПОБУДОВИ РОЗПОДІЛЕНИХ УЗАГАЛЬНЕНИХ СУФІКСНИХ ДЕРЕВ

Суфіксні дерева є важливими структурами даних, що застосовуються для ефективного пошуку підрядків та аналізу великих текстових масивів. Вони дозволяють виконувати такі операції, як пошук підрядків, порівняння рядків, визначення повторюваних послідовностей та інші завдання з лінійною або майже лінійною складністю [1]. Однак побудова таких структур при значних обсягах даних досі залишається складною задачею.

В умовах сучасного інформаційного середовища спостерігається постійне зростання обсягів даних. Наприклад, у галузі геноміки секвенування ДНК породжує великі масиви інформації, що потребують швидкої обробки. Подібним чином, пошукові системи висувають дедалі вищі вимоги до швидкого пошуку й аналізу текстових даних. Стандартні підходи до побудови суфіксних дерев, зокрема алгоритм Укконена [2], не завжди забезпечують достатню ефективність при обробці значних масивів інформації. Через це виникає необхідність застосування розподілених методів, які дозволяють розподілити обчислення між кількома вузлами чи процесами, що забезпечує вищу продуктивність і масштабованість.

Однією з ключових проблем при розподіленій побудові узагальнених суфіксних дерев є ефективна організація поділу даних на сегменти. Некоректний поділ може спричинити втрату інформації на межах сегментів, оскільки суфікси, що починаються на цих межах, можуть бути оброблені неправильно або зовсім втрачені. Це суттєво знижує точність та ефективність обчислень. Крім того, невдалий поділ здатний створити нерівномірне навантаження на окремі вузли кластеру, що призводить до неефективного використання ресурсів та зниження загальної продуктивності системи.

Можна виокремити три алгоритми оптимізації процесу сегментації даних для побудови розподілених узагальнених суфіксних дерев: гібридний поділ (ГП), рекурсивний поділ (РП) і динамічний адаптивний поділ (ДАП). Застосування цих алгоритмів дозволяє отримати широкий набір результатів для аналізу ефективності методів побудови суфіксних дерев на різних типах даних.

– Гібридний поділ із балансуванням навантаження поєднує декілька підходів до сегментації даних: початковий розподіл за допомогою фіксованих сегментів та подальше динамічне коригування сегментів з урахуванням реального навантаження вузлів. Це дозволяє оптимізувати розподіл даних та ефективніше використовувати обчислювальні ресурси.

– Рекурсивний поділ базується на принципі поділу даних на частини, що зберігають властивості початкової множини в меншому масштабі. Це дозволяє структуровано організовувати інформацію зі збереженням її внутрішньої структури. Основні переваги алгоритму—ітеративний підхід до сегментації та адаптивність до різних типів і структур даних.

– Динамічний адаптивний поділ уможливлює зміну розміру сегментів під час роботи, реагуючи на зміни навантаження й забезпечуючи оптимальний розподіл ресурсів.

Дослідження проводилось на п'яти різнорідних наборах даних: геномні послідовності, тексти природної мови, логи веб-серверів, програмний код, дані сенсорів. Такий вибір пояснюється різноманітністю структури та складності даних, що дозволяє всебічно оцінити ефективність алгоритмів для різних типів інформації, отримати репрезентативні результати та перевірити адаптивність алгоритмів до різних задач.

Отримані результати підтверджують, що всі три алгоритми демонструють покращення часу виконання, прискорення, ефективності використання ресурсів та точності об'єднання сегментів порівняно з послідовним алгоритмом побудови дерева. Алгоритм ДАП показав найкращі результати за всіма метриками серед досліджуваних методів. Особливо ефективними для великих наборів даних є алгоритми на основі ДАП і ГП, які значно зменшують час обчислень та підвищують ефективність аналізу. Використання архітектури Master-Worker забезпечує масштабованість системи за рахунок можливості додавання нових вузлів, підвищуючи обсяги та ефективність обробки даних, що особливо важливо для сучасних високопродуктивних систем.

Список використаних джерел:

1. Gagie, T., Navarro, G., & Prezza, N. Fully functional suffix trees and optimal text searching in BWT-runs bounded space. Journal of the ACM (JACM), 67(1), 2020.C.1-54.

2. Ukkonen, E. On-line construction of suffix trees. Algorithmica, 14(3), 1995. C. 249-260.

УДК 004.7

Зощак Т. А., здобувач,
Чижмотря О. В., ст. викладач
Державний університет «Житомирська політехніка»

SUPABASE ЯК СУЧАСНА АЛЬТЕРНАТИВА FIREBASE ДЛЯ РОЗРОБКИ ВЕБ-ЗАСТОСУНКІВ

Розробники сучасних веб-застосунків потребують надійних і масштабованих платформ для управління базами даних та автентифікацією. Firebase тривалий час займав домінуючу позицію на ринку Backend-as-a-Service (BaaS) рішень, проте зростаючі вимоги розробників стимулювали появу нових альтернатив. Однією з найбільш перспективних є Supabase – відкрита платформа, що забезпечує функціональність, аналогічну Firebase, але з використанням відкритих технологій та PostgreSQL як основи.

В основі Supabase лежать чотири ключові технології, що забезпечують його функціональність: PostgreSQL. На відміну від Firebase, який використовує NoSQL підхід, Supabase базується на потужній реляційній СУБД PostgreSQL, надаючи доступ до всіх її можливостей, включаючи розширену типізацію даних, складні запити та транзакції.

Row Level Security (RLS). Supabase реалізує безпеку на рівні рядків PostgreSQL, що дозволяє точно налаштувати права доступу до даних. Політики безпеки визначаються SQL-запитами, що забезпечує гнучкість та потужність контролю доступу.

Платформа автоматично створює RESTful API та інтерфейси для роботи з базою даних, що значно прискорює процес розробки. Розробникам не потрібно писати бекенд для стандартних операцій з даними. Supabase надає готові TypeScript-типи для схеми бази даних, що забезпечує типобезпечність при розробці та зменшує ймовірність помилок під час виконання.

Серед основних переваг використання Supabase варто відзначити відкритість і незалежність, оскільки Supabase – це відкрита платформа, що дозволяє розгортати рішення на власних серверах. SQL-потужність також є значною перевагою, адже повний доступ до можливостей PostgreSQL забезпечує гнучкість та ефективність запитів, що особливо важливо для складних даних.

Масштабованість є ще однією перевагою, оскільки архітектура Supabase дозволяє легко масштабувати застосунки від невеликих проєктів до великих систем. Низька вартість досягається завдяки використанню відкритих технологій та гнучкій моделі ціноутворення,

тому Supabase часто є економічно вигіднішим порівняно з Firebase. Реальний час забезпечується підтримкою RealTime підписок для миттєвого оновлення даних без складної інфраструктури.

Порівнюючи моделі ціноутворення, Supabase пропонує більш прозору структуру витрат, де оплата здійснюється за фактично використані ресурси (обчислювальна потужність, сховище даних та пропускна здатність), а не за активних користувачів, як часто робить Firebase.

Це може бути особливо вигідним для проектів з великою кількістю неактивних користувачів або для додатків, які здійснюють значну кількість операцій з невеликою кількістю даних. Окрім цього, важливою перевагою є можливість самостійного хостингу Supabase, що дозволяє уникнути витрат на хмарну інфраструктуру для проектів, які мають власні сервери.

Незважаючи на переваги, Supabase має певні обмеження, зокрема меншу екосистему, адже будучи відносно новою технологією, Supabase має меншу спільноту та кількість готових інтеграцій порівняно з Firebase. Вища складність є ще одним обмеженням, оскільки використання SQL вимагає більш глибоких знань у порівнянні з NoSQL підходом Firebase, що може бути викликом для початківців. Також Supabase має обмежені можливості аналітики, оскільки поки не пропонує вбудованих інструментів аналітики, аналогічних Firebase Analytics.

Практичний досвід використання Supabase у веб-проєктах показує значне прискорення розробки та покращення продуктивності завдяки потужній типізації та автоматичній генерації API. Інтеграція з сучасними фреймворками, такими як Next.js, робить Supabase привабливим вибором для розробки сучасних веб-застосунків.

Список використаних джерел:

1. Supabase Documentation [Електронний ресурс]. – Режим доступу:https://supabase.com/docs. (дата звернення: 12.03.2025).

2. PostgreSQL: Technical Documentation. [Електронний ресурс]. – Режим доступу: https://www.postgresql.org/docs/ (дата звернення: 09.03.2025).

3. Supabase GitHub Repository [Електронний ресурс]. – Режим доступу: https://webdevtrends.io/supabase-vs-firebase-performance-2024 (дата звернення: 13.03.2025).

УДК 004

Гаманюк І.А., здобувач,
Локтікова Т.М., ст. викладач
Державний університет «Житомирська політехніка»

ПРИНЦИПИ РОЗРОБКИ СУЧАСНИХ ОСВІТНЬО-ТЕСТУВАЛЬНИХ ПЛАТФОРМ З ІГРОВОЮ МОТИВАЦІЄЮ

У сучасному світі розробки освітніх платформ ключовим завданням є утримання уваги здобувачів освіти та забезпечення високої залученості. Ігрова мотивація навчання є однією з найефективніших методик, що використовує ігрові механіки для стимулювання мотивації користувачів. Її успішність обумовлена психологічними особливостями сприйняття інформації: система нагород, змагальний ефект, миттєвий зворотний зв'язок та елементи несподіванки сприяють формуванню звички до навчання і підвищенню зацікавленості.

Одним із основних елементів ігрової мотивації платформ є рейтинги, лідерборди та система досягнень. Вони базуються на алгоритмах обчислення балів, що можуть враховувати як правильність відповідей, так і швидкість виконання тестових завдань. Використання NoSQL баз даних, таких як MongoDB [1], дозволяє ефективно працювати з динамічними структурами даних та зберігати інформацію про прогрес користувачів у форматі документів. Для більш складних навантажених систем доцільним є використання PostgreSQL [2] з підтримкою JSONB або BigQuery для аналізу великих масивів даних.

Важливою складовою є механіка відкриття кейсів, що створює елемент азарту і заохочує користувачів повертатися до платформи. Для цього використовують алгоритми генерації випадкових винагород, такі як Pseudo-Random Number Generators (PRNG), що можуть працювати на основі хеш-функцій або криптографічних методів. У сучасних serverless-архітектурах можна реалізувати ці механіки через Cloud Functions, які генерують результати подій у реальному часі, не потребуючи постійно активного сервера.

Соціальні елементи, а саме можливість додавати друзів, ділитися досягненнями та взаємодії здобувачів освіти, підвищують рівень залученості. Для реалізації цього можна застосувати підхід довгого опитування (long polling) або черг повідомлень.

Інтерактивний зворотний зв'язок (instant feedback) є критичним для освітніх платформ. Використання алгоритмів адаптивного тестування (наприклад, Item Response Theory [3]) дозволяє підбирати завдання відповідно до рівня користувача, зменшуючи ймовірність фрустрації та підтримуючи оптимальний рівень складності.

Принцип «easy to learn, hard to master» є ключовим у розробці освітніх платформ. Інтуїтивний UI/UX, заснований на гейміфікованих патернах, таких як підказки, мікроанімації та адаптивний контент, забезпечує плавне занурення в процес навчання. Використання бібліотек на кшталт Framer Motion або GSAP дозволяє створити візуально привабливий інтерфейс без значного навантаження на рендеринг.

З точки зору архітектури, розглядувані платформи можуть будуватися як за класичною «монолітною» серверною архітектурою, так і за більш сучасною serverless-моделлю, яка забезпечує автоматичне масштабування та зменшує витрати на інфраструктуру. Тоді платформа може бути реалізованою із використанням фреймворку Next.js [4]. Для обробки статистики можна застосовувати Edge Functions та Vercel KV для швидкого кешування, включно з системою рекомендацій.

У роботі пропонується розробка інтерактивної освітньо-тестувальної платформи з ігровою мотивацією, побудованої за serverless-архітектурою, завдяки якій платформа ефективно та просто масштабується. Для реалізації платформи вибрано Next.js, оскільки цей фреймворк найкраще підходить для створення високоякісного UI/UX, що є критично важливим для застосунків, орієнтованих на ігрову мотивацію. Також Next.js дозволив об’єднати фронтенд і бекенд в єдине рішення, що значно спростило розробку. Як база даних застосовується MongoDB, яка дозволяє гнучко керувати динамічними структурами даних, що найкраще підходить для таких платформ. Інтеграція алгоритмів генерації випадкових винагород, системи рейтингів, лідербордів та адаптивного тестування сприяє постійній залученості здобувачів освіти. Такий комплексний підхід дозволив оптимально використати сучасні ресурси та технологічні здобутки, перетворюючи рутинний процес навчання на цікаву гру.

Список використаних джерел:

1. Team M. D. MongoDB documentation. MongoDB: The Developer Data Platform | MongoDB. URL: https://www.mongodb.com/docs/ (дата звернення: 11.03.2025).

2. Admin. PostgreSQL: documentation. PostgreSQL: The world's most advanced open source database. URL: https://www.postgresql.org/docs/ (дата звернення: 12.03.2025).

3. Admin. Item response theory. Columbia University. URL: https://www.publichealth.columbia.edu/research/population-health-methods/item-response-theory (дата звернення: 12.03.2025).

4. Next.js Team. Introduction | next.js. Next.js by Vercel - The React Framework. URL: https://nextjs.org/docs (дата звернення: 13.03.2025).

УДК 004.65

Волківський Я. С., здобувач,
Чижмотря О. В., ст. викладач
Державний університет «Житомирська політехніка»

ВИКОРИСТАННЯ TELEGRAM-БОТІВ ДЛЯ АВТОМАТИЗАЦІЇ ОСВІТНІХ ПРОЦЕСІВ ТА ПОКРАЩЕННЯ ВЗАЄМОДІЇ СТУДЕНТІВ І ВИКЛАДАЧІВ

Сучасні технології автоматизації мають величезне значення для вдосконалення освітніх процесів, особливо в контексті взаємодії студентів, викладачів та адміністрацій університетів. Одним із найбільш популярних і доступних інструментів для автоматизації освітніх завдань є Telegram-боти. Вони дозволяють значно знизити навантаження на викладачів, автоматизувати процеси реєстрації, сповіщення та збору зворотного зв'язку, що значно полегшує організацію навчального процесу і робить його більш ефективним [1].

Інформаційні технології вже давно стали невід'ємною частиною сучасного освітнього середовища. Одним з важливих напрямів є застосування автоматизованих систем для зменшення адміністративного навантаження як на викладачів, так і на студентів. Telegram-боти є ідеальним інструментом для автоматизації рутинних процесів, таких як реєстрація на заняття, сповіщення про зміни в розкладі, надання завдань, збір зворотного зв'язку тощо [2]. Вони також дають змогу значно полегшити організацію навчальних процесів і зробити їх більш персоналізованими. Бот «Dehto» є прикладом такої системи, яка дозволяє автоматизувати і персоналізувати освітній процес, забезпечуючи зручність як для студентів, так і для викладачів.

Telegram-боти можуть виконувати широкий спектр функцій в рамках освітнього процесу. Вони не лише дозволяють реєструвати студентів на заняття, але й доставляти завдання та тести, нагадувати про майбутні заняття, інформувати про зміни в розкладі, а також автоматично збирати зворотний зв'язок від студентів через анкети або опитування [3].

Такі боти можуть бути інтегровані з платіжними системами для здійснення оплат за навчальні послуги, що спрощує фінансові процедури. Вони також можуть автоматично створювати анкети і опитування для оцінки якості навчання, взаємодії з викладачами або задоволення від курсу. Це дозволяє адміністраціям університетів оперативно отримувати і аналізувати інформацію для поліпшення якості освіти.

Одним із ключових завдань, які Telegram-боти виконують у навчальному процесі, є оптимізація комунікації між студентами та викладачами. Бот може надавати миттєвий доступ до всіх необхідних навчальних матеріалів, забезпечувати швидку передачу завдань і зворотного зв'язку, а також дозволяти студентам ставити запитання викладачам або одногрупникам через інтерфейс бота.

У випадку, якщо питання потребує детальнішої відповіді, бот може перенаправляти студента до викладача для подальшого обговорення. Це дозволяє значно покращити взаємодію і забезпечити швидке вирішення будь-яких питань, що виникають у процесі навчання [2].

Telegram, як платформа, забезпечує високий рівень безпеки завдяки використанню шифрування даних на всіх етапах передачі. Це гарантує конфіденційність персональних даних студентів і захищає їх від несанкціонованого доступу або розголошення [3]. Така безпека є важливою умовою для застосування Telegram-ботів в освітньому процесі, оскільки необхідно дотримуватися вимог законодавства щодо захисту персональних даних студентів.

Бот «Dehto» є конкретним прикладом застосування Telegram-ботів в освітньому процесі. Студенти можуть через бота автоматично реєструватися на заняття, отримуючи підтвердження або відмову залежно від наявності вільних місць. Бот також надсилає автоматичні нагадування за 40 хвилин до початку заняття, що дозволяє студентам ефективно планувати свій час.

Завдяки інтеграції з платіжними системами, студенти можуть безпосередньо через бота здійснювати оплату за заняття, що спрощує процес. Крім того, викладачі можуть передавати завдання студентам і отримувати зворотний зв'язок через зручний канал комунікації.

Таким чином, Telegram-боти мають значний потенціал у вдосконаленні освітнього процесу, завдяки своїй здатності автоматизувати рутинні завдання, забезпечити персоналізований підхід до навчання та значно полегшити організацію комунікації між студентами, викладачами та адміністрацією.

Список використаних джерел:

1. Хижняк О. О., Фролова І. В. Використання чат-ботів для автоматизації процесів вищої освіти // Освітні технології: сучасні тренди та перспективи розвитку. Київ: Освіта, 2023. С. 50-57.

2. Іванова Т. В. Чат-боти в освіті: переваги та виклики // Науковий вісник університету. 2022. Т. 35, № 2. С. 80-85.

3. Мельник Л. І. Технології автоматизації в навчальному процесі // Наука і освіта. 2021. Т. 19, № 4. С. 150-154.

УДК 004.4

Свіргун А. В., здобувач,
Савіцький Р.С., ст. викладач
Державний університет «Житомирська політехніка»

ВПЛИВ ТЕХНОЛОГІЙ НА НАДАННЯ ПСИХОЛОГІЧНОЇ ДОПОМОГИ

Тяжкий стрес стає причиною великого попиту на психологічну допомогу, який значно переважає пропозицію. Проблема постає у багатьох країнах світу. До прикладу, у країнах з малим та середнім доходом на 1 мільйон людей припадає близько 0,1 психіатра, тоді як у країнах з великим прибутком – у середньому по 90 психіатрів на таку ж кількість осіб [1].

Прямим результатом нехтування психологічними хворобами людей з боку держави стане нестача людського ресурсу, а отже втрата великих фінансів. Через втрату працездатності людей із загальними ментальними розладами, країни у всьому світі прогнозовано понесуть втрати до 16 трильйонів доларів у період з 2011 та до 2030 року [1].

У період COVID-19 на допомогу прийшли різноманітні застосунки, що надали можливість проводити терапевтичні сеанси дистанційно. Криза під час коронавірусу проклала шлях до діджелітизації лікування, яка у подальшому дозволить вивести медицину на вищий рівень, зробивши її більш якісною та доступною для загалу [2].

Попередньо, ще у 2015-2018 роках, проводилося дослідження щодо інтеграції чат ботів як допоміжного засобу у процес терапії, що відобразило лише різко позитивну тенденцію у самопочутті пацієнтів. Проте варто зауважити, що дані були зібрані з громадських опитувань, а отже з медичної точки зору ніяк не підкріплені [1].

З іншого боку, не тільки спілкування під час сеансів може бути замінено технологіями. Одним з аспектів є “перебіг дня”, а саме повсякденні звички, які часто неможливо відстежити. Існує велика кількість досліджень, які підтверджують, що тренування, сон та дієта мають неабиякий вплив на самоконтроль психологічного стану. Поєднання традиційної терапії із використанням застосунків з таким функціоналом стало б проривом у вдосконаленні процесу психотерапії, адже всі рішення щодо плану лікування з боку лікаря прийматимуться, беручи до уваги деталізовану інформацію, яку пацієнт може надати у застосунку [2].

reSET – це перша оздоровча програма для відстеження поведінки, яка була затверджена FDA, однак всі її перевірки націлені лише на вебверсії, оминаючи мобільний застосунок. У результаті постала

проблема: ті пацієнти, які обрали вебсайтну версію реалізації програми, та ті, що надали перевагу мобільному застосунку, звітувалися із результатами про власне самопочуття. Отримані результати мали велику розбіжність [3].

Інша складність, яка може виникнути під час тестування застосунку, це випробування не на всіх можливих групах користувачів. Наприклад, левова частка майбутніх користувачів застосунку – це пацієнти з депресивними розладами. Проте до тестування залучатимуться лише людей із легкою формою хвороби. Як наслідок, неможливо буде передбачити, як саме у подальшому програма впливатиме на самопочуття пацієнтів, а особливо тих, хто має більш складні форми захворювань [3].

Продовжуючи тему депресії, часто із погіршенням стану у деяких пацієнтів з'являться суїцидальні наміри, що є абсолютним показом до госпіталізації. Лікар-психотерапевт здебільшого може розпізнати таку поведінку пацієнта під час регулярних сеансів терапії. Однак, якщо лікування проходитиме онлайн, то навіть досвідчений спеціаліст може помилитися і не вжити потрібних заходів для перестереження руйнівних дій пацієнта. Це можна попередити за допомогою функції цілодобового зв'язку з медичним персоналом за допомогою створення протоколу об'єктивного оцінювання нагальності кожного виклику пацієнту та впровадження плану дій для різних сценаріїв подій.

Отже, можна точно сказати, що сфера психологічної допомоги не залишиться без технологічних нововведень. Вони зможуть поліпшити методи лікування та відслідковування змін у стані пацієнта. Хоча потрібно звернути увагу, що дотримання всіх вимог та застережних заходів для даного виду застосунків критично важливе. Медичний світ досить непростий для діджиталізації, адже від цього напряму залежить стан пацієнта.

Список використаних джерел:

1. Alaa Ali Abd-Alrazaq, Asma Rababeh, Mohannad Alajlani, Bridgette M Bewick, Mowafa Househ. Effectiveness and Safety of Using Chatbots to Improve Mental Health: Systematic Review and Meta-Analysis, 13 липня 2020 р. URL : https://www.jmir.org/2020/7/e16021/ (дата звернення: 13.02.2025)

John Torous, Keris Jän Myrick, Natali Rauseo-Ricupero, Joseph Firth. Digital Mental Health and COVID-19: Using Technology Today to Accelerate the Curve on Access and Quality Tomorrow, 26 березня 2020 р. URL : https://mental.jmir.org/2020/3/e18848/ (дата звернення: 13.02.2025)

УДК 004.9:004.8

Кочура В.В., магістрант,
Локтікова Т.М., ст. викладач,
Кушнір Н.О., ст. викладач
Державний університет «Житомирська політехніка»

АНАЛІТИЧНИЙ ВЕБСЕРВІС ДЛЯ ВИЯВЛЕННЯ РИЗИКОВИХ ТРАНЗАКЦІЙ ЦИФРОВИХ АКТИВІВ НА ОСНОВІ AML ТА KYC

Розвиток цифрових активів і глобальна популяризація криптовалютних технологій сприяли зростанню обсягу транзакцій, що відбуваються поза межами традиційної фінансової системи. Децентралізована сутність блокчейнів забезпечує високу швидкість і доступність операцій, водночас створює серйозні виклики у сфері фінансового контролю та дотримання міжнародних норм боротьби з відмиванням коштів (AML) і політик ідентифікації клієнтів (KYC) [1, 2]. Анонімність та відсутність централізованого управління цифровими активами ускладнюють відстеження транзакцій, що може сприяти їхньому використанню в незаконних схемах, включаючи фінансування тероризму, шахрайства та відмивання грошей.

Попри наявність комерційних інструментів для моніторингу криптовалютних транзакцій, більшість із них мають низку обмежень: недостатня інтеграція із різними блокчейнами, високий поріг входу через значну вартість послуг, а також обмеженість аналітичних алгоритмів для виявлення складних схем фінансових махінацій. Це створює необхідність розробки інноваційного інтегрованого вебсервісу, який дозволить здійснювати поглиблений аналіз транзакцій цифрових активів, автоматизувати процеси ідентифікації ризикованих операцій та відповідати вимогам міжнародного фінансового регулювання.

Вебсервіс автоматизує аналіз транзакцій цифрових активів для виявлення фінансових ризиків, допомагаючи мінімізувати незаконні операції й підвищити безпеку та прозорість крипторинку.

Зі зростанням популярності криптовалют та збільшенням обсягу транзакцій з’явилась потреба у спеціалізованих інструментах для їхнього аналізу та моніторингу. Існує достатня кількість аналогів запропонованого програмного продукту на ринку.

Серед найбільш відомих платформ можна виділити Elliptic, Crystal Blockchain та Check Crypto Address. Elliptic (https://www.elliptic.co/) використовує алгоритми машинного навчання для виявлення складних схем відмивання грошей, однак підтримує обмежену кількість блокчейнів і орієнтований переважно на корпоративних клієнтів. Crystal Blockchain (https://crystalintelligence.com/) пропонує потужні

інструменти візуалізації, що спрощують аналіз транзакцій, але також має обмежену підтримку блокчейнів. Check Crypto Address (https://checkcryptoaddress.com/), навпаки, підтримує широкий спектр криптовалют, проте має обмежені аналітичні можливості.

Завдяки проведеному порівнянню, важливими аспектами стали: висока точність аналізу, широка підтримка блокчейнів, зручний інтерфейс, розширені можливості візуалізації, а також застосування методів штучного інтелекту для виявлення ризикових транзакцій.

Дана розробка базується на аналізі транзакцій цифрових активів. Головна його мета – виявити ризикові транзакції, визначити джерела та кінцеві точки руху активів, оцінити «репутацію» гаманців. Основними підходами при цьому стали графовий аналіз та методи машинного навчання. Графовий аналіз дозволяє будувати моделі взаємозв'язків між криптовалютними адресами, що допомагає виявляти підозрілі кластери, циклічні перекази та ключових посередників у транзакційних мережах [3]. Методи машинного навчання застосовуються для автоматизованого виявлення шахрайських схем та нелегальних операцій. Вони ефективні при обробці великих обсягів даних, адже дозволяють аналізувати багатовимірні параметри транзакцій, адаптуючись до нових схем шахрайства. Комбінування методів машинного навчання та графового аналізу забезпечило комплексний підхід до аналізу даних.

Вибір засобів реалізації вебсервісу базується на критеріях продуктивності, безпеки, гнучкості та масштабованості. Серверна частина створена на PHP (Symfony) з API Platform для роботи з запитами. Python разом із бібліотеками використовується для аналізу даних. React забезпечує інтерактивний інтерфейс, MySQL – надійне зберігання даних, Docker – стабільність і гнучкість розгортання, а Nginx виконує роль вебсервера. Така комбінація дозволила досягти балансу між швидкістю розробки, масштабованістю та надійністю вебсервісу.

Список використаних джерел:

1. What Is Anti-Money Laundering (AML)? [Електронний ресурс] - Режим доступу до ресурсу: https://blog.whitebit.com/en/what-is-anti-money-laundering/.

2. What Is KYC or Identity Verification, and How Is It Increasingly Important for Crypto? [Електронний ресурс] - Режим доступу до ресурсу: https://www.binance.com/en/blog/ecosystem/%E2%80%8Bwhat-is-kyc-or-identity-verification-and-how-is-it-increasingly-important-for-crypto-421499824684902130.

3. Graph Algorithms: Practical Examples in Apache Spark and Neo4j / Mark Needham, Amy E. Hodler, – O'Reilly, 2019. 268 c.

УДК 004.7

Волков О.М., здобувач,
Савіцький Р.С., ст. викадач
Державний університет «Житомирська політехніка»

ВПЛИВ SSR ТА SSG НА ПРОДУКТИВІСТЬ ТА SEO

Серверний рендеринг (SSR) і статична генерація сторінок (SSG) є двома основними підходами до рендеренгу вебсторінок, які мають різний вплив на продуктивність та SEO оптимізацію.

SSR (Server-Side Rendering) генерує контент на сервері під час кожного запиту користувача. Це гарантує, що користувач одразу отримує актуальні дані, оскільки вони оновлюються на сервері перед відправкою сторінки. Однак SSR може знижувати продуктивність через додаткове навантаження на сервер, що може вплинути на час завантаження сторінки та користувацький досвід. Проте цей підхід є корисним для сайтів, де важлива динамічність, наприклад, інтернет-магазинів або платформ для розміщення відеоматеріалів (YouTube). Крім того, для оптимізації продуктивності можна використовувати кешування запитів або комбінувати SSR з іншими підходами, такими як статичний рендеринг (SSG), щоб зменшити навантаження на сервер для менш динамічного контенту. Процес серверного рендерингу сторінки представлений на рисунку 1 [1].

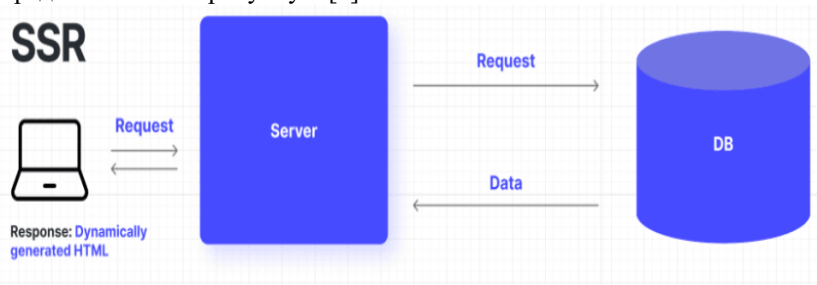


Рис. 1. Процес серверного рендерингу сторінки (SSR)

SSG (Static Site Generation) генерує всі сторінки вебсайту заздалегідь під час побудови сайту, що забезпечує миттєве завантаження та високі показники продуктивності. Оскільки сторінки вже існують у вигляді статичних HTML-файлів, вони швидко доставляються користувачам без додаткових запитів до сервера. Однак цей метод підходить не для всіх типів сайтів, оскільки може бути складним для динамічних сайтів,

де контент змінюється регулярно, наприклад, для сайтів з великим обсягом користувацьких даних. До того ж, при великій кількості сторінок чи частих змінах контенту, процес генерації може зайняти значний час, що збільшує час побудови сайту. Проте для сайтів з обмеженим або малим обсягом контенту, який рідко змінюється, SSG є ефективним і швидким рішенням. Процес статичної генерації сторінки представлений на рисунку 2 [1].

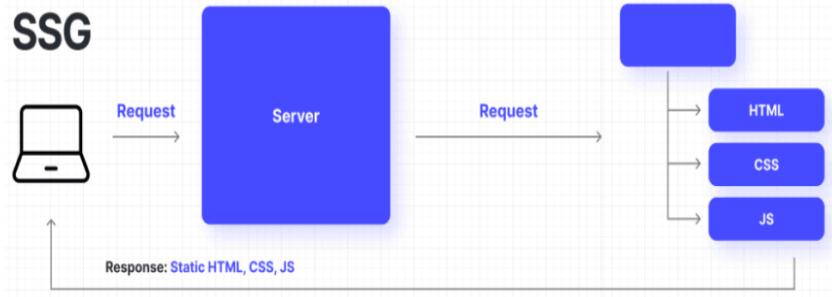


Рис. 2. Процес статичної генерації сторінки (SSG)

SEO (Search Engine Optimization) є важливим аспектом при виборі між SSR та SSG. Статичні сторінки з SSG отримують всі переваги швидкого завантаження і високої індексації пошуковими системами. SSR також має перевагу в SEO, оскільки сторінки рендеряться на сервері, що дозволяє пошуковим системам індексувати зміст, навіть якщо JavaScript виконується на клієнтському боці.

Загалом, вибір між SSR та SSG залежить від вимог до контенту вебсайту та необхідності в динамічних оновленнях. Для сайтів, де важлива швидкість і SEO, використання SSG є більш оптимальним рішенням. Проте для проектів, які потребують динамічного контенту, SSR може бути необхідним для забезпечення актуальності даних [2].

Список використаних джерел:

1. Tanga M. SSR vs. SSG in Next.js: Differences, Advantages, and Use Cases. STRAPI. 30.10.2024. URL: https://strapi.io/blog/ssr-vs-ssg-in-nextjs-differences-advantages-and-use-cases (дата звернення: 14.03.2025).

2. Caio R. P. Server-side Rendering (SSR) vs Static Site Generation (SSG) in Next.js. Medium. 03.01.2023.

URL: https://medium.com/@crp_underground/server-side-rendering-ssr-vs-static-site-generation-ssg-in-next-js-72b086a373e6 (дата звернення: 12.03.2025).

УДК 004.65

Волківський Я. С., здобувач,
Чижмотря О. В., ст. викладач
Державний університет «Житомирська політехніка»

ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ТА ЗАХИСТУ ОСОБИСТИХ ДАНИХ В ЧАТ-БОТАХ

В умовах швидкого розвитку цифрових технологій чат-боти набули широкого застосування у різних сферах: від бізнесу та маркетингу до освіти і державного управління. Вони є ефективними інструментами для автоматизації процесів, таких як реєстрація, комунікація з користувачами, надання послуг та збору інформації.

Однак, з розширенням використання чат-ботів, виникає необхідність у забезпеченні високого рівня захисту особистих даних користувачів, адже збір і обробка персональної інформації є невід'ємною частиною їх роботи.

Чат-боти активно використовуються для збору особистих даних, таких як імена, електронні адреси, номери телефонів, а іноді й фінансова інформація, історія покупок або взаємодії. Усі ці дані можуть бути вразливими, якщо їх не захищати належним чином. Саме тому питання забезпечення конфіденційності та захисту особистих даних у чат-ботах є надзвичайно важливим [1].

Одним із основних інструментів захисту особистих даних є шифрування інформації, що передається через чат-боти [2]. Багато популярних платформ, таких як Telegram, використовують надійне шифрування повідомлень, що гарантує безпеку переданої інформації на всіх етапах її пересування через мережу. Однак цього недостатньо для забезпечення повного захисту персональних даних.

Важливо також розробити системи аутентифікації користувачів, щоб уникнути несанкціонованого доступу до їхніх даних [4]. Для цього можна використовувати двофакторну аутентифікацію або інші сучасні методи перевірки особи.

Особливу увагу слід приділяти збереженню даних. Чат-боти повинні дотримуватись вимог законодавства, такого як GDPR (Загальний регламент захисту даних в Європейському Союзі) [5], яке вимагає від організацій належної обробки персональних даних. Користувачі повинні бути інформовані про те, які саме дані збираються, для яких цілей вони використовуються та як довго вони зберігаються. Важливо, щоб у користувачів була можливість видаляти свої дані або відмовлятись від їх обробки [3].

Захист даних також вимагає використання ефективних механізмів обмеження доступу до конфіденційної інформації. Наприклад, чат-бот може надавати доступ до певних функцій лише авторизованим користувачам.

Крім того, варто враховувати ситуації, коли особисті дані можуть бути оброблені не лише ботом, а й іншими сторонніми системами, такими як платіжні шлюзи або системи збору зворотного зв'язку. У таких випадках слід впроваджувати додаткові заходи безпеки, щоб забезпечити захист даних на кожному етапі їх обробки [4].

Інші аспекти безпеки чат-ботів включають регулярні перевірки безпеки їх програмного забезпечення, а також оновлення протоколів шифрування та аутентифікації, щоб відповідати новітнім вимогам безпеки. Це допомагає мінімізувати ризики витоків даних або атак на систему [2].

Забезпечення конфіденційності та захисту особистих даних користувачів чат-ботів є ключовим елементом для підтримки довіри до таких систем. Якщо чат-боти правильно налаштовані і відповідають усім вимогам безпеки, вони можуть стати ефективним і безпечним інструментом для автоматизації різних процесів, включаючи освітні, фінансові та інші завдання. Однак для цього потрібно впроваджувати передові технології безпеки, дотримуватися законодавчих норм і постійно оновлювати системи захисту [1]. Лише за таких умов чат-боти можуть стати надійними помічниками в сучасному цифровому середовищі.

Список використаних джерел:

1. Дьяків О. О. Захист персональних даних в умовах цифровізації // Журнал інформаційної безпеки. 2023. №2(15). С. 45-50.

2. Іванова Т. В. Шифрування даних у чат-ботах: ключові аспекти // Безпека інформаційних технологій. 2022. №1(10). С. 30-35.

3. Карпенко Л. І. Регулювання обробки персональних даних за допомогою чат-ботів // Науковий вісник права та інформаційних технологій. 2021. №3(7). С. 88-93.

4. Євген Р. М. Роль аутентифікації та захисту даних в цифрових платформах // Технології захисту даних в Інтернеті. 2020. №4(5). С. 56-60.

5. General Data Protection Regulation (GDPR). Офіційний сайт Європейської Комісії, 2018. URL: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en (дата звернення: 19.03.2025).

УДК 004.7

***Гладка К.В.*, здобувач,**
Фант М.О., к.філол.н.
Державний університет «Житомирська політехніка»

АНАЛІЗ І РОЗРОБКА ФУНКЦІОНАЛЬНИХ ВИМОГ ДО ІНТЕРНЕТ-МАГАЗИНІВ ДИТЯЧИХ ІГРАШОК

Ринок інтернет-магазинів дитячих товарів в Україні є конкурентним, і його детальний аналіз дозволяє визначити ключові переваги та недоліки існуючих платформ, що досліджено у роботі Петренко І.В. та Коваленка О.М. [1]. Особливу роль у привабливості онлайн-магазину відіграє адаптивний веб-дизайн, який забезпечує зручність користувацького досвіду та позитивно впливає на рівень конверсії, що підтверджують дослідження Сидоренко Л.П. та Іванченка М.Г. [2]. Крім того, ефективна інтеграція платіжних систем і логістичних сервісів є важливим фактором успішності електронної комерції, оскільки впливає на швидкість обробки замовлень і рівень задоволеності клієнтів, що розглядається у роботі Мельник О.В. та Гончарук Т.С. [3]. Комплексний підхід до створення інтернет-магазину, що включає конкурентний аналіз, адаптивний дизайн і оптимізацію платіжно-логістичних процесів, є ключем до успішного функціонування онлайн-торгівлі дитячими іграшками.

Розробка-інтернет магазину дитячих іграшок потребує здійснити аналіз конкурентів на ринку, що дозволить зрозуміти сильні та слабкі сторони наявних пропозицій, визначити популярні тренди, а також виявити потенційні можливості для вдосконалення власного бізнесу та привабливості для цільової аудиторії.

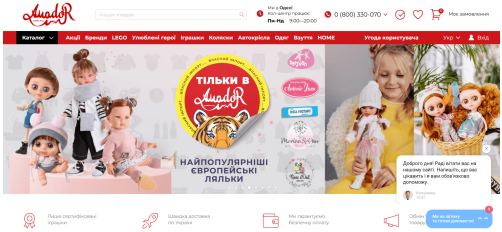


Рис.1. Вигляд головного вікна інтернет-магазину Amador [1]

Amador – це інтернет-магазин, фізичного Одеського магазину іграшок (див. Рис.1), де можна придбати не лише іграшки для дітей, але й засоби гігієни для малюка. Основні переваги Amador є: інтуїтивно зрозумілий інтерфейс; підтримка двох мов; наявність онлайн-чату з менеджером. Недоліками є: проблеми з інтерфейсом на мобільних пристроях (ціни не вирівняні, що ускладнює читання); неможливість

додати товар до кошика з головної сторінки, попередньо не перейшовши на сторінку з товаром.

Враховуючи інформацію отриману при дослідженні конкурентного ринку, було прийнято рішення створити сайт з повністю адаптивним дизайном, що забезпечить коректне відображення на мобільних пристроях та зручність для користувачів. Також на головній сторінці буде реалізована можливість додавання товарів до кошика без необхідності переходити на окрему сторінку товару. Метою дослідження є розробка зручного інтернет-магазину іграшок, з інтуїтивно зрозумілим користувацьким інтерфейсом. Крім того, магазин забезпечить інтеграцію з платіжною системою та системою доставки, що надасть швидку та безпечну обробку замовлень. Також користувачі отримають зручні інструменти для фільтрації товарів, пошуку товарів, перегляду історії покупок та можливість залишити відгуки, що підвищить загальний досвід купівлі. Інтернет-магазин дитячих іграшок пропонуватиме не лише стандартні товари, а й унікальну послугу створення власних іграшок на замовлення. Користувачі зможуть легко перейти до сторінки замовлення, де потрібно буде описати деталі того, якою іграшка повинна бути: тип тканин, наповнювач, розміри та інші характеристики. Також сайт надаватиме можливість прикріпити фото або малюнок дитини, що дозволить зробити іграшку ще більш персоналізованою та відповідною до фантазії дитини. Це зможе стати не лише гарним подарунком, але й важливим сімейним спогадом.

На сайті також буде доступна можливість безкоштовної консультації з менеджером всього за один клік. Користувачеві потрібно лише вказати свій номер телефону і найближчий доступний спеціаліст миттєво зателефонує для надання консультації. Ця функція забезпечить швидкий доступ до професійної допомоги без зайвих затримок.

Список використаних джерел:

1. Петренко І. В., Коваленко О. М. Аналіз конкурентоспроможності інтернет-магазинів дитячих товарів в Україні. *Маркетинг і менеджмент інновацій.* 2021. Т. 4. С. 112–120.

2. Сидоренко Л. П., Іванченко М. Г. Розробка адаптивного веб-дизайну для електронної комерції: підхід на основі користувацького досвіду. *Інформаційні технології та комп'ютерна інженерія.* 2020. Т. 2, № 45. С. 85–92.

3. Мельник О. В., Гончарук Т. С. Інтеграція платіжних систем та систем доставки в інтернет-магазинах: сучасні підходи та технології. *Системи обробки інформації.* 2019. Т. 1, № 162. С. 45–50.

УДК 004.7

Пархоменко О.Є., здобувач,
Савіцький Р.С., ст. викладач
Державний університет «Житомирська політехніка»

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У NEXT.JS

Використання штучного інтелекту (ШІ) у Next.js дозволяє створювати розумні та інтерактивні вебзастосунки. Завдяки вбудованій підтримці серверних функцій та API-роутів, Next.js можна легко інтегрувати з AI-сервісами, такими як OpenAI, Hugging Face або власними ML-моделями, що відкриває можливості для автоматизації контенту, персоналізації досвіду користувача, обробки природної мови та інших розумних функцій [1].

OpenAI (GPT) є одним із найпопулярніших AI-сервісів, який інтегрується з Next.js надзвичайно просто завдяки REST API, що робить його зручним для швидкого впровадження у вебзастосунки. Проте OpenAI має обмежену гнучкість у налаштуванні, оскільки доступні лише моделі, що надаються компанією. Щодо підтримки української мови, GPT-4 добре справляється із завданнями на цій мові.

Hugging Face є платформою, що спеціалізується на NLP, машинному навчанні та власних AI-моделях. Вона має доволі просту інтеграцію з Next.js завдяки Transformers API, який дозволяє використовувати готові моделі або навчати власні [2]. Основна перевага Hugging Face – велика бібліотека моделей із можливістю вибору під конкретні задачі. Підтримка української мови залежить від вибраної моделі, але загалом вона доволі непогана.

Google Vertex AI орієнтований на модельний хостинг та аналітику, пропонуючи можливість створювати та навчати кастомні AI-моделі. Його інтеграція з Next.js складніша, оскільки потребує використання Google Cloud Platform (GCP). Проте він надає гнучкі налаштування, дозволяючи працювати з власними моделями.

IBM Watson більше орієнтований на аналіз даних та корпоративні рішення, включаючи чат-боти для бізнесу. Інтеграція з Next.js ускладнена, оскільки платформа розрахована переважно на великі компанії. Підтримка української мови менш розвинена, порівняно з OpenAI чи Google Vertex AI.

Серед різних варіантів використання штучного інтелекту в Next.js найкращим вибором є OpenAI. Його легко інтегрувати через REST API, і він чудово підходить для створення чат-ботів, генерації тексту та аналізу даних. Багато відомих компаній використовують OpenAI у поєднанні з Next.js, щоб створювати швидкі, інтерактивні та розумні

вебзастосунки. Завдяки серверним можливостям Next.js та гнучкості у рендерингу, інтеграція штучного інтелекту стає більш ефективною та масштабованою.

Microsoft активно застосовує OpenAI у своїх продуктах, використовуючи Next.js для побудови динамічних інтерфейсів. Зокрема, GitHub Copilot (тепер Microsoft Copilot) використовує GPT-4 для генерації коду, а завдяки архітектурі Next.js забезпечується швидка та зручна інтеграція AI-функцій у браузері [3].

Snapchat інтегрував OpenAI у свій чат-бот "My AI", який надає рекомендації та допомагає користувачам у спілкуванні. Використання Next.js допомогло Snapchat реалізувати плавний досвід взаємодії з ботом, забезпечуючи швидкий рендеринг відповідей та оптимізоване завантаження компонентів.

Duolingo, популярна платформа для вивчення мов, додала функцію Duolingo Max, яка використовує GPT-4 для детальних пояснень і симуляції розмов. Завдяки можливостям Next.js, інструмент інтегрується безпосередньо в інтерфейс застосунку, забезпечуючи миттєвий зворотний зв’язок для користувачів.

Shopify також активно використовує OpenAI у своєму інструменті Shopify Magic, який допомагає продавцям швидко створювати унікальні описи товарів. Завдяки Next.js, генерація описів відбувається у реальному часі, а використання API-роутів забезпечує безперебійну взаємодію з OpenAI без втрати продуктивності.

Таким чином, поєднання OpenAI та Next.js дозволяє компаніям створювати високопродуктивні вебзастосунки, що підтримують AI-функції без втрати швидкості та ефективності. Завдяки серверним API-роутам, стрімкому рендерингу та можливостям SSR (Server-Side Rendering), Next.js стає ідеальним вибором для інтеграції штучного інтелекту у масштабовані проєкти.

Список використаних джерел:

1. Bina Nusantara IT Division. GPT-4: OpenAI’s game-changing language model [Електронний ресурс]. Medium. Режим доступу: https://medium.com/bina-nusantara-it-division/gpt4-openais-game-changing-language-model-2b4059189646.

2. Hugging Face. Documentation [Електронний ресурс]. Hugging Face. Режим доступу: https://huggingface.co/docs.

3. Hackable Projects. Building an AI-powered support assistant with Next.js and OpenAI [Електронний ресурс]. Medium. Режим доступу: https://medium.com/@hackable-projects/building-an-ai-powered-support-assistant-with-next-js-and-openai-3c2c8e18cd4c.

УДК 004.58

Грицюк В.І., здобувач,
Лобанчикова Н.М., к.т.н., доцент
Державний університет «Житомирська політехніка»

ПРОЄКТ ВЕБОРІЄНТОВАНОЇ СИСТЕМИ ОПЕРАТОРА МОБІЛЬНОГО ЗВ'ЯЗКУ

Цифровізація суспільства та сучасний розвиток інформаційних технологій створюють позитивні умови для підвищення якості надання послуг, зокрема у комунікаційній сфері. Стрімкий розвиток електронних комунікацій, а саме сфери послуг мобільного зв'язку сьогодні є необхідною умовою нормального функціонування суб'єктів господарювання, суспільного життя громадян. Сучасне цифрове суспільство стало доволі залежним від цифрових технологій, що автоматизують процеси життєдіяльності людства, створюючи комфортні умови для спілкування та обміну інформацією.

Значну роль у комунікації суспільства відіграють мобільні оператори зв'язку. Проведений аналіз тарифних пакетів та функціональних можливостей відомих українських операторів та операторів інших країн, зокрема Польщі, Угорщини, Німеччини дозволив виявити переваги та недоліки вітчизняних операторів. Визначено, що недоліком надання послуг українських операторів мобільного зв'язку є недостатньо гнучка тарифна та маркетингова політика. Переважна більшість сучасних тарифів пропонує обов'язкові пакети послуг, що розраховані на 4 тижні або місяць.. Було відмічено, що іноді оператори нав'язують автоматичне підключення додаткових послуг, які зазвичай є платними, що відповідно є гарним маркетинговим ходом. Однак досвід європейських операторів демонструє велику зацікавленість користувачів у тарифних планах, де пакети послуг надаються в залежності від наявності коштів на рахунку та отриманих послуг. Тобто, клієнти самі можуть визначати потрібні їм ресурси на вказаних період, зокрема швидкість та об'єм інтернету, підключення соціальних месенджерів, телебачення та ін. Це звичайно створює певні складності для операторів, однак ринок показує ефективність такого підходу за рахунок збільшення клієнтів та прибутків компаній.

Для тарифікації телеком-сервісу кожному провайдеру необхідна білінгова система. Це спеціальний софт для розрахунку, який збирає первинні дані про постачання телеком-послуг і структурує їх для подальшої обробки, зокрема тривалість дзвінка, кількість інтернет-трафіку, що споживається, і т.д. У систему потрапляє дуже багато інформації, після чого вона структурується й обробляється.

Метою роботи є розробка моделей, методів та алгоритмів удосконалення програмного комплексу білінгової системи оператора для підвищення комфортних умов обслуговування абонентів, прискорення процесу взаємодії між клієнтом та оператором. Веборієнтована система, що пропонується, дозволить забезпечити отримання безпечного доступу до структурованої, узагальненої і деталізованої інформації про надані послуги у реальному часі.

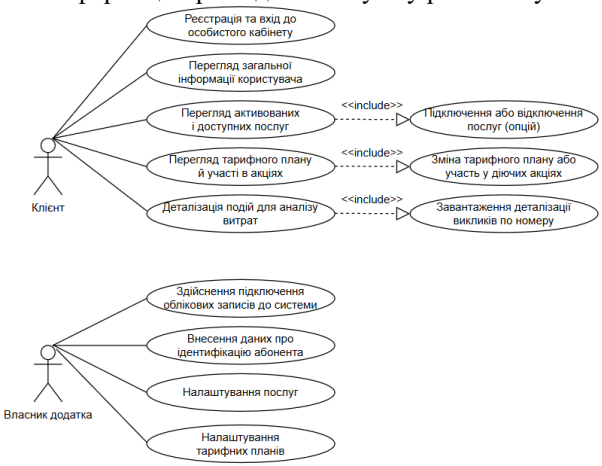


Рис. 1. Діаграма варіантів використання веборієнтованої підсистеми

Це підсистема, яка дасть змогу розширити можливості білінгу та вивести клієнтів на самообслуговування. Тобто користувач буде мати змогу самостійно замовляти або відмовлятися від послуг мобільного зв'язку; змінювати тарифний план, його тривалість або подавати заявки на участь у акціях (у тому числі налаштовувати індивідуальний тариф); контролювати залишки коштів по кожному особовому рахунку і поповнювати рахунок, тощо. Орієнтовна діаграма варіантів використання, в якій реалізовані основні функції, представлена на рисунку 1. У разі необхідності, можна буде звернутися до контакт-центру.

Список використаних джерел:

1. Білінгові системи: як працює діджитал у телеком-бізнесі. [Електронний ресурс] – Режим доступу: https://wezom.com.ua/ua/blog/billingovye-sistemy-kak-rabotaet-didzhital-v-telekom-biznese (дата доступу 10.03.2025).

УДК 004.4

Білецький Є.В., здобувач
Савіцький Р.С., ст. викладач
Державний університет «Житомирська політехніка»

ВПЛИВ ШТУЧНОГО ІНТЕЛЕКТУ НА ТРАНСФОРМАЦІЮ ЮРИДИЧНИХ ПОСЛУГ

В умовах розвитку штучного інтелекту (ШІ) галузь права зазнає справжньої трансформації. Технологічні розробки в сфері ШІ не лише оптимізують стандартні процедури, а й дають змогу переосмислити саму сутність юридичних послуг. Завдяки ШІ вдається автоматизувати рутинні процеси в юридичній діяльності, зокрема складання документів, аналіз контрактів та перегляд правових прецедентів, що значно скорочує час обробки інформації та знижує ризик виникнення людських помилок [1].

Одним із ключових факторів, що визначають трансформацію юридичних послуг під впливом ШІ, є зміна бізнес-моделей. Класична система погодинної оплати поступово поступається місцем новим підходам, які базуються на фіксованих або продуктивних тарифах. Такий перехід зумовлений автоматизацією багатьох рутинних процесів за допомогою ШІ, завдяки чому знижуються загальні витрати та підвищується ефективність роботи юристів. У результаті юридичні послуги стають доступнішими для ширшого кола клієнтів, що особливо важливо в умовах сучасної цифрової епохи. Розвиток LegalTech відіграє ключову роль у трансформації юридичної галузі. На ринку з'являється чимало стартапів, які за допомогою штучного інтелекту пропонують новаторські рішення для автоматизації аналізу документів та укладання контрактів. Зокрема, існують такі приклади проєктів, як LawGeex та ContractPodAI, що дозволяють швидко та ефективно перевіряти й узгоджувати договори відповідно до вимог законодавства [2].

Водночас, застосування штучного інтелекту впливає на ринок праці у сфері права. Завдяки автоматизації зменшується кількість рутинних завдань, які раніше виконували молоді спеціалісти, тож юридичні установи змушені переглядати ролі, а працівники – розвивати додаткові навички. Відповідно, навчальні заклади вже запроваджують спеціальні курси з технологій штучного інтелекту, щоб майбутні фахівці вміли ефективно працювати з інноваційними розробками та успішно адаптуватися до змін на ринку.

Окрім помітних економічних та операційних переваг, застосування ШІ ставить перед галуззю і численні етичні та регуляторні виклики [3]. Забезпечення захисту персональних даних, прозорості алгоритмів і

мінімізація упередженості моделей – це лише деякі з проблем, що потребують ретельного аналізу та розробки спеціальних нормативних актів [3].

Важливим є формування системи «compliance by design», яка дозволить гарантувати, що технології використовуються відповідально та відповідно до стандартів безпеки і етики. Не менш важливою є трансформація самої ролі юриста. Завдяки ШІ зменшується обсяг рутинної роботи, що дозволяє спеціалістам зосередитися на стратегічних аспектах, розвитку клієнтських відносин та вирішенні складних правових питань. Вони стають не просто виконавцями, а активними учасниками впровадження інноваційних технологій у правовій сфері. Також інтеграція ШІ набуває особливого значення в судочинстві. Автоматизація процесів, таких як нотифікація сторін або встановлення дат судових засідань, сприяє скороченню операційних витрат і підвищенню ефективності розгляду справ, що може позитивно вплинути на загальну продуктивність судової системи.

Таким чином, штучний інтелект стає потужним інструментом, який не тільки оптимізує існуючі процеси, але й відкриває нові горизонти для трансформації юридичної практики. Його інтеграція сприяє економії часу і ресурсів, розширює можливості для клієнтів та стимулює появу нових бізнес-моделей. Проте, для повної реалізації потенціалу ШІ необхідно водночас розв'язувати питання етики, безпеки та правового регулювання. Лише поєднання технічних інновацій із готовністю юристів адаптуватися до нових умов дасть змогу створити сучасну, ефективну та етичну систему надання юридичних послуг, яка відповідає викликам часу.

Список використаних джерел:

1. Reuters. AI: the new legal powerhouse — why lawyers should befriend the machine to stay ahead [Електронний ресурс]. Reuters, 24.10.2024. Режим доступу: https://www.reuters.com/legal/legalindustry/ai-new-legal-powerhouse-why-lawyers-should-befriend-machine-stay-ahead-2024-10-24/.

2. Financial Times. Legal AI is reaching deep into the workplace [Електронний ресурс]. Financial Times, н.д. Режим доступу: https://www.ft.com/content/bdc2250f-fbd9-4c4a-98cf-42e389e5b6c0.

3. ЕВА. Штучний інтелект в юриспруденції. Виклики, загрози, перспективи [Електронний ресурс]. ЕВА, н.д. Режим доступу: https://eba.com.ua/shtuchnyj-intelekt-v-yurysprudentsiyi-vyklyky-zagrozy-perspektyvy-2/.

УДК 004.7

Шумський О.В., здобувач,
Савіцький Р.С., ст. викладач
Державний університет «Житомирська політехніка»

ВІДМІННОСТІ РЕЛЯЦІЙНИХ БАЗ ДАНИХ

Реляційні бази даних мають перевагу через свою надійність, швидкість та універсальність, проте багато розробників не розуміють їх відмінностей. При некоректному виборі бази даних деякі з проблем, такі як масштабованість, продуктивність, несумісність з іншими технологіями, вартість підтримки та безпека можуть проявитися лише на пізньому етапі розробки, коли зміна основної бази даних стане дуже проблемною. Вибір правильної бази даних вимагає детального аналізу вимог проєкту і обрахунку приблизної кількості даних.

Останні публікації відзначають, що реляційні бази даних – це невід'ємна складова продуктових рішень найбільших IT компаній. Ось приклад відомих компаній, які використовують реляційні бази даних:

- PostgreSQL – Reddit, Apple, Meta;
- MySQL – Wikipedia, Uber, Github, Meta;
- SQLite – Adobe, Apple, Google;
- MS SQL – Microsoft, Grammarly, Mastercard;
- Oracle – Netflix, IBM, Intel.

PostgreSQL має переваги під час розробки для розробки аналітичних сервісів [1], натомість MySQL переважає як основна база даних проєкту, яка зберігає велику кількість записів. SQLite в свою чергу використовується для прототипування та для мобільних додатків.

PostgreSQL надає перевагу конфігурації типів (наприклад для зберігання IP адрес або геометричні типи для ГІС систем), підтримує роботу з масивами і дає можливість використання мов програмування відмінних від SQL. Також PostgreSQL є чудовим вибором при розробці систем аналітичних обробок у реальному часі (OLAP) та онлайнових обробок транзакцій (OLTP) систем завдяки оптимізації комплексних запитів.

MySQL буде хорошим вибором для малих систем через простоту. Навідміну від PostgreSQL має вищу швидкість для простих запитів, а також має можливість простої заміни на MariaDB якщо цього вимагає проєкт. MariaDB – це проєкт на основі MySQL, який розвивається в бік покращення швидкодії таких аспектів, швидкість індексів, кількість одночасних підключень, швидкість отримання даних та реплікації. Багато популярних платформ (наприклад Wordpress, Drupal та Magento) використовують саме MySQL.

SQLite зберігає дані в одному файлі навідміну від купи директорій і DBMS на сервері [2]. Цей унікальний підхід дає змогу використовувати її там, де немає змоги використовувати інші бази даних (наприклад, в мобільних додатках або у веббраузерах за допомогою WebAssembly). Попри свої недоліки з масштабуванням, вона є хорошим вибором для прототипів проєктів, за рахунок можливості робити копії бази даних за допомогою одного файлу. Також SQLite має більшу швидкість за MySQL та Postgres, хоча поступається їм у кількості функціоналу. Також потрібно зазначити що SQLite має проблеми з транзакціями (для виконання деяких рівнів транзакції вимагає повного блокування бази даних), що робить її поганим вибором в банківських системах.

Перевагою MS SQL є текстовий пошук завдяки можливості знаходити записи за словами, фразами та символами. База даних дуже добре інтегрується з іншими продуктами компанії Microsoft, що є великим плюсом, але в той же час може викликати труднощі при використанні на операційних системах, відмінних від Windows.

Oracle – є чудовим рішенням для високонавантажених проєктів за рахунок оптимізацій. Це помітно, коли розмір однієї бази даних сягає понад 1 ТБ на жорсткому диску. З мінусів можна зазначити достатньо високу вартість використання та проблемність з розробкою локально на власному сервері.

Вибір реляційної бази даних має великий вплив на продуктивність, масштабованість, та простоту інтеграцій з технологіями, тому потрібно робити вибір відштовхуючись від вимог застосунку.

Кожна з баз даних має свої унікальні переваги: PostgreSQL підходить для аналітичних систем та місць де потрібні складні запити, MySQL – для швидких та простих запитів, а SQLite – для прототипування і мобільних додатків. Важлива не лише оцінка поточних потреб, а й урахуванням можливих майбутніх змін вимог, щоб уникнути складнощів в подальшому.

Список використаних джерел:

1. Salunke S. V., Ouda A. A Performance Benchmark for the PostgreSQL and MySQL Databases. Future Internet. 2024. Т. 16, № 10. С. 382. URL: https://doi.org/10.3390/fi16100382 (дата звернення: 05.03.2025).

2. SQLite / K. P. Gaffney та ін. Proceedings of the VLDB Endowment. 2022. Т. 15, № 12. С. 3535–3547. URL: https://doi.org/10.14778/3554821.3554842 (дата звернення: 05.03.2025).

UDC 004.7

Melnychenko N.M., master`s student,
Vakaluk T.A., d.ped.s, professor,
Zhytomyr Polytechnic State University

METHODS OF CONTENT-BASED FILTERING IN RECOMMENDER SYSTEMS

Today, the need for innovations to attract customers and stand out from competitors is growing. One effective method is creating personalized recommendations using content-based filtering (CBF). This approach analyses object attributes and generates recommendations based on the similarity between user preferences and object characteristics.

CBF allows the similarity of objects to be determined using parameters such as genre, author, tags, or keywords. The main advantages of content-based filtering include independence from other users' data, transparency of recommendations, ease of adding new objects, and the ability to operate with limited data [1].

Thus, recommendations are generated solely based on an individual user's data, avoiding issues associated with the behaviour of other system users. This ensures the accuracy of results and minimizes the risk of including irrelevant preferences. Users can easily understand why a particular item has been recommended, as the suggestions are based on clear parameters, such as characteristic similarity.

Additionally, new products or services can be integrated into the system without waiting for feedback from other users. The system performs well even in its initial stages, when user preference data is minimal, ensuring satisfactory personalization despite limited information.

Thus, content-based systems can operate effectively without a large volume of data on other users' preferences, making them suitable for startups or niche domains [2].

However, this approach has its limitations. Specifically, the system recommends only items similar to those already rated, failing to surprise users with novelty [3]. This currently poses a problem, as users value the opportunity to get a ready-made solution, selected for them, something new and interesting, more than to come up with it themselves, using only what was there before.

Another significant challenge is the "cold start" problem, where the system struggles to provide recommendations for new objects with no prior ratings [4]. As a result, new objects that could be pretty interesting are "lost" among ordinary users, turning the mass into a homogeneous one. Additionally,

particular objects, such as music or artwork, have complex characteristics that are difficult to analyze effectively.

Hybrid models are increasingly utilised to address these limitations and enhance efficiency, combining content-based approaches with collaborative filtering. For instance, systems like Fab integrate content analysis by finding similarities in other users' preferences, improving recommendation quality, and ensuring adaptability across various usage scenarios [4].

Among the examples of content-based filtering applications are several popular systems that effectively implement this approach. For instance, Netflix generates movie and TV show recommendations by considering genres, actors, and user viewing history, providing personalized suggestions for each viewer. Online stores like Amazon or Rozetka use content-based filtering to suggest products similar to those the user has previously purchased or viewed. This approach helps to increase sales and retain customers.

Educational platforms like Coursera recommend courses based on previously selected topics and rated content. This allows users to receive learning materials that best match their interests and level of preparation.

In conclusion, content-based filtering methods remain crucial to modern recommender systems, especially when combined with other approaches. They are a powerful tool for creating individualized user experiences while requiring further refinement to overcome limitations.

References:

1. Korniychuk, V. O. “Research on recommender systems for searching for vacation spots on the Internet”, 2019. URL: https://openarchive.nure.ua/entities/publication/e7f78418-deef-4db7-8758-4600bf348926 (accessed: 27.11.2024).

2. Zeynep B. A. «Recommendation Systems: Content-Based Filtering», електронний ресурс. URL:https://medium.com/@zbeyza/recommendation-systemscontent-based-filtering-e19e3b0a309e (accessed: 27.11.2024).

3. Prem Melville, Raymond J. Mooney, and Ramadass Nagarajan. Contentboosted collaborative filtering for improved recommendations. In Proceedings of the Eighteenth National Conference on Artificial Intelligence (AAAI02), Edmonton, Alberta, 2002 P. 187-193. URL: https://cdn.aaai.org/AAAI/2002/AAAI02-029.pdf

4. Marko Balabanovic and Yoav Shoham. Content-based, collaborative recommendation. Communications of the Association for Computing Machinery, 40(3): 66–72, 1997. https://dl.acm.org/doi/pdf/10.1145/245108.245124 (accessed: 27.11.2024).

UDC 004.7

Kholodnitskyi Vladylsav, 1st-year master's student,
Vakaliuk Tetiana, Dr Sc., professor
Vlasenko Oleh, Senior lecturer
Zhytomyr Polytechnic State University

USING BLOCKCHAIN TECHNOLOGY TO ENHANCE DATA PRIVACY IN E-COMMERCE

Preserving user data privacy is one of the most significant concerns in today's digital economy, especially for visitors engaging in e-commerce activities. As online transactions increase, concerns about data leakages, misuse, and manipulation have grown significantly. When e-commerce platforms sell directly to customers, they rely on traditional 'centralized' systems, which contain customer data integrated into large systems, raising the attractiveness of such systems to hackers. Often, such systems share information with third parties, which poses a degree of unauthorized or leak usage. Losses resulting from critical security incidents and privacy violations have impacted consumer trust. Various innovative technologies are urgently required to address these instances. The uniqueness of blockchain technology, which offers a decentralized and tamper-resistant structure, provides an adequate answer to these questions and improves data security while giving back the customer's control of their data [1].

Thanks to blockchain, sensitive user information cannot be stored in a central place, eliminating single points of failure; in contrast to centralized systems, blockchain stores data in encrypted form, accessible only with the user's private key, which enhances security to the maximum level. However, blockchain systems also have disadvantages: for example, smart contracts facilitate the completion without needing users to disclose their identities and details to third parties since smart contracts automate the process. Also, blockchain provides pseudonymity to the users - the anonymity of users is guaranteed by unique cryptographic methods that prevent tracing while the data remains clear [2].

One of blockchain's most substantial benefits is its empowering users by returning control of personal data to them. Users of decentralized identity systems will have their personal information protected and can grant access to it on a need-to-know basis, reducing reliance on intermediaries. Such change can revolutionize e-commerce by restoring consumer confidence and giving companies an upper hand in a growing privacy-centered market [3].

The possibility of immutable information protected from fraud appeals to e-commerce, an industry frequently affected by fraud. E-commerce platforms are gradually shifting to blockchain technology, where data interference is highly unlikely due to the network's consensus mechanism, which makes

every change dependent on all other network participants. In addition, the power of blockchain can also enhance customer trust in businesses, as companies may be able to prove regulatory compliance in terms of personal data processing using blockchain.

Apart from privacy and security, e-commerce platforms can take advantage of blockchain technology in a more customer-friendly manner by allowing customers to define the terms of data sharing. Users selling access to their data to companies instead of the other way around will make data commercialization more ethical and open. Not only does this model maintain privacy, but it also allows users to be compensated for their data, benefiting both consumers and companies. Such a shift can influence user behaviour, encouraging businesses to adopt more customer-focused strategies, which incorporate user data in a more decentralized way and allow networks to be more user-oriented [4].

However, there are some constraints when implementing a blockchain-based model. First among the issues is scalability, where, as in many popular blockchain networks, including Bitcoin and Ethereum, the volume of transactions is high but limited on a global scale. Another disadvantage is the high power usage, especially in blockchain networks, using the Proof of Work method to achieve consensus, making a Proof of Stake preferable. On top of this, the usability of a blockchain-based system is not adequate for the masses who are not tech-informed [5].

In conclusion, it is possible to consider the application of technologies based on blockchain for individuals as an advanced method of providing privacy, confidentiality, and anonymity in online and offline activities related to e-commerce.

References:

1. Buterin V. Ethereum White Paper: A Next-Generation Smart Contract and Decentralized Application Platform. URL: https://ethereum.org/en/whitepaper/.

2. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. URL: https://bitcoin.org/bitcoin.pdf.

3. Kshetri N. Blockchain's roles in meeting key supply chain management objectives. International Journal of Information Management, 2018. Vol. 39, 80–89 p.

4. Swan M. Blockchain: Blueprint for a New Economy. O'Reilly Media, 2015. 152 p.

5. Zheng Z., Xie S., Dai H.-N., Chen X. Blockchain Challenges and Opportunities: A Survey. International Journal of Web and Grid Services, 2018. Vol. 14, No. 4. 352–375 p.

УДК 004.7

Бабушко А.С., здобувач,
Власенко О.В., ст. викладач,
Янчук В.М., к.т.н., доцент
Державний університет «Житомирська політехніка»

МОДЕЛЮВАННЯ ТА ВІЗУАЛІЗАЦІЯ АДАПТИВНИХ АЛГОРИТМІВ РЕГУЛЮВАННЯ ДОРОЖНЬОГО РУХУ

Актуальність дослідження адаптивних алгоритмів регулювання дорожнього руху обумовлена гострою проблемою заторів у сучасних містах, що негативно впливає на якість життя громадян, економічну ефективність міської інфраструктури та стан навколишнього середовища. Традиційні системи світлофорного регулювання з фіксованими циклами не здатні ефективно реагувати на динамічні зміни транспортних потоків, що призводить до нераціонального використання дорожнього простору та збільшення часу пересування.

Основна мета дослідження полягає у створенні ефективної моделі «Green wave», яка оптимізує прохід транспортних засобів через перехрестя та скорочує час простою на світлофорах.

Для моделювання міської дорожньої мережі використовується графова структура, де вершинами виступають перехрестя, а ребрами – окремі ділянки доріг (див. рис. 1). Кожне перехрестя характеризується такими параметрами, як навантаження, довжина черги та тривалість циклу світлофора, тоді як дорожні відрізки описуються пропускною здатністю та довжиною.

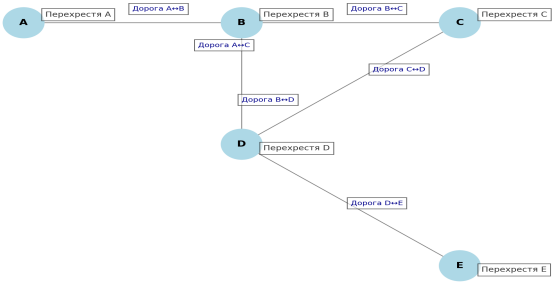


Рис. 1. Двонаправлений граф адаптивного регулювання дорожнього руху

Розроблено візуалізаційний модуль, який дозволяє в режимі реального часу спостерігати за рухом транспортних засобів у мережі. При проектуванні системи було дотримано принципів SOLID та DRY

[1, 2], що сприяло створенню модульної архітектури з можливістю повторного використання коду. В процесі розробки застосовано наступні патерни проектування: Factory – для генерації різних типів адаптивних алгоритмів, наприклад, з пріоритетом для громадського транспорту або з динамічною регуляцією світлофорних циклів; Singleton – для реалізації глобального контролера симуляції, що централізовано керує налаштуванням параметрів світлофорів та збором статистичних даних; Observable – для оперативного сповіщення про зміну стану світлофорів або виникнення заторів у певних ділянках мережі. Основою адаптивних алгоритмів у межах використання середовища SUMO (Simulation of Urban MObility) є ідея динамічного перерозподілу фаз світлофора залежно від поточного та прогнозованого навантаження на перехрестях. Для цього в SUMO реалізовано підсистему збору даних на основі віртуальних датчиків, що моделюють роботу камер спостереження та індуктивних детекторів. Отримана інформація надходить до модуля прийняття рішень, що дає змогу в режимі реального часу коригувати параметри регулювання руху, підлаштовуючи фази світлофора під актуальні умови.

Запропонована модель "Green wave" представляє інноваційний підхід до оптимізації руху транспортних засобів через систему перехресть, що дозволяє суттєво скоротити час простою на світлофорах та підвищити загальну пропускну здатність дорожньої мережі. Моделювання та візуалізація роботи таких алгоритмів надає можливість не лише теоретично обґрунтувати їх ефективність, але й перевірити в умовах, наближених до реальних, враховуючи різноманітні сценарії навантаження (пікові години, аварійні ситуації, дорожні роботи). Таким чином, дослідження спрямоване на вирішення актуальної проблеми підвищення ефективності міської транспортної системи шляхом впровадження інтелектуальних технологій регулювання дорожнього руху.

Список використаних джерел:

1. Zhang Y., Chen X., Li Y. A deep reinforcement learning approach for real-time adaptive traffic signal control // IEEE Transactions on Intelligent Transportation Systems. – 2021. – Т. 22, № 4. – С. 2090–2100.

2. Wang J., Liu S. Modern UML modeling tools for software engineering // Journal of Software Engineering and Applications. – 2020. – Т. 13, № 1. – С. 45–60.

3. Wirth N. Modern C++20: A comprehensive guide. – O’Reilly Media, 2022. – N.p.

UDC 004

Kostyuchenko Artem, master's student,
Loktikova Tamara, Senior Lecturer at the Department of Software Engineering,
Lysogor Iurii, Senior Lecturer at the Department of Software Engineering
Zhytomyr Polytechnic State University

DEVELOPMENT OF A NEURAL MODEL FOR IMAGE AND VIDEO RESOLUTION ENHANCEMENT

With the development of artificial intelligence and deep learning, effective methods for improving the quality of digital content have emerged. One of these areas is the creation of neural models to increase the resolution of images and videos, known as Super-Resolution.

Super-Resolution technology can restore details and improve the clarity of low-quality content and has a wide range of applications, from medicine to video games.

Modern neural networks use sophisticated algorithms to reconstruct a high-quality image from an input low-resolution image. The basic principle of these models is to train a neural network on a large set of paired images: a low-resolution image and its high-quality counterpart.

This principle allows the model to learn to restore fine details that are lost when the resolution is reduced.

In addition to traditional methods, approaches based on generative adversarial networks (GANs) are becoming increasingly popular [1]. These methods create more realistic and detailed images by using a discriminator that distinguishes between generated models and real photos, prompting the generator to improve the quality of the output.

Today, there are many networks, but let's mention the most famous ones. SRCNN, EDSR, ESRGAN are networks that have significant success in restoring details and improving image quality but also have certain limitations that complicate their practical use [2].

Models based on SRCNN [3] and EDSR [4] networks focus only on improving spatial resolution, without taking into account contextual details and textures, which can lead to smoothed or less natural results.

Generative models such as ESRGAN, although they can produce realistic high-frequency details, often lead to artifacts that can distort the original image, making it impossible to use, for example, in medicine.

The problems of these neural networks allow us to think about creating our own improved model that can reduce the existing shortcomings and provide a better resolution.

The proposed model is based on EDSR and VSRN network architectures with partial integration of ESRGAN principles.

The developed model has the ability to increase the resolution of both images and video, with support for processing on both the central processing unit (CPU) and graphics processing unit (GPU) to optimize performance.

The system supports automatic optimization for different hardware configurations: the ability to choose between fast mode for less powerful devices or high-quality mode for high-performance graphics cards.

The model supports noise and compression artifact removal, which is useful for processing old or low-quality materials.

The model is equipped with intuitive software that allows you to easily upload files, adjust processing parameters, and save improved results. It is possible to change the degree of magnification (2×, 4×, 8×) and choose between different super-resolution algorithms to achieve the optimal balance between detail and speed.

The developed model uses the TensorFlow library from Google and the Python programming language with the corresponding libraries for image and video processing. To implement the graphical interface, the PySide6 library is used in combination with the declarative language QML.

References:

1. Generative Adversarial Network.
URL: https://www.geeksforgeeks.org/generative-adversarial-network-gan/.
2. Image Super-Resolution: A Comprehensive Review.
URL: https://www.digitalocean.com/community/tutorials/image-super-resolution.
3. SRCNN (Super Resolution) Review.
URL: https://arxiv.org/abs/1904.07470
4. Enhanced Deep Residual Networks for single-image super-resolution.
URL: https://keras.io/examples/vision/edsr/.

УДК 004.7

Маньківський В.В., здобувач
Савіцький Р.С., ст. викладач
Державний університет «Житомирська політехніка»

ПРОЄКТУВАННЯ ТЕХНОЛОГІЧНОГО СТЕКУ КОЛАБОРАТИВНОГО РЕДАКТОРУ

В умовах сучасної розробки програмного вебпродукту, в той чи інший час може знадобитися колаборативний редактор, наприклад для спільного редагування електронного листа чи будь-якого іншого тексту, який потребує HTML-структури. Основною проблемою є те, що більшість готових редакторів складно налаштовувати. Крім того, виникає потреба забезпечити можливість декільком користувачам працювати над одним документом одночасно, не заважаючи один одному.

Основна ідея – обрати технології, які підтримуються, розвиваються та є безпечними для використання. Крім того, це має бути технологічний стек, який легко модифікується та може бути інтегрованим у більшість існуючих проєктів, що вимагають сумісності з популярними технологіями та програмним забезпеченням [1].

Важливо, щоб обрані технології підтримували активні спільноти розробників, які забезпечують оновлення, а саме: виправлення помилок та нові функціональні можливості. Це не лише підвищує надійність системи, але й також знижує ризик виникнення проблем з безпекою. Слід акцентувати увагу на тому, що наявність документації та прикладів використання полегшить процес входження нових розробників, що будуть використовувати ці технології, а, також, сприятиме швидшій розробці додатку. TipTap – open source фреймворк редактора, заснований на бібліотеці ProseMirror. Він легко адаптується завдяки модульній архітектурі, що дозволяє розширювати функціонал [2]. TipTap розроблено таким чином, щоб була відсутня залежність від фреймворків, що дозволяє без проблем інтегрувати у React, Vue, Svelte тощо. Для забезпечення синхронізації змін між клієнтами та уникнення конфліктів при одночасному редагуванні документа кількома користувачами, підходить бібліотека Yjs, для роботи з CRDT (Conflict-free Replicated Data Types), та Hocuspocus, Node.js бібліотека. Hocuspocus може бути самостійним Websocket сервером, що працює разом із Yjs та TipTap, ефективно отримуючи і передаючи зміни користувачам, зберігаючи їх у базі даних (рис. 1). Всі три технології знаходяться під MIT ліцензіями.

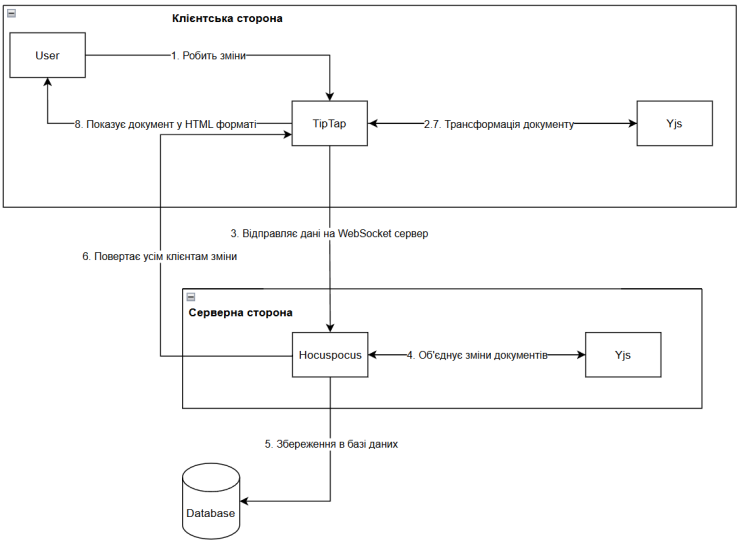


Рис. 1. Діаграма взаємодії TipTap, Hocuspocus та Yjs

Використання бібліотек та фреймворків дозволяє створити редактор, який забезпечує роботу в реальному часі, є швидким у налаштуванні та є відкритим для кастомізації. TipTap надає гнучкість у налаштуванні редактора, що дозволяє адаптувати його під специфічні потреби користувачів. Yjs забезпечує надійну синхронізацію між користувачами, що дозволяє уникнути конфліктів і досягти безперервність роботи. Hocuspocus гарантує ефективну передачу та збереження даних, що підвищує загальну продуктивність системи.

Обраний стек технологій не лише відповідає вимогам сучасних вебдодатків, але й забезпечує високу продуктивність, безпеку та зручність у використанні, що робить ідеальним вибором для інтеграції редактора, який задовольнить потреби різних користувачів і команд.

Список використаних джерел:

1. Which rich text editor framework should you choose in 2025 [Електронний ресурс]. Liveblocks Blog. Режим доступу: https://liveblocks.io/blog/which-rich-text-editor-framework-should-you-choose-in-2025.

2. Why we choose TipTap [Електронний ресурс]. Medium. Режим доступу:https://medium.com/@sansil32/why-we-choose-tiptap-b763d6b6330a

УДК 004.7

Кравченко С.М., ст. викладач,
Гришкун Є.О., ст. викладач
Державний університет «Житомирська політехніка»

А/В-ТЕСТУВАННЯ МОБІЛЬНОГО ДОДАТКА ЗАПИСУ В APP STORE

А/В-тестування – це процес створення варіантів із активу списку програм у магазині, розділення аудиторії на дві групи та визначення того, який варіант приніс більше користувачів, відвідувачів або будь-який KPI (key performance indicators), який необхідно знайти.

А/В-тестування мобільних додатків полягає в тому, що відбувається експериментування з варіантами запису в APP STORE, щоб побачити, який із них має найкращу ефективність.

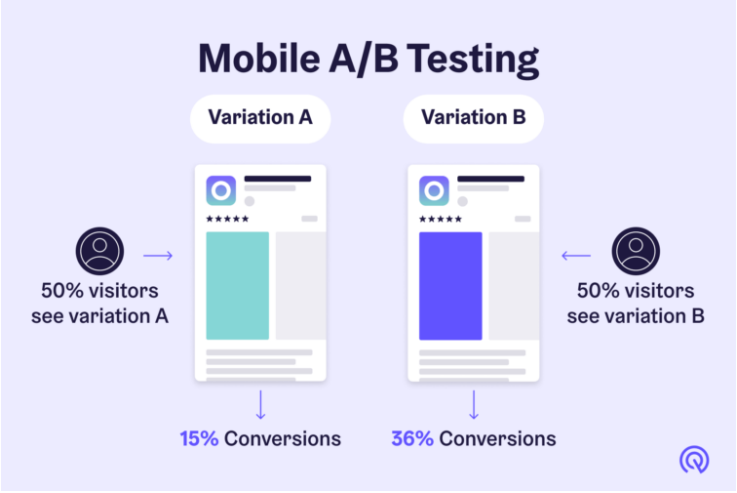


Рис. 1. А/В-тестування мобільних додатків для отримання кращих результатів

Мобільне А/В тестування складається з основних наступних етапів:

1. Дослідження. Визначається, чого саме не вистачає в додатку, і що потрібно покращити.
2. Гіпотеза. Продумати вірні запитання. Наприклад, що ми хочемо змінити на сторінці магазину?
3. Проведення експерименту. В ідеалі А/В-тести для мобільних

пристроїв триватимуть від 7 до 14 днів.

4. Аналіз та впровадження. Збираються дані і приймається рішення. Визначається рівень достовірності та багато інших критеріїв.

Які елементи тестувати A/B?

Найвпливовішими елементами в списку додатків є: піктограма програми, знімки екрана та відео. Піктограма програми – це перше враження про програму, і тому це такий важливий елемент, який потрібно перевірити.

Існують такі варіанти тестування мобільних додатків:

- Тестування на етапі перед запуском. Перевірити сторінку до її випуску.

- Тестування експериментів у програмі. Експеримент у додатку - ще один аспект мобільного A/B-тестування, який також дуже важливий. Таким чином можна перевірити, щоб забезпечити найкращу роботу програми для користувачів, змусивши їх повертатися та часто використовувати існуючу програму.

Отже, тестування A/B вимірює фактичну поведінку клієнтів у реальних умовах, може виміряти дуже невеликі відмінності в продуктивності з високою статистичною значущістю. Тестування може вирішувати компроміси між суперечливими настановами або якісними результатами зручності використання, визначаючи, який із них має найбільшу вагу за даних обставин.

Список використаних джерел:

1. How to do Mobile App A/B Testing for Your App Store Listing [Electronic resource]. – Access mode: https://appradar.com/academy/app-store-listing-a-b-testing

Секція 2
КОМП'ЮТЕРНА ІНЖЕНЕРІЯ, КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

УДК 004.056

Маєвський О.В., к.т.н., доцент
Державний університет «Житомирська політехніка»

КОМП'ЮТЕРНА СИСТЕМА ПРОГНОЗУВАННЯ РИЗИКУ ВИНИКНЕННЯ ПОЖЕЖ НА ОСНОВІ НЕЙРОМЕРЕЖІ

В умовах інтенсивного інформаційно – технологічного розвитку суспільства зростає різнополярне навантаження на оточуюче середовище, що певним чином деформує сформовані закони і механізми розвитку навколишнього середовища. Як наслідок, формується комплексна реакція довкілля на зовнішні впливи, яка може набувати катастрофічних маштабів.

Одним з проявів реакції навколишнього середовища на зовнішній вплив, як природного, так і антропогенного характеру, є ризик виникнення пожеж не тільки в окремому регіоні (наприклад, Житомирському), а й інших, що приводить до надзвичайних систуацій глобального рівня. Тому, своєчасне попередження ризику виникнення пожеж дозволить оперативно прийняти ефективні управлінські рішення з метою уникнення або пом'якшення екологічних руйнувань та економічних втрат.

Метою дослідження є створення інтелектуальної системи прогнозування ризику виникнення пожеж на регіональному рівні в рамках концептуального підходу до створення регіонального ситуаційного центру [1, 5].

Зростаюча складність та непередбачуваність регіональних ризиків потребують вдосконалених прогнозних підходів для забезпечення своєчасного втручання та ефективного пом'якшення наслідків пожеж.

У доповіді буде продемонстровано проект інтелектуальної системи, основу якої складає навчена ймовірнісна нейромережа, яка дозволяє виконати своєчасне прогнозування ризикової ситуації виникнення пожеж на регіональному рівні з метою прийняття ефективних управлянських рішень.

Використовуючи дані в режимі реального часу з різних джерел (засоби ДЗЗ, датчики IoT), ці системи підвищують можливості оцінки ризику пожеж в регіоні.

Для навчання ймовірнісної нейромережі [2, 3] використовувався алгоритм кластерізації k – means та непараметричні методи

класифікації [4], які базуються на локальному оцінюванні щільності розподілу класів ру(х) в околиці класифікованого об'єкту х є Х.

У випадку класифікації багатовимірних об'єктів, які описуються n числовими ознаками $f_j : X \to R,\ j = 1,.....n$, непараметрична оцінка щільності в точці $x \in X$ записується наступним чином:

$$\hat{p}_h(x) = \frac{1}{m} \sum_{i=1}^{m} \prod_{j=1}^{n} \frac{1}{h_j} K\left(\frac{f_j(x) - f_j(x_i)}{h_j} \right), \qquad (1)$$

де $K\left(\frac{f_j(x) - f_j(x_i)}{h_j} \right)$ - Гаусове ядро, тобто функція типу:

$$K(r) = (2\pi)^{-1/2} \exp\left(-\frac{1}{2} r^2 \right), \qquad (2)$$

m – кількість елементів вибірки (кількість векторів класу у ϵY);

h_j – ширина ядра;

До переваг запропонованої інтелектуальної системи прогнозування ризикових ситуацій можна віднести стабільну активність в режимі реального часу, доступність вхідних даних для прийняття рішення, зручність у використанні, оскільки функціонал інтелектуальної системи являє собою імпортований модуль.

Запропонована інтелектуальна система прогнозування ризиків виникнення пожеж на регіональному рівні, може бути включена, як одна з функціональних компонент інформаційно-комунікаційної системи комплексного моніторингу регіонального ситуаційного центру.

Список використаних джерел:

1. Бродський Ю. Б., Ковбасюк С. В. Концептуальний підхід до створення ситуаційного центру сталого розвитку регіону. Сучасні інформаційні технології у сфері безпеки та оборони. 2024. № 1 (49). С. 151–159.
2. Russell, S., & Norvig, P. (3d or 4th Edition). Artificial intelligence: a modern approach. 5 Goodfellow I, Bengio Y, Courville A., Deep Learning // MIT, 2017 – 800 с.
3. Шолле Франсуа. Глибоке навчання на Python. — К. Наукова думка, 2018. — 400 с.: іл. —. ISBN 978-5-4461-0770-4
4. Гифт Ной. Прагматичний ШІ. Машинне навчання і хмарні технології. – К. 2019. - 304 с.: ISBN 978-5-4461-1061-2
5. Стратегія розвитку штучного інтелекту в Україні: монографія / за заг. ред. А. І. Шевченка. Київ, 2023. 305 с. URL: https://jai.in.ua/archive/2023/ai_mono.pdf (дата звернення: 21.03.2025).

УДК 004.056

Дячук О.Ю., ст. викладач
Колощук М.С., асистент
Макаревич С.О., здобувач
Цимбалюк І. І., здобувач
Державний університет «Житомирська політехніка»

МЕТОДИ ЗАХИСТУ ВІД BGP-HIJACKING В ЕПОХУ ГІБРИДНИХ ЗАГРОЗ

BGP-hijacking є серйозною загрозою для глобальної мережевої безпеки, особливо в контексті гібридної війни, де кіберзагрози поєднуються з військовими операціями, економічним тиском та інформаційними атаками. Ефективний захист вимагає комплексного підходу, який включає аутентифікацію BGP-оголошень, використання штучного інтелекту (ШІ) для виявлення атак, нормативні заходи та підготовку фахівців у сфері кібербезпеки.

Оскільки протокол BGP не має вбудованої аутентифікації маршрутних оголошень, це створює вразливість для атак, таких як підміна маршрутів (BGP-hijacking). Щоб мінімізувати ці ризики, впроваджуються сучасні механізми захисту, серед яких найпоширенішими є RPKI, BGPsec і ROV.

RPKI (Resource Public Key Infrastructure) – криптографічний механізм для перевірки права власності на IP-адреси. Він дозволяє підписувати BGP-оголошення за допомогою цифрових сертифікатів, що значно знижує ймовірність маніпуляцій із маршрутною інформацією [1].

BGPsec – це розширення BGP, яке додає криптографічний захист маршрутної інформації. Воно забезпечує аутентифікацію кожного етапу маршруту, ускладнюючи несанкціоновані зміни. Основними викликами є високе навантаження на обладнання та складність імплементації.

ROV (Route Origin Validation) працює у зв'язці з RPKI та блокує оголошення від автономних систем, які не мають підтвердженого права на певний IP-префікс. Незважаючи на ефективність, компрометація ключової інфраструктури може спричинити масштабні проблеми в глобальній маршрутизації.

Фільтрація маршрутів це ще один важливий механізм захисту від BGP-hijacking. Вона дозволяє інтернет-провайдерам контролювати, які маршрути приймаються та передаються їхньою мережею, запобігаючи поширенню несанкціонованих або шкідливих оголошень. Одним із найефективніших підходів є використання суворих політик фільтрації,

де оператори мережі приймають маршрути лише від перевірених джерел, зокрема через списки дозволених префіксів (whitelisting). Це значно знижує ризик підміни маршрутів і мінімізує вплив потенційних атак. Також застосовується чорний список (blacklisting) для блокування підозрілих або вже відомих зловмисних автономних систем. Завдяки такому підходу можна оперативно реагувати на загрози та захищати критичні мережеві інфраструктури.

Крім вище зазначених механізмів велику роль відіграє ШІ, який активно використовується для аналізу аномалій у маршрутизації. Наприклад, нейромережі можуть навчатися на історичних даних про нормальну роботу мережі та виявляти відхилення, які можуть свідчити про потенційні атаки [2].

Одним із важливих підходів є прогнозування атак. Використовуючи методи машинного навчання, можливо аналізувати великі обсяги BGP-даних і виявляти загрози ще до того, як вони завдадуть шкоди.

На практиці вже існують ефективні рішення, які застосовують ШІ для моніторингу та захисту BGP-маршрутизації. Наприклад, ARTEMIS автоматично виявляє спроби BGP-HIJACKINGта допомагає операторам швидко реагувати на атаки [1].

Оскільки BGP-hijacking є серйозною загрозою, освітнім установам варто розширювати навчальні програми, включаючи теми, пов'язані з BGP, у курси з мережевої безпеки. Лабораторні роботи з використанням Cisco Packet Tracer, GNS3 та інших симуляторів дають студентам змогу практично вивчати атаки та методи захисту. Аналіз реальних кейсів та участь у CTF-змаганнях сприяють глибшому розумінню загроз та способів їх нейтралізації.

Крім аудиторних занять, важливу роль відіграє стажування у центрах реагування на кіберінциденти (CERT) та кібербезпекових лабораторіях.

Ще одним перспективним напрямом є розробка відкритих платформ для моделювання BGP-атак, які дозволять студентам та дослідникам експериментувати з різними сценаріями загроз.

Зростання кількості автономних систем (AS) ускладнює контроль маршрутизації. До того ж автоматизація атак за допомогою ШІ дозволяє зловмисникам швидше знаходити вразливості та здійснювати більш витончені атаки.

Хмарні сервіси (AWS, Google Cloud, Azure) є особливо вразливими до BGP-атак, оскільки будь-яке порушення їхньої роботи може призвести до значних фінансових та репутаційних втрат [3].

Серед перспективних методів захисту можна виділити:

1. Децентралізовану аутентифікацію на основі блокчейн-технологій.
2. Активне застосування ШІ для моніторингу BGP-трафіку.
3. Міжнародну співпрацю між провайдерами, державними установами та організаціями, що займаються кібербезпекою.
4. Юридичну відповідальність для інтернет-провайдерів, які нехтують належними стандартами безпеки [4].

BGP-хайджекінг залишається серйозною загрозою для стабільності інтернету, особливо в умовах кіберконфліктів та зростаючої залежності від цифрових технологій. Існуючі методи захисту, зокрема криптографічна аутентифікація та автоматизований моніторинг, значно знижують ризики, але потребують подальшого вдосконалення. У майбутньому розвиток штучного інтелекту дозволить не лише виявляти атаки, а й передбачати їх, а впровадження децентралізованих систем верифікації на основі блокчейну може створити більш надійну модель маршрутизації. Важливу роль також відіграватиме міжнародна співпраця та оновлення нормативної бази, що зобов’яже провайдерів дотримуватися високих стандартів безпеки. Поєднання технологічних рішень, регулювання та освітніх ініціатив допоможе сформувати більш стійку та захищену інтернет-інфраструктуру.

Список використаних джерел:

1. Monitor, Detect, Mitigate: Combating BGP Prefix Hijacking in Real-Time with ARTEMIS / P. Sermpezis та ін. Networking and Internet Architecture. 2016. URL: https://arxiv.org/abs/1609.05702 (дата звернення: 15.03.2025).
2. Shapira T., Shavitt Y. A Deep Learning Approach for IP Hijack Detection Based on ASN Embedding. NetAI '20: Proceedings of the Workshop on Network Meets AI & ML. 2020. С. 35–41. URL: https://dl.acm.org/doi/10.1145/3405671.3405814 (дата звернення: 15.03.2025).
3. Shepardson D. White House asks agencies to step up internet routing security efforts. Reuters. URL: https://www.reuters.com/world/us/white-house-asks-agencies-step-up-internet-routing-security-efforts-2024-09-03/ (дата звернення: 15.03.2025).
4. Rundle J. White House Takes Aim at Internet Security. The Wall Street Journal. URL: https://www.wsj.com/articles/white-house-takes-aim-at-internet-security-78103a69 (дата звернення: 15.03.2025).
5. Zubok V. Y. Поєднання традиційних методів і метричного підходу до оцінки ризиків від кібератак на глобальну маршрутизацію. Реєстрація, зберігання і обробка даних. 2019. Т. 21, № 2. С. 41–48. URL: https://doi.org/10.35681/1560-9189.2019.21.2.180256 (дата звернення: 20.03.2025).

УДК 004:35+623:7

Устименко І.І., здобувач,
Куліш М. В., здобувач,
Коломієць Р.О., к.т.н. , доцент,
Котенко В.М., к.т.н. , доцент
Державний університет «Житомирська політехніка»

ТЕХНІЧНІ АСПЕКТИ СТВОРЕННЯ АКУСТИЧНОГО ДЕТЕКТОРА

Створення акустичного детектора дронів є надзвичайно важливим завданням для забезпечення безпеки й моніторингу в сучасному світі. Основою такого пристрою є акустичні сенсори, які працюють на основі виявлення звукових хвиль, створених дронами. Звук гвинтів та двигунів кожного дрона має унікальну акустичну підпис, що дозволяє відрізняти їх від інших джерел звуку. Для аналізу цих даних використовуються спектрограми, які виділяють характерні частоти звуку. Таким чином, акустичний детектор може виявляти дрони навіть у складних умовах.

Ключовою частиною технології є обробка звукових сигналів. Застосування цифрової обробки сигналів (DSP) дозволяє відфільтровувати шум та виділяти необхідні звукові підписи. Сучасні системи використовують алгоритми машинного навчання, зокрема нейронні мережі, які дозволяють ефективніше класифікувати звуки та знижувати кількість помилкових спрацьовувань. Ці технології відкривають можливість автоматизації виявлення дронів, що є важливим для зон підвищеного ризику, таких як аеропорти, військові бази або критична інфраструктура.

Розробка таких систем стикається з технічними викликами, зокрема фоновим шумом у міських чи природних умовах, який ускладнює роботу детекторів. Для вирішення цієї проблеми впроваджуються адаптивні фільтри та алгоритми шумозаглушення, що ізолюють корисний сигнал. Також погані погодні умови, як-от вітер і дощ, впливають на якість даних, що потребує створення стійких сенсорів.

Ще одним викликом є дальність виявлення. Звукові хвилі мають обмежений радіус поширення через затухання в повітрі, що зменшує ефективність акустичних детекторів на великих відстанях. Для подолання цієї проблеми використовуються високочутливі мікрофони, а також комбінуються кілька сенсорів у єдину систему. Іншим важливим аспектом є енергоспоживання таких пристроїв. Оскільки обробка даних вимагає значної обчислювальної потужності, автономні системи можуть швидко витрачати заряд, що є проблемою для довготривалого використання.

Акустичні детектори також інтегруються з іншими технологіями, такими як радіочастотні або оптичні сенсори, для підвищення загальної надійності системи. Такий підхід допомагає зменшити кількість помилкових спрацьовувань і покращити точність ідентифікації. Інтеграція різних методів розширює можливості системи, роблячи її більш адаптивною до різних умов.

Акустичні сенсори можна використовувати в міських умовах для безпеки під час масових заходів, встановлюючи їх на дахах або в ключових точках. Вони допомагають оперативно реагувати на загрози, зокрема незаконне використання дронів. У Європі такі технології вже інтегрують у системи громадської безпеки.

Один із цікавих прикладів використання акустичних детекторів дронів стосується охорони національних кордонів. Наприклад, у США вони використовуються у взаємодії з іншими технологіями, такими як радарні системи та радіочастотний моніторинг. Акустичні системи дозволяють фіксувати дрони, які можуть використовуватися для нелегального транспортування через кордон, що є серйозною загрозою. Ця інтеграція демонструє ефективність багатосенсорного підходу для вирішення складних завдань моніторингу.

Серед готових рішень можна виділити проєкт DroneShield, який розробляє акустичні системи для виявлення дронів. Їхні пристрої працюють на основі аналізу звукових хвиль, що дозволяє ідентифікувати дрони навіть у складних умовах. Інший приклад — система AUDS (Anti-UAV Defence System), яка включає акустичні модулі в поєднанні з радаром і оптичними камерами для багаторівневого моніторингу.

Отже, акустичні детектори дронів є важливим інструментом, що, підвищує безпеку завдяки DSP, машинному навчанню та багатосенсорним системам, що вже активно впроваджуються у світі.

Список використаних джерел:

1. AUDS: Anti-UAV Defence System. Blighter Surveillance Systems. URL: https://www.blighter.com/products/auds-anti-uav-defence-system/ (дата звернення: 13.03.2025).

2. DroneShield – Advanced Counter-UAS Solutions. DroneShield. URL: https://www.droneshield.com/media/news-coverage/advanced-counter-drone-solutions-drive-growth-in-emerging-security-industry (дата звернення: 13.03.2025).

3. Acoustic Detection and Tracking of Unmanned Aerial Vehicles. Sensors. 2020. URL: https://www.mdpi.com/1424-8220/20/17/4870 (дата звернення: 13.03.2025).

4. Deep Learning-Based UAV Detection Using Acoustic Data. Drones. 2021. URL: https://www.mdpi.com/2504-446X/5/3/54 (дата звернення: 13.03.2025).

УДК 004.056

Савчук В.С., здобувачка
Ніколаєнко М.В., здобувачка
Шелуха О.О., к.т.н., доцент
Державний університет «Житомирська політехніка»

АНАЛІЗ МОДЕЛЕЙ ІНФОРМАЦІЙНОЇ ЗАХИЩЕНОСТІ ОСОБИСТОСТІ

В умовах сучасних кібервійн та інформаційно-психологічних впливів забезпечення інформаційної захищеності особистості є основою системи, яка визначає рівень захисту особистих даних та психічного здоров'я пересічного користувача. Тому варто розглянути відмінності підходів до захисту інформаційної безпеки, що застосовуються різними методами.

Перш за все визначимо що таке інформаційна захищеність особистості – це стан, при якому особисті дані та психічне здоров'я людини захищені від загроз, які можуть призвести до витоку чи зміни персональних даних, а також до психологічного впливу через маніпуляцію інформацією або дезінформацію.

Проведемо порівняння моделей захисту:

- Модель інтегрованого захисту (Технологічний підхід + Психологічний підхід). Ця модель фокусується на комплексному підході, поєднуючи технологічні засоби захисту (шифрування даних, антивірусне програмне забезпечення) з психологічними заходами (розвиток критичного мислення, навчання стійкості до інформаційного впливу). Такий підхід забезпечує високий рівень захищеності, але потребує значних витрат на впровадження як технічних, так і психологічних програм.
- Модель на основі технологічних засобів захисту. Ця модель орієнтується на використання новітніх технологій для забезпечення безпеки даних, таких як фаєрволи, шифрування, антивірусне програмне забезпечення. Вона дозволяє гарантувати захист від зовнішніх загроз та маніпуляцій з інформацією, проте не включає психологічні аспекти захисту, що може бути критично важливим для запобігання психологічним атакам або маніпуляціям в інформаційних потоках.
- Модель на основі психологічного захисту особистості. Тут основний акцент зроблено на розвиток психологічної стійкості особистості, уміння протистояти інформаційним загрозам, таким як дезінформація, маніпуляція в соціальних мережах, фальшиві новини. Така модель може бути менш затратною, проте вона потребує значних ресурсів для освіти і тренування користувачів, щоб вони могли

критично оцінювати інформацію та захищати свою психіку від зовнішніх впливів.

Вибір моделі для захисту особистості від соціологічної інформації є важливим кроком у розробці системи безпеки. Можна виділити кілька ключових факторів, які слід враховувати під час вибору моделі:

- Психологічний вплив соціологічної інформації. Соціологічна інформація, яка включає в себе новини, соціальні медіа, пропаганду, може мати сильний вплив на психіку людини. Моделі, які забезпечують психологічну стійкість, допоможуть знизити ризик маніпуляцій та психологічних атак.
- Захист від дезінформації. Моделі, які використовують технології перевірки фактів, шифрування та анонімізації, можуть допомогти користувачеві уникнути попадання під вплив неправдивої або маніпулятивної інформації.
- Навчання та освіта. Моделі, що включають в себе освітні програми з підвищення інформаційної грамотності та критичного мислення, можуть допомогти особистості розпізнати і протистояти загрозам, які виникають через соціологічну інформацію.

Якщо йдеться про захист психічного здоров'я, то важливими факторами будуть:

- Психологічна стійкість та критичне мислення. Моделі, які розвивають ці навички, будуть дуже корисні для людей, які постійно перебувають під впливом соціологічної інформації. Це включає програми тренінгів та освітні кампанії.
- Інформаційна грамотність. Моделі, що підвищують рівень інформаційної грамотності, допоможуть користувачам відрізняти правдиву інформацію від маніпулятивної, що особливо важливо в умовах сучасних соціальних медіа.
- Технічні засоби захисту. Використання фільтрів для блокування шкідливих або маніпулятивних повідомлень, шифрування повідомлень та захист даних також допоможе запобігти небезпечному впливу на особистість.

Отже, при розробці моделі для інформаційної захищеності особистості в умовах впливу соціологічної інформації важливо знайти оптимальне поєднання технологічних і психологічних підходів. Це дозволить забезпечити максимальний рівень захисту як від зовнішніх загроз, так і від маніпуляцій на рівні свідомості.

Список використаних джерел:

1. Ветлицька О. С., Дзюба Т. М. Модель оцінки впливу соціологічної інформації на поведінку людини в контексті її інформаційної безпеки. Телекомунікаційні та інформаційні технології. 2022. № 4 (77). С. 35–45. DOI: https://doi.org/10.31673/2412-4338.2022.043545 (дата звернення: 21.03.2025).

УДК 004.056

Дячук О.Ю., ст. викладач
Іваницький Р.В., здобувач
Державний університет «Житомирська політехніка»

КОМПРОМЕТАЦІЯ ПРОТОКОЛІВ КВАНТОВИХ КОМУНІКАЦІЙ ТА ВПЛИВ НА БЕЗПЕКУ МЕРЕЖ МАЙБУТНЬОГО

З розвитком квантових технологій виникає необхідність дослідження потенційних загроз у протоколах квантових комунікацій та їхнього впливу на безпеку інформаційних мереж. Квантові комунікації пропонують революційні методи захисту даних, такі як квантовий розподіл ключів (QKD), однак вони також мають власні вразливості, що можуть бути експлуатовані зловмисниками.

Одним із головних принципів квантової криптографії є неможливість перехоплення інформації без її зміни, що базується на фундаментальних законах квантової механіки. Найпоширенішим протоколом є BB84, який дозволяє обмінюватися ключами без ризику перехоплення. Однак у практичних реалізаціях таких протоколів існують фізичні вразливості, що можуть бути використані для атак. Наприклад, лазерні атаки на детектори або атаки за допомогою маніпуляцій джерелом світла можуть дозволити зловмиснику зчитувати інформацію без порушення узгоджених правил передачі квантових даних .

Квантові комп'ютери також становлять серйозну загрозу для сучасних криптографічних методів, що базуються на складності обчислення, таких як RSA та алгоритми на основі еліптичних кривих. Завдяки алгоритму Шора квантові обчислювальні пристрої зможуть розкладати великі числа на множники в експоненційно коротший термін порівняно з класичними комп’ютерами. Це призведе до необхідності розробки квантово-стійкої криптографії, що базується на задачах, які складно вирішити навіть для квантових обчислень .

Окрім вразливостей на рівні криптографії, існують ризики, пов’язані із фізичною інфраструктурою квантових мереж. Наприклад, квантові повторювачі, що використовуються для збільшення дальності передачі квантових сигналів, можуть стати об’єктом атак. Вразливості можуть включати маніпуляції з квантовими станами або створення штучних заплутаних пар частинок для введення системи в оману. Також існує ризик атак на рівні синхронізації квантових сигналів, що може призвести до збільшення похибок у передачі даних [1].

Для мінімізації ризиків у квантових комунікаціях розглядаються кілька напрямків розвитку безпеки. По-перше, це вдосконалення механізмів виявлення атак, включаючи використання нових методів контролю параметрів переданих квантових частинок. По-друге, досліджується можливість створення гібридних криптографічних протоколів, що поєднують квантові та постквантові методи захисту. Крім того, тривають дослідження з розробки більш надійних квантових повторювачів та методів компенсації можливих атак на фізичному рівні [2].

Одним із перспективних напрямків є створення постквантових алгоритмів, що базуються на математичних задачах, які не піддаються ефективному вирішенню квантовими комп'ютерами. Прикладами таких алгоритмів є криптографія на основі решіток, хеш-функцій та ізогеній еліптичних кривих. Ці алгоритми вже активно досліджуються в рамках міжнародних стандартів, таких як ініціатива NIST щодо постквантової криптографії [3].

Ще одним важливим напрямком є застосування блокчейн-технологій для забезпечення цілісності квантових комунікацій. Розподілені реєстри можуть гарантувати достовірність переданих квантових ключів, унеможливлюючи їхню компрометацію з боку зловмисників.

Таким чином, дослідження вразливостей квантових комунікаційних систем та їхній вплив на безпеку майбутніх мереж є критично важливим завданням. Попри переваги квантової криптографії, залишається низка викликів, що потребують вирішення, включаючи як фізичні атаки, так і ризики, пов’язані з появою квантових обчислень. Розвиток нових захисних механізмів та адаптація криптографії до нових реалій є ключовими напрямками для забезпечення інформаційної безпеки у майбутньому.

Список використаних джерел:

1. Xu F., Ma X., Zhang Q., Lo H. K., Pan J. W. Secure quantum key distribution with realistic devices. Reviews of Modern Physics. 2020. Vol. 92, No. 2. P. 025002. URL: https://arxiv.org/abs/1903.09051 (дата звернення: 15.03.2025).
2. Pirandola S., Andersen U. L., Banchi L., Berta M., Bunandar D., Colbeck R., ... Wallden P. Advances in quantum cryptography. Advances in Optics and Photonics. 2020. Vol. 12, No. 4. P. 1012–1236. URL: https://arxiv.org/abs/1906.01645 (дата звернення: 15.03.2025).
3. Chen L., Jordan S., Liu Y. K., Moody D., Peralta R., Perlner R., Smith-Tone D. Report on post-quantum cryptography. National Institute of Standards and Technology, 2016. URL: https://www.scirp.org/reference/referencespapers?referenceid=3702424 (дата звернення: 15.03.2025).

УДК 004.75

Приходько Д.С., здобувач
Шелуха О.О., к.т.н., доцент
Державний університет «Житомирська політехніка»

ЗАСТОСУВАННЯ ТОПОЛОГІЇ SPINE-LEAF У ВЕЛИКИХ ДАТА-ЦЕНТРАХ

У сучасних умовах розвитку інформаційних технологій дата-центри відіграють ключову роль у забезпеченні стабільного функціонування хмарних сервісів, інтернет-компаній та цифрової економіки загалом. В результаті зростає попит на обробку великих обсягів даних та високі вимоги до швидкості передачі інформації, які вимагають вдосконалення мережевої інфраструктури дата-центрів. Однією з найважливіших складових цієї інфраструктури становить система маршрутизації, від ефективності якої залежить продуктивність, масштабованість та відмовостійкість всієї мережі. Проблема полягає в тому, що традиційні протоколи маршрутизації, які широко використовуються в корпоративних або глобальних мережах, не завжди здатні забезпечити потреби великих дата-центрів. Тому, зазвичай постає проблема забезпечення високої пропускної здатності, мінімізації затримок, рівномірного розподілу трафіку та забезпечення стабільної роботи мережі навіть у разі відмови окремих її компонентів.

Проведемо аналіз сучасних підходів до маршрутизації у великих дата-центрах, актуальних протоколів та технологій, а також шляхів оптимізації процесів маршрутизації і архітектурних рішень, протоколів маршрутизації і програмно-конфігурованих мереж SDN. Із зростанням обсягів даних і кількості підключених пристроїв виникає необхідність побудови такої мережі, яка здатна динамічно адаптуватися до змін навантаження, забезпечувати рівномірний розподіл трафіку та мати високу відмовостійкість. Для її вирішення потрібне впровадження сучасних методів маршрутизації та інноваційних технологій.

Однією з технологій, які можуть використовувати сучасні дата-центри це застосування топології Spine-Leaf, яка дозволяє уникнути класичних вузьких місць, властивих ієрархічним мережам. В основі цієї архітектури лежить концепція рівномірного з'єднання leaf-комутаторів із spine-комутаторами, яка забезпечує однакову кількість переходів між будь-якими двома вузлами мережі. Це сприяє вирішенню одразу кількох проблем, таких як: мінімізація затримок та легке масштабування інфраструктури без потреби кардинальних змін у її побудові. Щодо протоколів маршрутизації, то в дата-центрах широко застосовується ECMP (Equal-Cost Multi-Path), який дозволяє рівномірно розподіляти трафік між декількома маршрутами з однаковою метрикою. Такий спосіб дає змогу уникнути перевантаження окремих каналів зв'язку та забезпечує балансування навантаження.

Особливої уваги заслуговує протокол BGP, який зазвичай використовувався для маршрутизації між автономними системами, однак у великих дата-центрах все частіше застосовується і всередині мережі. Використання внутрішнього BGP дає змогу краще контролювати маршрути та масштабувати мережу, уникнувши обмежень, притаманних протоколам типу OSPF. Комбінація BGP із технологією VXLAN та EVPN дозволяє створювати віртуальні підмереж поверх фізичної інфраструктури, що значно спрощує сегментацію та ізоляцію трафіку між різними клієнтами чи сервісами. Усе більшого значення набуває використання програмно-конфігурованих мереж (SDN), що дозволяють централізовано керувати всією мережею за допомогою спеціального контролера, який отримує актуальну інформацію про стан мережі й динамічно змінює маршрути відповідно до поточного навантаження або при відмові окремих її елементів.

Попри зазначені переваги, існує і низка проблем. Зокрема, складнощі виникають при необхідності масштабування мережі до сотень або навіть тисяч комутаторів. Тоді важливим питанням постає забезпечення відмовостійкості, адже вихід з ладу spine-комутатора може вплинути на працездатність великої кількості сервісів. Також слід приділити увагу питанням безпеки, зокрема захисту від можливих атак на протоколи маршрутизації, таких як BGP hijacking. Особливим викликом також залишається автоматизація процесів моніторингу та конфігурації мережі.

Отже, для ефективної роботи великих дата-центрів доцільно використовувати топологію Spine-Leaf у поєднанні з сучасними протоколами маршрутизації, такими як BGP, ECMP, а також технологіями віртуалізації мережі VXLAN та EVPN. Застосування SDN-підходів дає змогу спростити управління мережею та швидко реагувати на зміни. Слід також відмітити необхідність ретельного планування масштабування мережевої інфраструктури, забезпечення надійного механізму відмовостійкості, а також впровадження засобів автоматизації управління мережею.

Список використаних джерел:

1. What is data center networking? *VMware.* URL: https://www.vmware.com/topics/data-center-networking (дата звернення: 12.03.2025).

2. Data Center Networking Technologies. *Data Centre Magazine.* URL: https://datacentremagazine.com/top10/top-10-data-centre-networking-technologies (дата звернення: 12.03.2025).

3. Use of BGP for Routing in Large-Scale Data Centers. *IETF Datatracker.* URL: https://datatracker.ietf.org/doc/draft-ietf-rtgwg-bgp-routing-large-dc/00/ (дата звернення: 12.03.2025).

4. Data Center Spine-and-Leaf Architecture. *TechTarget.* URL: https://www.techtarget.com/searchdatacenter/definition/Leaf-spine (дата звернення: 12.03.2025).

5. Software-Defined Networking (SDN) Definition. *VMware.* URL: https://www.vmware.com/topics/software-defined-networking (дата звернення: 12.03.2025).

УДК 004.7

Єфіменко Д.А., здобувач,
Карманюк В.С., здобувач,
Ковальчук О.М., здобувач,
Колощук М.С., асистент
Державний університет «Житомирська політехніка»

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ LI-FI ДЛЯ ПІДВИЩЕННЯ БЕЗПЕКИ КОРПОРАТИВНИХ БЕЗДРОТОВИХ МЕРЕЖ

Сьогодні людство активно використовує технологію Wi-Fi, навіть не маючи приводу замислюватися про альтернативи. Проте, вчені в усьому світі продовжують вивчати й інші способи передачі даних, у тому числі, ті, про які більшість з нас навіть не може помислити. Серед нових віянь слід виділити технологію Li-Fi, якій пророкують досить великі перспективи використання, аж до повного витіснення більшості з відомих на сьогодні способів передачі інформації.

Термін «Li-Fi» був придуманий та введений у широкий ужиток у 2011-тому році вченим-фізиком німецького походження, фахівцем у області бездротової та оптичної передачі даних, професором, завідувачем кафедри мобільного зв'язку у Університеті Едінбургу Харальдом Хаасом. Він представив свої напрацювання у рамках конференції «TED Global», використавши досить звичайну світлодіодну лампу для передачі інформації. Досвід, що був продемонстрований, полягав у тому, що лампочка випускала хвилі, завдяки яким на екран проектувалося відео з квіткою, а на підтвердження того, що джерелом трансльованих відеоданих є саме світлоприлад, Хаас періодично перекривав її світло рукою, викликаючи перешкоди.

Принцип роботи Li-Fi

Принцип роботи Li-Fi заснований на передачі даних за допомогою амплітудної модуляції джерела світла у чітко визначений і стандартизований спосіб. Світлодіоди можуть вмикатися і вимикатися швидше, ніж людське око може це помітити, оскільки швидкість роботи світлодіодів становить менше 1 мікросекунди. Це невидиме вмикання-вимикання дозволяє передавати дані за допомогою двійкових кодів. Якщо світлодіод увімкнений, передається цифрова «1», а якщо світлодіод вимкнений, передається цифровий «0».

Як працює технологія Li-Fi

Принцип роботи Li-Fi дуже простий. На одному кінці є випромінювач світла, тобто світлодіодний передавач, а з іншого - фотодетектор (датчик освітленості). Дані, що надходять на світлодіодний передавач, кодуються у світлі (технічно це називається

видимим світловим зв'язком) шляхом зміни частоти мерехтіння світлодіодів швидкості, з якою світлодіоди мерехтять «увімкненими» і «вимкненими», генеруючи різні послідовності 1 і 0.

Принцип роботи зображений на рисунку 1.1

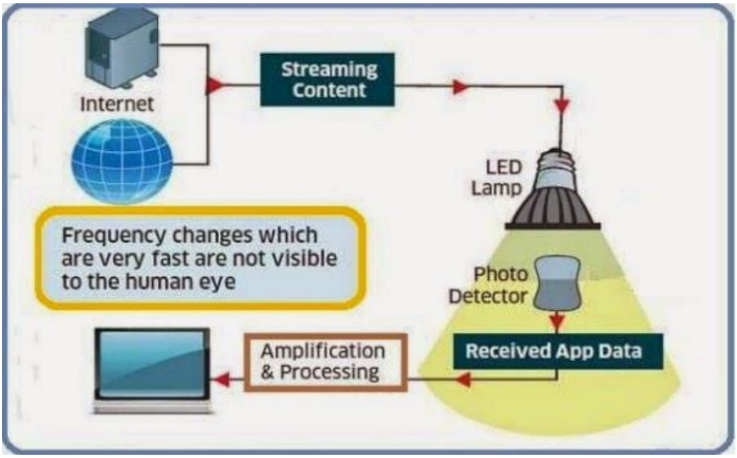


Рис. 1.1. Принцип роботи Li-Fi

Рис. 1.2. Принцип роботи Li-Fi

Переваги застосування технології Li-Fi для організації корпоративних мереж

1. Сегментація мережі. Оскільки Li-Fi має локалізоване покриття, його можна використовувати для фізичного розділення мереж задля забезпечення безпеки. Поділ можна застосувати як і для цілих приміщень чи корпусів, так і для окремих робочих місць, без ризику витоку трафіку за межі цих зон.

2. Контроль доступу та управління ідентифікацією. Використовуючи ту саму властивість локалізованого покриття Li-Fi змушує користувачів фізично перебувати в зоні покриття сигналу, що значно знижує ризики несанкціонованого доступу.

3. Принцип мінімальних прав. Li-Fi може підтримувати принцип мінімальних привілеїв, оскільки доступ обмежується не лише принципами ідентифікації, аутентифікації та авторизації, а й фізичною присутністю пристроїв в певній зоні.

4. Принципи нульової довіри. Підхід коли жоден користувач або пристрій за своєю суттю не є надійним, навіть у середині мережі. Це передбачає перевірку ідентичності та суворе дотримання доступу з найменшими привілеями, що і LiFi може забезпечити при грамотному фізичному розподілі пристроїв.

5. Шифрування даних. Шифрування даних перетворює дані в нечитабельні формати для неавторизованих користувачів, забезпечуючи конфіденційність і запобігаючи неавторизованому доступу. Це критично важливий компонент у захисті конфіденційної інформації, від особистих даних до інтелектуальної власності, у мережах і системах зберігання. Ризик перехоплення даних значно зменшується за рахунок обмеження поширення світла.

Якщо дивитися правді у очі, то ймовірність експансії Li-Fi є великою вже у найближчі п'ять років. Для цього вже зараз є багато передумов не тільки технічного характеру, але також у запитах суспільства, його підготовленості та наявності базової інфраструктури. Відомо, що енергоефективність, яка вже сьогодні знаходиться у тренді, у подальшому буде тільки набирати оберти, а це означає неминучий попит на таку продукцію. Той самий Wi-Fi, за усіх його сильних боків, має мізерний ККД, якщо розглядати його з точки зору техніки – усього лише 5-7%. У діодах же при виконанні сполученої задачі освітлення та передачі даних сукупний ККД починається від 65%, й уже відомо, що у самому найближчому майбутньому він зможе досягати 90%.

Список використаних джерел:

1. Network Security Architecture: 8 Key Components and Best Practices. Faddom. URL: https://faddom.com/network-security-architecture-8-key-components-and-best-practices/ (дата звернення: 11.03.2025).
2. Why LiFi is More Secure Than WiFi. LiFi.com. URL: https://lifi.co/why-lifi-is-more-secure-than-wifi/ (дата звернення: 11.03.2025).
3. Li-Fi: передача даних за допомогою світлодіодів. 5Watt.ua. URL: https://5watt.ua/uk/blog/statti/li-fi-peredacha-danikh-za-dopomogoyu-svitlodiodiv (дата звернення: 11.03.2025).
4. LiFi Study Paper. Telecommunication Engineering Centre (TEC), India. URL: https://tec.gov.in/pdf/Studypaper/lifi%20study%20paper%20-%20approved.pdf (дата звернення: 11.03.2025).

УДК 004.056

Дячук О.Ю., ст. викладач
Окунькова О.О., ст. викладач
Млинський Б.М., здобувач
Державний університет «Житомирська політехніка»

ЕВОЛЮЦІЯ ТА ПЕРСПЕКТИВИ ЗАГРОЗ BGP-HIJACKING У КВАНТОВУ ЕПОХУ

Розвиток Інтернету привів до ускладнення його інфраструктури, що зробило безпеку маршрутизації одним із пріоритетних завдань. Протокол BGP (Border Gateway Protocol) залишається основою маршрутизації глобального трафіку, однак він не передбачає вбудованих механізмів аутентифікації та перевірки достовірності маршрутних оголошень. Це створює передумови для атак на маршрутизацію, серед яких найсерйознішою є BGP-hijacking. Останні дослідження вказують на те, що поява квантових комп'ютерів може як посилити загрози, так і надати нові можливості для захисту.

Історично атаки на BGP розпочалися з локальних маніпуляцій маршрутами, але згодом отримали глобальний масштаб, що підтверджують випадки зловживання в міжнародних телекомунікаційних мережах. З розвитком штучного інтелекту автоматизація таких атак стала ще більш витонченою, а з появою квантових обчислень можливості для маніпуляції маршрутами можуть зрости експоненційно.

BGP-hijacking передбачає зловмисне внесення змін до маршрутних таблиць, що дозволяє перенаправляти трафік через неконтрольовані вузли. Основними видами таких атак є:

1. Перехоплення трафіку – перенаправлення даних через вузли, які можуть аналізувати або змінювати інформацію.
2. Дестабілізація мережі – створення конфліктів у маршрутах, що може призвести до порушення доступності певних ресурсів.
3. Фальсифікація маршрутних оголошень – видавання автономної системи за власника IP-префіксу з метою маніпуляції трафіком.

Відсутність централізованої аутентифікації у BGP призводить до того, що будь-який оператор мережі може зробити оголошення про доступність певного маршруту, навіть якщо це не відповідає дійсності. Це дозволяє зловмисникам експлуатувати вразливості маршрутизації та завдавати значної шкоди інформаційному обміну.

Основний вплив квантових технологій на безпеку BGP полягає в тому, що квантові комп'ютери мають потенціал значно вплинути на традиційні методи захисту. З одного боку, вони можуть прискорити

процес зламу класичних криптографічних алгоритмів, що використовуються для захисту BGP. З іншого боку, квантова криптографія відкриває можливості для створення нових механізмів автентифікації, які будуть стійкими до атак квантових комп'ютерів.

Серед основних загроз, які може створити квантова епоха для BGP, можна виділити:

1. Злам криптографічних методів – квантові алгоритми, зокрема алгоритм Шора, здатні розшифровувати існуючі криптографічні протоколи, що робить нинішні методи аутентифікації вразливими.
2. Автоматизація атак – завдяки квантовим обчисленням можливим стає швидке тестування слабких місць у маршрутизації та прогнозування змін у мережі для її компрометації.

Попри нові загрози, квантова криптографія відкриває перспективи у створенні нових методів безпеки, які можуть підвищити захищеність BGP. Одним із найбільш перспективних напрямів є квантове розподілення ключів (QKD – Quantum Key Distribution), яке дозволяє обмінюватися криптографічними ключами так, що будь-яка спроба перехоплення буде виявлена.

Квантові комп'ютери можуть використовуватися не лише для атак, а й для їх виявлення. Завдяки здатності швидко обробляти величезні масиви даних, вони можуть аналізувати мережевий трафік у реальному часі, ідентифікуючи підозрілі маршрути.

У найближчі десятиліття, в міру того як квантові обчислення ставатимуть доступнішими, методи атак BGP-hijacking можуть кардинально змінитися. З одного боку, це підвищує загрози компрометації маршрутизації на глобальному рівні, а з іншого – змушує операторів мережевої інфраструктури адаптуватися до нових викликів. Майбутні розробки у сфері постквантової криптографії та автоматизованих систем моніторингу маршрутизації визначать стійкість Інтернету перед загрозами квантової епохи.

З огляду на майбутні виклики, необхідно розробляти адаптивні підходи до безпеки BGP, поєднуючи криптографічні, аналітичні та інтелектуальні методи захисту. Це дозволить не лише знизити ризики атак, а й забезпечити стабільність глобальних мереж у майбутньому.

Список використаних джерел:

1. Ekparinya P., Gramoli V., Jourjon G. Double-Spending Risk Quantification in Private, Consortium and Public Ethereum Blockchains. Cryptography and Security. 2018. URL: https://arxiv.org/abs/1805.05004?utm_source=chatgpt.com (дата звернення: 15.03.2025).
2. Estimating the Impact of BGP Prefix Hijacking / P. Sermpezis та ін. Networking and Internet Architecture. 2021. URL: https://arxiv.org/abs/2105.02346v1 (дата звернення: 15.03.2025).

УДК 004:35+623:7

Куліш М. В., здобувач
Устименко І. І., здобувач
Коломієць Р. О., к.т.н. , доцент
Котенко В. М., к.т.н. , доцент
Державний університет «Житомирська політехніка»

АКТУАЛЬНІСТЬ ТА ПРИНЦИП РОБОТИ ДЕТЕКТОРІВ ДРОНІВ

У сучасних умовах безпілотні літальні апарати (БПЛА) відіграють важливу роль у різних сферах, включаючи військову, комерційну та приватну діяльність. Вони використовуються для розвідки, моніторингу, логістики, сільського господарства, а також у військових конфліктах. Проте зростання кількості дронів супроводжується і збільшенням загроз безпеці, таких як незаконне спостереження, контрабанда, несанкціоноване проникнення на територію та використання у військових цілях.

В Україні дедалі більше уваги приділяється розробці та впровадженню систем виявлення дронів, оскільки їхнє широке застосування у воєнних умовах вимагає ефективних рішень для протидії. Вітчизняні підприємства вже почали розробляти сенсори для виявлення артилерії та інших повітряних загроз, що є важливим кроком у зміцненні обороноздатності країни.

Сучасні системи детекції дронів використовують комплексний підхід для виявлення та ідентифікації безпілотників. Основні методи включають [1, 2]:

1. Радіочастотний аналіз – детектори сканують частоти, на яких працюють дрони, зокрема 2,4 ГГц та 5,8 ГГц. Виявлення сигналів зв'язку між оператором і дроном дозволяє не лише визначити наявність БПЛА, а й встановити місцезнаходження його пілота.

2. Акустичне розпізнавання – деякі детектори використовують мікрофони для ідентифікації звуків, що видають дрони. Цей метод ефективний у ситуаціях, коли радіочастотний моніторинг не дає результату, наприклад, у випадку автономних дронів.

3. Оптичні та тепловізійні сенсори – камери високої роздільної здатності та інфрачервоні датчики дозволяють розпізнавати дрони візуально навіть у темний час доби.

4. Радарні системи – радари здатні виявляти дрони на основі відбитого сигналу. Вони дозволяють працювати незалежно від погодних умов та часу доби, що робить їх ефективним рішенням для військового використання.

5. Штучний інтелект та нейронні мережі – інтелектуальні системи використовують алгоритми машинного навчання для підвищення

точності ідентифікації дронів. Вони можуть розрізняти БПЛА від птахів, літаків та інших об’єктів у повітрі.

На ринку вже існує низка ефективних систем виявлення дронів, серед яких [3]:

- Dedrone – комплексне рішення, що поєднує радіочастотний моніторинг, камери та штучний інтелект для детекції дронів у міських та військових умовах.
- DroneShield – система, що використовує акустичні сенсори та штучний інтелект для розпізнавання дронів на основі їхнього шуму.
- Black Sage Defense – рішення, яке інтегрує радари, камери та системи активного захисту від БПЛА.
- Антидронові комплекси в Україні – вітчизняні розробки, зокрема нові сенсори для виявлення артилерії та безпілотників [4].

З розвитком безпілотних технологій методи їхнього виявлення та нейтралізації також вдосконалюються. Сучасні дослідження спрямовані на:

- Розробку більш точних і мобільних детекторів
- Інтеграцію з системами активного придушення дронів
- Використання розподілених мереж сенсорів

У військовій сфері впроваджуються автоматизовані системи, які поєднують декілька методів детекції для забезпечення максимальної ефективності та оперативного реагування на злочинні чи бойові загрози.

Отже, зростання використання дронів зумовлює необхідність розвитку технологій їхнього виявлення та протидії. Інтеграція сучасних рішень, включаючи радіочастотний аналіз, акустичне та оптичне розпізнавання, штучний інтелект і тепловізійні сенсори, забезпечує високий рівень безпеки. Україна активно розвиває власні технології у сфері детекції повітряних загроз, що є важливим внеском у захист критичної інфраструктури та військових об'єктів.

Список використаних джерел:

1. Blue Bird Tech. Детектор дронів: що це? [Електронний ресурс]. – Режим доступу: *URL* Blue Bird Tech. "Детектор дронів: що це?" (дата звернення: 13.03.25).

2. Безпека Veritas. Детектори FPV-дронів і БПЛА: захист і безпека на передовій [Електронний ресурс]. – Режим доступу: *URL* Безпека Veritas. "Детектори FPV-дронів і БПЛА: захист і безпека на передовій" (дата звернення: 13.03.25).

3. Elartu. Drone detection: технології та методи [Електронний ресурс]. – Режим доступу: *URL* Elartu. "Drone detection: технології та методи"(дата звернення: 13.03.25).

4. Економічна правда. В Україні почали виробляти сенсори для виявлення артилерії [Електронний ресурс]. – Режим доступу: *URL* Економічна правда. "В Україні почали виробляти сенсори для виявлення артилерії" (дата звернення: 13.03.25).

УДК 004.45:004.7

Шитов Є.А., магістрант
Фальковський І. Г., ст. викладач
Державний університет «Житомирська політехніка»

АНАЛІЗ СИСТЕМИ РЕЄСТРАЦІЇ ПОДІЙ GRAYLOG ТА ЇЇ АНАЛОГІВ, А ТАКОЖ МЕТОДИ ЇХ ЗАСТОСУВАННЯ ДЛЯ ЗАХИСТУ ДОМЕННИХ КОНТРОЛЕРІВ AD

В умовах сучасних кіберзагроз доменні контролери (DC), що є ключовими компонентами інфраструктури Active Directory (AD), потребують ефективних рішень для моніторингу та виявлення атак. Системи реєстрації подій, такі як Graylog, Splunk, ELK Stack та Wazuh, забезпечують централізований збір, аналіз та кореляцію логів, що є важливим елементом кібербезпеки організації.

У ході дослідження проведено порівняльний аналіз Graylog, Splunk, ELK Stack та Wazuh за ключовими критеріями: тип ліцензії, продуктивність обробки логів, інструменти аналізу загроз, можливості інтеграції з SIEM/SOAR-рішеннями, гнучкість налаштувань та спрощеність розгортання. Graylog, як система з відкритим кодом, забезпечує хорошу продуктивність та можливість розширення через власні плагіни. Splunk, хоч і є комерційним продуктом, має розвинені механізми поведінкового аналізу та підтримку машинного навчання. ELK Stack надає високу продуктивність та потужну систему індексації даних завдяки Elasticsearch, а Wazuh спеціалізується на виявленні загроз із вбудованими механізмами SIEM.

Graylog є рішенням з відкритим вихідним кодом, що підтримує централізований збір логів через Windows Event Forwarding (WEF) та дозволяє створювати гнучкі конвеєри обробки даних (pipelines) для ефективного аналізу без значного навантаження на систему. Splunk, будучи комерційним продуктом, забезпечує потужний аналітичний інструментарій, включаючи засоби машинного навчання для виявлення аномалій та аналізу поведінки користувачів (UEBA). ELK Stack, завдяки Elasticsearch, оптимізований для швидкої обробки великих обсягів даних та підтримує інтеграцію з Logstash для складних схем обробки подій. Wazuh спеціалізується на безпеці, пропонуючи вбудовані механізми SIEM та IDS/IPS, що дозволяють оперативно виявляти загрози, зокрема атаки Pass-the-Hash, Golden Ticket та інші методи компрометації облікових записів AD. [1]

Дослідження показало, що застосування Graylog для захисту доменних контролерів Active Directory дозволяє оперативно виявляти спроби компрометації облікових записів, атаки типу Pass-the-Hash,

Golden Ticket та інші методи зловмисників. Використання автоматизованих правил кореляції подій дає змогу швидко ідентифікувати аномальну активність, а інтеграція з системами реагування SOAR сприяє своєчасному нейтралізуванню загроз.

Аналіз ефективності систем реєстрації подій показав, що централізований моніторинг і аудит змін у критичних об’єктах AD значно знижує ризики несанкціонованого доступу. Впровадження Graylog дозволяє забезпечити відповідність міжнародним стандартам безпеки, зокрема ISO/IEC 27001, та підвищити рівень захисту корпоративних мереж.[2]

Окрім технічних аспектів, важливим фактором ефективного використання систем реєстрації подій є правильна організація політик безпеки та навчання персоналу. Недостатня обізнаність адміністраторів та операторів SOC щодо можливостей сучасних засобів моніторингу може призвести до пропуску критичних загроз. Тому доцільно розробляти стандартизовані сценарії реагування, регулярно оновлювати правила кореляції подій та проводити тренінги з аналізу інцидентів на основі отриманих журналів.[3]

Таким чином, результати дослідження підтверджують необхідність використання систем реєстрації подій для контролю безпеки доменних контролерів. Впровадження Graylog та аналогічних рішень дозволяє створити ефективну систему моніторингу та захисту від сучасних кіберзагроз.

Список використаних джерел:

1. What is Graylog?. [Електронний ресурс] /Graylog.org. – 2025. – Режим доступу до ресурсу: https://go2docs.graylog.org/current/what_is_graylog/what_is_graylog.htm

2. Тернистим шляхом до системи логування Graylog. [Електронний ресурс] / Євгеній Сафонов – 2019. – Режим доступу до ресурсу: https://dou.ua/lenta/articles/graylog-system/

3. Організація навчання працівників обізнаності з кібербезпеки [Електронний ресурс] / ITS CSAT. – 2025. – Режим доступу до ресурсу: https://my-itspecialist.com/organizing-employee-cybersecurity-awareness-with-its-csat

УДК 004.7

Лелета В. Р., здобувачка
Колощук М.С., асистент
Дячук О.Ю., ст. викладач
Державний університет «Житомирська політехніка»

ШТУЧНИЙ ІНТЕЛЕКТ ЯК ЗАСІБ РЕАГУВАННЯ НА МЕРЕЖЕВІ ЗАГРОЗИ

Зростання обсягів даних та складності кіберзагроз вимагає впровадження передових технологій для забезпечення безпеки інформаційних систем. Штучний інтелект (ШІ), завдяки своїм можливостям автоматизації та аналізу великих обсягів даних, стає ключовим інструментом у боротьбі з кіберзагрозами. Використання алгоритмів машинного навчання дозволяє ефективно класифікувати мережевий трафік, виявляти аномалії та реагувати на потенційні загрози в реальному часі.

На сьогоднішній день штучний інтелект стає досить потужним інструментом для різних цілей, зокрема для аналітики трафіку та прогнозування загроз в контексті кібербезпеки. Проте штучний інтелект має дві сторони: він може бути як найбільшою загрозою, так і виступати найефективнішим засобом захисту.

Такий багатогранний інструмент активно можуть використовувати як «червоні» хакери для спрощення та автоматизації цільового фішингу для викрадення особистих даних, виготовлення дипфейків для шахрайства та спрощення розробки шкідливого софту, так і «сині» хакери для виявлення DDoS-атак, фішингових кампаній, несанкціонованих доступів та аналізу великих обсягів логів у реальному часі.

Трафік можна класифікувати за кількома основними ознаками, залежно від його природи та цілей. Легітимний трафік включає запити від реальних користувачів або авторизованих систем, які виконують звичайні операції, такі як перегляд веб-сторінок або покупка товарів. Шкідливий трафік, натомість, містить атаки, направлені на злам або пошкодження системи, зокрема через методи, як DoS, DDoS або фішинг. Що стосується ботнет-трафіку, то це трафік, що генерується зловмисними мережами ботів, які можуть бути використані для розподілених атак або розповсюдження шкідливих програм.

Застосування сучасних алгоритмів машинного навчання для класифікації мережевого трафіку показало високу ефективність нейронних мереж глибокого навчання (94,7% точності), метод опорних векторів продемонстрував баланс точності (91,2%) та швидкодії, а

LSTM-архітектура досягла найкращого результату (97,3%) для виявлення часових атак.

Штучний інтелект виявляє аномалії в поведінці мережі через аналіз часових патернів, підозрілих IP-адрес та характерних ознак атак. Комбінований підхід з автоенкодерами та класифікаторами на основі градієнтного бустингу зменшує час реакції на загрози на 67% і знижує частоту помилкових тривог на 42% порівняно з традиційними системами.

Штучний інтелект дозволяє автоматично визначати відхилення від нормальної поведінки у трафіку, що є ключовим у виявленні загроз, таких як DDoS-атаки або спроби несанкціонованого доступу. Автоенкодери та рекурентні нейронні мережі навчаються на нормальному трафіку та виявляють незвичайні патерни, що може сигналізувати про потенційну атаку.

Штучний інтелект є потужним інструментом для підвищення рівня кібербезпеки завдяки здатності автоматизувати процеси аналізу трафіку та реагування на загрози. Використання нейронних мереж та інших алгоритмів машинного навчання дозволяє ефективно адаптуватися до нових типів атак і забезпечувати безперебійну роботу інформаційних систем навіть у складних умовах кіберзагроз. Подальші дослідження можуть бути спрямовані на вдосконалення моделей ШІ для роботи з великими обсягами даних у реальному часі.

Список використаних джерел:

1. Глоба, О. О. Трафік в Інтернеті та його класифікація: практичні аспекти / О. О. Глоба. – Харків : Національний університет радіоелектроніки, 2023. URL: https://pt.nure.ua/wp-content/uploads/2023/12/223_globa_traffic_.pdf

2. Ткачук, М. В. Інтелектуальний аналіз мережевого трафіку для виявлення шкідливих атак / М. В. Ткачук. – Вінниця : Вінницький національний технічний університет, 2022. URL: https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/42057/20610.pdf?sequence=3

3. Застосування ШІ у кібербезпеці: роль та переваги / Wezom. URL: https://wezom.com.ua/ua/blog/zastosuvannya-shi-u-kiberbezpetsi-rol-ta-perevagi

4. Штучний інтелект у корпоративній кібербезпеці: роль у захисті даних / BDO. URL: https://www.bdo.ua/uk-ua/insights-2/information-materials/2024/corporate-cybersecurity-ai-role-in-data-protection

5. Захист від ботнетів / ESET. URL: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/zashchita-ot-botnetov/?srsltid=AfmBOoppW3Y_7jXSFBRjelztS6qKBpa5qMRLKm9Qml0mLrLsTa78qWWg

6. DDoS-атаки: типи атак та рівні моделі OCI / AlexHost. URL: https://alexhost.com/uk/faq/ddos-ataky-typy-atak-ta-rivni-modeli-osi/

УДК 004.7

Шнипко Т. А., магістрантка
Бродський Ю. Б., к.т.н., доцент
Державний університет «Житомирська політехніка»

ЗАБЕЗПЕЧЕННЯ МЕРЕЖЕВОЇ БЕЗПЕКИ: КОМПЛЕКСНИЙ ПІДХІД ДО ЗАХИСТУ ІНФРАСТРУКТУРИ

Захист інформації в сучасних інфокомунікаційних мережах є одним із визначальних пріоритетів. Серед основних загроз слід виділити викрадення конфіденційної інформації, знищення даних, спотворення інформації та виведення з ладу комп'ютерних систем. Ефективна система безпеки повинна мати комплексний характер і забезпечувати захист від різноманітних загроз, включаючи контроль за діяльністю працівників, які мають доступ до внутрішніх ресурсів автоматизованої інформаційної системи.

Для досягнення цієї мети необхідно використовувати спеціалізовані апаратно-програмні засоби, які забезпечують високий рівень безпеки, здійснюють моніторинг комп'ютерної системи в режимі реального часу, захищають дані від зовнішніх і внутрішніх атак, а також своєчасно реагують на спроби несанкціонованого доступу.

У зв'язку з тим, що традиційні моделі безпеки комп'ютерних мереж поступово втрачають свою ефективність, виникає нагальна потреба у розробленні та впровадженні нових підходів для забезпечення захисту автоматизованих інформаційних систем від сучасних кіберзагроз.

Використання програмного середовища Cisco Packet Tracer дозволило моделювати можливі загрози та тестувати різні конфігурації захисту. У процесі дослідження особливу увагу було зосереджено на впровадженні пристроїв та архітектури безпеки, що забезпечують захист від сучасних кіберзагроз. Було проаналізовано кілька способів вдосконалення сегменту локальної мережі (LAN) за допомогою даного програмного забезпечення, а саме:

- сегментація мережі (поділ мережі на менші, ізольовані сегменти покращує безпеку та продуктивність);
- впровадження брандмауера (брандмауер – це ключовий елемент захисту мережі від зовнішніх загроз);
- використання систем IDS/IPS (системи виявлення та запобігання вторгненням (IDS/IPS) допомагають виявляти та блокувати шкідливу активність в мережі);

- налаштування VPN-з'єднань (віртуальні приватні мережі (VPN) забезпечують безпечне з'єднання між віддаленими користувачами та локальною мережею);

- застосування концепції Zero Trust (Zero Trust – це модель безпеки, яка передбачає, що жоден користувач або пристрій не є повністю довіреним, навіть якщо він знаходиться всередині мережі; Cisco Packet Tracer дозволяє моделювати Zero Trust архітектури для посилення безпеки та контролю доступу);

- моніторинг та аналіз трафіку (Cisco Packet Tracer надає інструменти для моніторингу та аналізу мережевого трафіку);

- автоматизація завдань (Cisco Packet Tracer підтримує scripting та автоматизацію завдань);

- використання хмарних сервісів (Cisco Packet Tracer інтегрується з хмарними сервісами, що дозволяє моделювати гібридні мережі та перевіряти їхню роботу);

- безперервне навчання та експерименти (Cisco Packet Tracer – це чудовий інструмент для навчання та експериментів, його можна використовувати для вивчення нових технологій та перевірки своїх знань).

Таким чином, вдосконалення сегмента LAN засобами Cisco Packet Tracer – це безперервний процес, який залежить від наших потреб та цілей. Комбінуючи різні методи та технології, можна створити безпечну та ефективну мережу, яка відповідає сучасним вимогам захисту інфраструктури.

Список використаних джерел:

1. S. Anitha, S. Kavitha, and P. Kavitha, "Machine Learning for Operating Systems Security," International Journal of Scientific & Engineering Research, vol. 13, no. 2, pp. 243-246, 2022.

2. Навчальний курс CSOv1-ZH-POL: Співробітник CyberOps. URL: www.netacad.com.

3. Навчальний курс Вивчення мережі за допомогою Cisco Packet Tracer URL.: www.netacad.com.

4. Що таке Zero Trust і навіщо він потрібен. URL: https://www.softwareone.com/uk-ua/blog/articles/2021/06/17/zero-trust-security.

УДК 004.4

Ратушний М.О., магістрант
Хмельницький національний університет

СИСТЕМИ ТА МЕТОДИ ПЛАНУВАННЯ СПОЖИВАННЯ ЕЛЕКТРОЕНЕРГІЇ ПРИСТРОЯМИ У "РОЗУМНОМУ БУДИНКУ"

Розвиток технологій та зростання потреб у раціональному використанні електроенергії стимулюють створення систем управління споживанням електроенергії. Розумний будинок є ефективним рішенням, що дозволяє автоматизувати контроль за електропристроями, мінімізувати енергетичні втрати та оптимізувати використання електроенергії. Головною метою цієї роботи є аналіз сучасних методів та систем керування електроспоживанням у розумному будинку, а також виявлення перспективних напрямів їх розвитку.

Системи управління домашньою енергією (Home Energy Management Systems, HEMS) дозволяють контролювати та оптимізувати споживання електроенергії в режимі реального часу. Основними елементами таких систем є інтелектуальні лічильники, які збирають дані про витрати електроенергії, центральні контролери, що аналізують ці дані та приймають відповідні рішення, а також розумні пристрої, які можуть автоматично змінювати режими роботи. Використання HEMS дозволяє покращити енергоефективність житлових приміщень та забезпечити економію ресурсів за рахунок автоматичного регулювання навантаження як на рис. 1.

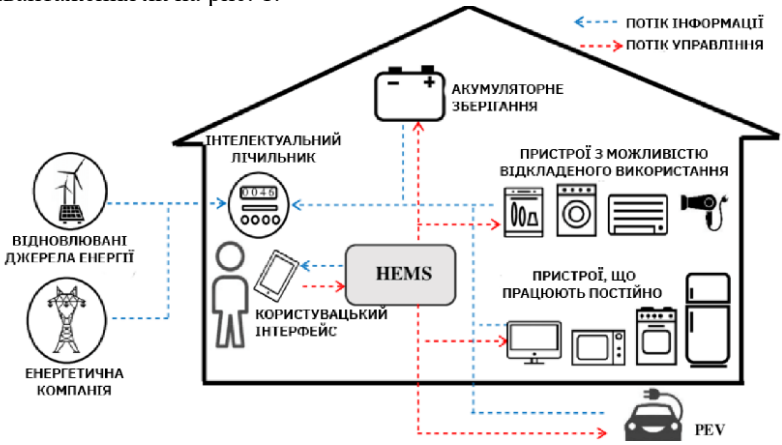


Рисунок 1 – Структура Системи управління домашньою енергією

Важливим аспектом ефективного управління енергоспоживанням є системи прогнозування та оптимізації [1, 2]. Прогнозування рівня споживання електроенергії є ключовим етапом, що дозволяє використовувати алгоритми машинного навчання для аналізу історичних даних і визначення закономірностей у споживанні енергії залежно від таких факторів, як час доби, погодні умови та змінні тарифи. Регресійні моделі, нейронні мережі та евристичні алгоритми забезпечують точне прогнозування, що дозволяє динамічно змінювати параметри роботи електропристроїв, зменшуючи перевантаження мережі та знижуючи витрати.

Для підвищення ефективності енергосистем використовується концепція інтелектуальних мереж (Smart Grid). Це комплексна система, що забезпечує двосторонній зв'язок між постачальниками та споживачами електроенергії, здійснює автоматичний розподіл навантаження, застосовує динамічне ціноутворення та інтегрує відновлювані джерела енергії. Використання Smart Grid у розумних будинках сприяє підвищенню стабільності електропостачання, зменшенню втрат енергії та підвищенню загальної ефективності роботи системи електропостачання.

Методи оптимізації енергоспоживання у розумних будинках передбачають застосування кількох підходів. Одним із найпоширеніших методів є керування навантаженням, яке передбачає диспетчеризацію за пріоритетами [3]. В цьому випадку електропристрої працюють у певній послідовності залежно від рівня їхньої важливості. Наприклад, система може автоматично зменшувати потужність роботи кондиціонерів або водонагрівачів у пікові години для зниження навантаження на мережу. Ще одним ефективним підходом є часове планування роботи пристроїв, що дозволяє виконувати найбільш енергоємні процеси (наприклад, зарядку електромобілів, нагрів води) у періоди низького тарифу на електроенергію.

Важливим напрямом є інтеграція відновлюваних джерел енергії, зокрема сонячних панелей та акумуляторних батарей. Розумні будинки можуть використовувати альтернативні джерела для автономного енергопостачання або накопичення енергії у періоди надлишкового виробництва, що дозволяє знизити залежність від традиційних енергомереж та забезпечити стабільне електропостачання навіть у разі аварійних ситуацій. Крім того, значну роль в управлінні енергоспоживанням відіграє Інтернет речей (IoT). Розумні датчики, сенсори руху та термостати дозволяють автоматично регулювати роботу освітлення, опалення та кондиціонування залежно від поточних умов та присутності людей у приміщенні. Це не лише знижує зайве

споживання електроенергії, але й створює комфортні умови для проживання.

Структура та реалізація системи керування електроспоживанням у розумному будинку включає кілька рівнів. Фізичний рівень містить пристрої, що здійснюють моніторинг і контроль енергоспоживання: розумні лічильники, датчики, контролери, розумні розетки та побутові прилади з дистанційним керуванням. Вони реєструють дані про споживання електроенергії та передають їх на наступний рівень для аналізу. Комунікаційний рівень забезпечує передачу даних між пристроями та центральною системою управління за допомогою технологій Wi-Fi, Zigbee, Bluetooth, Z-Wave та LoRaWAN.

Аналітичний рівень відіграє ключову роль у забезпеченні оптимального споживання електроенергії, використовуючи алгоритми машинного навчання та штучного інтелекту для аналізу отриманих даних, прогнозування навантаження на електромережу, оцінки ефективності роботи пристроїв та надання рекомендацій щодо їх оптимального використання. Наприклад, він може виявляти пікові години навантаження та пропонувати варіанти перенесення енергоємних процесів на періоди низького тарифу. Користувацький рівень включає мобільні додатки, веб-інтерфейси та голосових помічників, що дозволяють користувачам відстежувати споживання електроенергії, налаштовувати сценарії роботи пристроїв та отримувати аналітичні звіти.

Розробка таких систем здійснюється з використанням IoT-платформ, таких як OpenHAB, Home Assistant, Google Home або Apple HomeKit. Важливу роль відіграють стандарти інтероперабельності, такі як MQTT та CoAP, які забезпечують сумісність пристроїв різних виробників і дозволяють створювати гнучкі та масштабовані.

Список використаних джерел:

1. Mischos S., Dalagdi E., Vrakas D. Intelligent energy management systems: a review // Artificial Intelligence Review. 2023. №56. С. 11635–11674. DOI: 10.1007/s10462-023-10441-3.

2. Tomazzoli C., Scannapieco S., Cristani M. Internet of things and artificial intelligence enable energy efficiency // Journal of Ambient Intelligence and Humanized Computing. 2020. С. 1–22.

3. Şimşek U., Fensel A., Zafeiropoulos A., Fotopoulou E., Liapis P., Bouras T., Saenz F.T., Gómez A.F.S. A semantic approach towards implementing energy efficient lifestyles through behavioural change // Proceedings of the 12th International Conference on Semantic Systems. 2016. С. 173–176.

УДК 004.056

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

ШТУЧНИЙ ІНТЕЛЕКТ ПІД ПРИЦІЛОМ: ЕВОЛЮЦІЯ АТАК НА ML-СИСТЕМИ ТА ТЕХНОЛОГІЇ ЗАХИСТУ

Системи машинного навчання (ML) та штучного інтелекту (ШІ) стають невід’ємною частиною багатьох критичних сфер, таких як фінанси, медицина, транспорт і кібербезпека. Проте їх широке впровадження супроводжується зростанням ризиків, пов'язаних із кібератаками. У цьому дослідженні розглядаються нові вектори атак на ML/ШІ, оцінюється ефективність існуючих методів захисту та пропонуються покращені стратегії безпеки.

Одна з найнебезпечніших атак – це "отруєння даних" (Data Poisoning), коли зловмисники маніпулюють навчальними даними, щоб змусити модель навчитися неправильним патернам. Наприклад, якщо атака спрямована на систему розпізнавання загроз, хакер може додати у навчальний набір шкідливий код, який алгоритм помилково визначить як безпечний. Подібним чином працюють "атаки через білошум" (Adversarial Attacks) – вони використовують спеціально змінені вхідні дані, які здаються нормальними для людини, але вводять модель в оману. Достатньо незначних змін у зображенні, щоб система автономного транспорту сприйняла автомобіль за пішохода, що може призвести до критичних наслідків. Ще одним серйозним ризиком є "інверсія моделі" (Model Inversion Attack), коли хакери можуть отримати доступ до вихідних навчальних даних, аналізуючи відповіді моделі. Це особливо небезпечно у фінансових та медичних застосунках, де конфіденційність даних має першорядне значення.

Реальні випадки атак підтверджують загрозу таких векторів. Наприклад, дослідники Google виявили, що модифіковані аудіофайли можуть змусити голосових асистентів виконувати команди без відома користувача. У 2023 році хакери використали технологію діпфейків для обходу біометричної автентифікації в банківських системах, створивши підроблені відеодзвінки та отримавши доступ до рахунків клієнтів.

Для мінімізації ризиків атак необхідно застосовувати комплексні заходи захисту. Одним із найефективніших є адаптивне навчання (Adversarial Training), яке передбачає тренування моделей на спеціально змінених даних, що містять потенційні атаки. Це підвищує стійкість

алгоритмів, хоча вимагає значних обчислювальних ресурсів. Важливим є також захист навчальних даних, наприклад, за допомогою криптографічних методів, таких як гомоморфне шифрування чи диференційна конфіденційність, які дозволяють мінімізувати ризик витоку інформації. Моніторинг поведінки моделей, впровадження систем виявлення аномалій та обмеження доступу до моделі є додатковими ефективними методами протидії атакам.

Аналіз існуючих підходів до захисту показує, що адаптивне навчання та моніторинг аномалій є найбільш перспективними методами, але вони мають певні недоліки. Зокрема, адаптивне навчання потребує значних обчислювальних потужностей, а системи виявлення аномалій не гарантують стовідсоткового захисту від нових векторів атак. Тому доцільно застосовувати гібридний підхід, який поєднує адаптивне навчання та традиційні методи кіберзахисту. Перспективними напрямами є автоматизоване виявлення атак за допомогою самонавчальних алгоритмів, розподілене навчання (Federated Learning) для зменшення ризику компрометації даних, а також створення фільтрів для очищення вхідних даних, що дозволяє знизити ефективність adversarial атак.

Загалом атаки на системи ML/ШІ стають усе більш поширеними, і їхні наслідки можуть бути критичними для безпеки даних та функціонування автоматизованих систем. Впровадження передових методів захисту є необхідною умовою для забезпечення стійкості сучасних ШІ-алгоритмів. Найефективнішими на сьогодні є адаптивне навчання та моніторинг аномалій, проте для подальшого підвищення рівня безпеки необхідно розвивати комплексні підходи, що поєднують класичні методи кібербезпеки з інноваційними технологіями ML. Подальші дослідження в цій сфері відіграють ключову роль у розробці нових захисних механізмів, здатних ефективно протидіяти сучасним загрозам.

Список використаних джерел:

1. Biggio B., Roli F. Wild Patterns: Ten Years After the Rise of Adversarial Machine Learning. Pattern Recognition. 2022. DOI: https://doi.org/10.1016/j.patcog.2021.107384.

2. Papernot N., McDaniel P. Towards the Science of Security and Privacy in Machine Learning. IEEE Transactions on Information Forensics and Security. 2018. DOI: https://doi.org/10.1109/TIFS.2018.2871657.

3. Tramèr F., Zhang F. Stealing Machine Learning Models via Prediction APIs. USENIX Security Symposium. 2016. URL: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/tramer (дата звернення: 11.03.2025).

УДК 004.45:004.7

Хімічук О. В., магістрант
Фальковський І. Г., ст. викладач
Державний університет «Житомирська політехніка»

АКТУАЛЬНІСТЬ ВПРОВАДЖЕННЯ МОНІТОРИНГУ В СУЧАСНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ: ВИКЛИКИ, ТРЕНДИ ТА ПЕРСПЕКТИВИ

Світ інформаційних технологій змінюється з блискавичною швидкістю, і разом із цим зростає потреба у контролі за стабільністю, продуктивністю та безпекою інформаційних систем. Ще зовсім недавно компанії могли обходитися базовими засобами моніторингу, проте сьогодні складність інфраструктури та постійні кіберзагрози змушують їх впроваджувати сучасні, потужні рішення.

Без належного моніторингу компанії стикаються з численними проблемами: неочікувані збої в роботі серверів, втрати даних через атаки або програмні помилки, неефективне використання ресурсів, що призводить до зниження продуктивності. Моніторинг дозволяє завчасно виявляти ці проблеми та усувати їх ще до того, як вони спричинять серйозні наслідки.

Завдання моніторингу – не просто спостерігати за роботою систем, а й оперативно виявляти загрози, попереджати проблеми та оптимізувати ресурси. Але на шляху до ефективного моніторингу виникає низка викликів. По-перше, інформаційні системи стають дедалі складнішими. Вони об'єднують безліч компонентів, інтегруються з хмарними платформами, що ускладнює їх контроль. По-друге, продуктивність. Моніторингові системи повинні працювати без створення додаткового навантаження, що може вплинути на швидкодію бізнес-процесів. Крім того, важливо забезпечити безпеку даних, які обробляються під час моніторингу, адже вони можуть містити критично важливу інформацію. І, звісно, обробка великих обсягів даних – швидке виявлення аномалій вимагає потужних аналітичних алгоритмів [1].

У відповідь на ці виклики з'являються нові тренди у сфері моніторингу. Штучний інтелект та машинне навчання дозволяють автоматизувати аналіз даних, що суттєво підвищує швидкість реагування на проблеми. Контейнеризація та оркестрація змушують розробників адаптувати засоби моніторингу під динамічні середовища, такі як Kubernetes та Docker. Все більше компаній використовують хмарні рішення на кшталт AWS CloudWatch, Azure Monitor та Google Cloud Operations. Крім того, концепція Observability, що поєднує

логування, трасування та метрики, стає стандартом для комплексного моніторингу сучасних систем.

Серед найпопулярніших інструментів для моніторингу можна виділити: Zabbix, Nagios, Elastic Stack (ELK), Prometheus, Grafana, Datadog. Ці інструменти набагато спрощують роботу зі збором інформації, дозволяють візуалізувати дані, створювати дашборди, налаштовувати сповіщення, спрощують роботу з логами та журналами подій.

Для ефективного впровадження моніторингу необхідно, по-перше, визначити ключові показники (KPIs), що саме потрібно моніторити: продуктивність серверів, затримки в мережі, використання ресурсів тощо. По-друге, обрати відповідні інструменти. Залежно від масштабу та вимог до моніторингу слід використовувати відповідні рішення (наприклад, для DevOps середовищ найкраще підходять Prometheus та Grafana). По-третє, автоматизувати процеси, інтегрувати моніторинг у CI/CD пайплайни для раннього виявлення проблем. По-четверте, налаштувати сповіщення. Це критично важливо, щоб система повідомляла про проблеми у режимі реального часу [2]. На завершення, необхідно забезпечити безпеку моніторингових даних, обмежити доступ до метрик та логів, застосовувати політики шифрування, тощо.

Що чекає на цю сферу в майбутньому? Передусім – ще більше використання AI для прогнозування відмов та оптимізації процесів. Моніторинг стає невід'ємною частиною DevOps, а концепція Zero Trust Monitoring набирає популярності у сфері кібербезпеки. Крім того, з огляду на екологічні виклики, дедалі більше компаній зосереджуються на оптимізації ресурсів задля зменшення енергоспоживання.

Таким чином, моніторинг – це не просто додатковий компонент, а життєво необхідний елемент сучасної цифрової інфраструктури. Його правильне впровадження дозволяє не тільки забезпечити стабільність та безпеку, а й створює передумови для ефективного розвитку бізнесу в умовах швидкоплинного технологічного середовища.

Список використаних джерел:

1. Що таке моніторинг IT інфраструктури та чому це важливо? URL: https://vamark.ua/blog/shho-take-monitoryng-it-infrastruktury-ta-chomu-cze-vazhlyvo/. (дата звернення: 20.02.2025)

2. Важливість моніторингу мережі: забезпечення оптимальної продуктивності та безпеки. URL: https://www.globalyo.com/uk/blog/the-importance-of-network-monitoring-ensuring-optimal-performance-and-security/. (дата звернення: 20.02.2025)

УДК 004.7

Кравчук М.В., магістр
Павлова О.О., PhD
Хмельницький національний університет

МЕТОД ТА ПРОГРАМНО-ТЕХНІЧНИЙ ЗАСІБ ДЛЯ ВИЯВЛЕННЯ ТА АНАЛІЗУ РАДІОМЕРЕЖ

Сучасні бездротові радіомережі є ключовими компонентами телекомунікаційних систем. Вони використовуються у мобільному зв'язку, Інтернеті речей (IoT), військових та промислових системах. Одним із важливих завдань є виявлення та аналіз параметрів радіомереж для забезпечення ефективної роботи та запобігання несанкціонованому доступу. Дана доповідь розглядає методи та програмно-технічні засоби для аналізу радіомереж.

Існує кілька основних методів, які застосовуються для виявлення та аналізу радіомереж:

- спектральний аналіз – визначає частотні характеристики сигналів, використовуючи алгоритми перетворення Фур'є (FFT, STFT, Wavelet);
- методи часової кореляції – дозволяють виявляти повторювані сигнали, що використовуються у цифрових системах зв’язку;
- аналіз рівня потужності сигналу (RSSI) – оцінює силу сигналу у просторі, що може бути корисним для геолокації та визначення меж покриття мережі;
- методи машинного навчання – застосовуються для класифікації типів сигналів, виявлення аномалій та передбачення змін у спектрі;
- когнітивне радіо [1,2] – використовує динамічне управління спектром для адаптації до змін навколишнього радіосередовища.

Сучасні програмно-апаратні комплекси включають:

Програмні засоби:

- MATLAB, GNU Radio – використовуються для моделювання та аналізу сигналів;
- wireshark – для аналізу трафіку у бездротових мережах;
- tensorFlow/PyTorch – для реалізації алгоритмів глибокого навчання у розпізнаванні сигналів.

Технічні засоби:

- приймачі SDR (Software Defined Radio) – наприклад, USRP, HackRF, RTL-SDR;

- аналізатори спектру – для вимірювання параметрів сигналів у реальному часі;
- мобільні пристрої з Wi-Fi та Bluetooth модулями – для моніторингу бездротових мереж.

У цій роботі особливу увагу приділено методам сліпого автономного широкосмугового зондування, які спрямовані на виявлення сигналів із невідомими характеристиками. Ці методи особливо корисні для CR, що функціонують у широких частотних діапазонах, де одночасно можуть передаватися кілька сигналів із невідомими центральними частотами [3,4].

Зондування спектру є початковим етапом у ланцюжку обробки сигналів, після якого слідують класифікація сигналів і прийняття рішень. У цій роботі реалізована архітектура CR, яка відображає основні функції системи та їх взаємозв'язки (рис. 1).

Рисунок 1 – Структурна схема запропонованої моделі CR

У роботі розглядається новий метод та програмно-технічний засіб для виявлення та аналізу радіомереж. Основна увага приділяється адаптивним алгоритмам обробки сигналів, які дозволяють підвищити точність і швидкість визначення параметрів мереж навіть в умовах змінних характеристик радіочастотного середовища. Також досліджуються підходи до навчання порогів для оптимізації параметрів когнітивних радіомереж, що дозволяє покращити їхню адаптацію до динамічних умов роботи.

Основний внесок роботи полягає у створенні адаптивного підходу до обробки сигналів, який враховує змінні умови радіочастотного

середовища та дозволяє ефективно аналізувати активність у спектрі. Практичне значення отриманих результатів полягає у можливості впровадження запропонованого програмно-технічного засобу для вирішення завдань моніторингу та аналізу спектру у бездротових мережах різного типу, включаючи когнітивні радіосистеми та системи радіомоніторингу.

Список використаних джерел:

1. Mitola J. III, Maguire G. Jr. Cognitive radio: making software radios more personal. IEEE Personal Communications. 1999. Vol. 6, No. 4. P. 13–18. URL: https://www.semanticscholar.org/paper/Cognitive-radio%3A-making-software-radios-more-Mitola-Maguire/fb5d1bb23724d9a5a5eae036a2e3cf291cac2c1b (дата звернення: 11.03.2025).
2. Mitola J. Cognitive radio: An integrated agent architecture for software-defined radio. Дис. д-ра філософії. Royal Institute of Technology (KTH), Stockholm, Sweden, 2000. URL: https://www.semanticscholar.org/paper/Cognitive-Radio-An-Integrated-Agent-Architecture-Mitola/82dc0e2ea785f4870816764c25f3d9ae856d9809 (дата звернення: 11.03.2025).
3. Bkassiny M., Jayaweera S. K., Li Y., Avery K. A. Wideband spectrum sensing and non-parametric signal classification for autonomous self-learning cognitive radios. IEEE Transactions on Wireless Communications. 2012. Vol. 11, No. 7. P. 2596–2605. URL: https://www.researchgate.net/publication/230788566 (дата звернення: 11.03.2025).
4. Blind cyclostationary feature detection based spectrum sensing for autonomous self-learning cognitive radios. IEEE International Conference on Communications (ICC ’12). Ottawa, Canada, June 2012. URL: https://www.researchgate.net/publication/230788467 (дата звернення: 11.03.2025).

УДК 004.738

Фомін В.В., здобувач
Покотило О.А., ст. викладач
Державний університет «Житомирська політехніка»

АНАЛІЗ ТЕХНОЛОГІЙ ВІДДАЛЕНОГО ДОСТУПУ ДЛЯ ВИКОРИСТАННЯ У КОРПОРАТИВНОМУ СЕРЕДОВИЩІ

Зі зростанням кількості віддалених працівників, використання хмарних сервісів і потреби в оперативному вирішенні технічних проблем, віддалений доступ відіграє ключову роль у забезпеченні безперервності бізнесу та швидкому реагуванні на непередбачені ситуації.

Можна виділити такі найпоширеніші підходи до віддаленого доступу – це інфраструктури віртуальних робочих столів (VDI) у поєднанні з віртуальними мережевими обчисленнями (VNC) та протоколом віддаленого робочого столу (RDP) [1].

Virtual Desktop Infrastructure (VDI) працює на базі віртуальних машин (VM), що запускаються через гіпервізор на серверному обладнанні, де розміщується ОС, наприклад, Windows або Linux [2]. Існують два основні типи віртуальних робочих столів: персистентні, що зберігають всі налаштування, та неперсистентні, тимчасові середовища.

Протокол віддаленого робочого столу (RDP) є протоколом або технічним стандартом для віддаленого використання настільного комп'ютера. RDP є найбільш поширеним протоколом віддаленого доступу [3]. Він відкриває спеціальний мережевий канал для обміну даними між підключеними пристроями, використовуючи мережевий порт 3389. Всі дані передаються через цей канал за допомогою TCP/IP. RDP також шифрує всі дані.

RDP є прямим конкурентом протоколу Virtual Network Computing (VNC), який є відкритою альтернативою і часто використовується в системах на базі Linux та інших платформах [3].

Virtual Network Computing (VNC) – крос-платформенна система для спільного використання екрану, створена для віддаленого керування іншим комп'ютером [4]. VNC працює за моделлю клієнт/сервер. VPN-сервер встановлюється на віддаленому комп'ютері, яким потрібно керувати, а VNC-клієнт – на пристрої, з якого буде здійснюватися керування. VNC базується на протоколі Remote Framebuffer (RFB)[4].

На відміну від RDP, який глибоко інтегрований з Windows, VNC забезпечує ширшу сумісність із різними операційними системами, хоча може поступатися в продуктивності, оптимізованій для середовищ Windows.

Загалом, можна навести таку порівняльну характеристику згаданих технологій VNC та RDP:

Таблиця 1

Порівняльна характеристика технологій віддаленого доступу

	VNC	**RDP**
Призначення	*Віддалене керування екраном*	*Доступ до робочого столу Windows*
Протокол	*RFB*	*RDP*
Сумісність	*Кросплатформна*	*Переважно Windows*
Принцип роботи	*Передача зображення, введення з клавіатури/миші*	*Передача графічних команд*
Продуктивність	*Нижча, потребує високої пропускної здатності*	*Висока, оптимізована*
Безпека	*Вимагає додаткових налаштувань*	*Вбудоване шифрування*
Можливості користувача	*Керування екраном без зміни сесії*	*Окремі сеанси користувачів*
Функціональність	*Базовий доступ до екрану*	*Додаткові функції (файли, аудіо, USB)*
Використання ресурсів	*Високе навантаження*	*Оптимізоване кодування*
Кількість користувачів	*Декілька одночасно*	*1 на сесію, підтримка серверів*
Сфера застосування	*Адміністрування серверів, технічна підтримка*	*Корпоративні мережі, мультимедіа*

Підсумовуючи, RDP є оптимальним вибором для корпоративного середовища Windows завдяки продуктивності та безпеці. VNC, у свою чергу, забезпечує кросплатформну сумісність і гнучкість. Обидва протоколи потребують додаткових заходів безпеки для захисту даних.

Список використаних джерел:

1. VDI vs VPN vs RDP: Choosing a Secure Remote Access Solution URL: https://surl.li/kewcho (дата звернення: 21.02.2025)
2. What Is Virtual Desktop Infrastructure (VDI)?. URL: https://surl.li/krtozx (дата звернення: 22.02.2025)
3. What is the Remote Desktop Protocol (RDP)? URL: https://surl.li/gioneb (дата звернення: 22.02.2025)
4. What is VNC remote access technology? URL: https://salo.li/dE79588 (дата звернення: 22.02.2025)

УДК 004.4

Комаров О. В., магістрант
Хмельницький національний університет

БЛОКЧЕЙН-ТЕХНОЛОГІЇ В СИСТЕМАХ УПРАВЛІННЯ ДОСТУПОМ У РОЗУМНИХ МІСТАХ

Сучасні розумні міста базуються на інтеграції цифрових технологій у всі сфери міської інфраструктури. Автоматизовані системи контролю доступу є важливою складовою безпеки та ефективності управління міськими ресурсами [1, 2]. Проте централізовані рішення часто стикаються з проблемами кібербезпеки, збоїв у системах, високих витрат на адміністрування та ризиків витоку персональних даних. У цьому контексті блокчейн-технології пропонують революційний підхід до управління доступом, що базується на децентралізованих механізмах аутентифікації та перевірки прав доступу [3].

З метою забезпечення безпечного та ефективного обміну інформацією запропоновано модель управління доступом на основі блокчейн-технологій, яка інтегрує децентралізовані ідентифікаційні системи. Ключовим елементом цієї моделі є смарт-контракти, що автоматизують процес перевірки прав доступу та знижують необхідність у посередниках. Правила доступу до різних міських сервісів фіксуються у блокчейні, що запобігає можливості несанкціонованого втручання та підробки даних.

Архітектура системи побудована таким чином, щоб забезпечити ефективну взаємодію користувачів з міською інфраструктурою. Автентифікація користувачів відбувається за допомогою криптографічних методів, таких як біометричні дані, цифрові сертифікати або криптографічні ключі. Це дозволяє гарантувати точну ідентифікацію особи та запобігти шахрайству. Смарт-контракти визначають права доступу до міських сервісів, формують цифрові ключі для користувачів і контролюють виконання правил. Всі операції у системі реєструються у блокчейні, що робить їх прозорими, незмінними та доступними для аудиту.

Функціонування системи включає кілька ключових процесів. Перший етап – реєстрація користувача, що відбувається шляхом автентифікації через криптографічні методи. Після підтвердження особи користувач отримує цифровий ідентифікатор, що буде використовуватись у подальших запитах на доступ. Запити на доступ проходять через смарт-контракти, які автоматично перевіряють відповідність даних користувача встановленим правилам. Якщо всі

умови виконані, користувач отримує дозвіл на вхід у певну зону або доступ до ресурсу, а всі операції записуються в блокчейн.

Обмін інформацією між блокчейном і міськими інформаційними платформами забезпечується за допомогою міжланцюгових технологій, що дозволяють синхронізувати дані між різними блокчейн-мережами та централізованими базами даних. Це забезпечує можливість інтеграції блокчейн-системи з існуючими інформаційними структурами міста, що критично важливо для масштабованості та ефективного управління цифровими ресурсами. Використання децентралізованих ідентифікаційних платформ дозволяє організувати єдину систему обліку доступу, яка може застосовуватися у різних міських службах без необхідності дублювання даних.

Важливим аспектом впровадження системи є безпека транзакцій та захист конфіденційних даних. Застосування нульових доказів знання дозволяє підтвердити особу без розкриття персональних даних, що зменшує ризики витоку інформації. Гомоморфне шифрування забезпечує можливість проведення обчислень над зашифрованими даними без необхідності їх розшифровки, що підвищує рівень захисту в системі. Автоматизована система виявлення аномальних активностей дозволяє виявляти підозрілі запити на доступ і блокувати потенційні атаки.

Перевагою запропонованої системи є її автономність та відсутність єдиної точки відмови. Децентралізована природа блокчейну гарантує стійкість до атак і зовнішніх маніпуляцій. Смарт-контракти автоматизують процеси перевірки прав доступу, що дозволяє скоротити адміністративні витрати та виключити можливість людського фактору у прийнятті рішень. Використання блокчейну у системах управління доступом дозволяє знизити ризики шахрайства, покращити безпеку міської інфраструктури та підвищити рівень цифрової довіри між користувачами та міськими сервісами.

Запропонована архітектура створює передумови для ефективного управління цифровими ресурсами в умовах розумного міста. Система здатна адаптуватися до потреб різних міських сервісів, включаючи контроль доступу до будівель, управління транспортною інфраструктурою, автоматизований доступ до комунальних послуг та захист даних у цифрових реєстрах. Інтеграція з наявними системами міського управління дозволяє впровадити блокчейн без необхідності повної заміни існуючої інфраструктури, що робить її економічно доцільною та ефективною. Використання модульного підходу до реалізації системи дозволяє підключати нові компоненти без

необхідності кардинальної перебудови всієї платформи, що сприяє її довготривалому використанню та масштабованості.

Застосування штучного інтелекту у поєднанні з блокчейном дозволяє покращити механізми прогнозування безпеки, оптимізувати процеси обробки запитів та адаптувати політики доступу до змінних міських умов. Наприклад, система може автоматично аналізувати поведінку користувачів і пропонувати зміни в політиках безпеки на основі даних про реальні сценарії використання. Це дозволяє зробити систему не лише безпечною, а й гнучкою, здатною самостійно вдосконалювати механізми контролю доступу.

Таким чином, впровадження блокчейн-технологій у систему управління доступом створює ефективну, захищену та масштабовану екосистему, що відповідає сучасним викликам цифровізації розумних міст. Вона дозволяє не тільки покращити безпеку та автоматизацію, а й створити єдину децентралізовану платформу, яка може адаптуватися до різноманітних завдань міської інфраструктури.

Висновок. Таким чином впровадження блокчейн-технологій у системи управління доступом у розумних містах дозволяє кардинально змінити підхід до безпеки та цифрової ідентифікації. Децентралізовані реєстри надають можливість ефективного управління правами доступу без необхідності централізованого контролю, що підвищує стійкість до атак та мінімізує ризики несанкціонованого втручання. Автоматизація перевірки прав доступу за допомогою смарт-контрактів забезпечує швидке та прозоре виконання операцій без залучення третіх сторін, що знижує адміністративні витрати та виключає ризик людської помилки.

Список використаних джерел:

1. Treiblmaier H., Rejeb A., Strebinger A. Blockchain as a Driver for Smart City Development: Application Fields and a Comprehensive Research Agenda // Smart Cities. 2020. №3. С. 853–872. DOI: 10.3390/smartcities3030044.

2. Iansiti M., Lakhani K.R. The truth about blockchain // Harvard Business Review. 2017. №95. С. 118–127.

3. Khan M.A., Salah K. IoT security: Review, blockchain solutions, and open challenges // Future Generation Computer Systems. 2018. №82. С. 395–411.

УДК 004.7

Сенчило Т.С., магістрантка
Бродський Ю.Б., к.т.н., доцент
Державний університет «Житомирська політехніка»

СИСТЕМА ЗАХИСТУ ВІД АТАК НА BLOCKCHAIN-МЕРЕЖІ НА ОСНОВІ ПОВЕДІНКОВОГО АНАЛІЗУ СМАРТ-КОНТРАКТІВ

В умовах стрімкого розвитку децентралізованих фінансів (DeFi) та впровадження blockchain-технологій у критично важливі сфери діяльності, забезпечення безпеки смарт-контрактів стає першочерговим завданням. Згідно з даними аналітичних агентств, у 2023 році втрати від атак на смарт-контракти перевищили 2 мільярди доларів, що підкреслює актуальність розробки ефективних систем захисту.

Існуючі методи забезпечення безпеки blockchain-систем переважно базуються на статичному аналізі коду та моніторингу транзакцій. Проте такий підхід не враховує комплексний характер сучасних атак, які використовують складні сценарії взаємодії між смарт-контрактами та особливості роботи blockchain-протоколів. Показовим прикладом є атака на протокол Beanstalk у квітні 2022 року, де зловмисники використали складну послідовність flash-loan операцій та маніпуляцій з governance-механізмом для викрадення активів на суму понад 180 мільйонів доларів. Цей інцидент продемонстрував обмеженість традиційних методів захисту перед складними векторами атак, що використовують легітимні механізми протоколу у зловмисних цілях. [1]

Метою дослідження є розробка системи виявлення та запобігання атак на blockchain-мережі, що базується на поведінковому аналізі смарт-контрактів з використанням методів машинного навчання.

В рамках дослідження розроблено: математичну модель поведінкового аналізу смарт-контрактів, що враховує динамічні патерни взаємодії та контекст виконання транзакцій; архітектуру системи моніторингу реального часу з використанням розподілених сенсорів; алгоритм машинного навчання для класифікації аномальної поведінки; методику автоматизованого реагування на виявлені загрози.

Запропонована система включає три основні компоненти:

- модуль збору та попередньої обробки даних, що забезпечує моніторинг мережевої активності та виконання смарт-контрактів [2];
- аналітичний модуль на базі ансамблю моделей машинного навчання для виявлення аномалій;

- підсистему реагування, що реалізує механізми превентивного захисту.

Попередні симуляції та теоретичний аналіз розробленої системи дозволяють прогнозувати високу ефективність у виявленні найпоширеніших векторів атак на смарт-контракти. Очікується, що система буде здатна ідентифікувати:

- reentrancy-атаки з теоретичною ефективністю виявлення до 95%;
- маніпуляції з цінами в liquidity pools через фронтраннінг та інші техніки;
- комплексні атаки з використанням flash-loans та крос-протокольних взаємодій.

Для підтвердження ефективності запропонованого рішення планується проведення серії експериментів на тестовій мережі Ethereum з імітацією різних сценаріїв атак. Попередні результати на обмеженому наборі тестових даних демонструють перспективність підходу, однак потребують подальшої валідації в умовах, наближених до реальних [3].

Потенційна практична цінність розробленої системи полягає у можливості її інтеграції з існуючими DeFi-протоколами як додаткового шару безпеки, що дозволить значно зменшити ризики фінансових втрат від нових типів атак. Очікується, що впровадження подібних систем моніторингу може скоротити загальні збитки галузі від хакерських атак на 30-40% щорічно.

Таким чином, запропонована система повинна забезпечувати комплексний захист blockchain-мереж через поведінковий аналіз смарт-контрактів, що дозволяє виявляти та запобігати складним атакам ще до їх реалізації. Подальші дослідження спрямовані на розширення можливостей системи для роботи з різними blockchain-платформами та вдосконалення механізмів автоматизованого реагування.

Список використаних джерел:

1. CertiK. Beanstalk Farms Loses $182M in Flash Loan Attack. URL: https://www.certik.com/resources/blog/k6eZOpnK5Kdde7RfHBZgw-beanstalk-farms-exploit (дата звернення: 20.02.2025).

2. Kanga D., Azzouazi M., Ghoumrari M., Daif A. Management and Monitoring of Blockchain Systems / Dominique Kanga, Mohamed Azzouazi, Mohammed Ghoumrari, Abderrahmane Daif // Procedia Computer Science. – 2020. – T. 177. – P. 605-612. URL: https://www.researchgate.net/publication/346870622_Management_and_Monitoring_of_Blockchain_Systems (дата звернення: 19.02.2025).

3. Перелік токенів Ethereum. [URL].- Режим доступу: https://etherscan.io/tokens (дата звернення: 19.02.2025).

УДК 004.7

Петляк Н.С., асистент
Хмельницький національний університет

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ДЛЯ ІМІТАЦІЇ АТАК МЕТОЮ АНАЛІЗУ ТРАФІКУ

Імітація атак та аналіз мережевого трафіку є елементами забезпечення кібербезпеки, які дозволяють виявляти вразливості, тестувати достовірність систем захисту та покращувати стійкість інфраструктури до реальних загроз. Проведення тестування та імітація атак сприяють виявленню слабких місць у мережевих і веб-системах, вдосконаленню політик безпеки та підготовці персоналу до реагування на кібератаки. Усе це дозволяє підвищити рівень захисту інформаційно-комп'ютерних систем та мінімізувати ризики несанкціонованого доступу (НСД), витоку даних і фінансових втрат.

Аналіз та розвідка мережі спрямовані на збір інформації про відкриті порти, запущені служби та операційні системи, що дозволяє зловмиснику визначити потенційні цілі для подальших атак. Для реалізації таких атак використовуються Nmap, Masscan, Angry IP Scanner. Nmap дозволяє виконувати активне сканування мережі, визначати відкриті порти та запущені служби, тоді як Masscan відрізняється високою швидкістю сканування. Для тестування систем виявлення атак можна налаштувати розширене сканування з використанням різних режимів, наприклад, TCP SYN-сканування або сканування без встановлення з'єднання.

Атаки на автентифікацію та паролі базуються на методах підбору паролів, використанні словників або викраденні хешів з метою отримання НСД. Якщо така атака вдається, то зловмисник може заволодіти обліковими записами користувачів чи адміністраторів, що відкриває йому шлях до управління системою або мережею. Використовуються інструменти Hydra, Medusa, John the Ripper, Hashcat та Mimikatz. Hydra та Medusa дозволяють здійснювати перебір паролів у режимі brute-force або словникової атаки для мережевих сервісів, таких як SSH, FTP та RDP. Для тестування можна використовувати реальні або синтетичні паролі, а також обмежувати частоту запитів, щоб оцінити достовірність системи захисту.

Виявлення вразливостей та їх експлуатація передбачає пошук вразливих місць у програмному забезпеченні (ПЗ) та використання спеціальних скриптів або експлойтів для їх використання. Це може призвести до виконання довільного коду на сервері, отримання привілейованого доступу або крадіжки конфіденційних даних. Основними інструментами є Metasploit, SQLmap, Nikto, OpenVAS та

Burp Suite. Metasploit надає широкий вибір експлойтів для тестування мережевих систем, а SQLmap автоматично знаходить SQL-ін'єкції у веб-додатках. Для тестування можна використовувати симуляцію реальних атак на вразливі сервери у контрольованому середовищі.

Атаки типу "людина посередині" базуються на перехопленні трафіку між двома сторонами, що дозволяє зловмиснику змінювати або перенаправляти дані без відома жертв. Основні інструменти для реалізації цих атак – Ettercap, Bettercap, MITMf та Wireshark. Ettercap дозволяє виконувати отруєння ARP-кешу для перехоплення трафіку, а Bettercap підтримує інтеграцію з атаками на HTTPS-з'єднання. Для тестування можна використовувати емуляцію підміни DNS-запитів або перехоплення HTTP-трафіку.

DoS- та DDoS-атаки спрямовані на перевантаження сервера або мережевого пристрою великою кількістю запитів, що призводить до його недоступності для легітимних користувачів. Використовуються LOIC, HOIC, Slowloris, Hping3 та UFONet. Slowloris атакує сервер шляхом підтримки великої кількості відкритих підключень, а Hping3 дозволяє генерувати спеціалізовані пакети для перевантаження мережевої інфраструктури. Для тестування можна використовувати контрольовані атаки на тестові сервери з обмеженою частотою запитів.

Атаки на веб-додатки використовують методи SQL-ін'єкцій, XSS та CSRF для отримання контролю над веб-сайтами або даними їхніх користувачів. Найпоширенішими інструментами є Burp Suite, OWASP ZAP, SQLmap та BeEF. OWASP ZAP дозволяє автоматично знаходити вразливості у веб-додатках, а BeEF спеціалізується на XSS-атаках. Для тестування варто використовувати середовища, такі як DVWA або OWASP Mutillidae, що містять вразливі веб-додатки.

Однак, більшість програм поширюються під відкритими ліцензіями, такими як GPL, MIT або Apache, що дозволяє їх використання у навчальних цілях, дослідженнях та тестуванні безпеки за умови отримання дозволу власника мережі. Наприклад, Nmap, Wireshark, Metasploit та Aircrack-ng мають ліцензію GPL, яка передбачає можливість використання для освітніх і наукових досліджень, тоді як Burp Suite Community Edition має обмежений функціонал і доступний лише для некомерційного використання. Важливо дотримуватися законодавчих норм, оскільки несанкціоноване тестування або втручання в роботу комп’ютерних мереж може суперечити нормативно-правовим актам, що передбачають відповідальність за подібні дії.

Список використаних джерел:

1. NIST Special Publication 800-115: Technical Guide to Information Security Testing and Assessment. National Institute of Standards and Technology (NIST). URL: https://csrc.nist.gov/publications/detail/sp/800-115/final (дата звернення: 11.03.2025).

УДК: 004.9

Нестеров В.Ю., магістрант
Єфіменко А.А., к.т.н., доцент
Державний університет «Житомирська політехніка»

АЛГОРИТМ ТЕСТУВАННЯ БЕЗПЕКИ ANDROID-ДОДАТКІВ

У сучасних умовах швидкого розвитку мобільних технологій питання захисту Android-додатків набуває особливої актуальності. Зростання кількості кібератак, витоків даних та вразливостей у програмному забезпеченні створює ризики для конфіденційності, цілісності та доступності інформації користувачів. Відсутність належного тестування безпеки може призвести до серйозних наслідків, зокрема до викрадення персональних даних, фінансових втрат та репутаційних ризиків.

Метою цього дослідження є розробка алгоритму тестування безпеки Android-додатків, що дозволить ефективно виявляти потенційні загрози та надавати рекомендації щодо їх усунення. Алгоритм базується на сучасних підходах до мобільного пентестингу та стандартах безпеки, зокрема MASTG.

OWASP Mobile Application Security Testing Guide (MASTG) – це всеосяжний посібник з тестування безпеки мобільних додатків та reverse engineering. Він описує технічні процеси для перевірки засобів контролю, перелічених в OWASP MASVS, через слабкі місця, визначені OWASP MASWE [1].

Комплексне та результативне тестування безпеки Android-додатків передбачає виконання кількох етапів:

1. Збір та аналіз інформації про додаток: На першому етапі досліджується загальна структура Android-додатка, включаючи дозволи, компоненти та використані API. Аналізуються вихідні файли APK, визначаються можливі вразливості, пов'язані з некоректною конфігурацією безпеки та неправильним керуванням ресурсами;
2. Статичний аналіз: На другому етапі проводиться декомпіляція APK-файлу та аналіз його вихідного коду. Вивчається, чи використовуються незахищені механізми збереження даних, чи присутні слабкі алгоритми шифрування та некоректно налаштовані дозволи. Для цього застосовуються такі інструменти, як MobSF, JADX та інші засоби reverse engineering;
3. Динамічний аналіз безпеки: На третьому етапі тестується поведінка додатка під час його виконання в реальному середовищі або емуляторі. Виконується моніторинг мережевого трафіку за допомогою інструментів Burp Suite або MITMproxy, досліджується взаємодія

додатка із сервером та проводиться перевірка на можливі загрози, такі як MITM-атаки чи витоки даних;

4. Аналіз безпеки зберігання даних: На четвертому етапі перевіряється, як додаток обробляє та зберігає конфіденційну інформацію. Аналізується наявність незашифрованих файлів, неправильно налаштованих баз даних SQLite, кешу та SharedPreferences. Виявляються потенційні уразливості, що можуть спричинити витік або компрометацію даних користувачів [2];

5. Перевірка автентифікації та авторизації: На п'ятому етапі оцінюється безпека механізмів входу та управління сесіями. Досліджуються методи автентифікації, зокрема використання токенів, паролів та двофакторної аутентифікації. Перевіряються можливі атаки, такі як Brute Force, Session Hijacking або Replay-атаки;

6. Експлуатація вразливостей та розробка рекомендацій: На шостому етапі здійснюється перевірка можливості експлуатації знайдених вразливостей. Проводиться тестування методів атаки та аналіз наслідків потенційного компрометування додатка. Формується звіт з детальним описом знайдених проблем та рекомендаціями щодо їх усунення.

Запропонований алгоритм тестування безпеки Android-додатків поєднує теоретичні та практичні аспекти. Теоретично він ґрунтується на системному підході до аналізу безпеки Android-додатків, що враховує всі ключові аспекти їх захисту, включаючи безпеку коду, даних, комунікацій, механізмів автентифікації тощо. Практично алгоритм реалізує покроковий процес тестування, що дає змогу виявляти й усувати вразливості додатків, використовуючи актуальні методи, інструменти та техніки, що дозволяють підвищити їхній рівень захисту та стійкості до атак.

Перспективи подальших досліджень включають вдосконалення методів виявлення вразливостей, розширення спектру тестованих аспектів безпеки та підвищення ефективності автоматизації тестування.

Список використаних джерел:

1. OWASP MASTG - OWASP Mobile Application Security. *OWASP Mobile Application Security*. URL: https://mas.owasp.org/MASTG/.

2. Gunasekera S. Android Apps Security. Berkeley, CA : Apress, 2020.

УДК 004.45

Макаров О.В., магістрант
Шелуха О.О., к.т.н, доцент
Державний університет «Житомирська політехніка»

ТЕХНОЛОГІЇ АВТОМАТИЗОВАНОГО УПРАВЛІННЯ СЕРВЕРАМИ

У сучасному світі, де ефективність і надійність IT-інфраструктури є критично важливими для бізнесу, технології автоматизованого управління серверами набувають особливої актуальності. Постійне зростання обсягів даних, вимоги до безперервної роботи систем та необхідність оптимізації ресурсів ускладнюють ручне адміністрування серверів. Відповідно, розвиток інструментів автоматизації та їх впровадження стає ключовим фактором підвищення продуктивності й безпеки серверних середовищ.

Інфраструктура як код[1] (IaC) - це метод визначення та управління інфраструктурою вашої системи за допомогою коду. Подібно до того, як програмний код визначає логіку та функціональність програми, IaC описує архітектуру системи, включаючи такі компоненти, як сервери, мережі, сховища та операційні системи.

За допомогою IaC можна керувати ресурсами інфраструктури у послідовний та організований спосіб. Він розглядає конфігураційні файли як вихідний код, що дозволяє використовувати контроль версій, відстежувати помилки та легко вносити оновлення. Таким чином, за допомогою таких систем контролю версій можна відстежувати всі внесені зміни та ефективно співпрацювати з розробниками.

Для полегшення роботи з методом IaC розроблено спеціалізовані програмні засоби автоматизованого управління серверами, наприклад Terraform [2] та Ansible [3].

Було проведено порівняльний аналіз зазначених інструментів за наступними критеріями:

1. Синтаксис – формат і стиль запису конфігурацій, який використовується в інструменті.
2. Підхід – спосіб управління інфраструктурою (декларативний або імперативний підхід.
3. Складність – рівень складності в освоєнні, налаштуванні та підтримці, включаючи навчальний поріг і вимоги до знань користувача.
4. Використання – основні сценарії застосування інструмента.
5. Недоліки – обмеження та слабкі сторони інструмента, які можуть ускладнити його використання.

Таблиця 1

Порівняння інструментів

Критерії	Terraform	Ansible
Синтаксис	HCL або JSON	YAML
Використання	Розгортання інфраструктури з нуля, керування ресурсами у хмарі	Налаштування ПЗ, оновлення пакетів, управління користувачами, конфігурування сервісів
Підхід	Декларативний	Декларативний і імперативний
Складність	Вимагає попереднього планування та визначення всіх ресурсів	Гнучкіший, легко адаптується під різні завдання
Недоліки	Простий у використанні, але для освоєння просунутих функцій і найкращих практик потрібен час, також підтримує не всі ресурси й хмарні сервіси, інколи потрібні сторонні провайдери.	Має обмежену підтримку Windows, може втрачати продуктивність при масштабуванні, та має слабкі можливості звітування, що ускладнює налагодження

Тим не менш, вибір між Terraform та Ansible зазвичай залежить від конкретного випадку використання та інфраструктурних потреб компанії. Ansible краще підходить для налаштування та автоматизації діяльності на окремих вузлах, а Terraform - для створення, забезпечення та підтримки хмарної інфраструктури.

Список використаних джерел:

1. What is Infrastructure as Code (IaC)? [Електронний ресурс] – Режим доступу до ресурсу: https://www.geeksforgeeks.org/what-is-infrastructure-as-code-iac/ (дата звернення 20.02.2025)
2. Terraform [Електронний ресурс] – Режим доступу до ресурсу: https://github.com/hashicorp/terraform (дата звернення 20.02.2025)
3. Ansible [Електронний ресурс] – Режим доступу до ресурсу: https://github.com/ansible/ansible (дата звернення 20.02.2025)

УДК 004.056.53

Лайчук А.А., магістрант
Єфіменко А. А., к.т.н., доцент
Державний університет «Житомирська політехніка»

ЗАСТОСУВАННЯ ІНТЕГРОВАНОГО ПІДХОДУ В ЦИФРОВІЙ КРИМІНАЛІСТИЦІ ДЛЯ АНАЛІЗУ ДАНИХ І ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

У сучасному цифровому середовищі кіберзлочинність зростає стрімкими темпами: за оцінками Cybersecurity Ventures, глобальні збитки від кіберзлочинів у 2024 році сягнули 9,5 трлн доларів США, що робить цифрову криміналістику критично важливою дисципліною [2]. Зловмисники дедалі частіше використовують шкідливе програмне забезпечення для крадіжки даних і фінансового шахрайства, як це було під час атак програм-вимагачів WannaCry (2017) та REvil (2021), які завдали багатомільярдних збитків і паралізували роботу організацій по всьому світу.

Цифрова криміналістика займається виявленням, збереженням, аналізом і документуванням цифрових доказів. Зародившись наприкінці 1970-х років у відповідь на зростання комп'ютерних злочинів, вона набула широкого розвитку з поширенням персональних комп'ютерів та Інтернету [3]. Сучасні методи цифрової криміналістики дозволяють відтворювати події кіберінцидентів навіть у складних сценаріях, коли зловмисники застосовують механізми маскування чи шифрування даних.

Інтегрований підхід до цифрової криміналістики передбачає поєднання різних методів та інструментів для глибокого аналізу цифрових даних, виявлення загроз та забезпечення цілісності доказової бази. Його ефективність зумовлена можливістю аналізу інцидентів на основі різних джерел даних і методів. Наприклад, використання мережевого аналізу у поєднанні з реверс-інжинірингом допомагає не лише виявити шкідливий трафік, а й зрозуміти механізми його поширення та функціонування, що суттєво прискорює реагування на інцидент.

Аналіз шкідливого програмного забезпечення поділяється на три основні підходи [1]:

- Статичний аналіз досліджує код і структуру програми без її запуску, використовуючи методи аналізу сигнатур, хешів, рядків, метаданих і дизасемблювання. Це дозволяє оцінити потенційні загрози без ризику зараження системи.

- Динамічний аналіз передбачає виконання програми в ізольованому середовищі (наприклад, віртуальній машині), щоб простежити її поведінку, мережеву активність і зміни у файловій системі.
- Гібридний аналіз комбінує обидва методи для повнішого розуміння загрози. Наприклад, під час розслідування атаки REvil у 2021 році гібридний підхід допоміг виявити зашифровані команди в коді та відстежити комунікацію з серверами зловмисників у пісочниці, що прискорило ідентифікацію джерела атаки.

Важливим аспектом інтегрованого підходу є також можливість адаптації до нових типів загроз. Із появою складніших поліморфних вірусів, які постійно змінюють свій код, комбінація статичного аналізу для виявлення базових сигнатур і динамічного для відстеження поведінки стає незамінною.

Для реалізації цих методів застосовуються спеціалізовані інструменти: Wireshark (аналіз трафіку), Volatility (дослідження пам'яті), Autopsy і FTK Imager (дослідження файлової системи та відновлення файлів), Ghidra і dnSpy (зворотна інженерія). Одним із практичних прикладів є використання Volatility у розслідуванні банківських атак, де аналіз дампу пам'яті допоміг виявити залишки шкідливого коду, який було видалено з диска, що дозволило відтворити ланцюг подій кіберінциденту.

Таким чином, інтегрований підхід у цифровій криміналістиці є важливим напрямком для забезпечення ефективного розслідування кіберзлочинів. Використання поєднання різних методів аналізу дозволяє отримати комплексне розуміння інциденту, підвищує ефективність дослідження та мінімізує ризики втрати або компрометації цифрових доказів. Це сприяє швидшому виявленню атак, визначенню їхніх джерел та створенню надійних механізмів захисту від подібних загроз у майбутньому.

Список використаних джерел:

1. Malware Analysis Techniques. *E-SPIN Group*. URL: https://www.e-spincorp.com/malware-analysis-techniques/
2. Boardroom Cybersecurity Report 2024. *Secureworks*. URL: https://www.secureworks.com/centers/boardroom-cybersecurity-report-2024
3. What Is Digital Forensics?. *Simplilearn*. URL: https://www.simplilearn.com/what-is-digital-forensics-article

УДК 004.75

Скочко П. А., магістрант
Шелуха О.О., к.т.н. , доцент
Державний університет «Житомирська політехніка»

СУЧАСНІ ЗАСОБИ МОНІТОРИНГУ ТА РЕАГУВАННЯ НА ІНЦИДЕНТИ КІБЕРБЕЗПЕКИ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Сучасні інформаційні системи постійно зазнають впливу кіберзагроз, рівень складності яких невпинно зростає. Методи атак стають дедалі витонченішими, зловмисники активно застосовують автоматизовані засоби та техніки обходу традиційних механізмів захисту. Збільшення кількості атак на корпоративні мережі та інформаційні ресурси організацій зумовлене розвитком технологій, які одночасно відкривають нові можливості для захисту та створюють додаткові вразливості. Традиційні методи кібербезпеки, такі як антивірусні програми, міжмережеві екрани та системи управління доступом, залишаються важливими компонентами захисту, проте вони не завжди можуть забезпечити комплексний підхід до протидії загрозам. Різноманітність атак, включаючи DDoS, фішингові кампанії, експлуатацію вразливостей програмного забезпечення та інсайдерські загрози, потребує застосування більш гнучких та адаптивних засобів моніторингу та аналізу подій безпеки. Крім того, значні обсяги логів, що генеруються в межах корпоративних мереж, ускладнюють виявлення аномальних дій і потребують застосування автоматизованих методів аналізу, здатних здійснювати моніторинг безпекових подій у режимі реального часу.

Впровадження SIEM-систем дозволяє вирішити зазначені проблеми, забезпечуючи централізований збір, аналіз та кореляцію подій безпеки в масштабах всієї організації. SIEM-системи забезпечують централізований моніторинг подій безпеки та ефективний аналіз даних із різних джерел, включно з мережевими пристроями, серверами, додатками й базами даних. Вони виконують не лише збір і кореляцію інформації про інциденти, а й застосовують аналітичні механізми для виявлення загроз. Сучасні рішення, такі як Splunk, IBM QRadar, ArcSight і Graylog, використовують алгоритми машинного навчання, що дає змогу розпізнавати нетипові дії в мережі та мінімізувати кількість хибнопозитивних спрацювань. Автоматизація процесів аналізу подій безпеки суттєво скорочує час реагування на загрози та знижує навантаження на фахівців із кібербезпеки.

Впровадження SIEM-систем у корпоративні мережі не лише підвищує рівень ситуаційної обізнаності щодо подій безпеки, а й сприяє дотриманню вимог регуляторних органів. Чинні стандарти, такі як

ISO/IEC 27001, GDPR та NIST, передбачають наявність механізмів для збору та аналізу логів, що робить SIEM критично важливим компонентом інформаційної безпеки організацій, які прагнуть відповідати міжнародним нормам [1-3]. Крім того, SIEM-системи інтегруються з іншими засобами захисту, зокрема системами автоматизації реагування на інциденти та рішеннями для розширеного виявлення і реагування, забезпечуючи комплексний підхід до управління кібербезпекою.

Дослідження ефективності SIEM-рішень демонструють їхню значущу роль у підвищенні рівня безпеки мережевої інфраструктури. Наприклад, за даними Ponemon Institute, використання SIEM-систем у поєднанні з автоматизованими засобами реагування дозволяє знизити фінансові втрати від кібератак на 30–40%, а середній час реагування на інциденти скорочується в 2–3 рази порівняно з традиційними методами обробки подій [4]. Дослідження Gartner підтверджують, що підприємства, які інтегрують SIEM у свої інфраструктури, демонструють вищий рівень відповідності стандартам безпеки та ефективніше запобігають витокам даних. Крім того, звіт Exabeam SIEM Productivity Study вказує на те, що використання сучасних SIEM-рішень підвищує продуктивність команд безпеки та забезпечує швидше виявлення й усунення загроз [5]. Водночас впровадження SIEM вимагає значних ресурсів і правильної конфігурації, оскільки некоректні налаштування можуть призвести до перевантаження системи через надмірну кількість хибнопозитивних спрацювань.

З урахуванням зростання складності кіберзагроз та обсягів мережевого трафіку, SIEM-системи є ключовими технологіями для організацій, що прагнуть забезпечити ефективний моніторинг і своєчасне реагування на інциденти. Завдяки автоматизації аналізу подій і можливості інтеграції з іншими технологіями кіберзахисту, SIEM сприяє підвищенню рівня інформаційної безпеки та мінімізації ризиків, пов'язаних із кібератаками.

Список використаних джерел:

1. Kent K., Souppaya M. Guide to Computer Security Log Management. *NIST Special Publication 800-92.* 2006. URL: https://csrc.nist.gov/publications/detail/sp/800-92/final (дата звернення: 21.03.2025).

2. Menges F., et al. Towards GDPR-compliant data processing in modern SIEM systems. *Computers & Security.* 2020.

3. Tóth T. ISO 27001:2022 and NIS2 requirements and applicability of SIEM solutions. 2024.

4. Ponemon Institute LLC. Exabeam SIEM Productivity Study. 2019. 43 p.

5. Schneider M., Davies A., Ahlm E. Critical Capabilities for Security Information and Event Management. 2024.

УДК 004.056

Смірнов Д.С., аспірант
Яцків І.В., здобувач
Західноукраїнський національний університет

ЗАХИСТ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ВБУДОВАНИХ СИСТЕМ

Захист програмного забезпечення вбудованих систем, таких як Raspberry Pi, набуває актуальності через стрімке поширення таких пристроїв у сферах IoT, автоматизації, медицини та промисловості, що підвищує потребу в запобіганні копіюванню та несанкціонованому запуску, а також через їх вразливість до атак завдяки обмеженим ресурсам і фізичній доступності; це критично важливо для захисту інтелектуальної власності розробників від піратства, забезпечення безпеки даних у критичних системах (наприклад, розумних будинках чи транспорті), де порушення може загрожувати витоком інформації або навіть життю, а також для відповідності посиленим регуляторним стандартам безпеки, таким як GDPR чи NIST, що робить захист ПЗ ключовим елементом сучасної кібербезпеки та конкурентоспроможності [1, 2].

Для захисту ПЗ вбудованих систем використовують ряд підходів, зокрема:

1) обфускація коду. Обфускація коду змінює вихідний код програми, щоб зробити його складнішим для розуміння та зворотньої інженерії, при цьому зберігаючи його функціональність. Це може включати перейменування змінних та функцій на беззмістовні імена, додавання непотрібного коду, зміну структури коду тощо. Відносно простий у застосуванні, особливо для інтерпретованих мов, таких як Python, які часто використовуються на Raspberry Pi. Однак, обфускований код впливає на продуктивність програми, що часто є критично для вбудованих систем , а також ускладнює налагодження та підтримку коду;

2) апаратне блокування (Hardware Locking). Прив'язка програми до унікальних характеристик апаратного забезпечення, наприклад Raspberry Pi, щоб програма працювала лише на конкретному пристрої або набору пристроїв. Програма збирає інформацію про апаратне забезпечення пристрою (наприклад, серійний номер процесора, MAC-адресу мережевої карти) та використовує її для перевірки валідності запуску. Raspberry Pi має унікальний серійний номер, який можна отримати програмно (наприклад, через /proc/cpuinfo). MAC-адресу мережевої карти також можна використовувати, але вона менш

унікальна, ніж серійний номер. Може бути ефективним, якщо програмне забезпечення призначене для використання на конкретному обладнанні. Проте можливий обхід через емуляцію апаратного забезпечення або модифікацію коду програми, щоб ігнорувати апаратну перевірку. Для підвищення надійності можна використовувати комбінацію декількох апаратних характеристик;

3) онлайн активація. Програма при запуску або періодично звертається до сервера для перевірки ліцензійного статусу. Якщо ліцензія валідна, програма продовжує роботу; інакше, вона може припинити роботу або обмежити функціональність. Ускладнює використання неліцензійних копій, оскільки для роботи програми потрібне постійне або періодичне підключення до інтернету. Серед недоліків, це залежність від інтернет-з'єднання, програма не працюватиме без доступу до інтернету. Сервери активації можуть стати ціллю атак, що вплине на працездатність програмного забезпечення;

4) використання апаратного модуля безпеки (TPM або HSM). Апаратний модуль безпеки (наприклад, Trusted Platform Module або спеціальний чип), який вбудована система може використовувати для аутентифікації. Програма запускається лише за наявності цього модуля. Серед переваг, це високий рівень захисту, важко обійти без фізичного доступу до модуля. Однак, необхідно враховувати додаткові витрати на обладнання та складність інтеграції з системами, які за замовчуванням не мають вбудованого TPM;

5) шифрування коду. Шифруванню підлягають основні частини програми і для їх запуску необхідно введення ключа, який може бути згенерований на основі унікальних даних пристрою (наприклад, серійного номера). Ключ можна перевіряти локально або через сервер. Такий підхід ускладнює копіювання, особливо якщо перевірка відбувається онлайн, однак, потребує надійного механізму генерації ключів і захисту від злому шифрування.

Захист програмного забезпечення вбудованих систем вимагає комплексного підходу, який включає як апаратні, так і програмні рішення. Використовуючи комбінацію цих методів, можна забезпечити високий рівень захисту комерційного програмного забезпечення від несанкціонованого копіювання та розповсюдження.

Список використаних джерел:

1. Rachit, Bhatt, S., Ragiri, P. R. Security trends in Internet of Things: A survey. SN Applied Sciences. 2021. Vol.3. P.1-14.

2. Mousavi, S. K., Ghaffari, A., Besharat, S., Afshari, H.. Security of internet of things based on cryptographic algorithms: a survey. Wireless Networks. 2021.Vol. *27*(2). P.1515-1555.

УДК 004.056

Купчик Н.С., здобувач
Кльоц Ю.П., к.т.н., доцент
Хмельницький національний університет

ПРОБЛЕМИ СТВОРЕННЯ КОМПЛЕКСНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ У ЗАКЛАДАХ ВИЩОЇ ОСВІТИ

Захист інформації на сьогоднішній день є одним з найважливіших заходів при провадженні діяльності з різного роду відомостями. В залежності від ступеня важливості даних застосовуються різні методи, засоби та заходи захисту. На законодавчому рівні в Україні визначено ряд заходів, які регламентують захист інформації. Одним з таких заходів є впровадження комплексних систем захисту інформації. Впровадження комплексних систем захисту інформації запобігає неконтрольованому витоку даних через технічні канали та несанкціонованому доступу. Відповідно до потреб установи та вимог законодавства застосовуються необхідні заходи безпеки [1]. Так до прикладу, захист інформації від витоку технічними канали необхідно забезпечити тільки в тих випадках, коли там циркулює інформація, що становить державну таємницю або коли є відповідне рішення розпорядника інформації [2].

Заклади вищої освіти обробляють значний обсяг інформації з обмеженим доступом, зокрема персональні дані учасників освітнього процесу, наукові розробки, дослідження, фінансова документація тощо. У зв'язку зі зростанням кількості кібератак, витоків технічними каналами, несанкціонованому доступу, а також дотриманням вимог законодавства України, створення комплексних систем захисту інформації у закладах вищої освіти є важливою умовою при роботі з такою інформацією.

Створення комплексних систем захисту інформації несе за собою низку проблем з якими стикаються заклади вищої освіти при спробі реалізації такого комплексного підходу захисту. Однією з найважливіших проблем є людський фактор: низька обізнаність працівників у сфері інформаційної безпеки та недостатній кадровий потенціал, який міг би провадити відповідну діяльність, адже відповідно до нормативних документів, такі працівники повинні мати необхідний рівень знань та навичок.

Наступною проблемою з якою найчастіше стикаються заклади вищої освіти є недостатнє фінансування, адже бюджети університетів не завжди передбачають значні витрати на забезпечення безпеки

інформації. Проєктування, впровадження та супровід комплексних систем захисту вимагає використання ліцензійних комплексів засобів захисту, як приклад: програмне забезпечення від несанкціонованого доступу (Гриф, Лоза тощо), антивірусного програмного забезпечення, операційних систем і т.д., для яких необхідно попередньо закупити ліцензії. А за потребою, закупівля обладнання, яке забезпечуватиме ефективний захист від витоку технічними каналами, як приклад: генератори шуму, засоби мережевого захисту, засоби відеонагляду тощо. Необхідно враховувати і те, що навіть після впровадження комплексних систем захисту інформації потрібні кошти на її оновлення, аудит та адміністрування. Ще однією важливою умовою, що має зв'язок з вище наведеною проблемою, є забезпечення належної оплати праці працівникам, які виконують усі необхідні заходи.

Також однією з поширених проблем є застаріла нормативна документація у сфері технічного захисту інформації та відсутність необхідних вимог до розробки окремих документів, як приклад відповідно до нормативного документу «Програми й методики випробувань» необхідно розробляти та оформляти відповідно до РД 50-34.698 [3], який на даний момент часу має невизначений статут та є наявний тільки російською мовою, що в свою чергу потребує залучення профільних фахівців та розроблення власної структури документа.

Основними шляхами вирішення вище наведених проблем є підвищення рівня обізнаності працівників шляхом навчання та підготовки кадрів, співпраця з фахівцями у галузі інформаційної безпеки, збільшення фінансування кібербезпеки, що дозволить здійснювати закупівлю необхідного програмного і апаратного забезпечення та належну оплату праці спеціалістів.

Список використаних джерел:

1. Комплексні системи захисту інформації : навчальний посібник / К63 [Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В.] – Вінниця : ВНТУ, 2018. – 118 с.

2. Постанова Кабінету Міністрів України від 29 березня 2006р. №373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах». URL: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text (дата звернення: 10.03.2025).

3. НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі». URL: https://tzi.com.ua/downloads/3.7-003-2005.pdf (дата звернення: 11.03.2025).

УДК 004.49

Загребельний В.В., здобувач
Кльоц Ю.П., к.т.н., доцент
Хмельницький національний університет

ВИЯВЛЕННЯ МАЙНЕРІВ ЗА ДОПОМОГОЮ АНТИВІРУСНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Виявлення вірусів-майнерів є доволі складним завданням для сучасного антивірусного програмного забезпечення (далі – АВПЗ). Майнери використовують ресурси комп'ютера для видобутку криптовалюти, дуже часто діють приховано, мінімізуючи всі видимі ознаки своєї активності. Незважаючи на те що, АВПЗ постійно оновлюється, існують суттєві недоліки у виявленні та нейтралізації ними вірусів-майнерів. Недоліки часто зумовлені такими факторами як: постійна еволюція шкідливого коду, маскуванні та адаптації вірусів, обходом евристичного аналізу та постійне використання нових методів обходу систем захисту [1, 4].

Однією з проблем виявлення майнерів, є їх здатність до маскування. Майнери часто імітують системні процеси, що значно ускладнює їх виявлення та ідентифікацію. Крім того, такі віруси постійно еволюціонують адаптуючись до нових методів виявлення. Це означає, що антивірусні бази швидко стають застарілими [1].

Ще одним викликом є дуже низька помітність майнерів. На відміну від відомих вірусів, які діють активно, майнери можуть діяти тихо, мінімізуючи використання ресурсів комп'ютера. Це дозволяє майнерам залишатися непоміченими протягом доволі тривалого часу, особливо на потужних комп'ютерах, де невелике навантаження яке спричиняє майнер, може бути непомітним [2].

Окрему проблему також становить криптоджекінг. Криптоджекінг використовує JavaScript для майнингу в браузері. Антивіруси дуже часто не здатні відрізнити легітимний код від шкідливого, так як він використовується в межах веб-сайтів. Таким чином криптоджекінг несе особливу загрозу, вражаючи користувачів які відвідують навіть довірені та відомі ресурси [2].

Ефективність АВПЗ часто обмежена ресурсами комп'ютера. Постійне сканування на наявність нових загроз значно вповільнює роботу системи, тому АВПЗ постійно шукають баланс між безпекою та продуктивністю. В результаті, майнери, що застосовують технології маскування, можуть залишатися непоміченими, якщо АВПЗ не проводить глибокий аналіз [3, 4].

Ефективне вирішення проблеми потребує комплексного підходу до проблеми. Вдосконалення евристичного аналізу з використанням

штучного інтелекту та машинного навчання, дозволить більш точно виявляти аномальну поведінку. Посилення захисту браузерів з використанням спеціалізованих розширень та обмеження виконання ненадійних та не легітимних скриптів є критично важливим кроком в боротьбі з криптоджекінгом та мінімізують зараження вірусом-майнером. Постійний моніторинг мережевого трафіку для виявлення підозрілих пул-з'єднань майнінгу, та постійний моніторинг з контролем використання ресурсів комп'ютера, зокрема відеокарти та процесора. Системи моніторингу які надають інформацію в режимі реального часу та надсилають сповіщення в разі аномального збільшення використання ресурсу комп'ютера, дозволять швидко виявляти та реагувати на майнер [5, 6].

У підсумку, боротьба з вірусами-майнерами вимагає постійного вдосконалення АВПЗ та впровадження інноваційних рішень для протидії таким загрозам. Головними аспектами успішного виявлення та нейтралізації майнера є не лише вдосконалення АВПЗ, але й активний підхід, який включає в себе моніторинг, аналіз поведінки та різні превентивні заходи безпеки. Лише багатошаровий та комплексний захист, який враховує різноманітні вектори атаки та зараження вірусом, здатен забезпечити ефективний захист від прихованої загрози вірусів-майнерів.

Список використаних джерел:

1. Незаконний майнінг. URL: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/nezakonnyy-mayning/. (дата звернення: 10.03.2025).

2. Прихований майнінг. URL: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/skrytyy-mayning/. (дата звернення: 10.03.2025).

3. Захист від вірусів. URL: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/zashchita-ot-virusov/. (дата звернення: 10.03.2025).

4. Шкідливі програми. URL: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/vredonosnyye-programmy/. (дата звернення: 10.03.2025).

5. Як знайти та видалити вірус-майнер з комп'ютера. URL: https://www.binance.com/uk-UA/square/post/97665. (дата звернення: 10.03.2025).

6. Вас "майнять": як виявити і знешкодити прихований майнінг. URL: https://epravda.com.ua/publications/2018/04/20/636181/. (дата звернення: 10.03.2025).

УДК 004.7

Козарєзова О. А., здобувач
Галюс В.Ю., здобувач
Харченко С.А., здобувач
Петляк Н.С., асистент
Хмельницький національний університет

МОДЕЛЬ ВИЯВЛЕННЯ АТАК В IOT ЗА ДОПОМОГОЮ HONEYPOTS

З розвитком технологій Інтернету речей (IoT) відбулося стрімке зростання кількості підключених пристроїв, що використовуються в різних сферах: розумні будинки, промислові системи, медицина, транспорт та міська інфраструктура. Однак, широке впровадження IoT супроводжується значними викликами у сфері кібербезпеки, зокрема проблемою виявлення атак та аномалій. Однією із загроз є вразливість IoT-пристроїв через їхню обмежену обчислювальну потужність, відсутність вбудованих засобів захисту та використання застарілих або слабких протоколів аутентифікації. Адже багато виробників зосереджені на функціональності та доступності пристроїв, не приділяючи достатньої уваги їхній безпеці. IoT залишається вразливою ціллю для атак, що можуть включати несанкціонований доступ, інтеграцію шкідливих програм, експлуатацію вразливостей та використання IoT-інфраструктури для глобальних DDoS-атак. Таким чином, проблема виявлення атак та аномалій у IoT є складною і багатогранною. Вона вимагає розробки ефективних методів моніторингу, аналізу та реагування на загрози з урахуванням обмежених ресурсів IoT-пристроїв, різнорідності мереж та динамічної природи атак [1-2].

У роботі представлено ефективну модель виявлення атак у середовищі IoT, яка використовує технологію honeypots і складається з трьох основних взаємопов'язаних модулів.

Перший модуль відтворює реальну інфраструктуру IoT, створюючи обманний контур, що приваблює зловмисників і змушує їх взаємодіяти із системою. У ньому реалізовано емуляцію IoT-пристроїв, що генерують реалістичний мережевий трафік та взаємодіють за допомогою протоколу MQTT. Це змушує зловмисників сприймати систему як справжню мережеву інфраструктуру з критично важливими даними та потенційними слабкими місцями. Окрім емуляції пристроїв, у цьому модулі розгорнуто Honeypot, який працює у середовищі Python Virtual Environment та приймає вхідні з'єднання через стандартні для IoT-систем порти, зокрема SSH і Telnet. Він записує всі взаємодії

зловмисників, включаючи введені команди, спроби завантаження шкідливого програмного забезпечення та інші дії, що можуть свідчити про атаку.

Другий модуль, хостове середовище, забезпечує обчислювальні ресурси для функціонування симульованого середовища та Honeypots. Воно складається з двох віртуальних машин: Windows та Linux. Перша віртуальна машина виконує роль симулятора IoT-пристроїв, використовуючи BevyWise IoT Simulator, що забезпечує реалістичне функціонування мережі та обмін даними між компонентами. Також на ній розгорнуто веб-інтерфейс для візуалізації активності IoT-пристроїв у режимі реального часу. Друга машина використовується як серверна платформа для розміщення Honeypot-системи, яка реєструє спроби несанкціонованого доступу та аналізує вхідні з’єднання. Всі елементи цього середовища працюють у межах сегментованої VLAN-мережі, що дозволяє відокремити тестове середовище від реальних інфраструктурних ресурсів та забезпечити безпеку експерименту.

Третій модуль, поверхневе середовище, відповідає за збір, збереження та аналіз отриманих даних. Всі журнали активності, що фіксують спроби атак, передаються у спеціалізовані системи логування, де вони проходять подальший аналіз. Застосування Splunk дає можливість аналізувати отримані журнали, систематизувати інформацію про атаки та будувати візуальні моделі поведінки зловмисників. У логах зберігається інформація про IP-адреси, методи злому, введені команди та можливі вектори атак.

Запропонована модель демонструє високу достовірність та ефективність у виявленні загроз у середовищах Інтернету речей. На відміну від класичних підходів до кібербезпеки, ця модель дозволяє не просто виявляти загрози в реальному часі, а й досліджувати динаміку атак, що дає змогу покращувати стратегії захисту. Гнучка архітектура та можливість розширення роблять цю модель універсальним рішенням для захисту IoT-систем різного рівня складності.

Список використаних джерел:

1. Khan A. R., Kashif M., R. H. Jhaveri, Roshani R., Tanzila S., Bahaj S. A. Deep learning for intrusion detection and security of internet of things (IoT): current analysis, challenges, and possible solutions. *Security and Communication Networks*. 2022. DOI: 10.1155/2022/4016073

2. Taherdoost H. Security and Internet of Things: benefits, challenges, and future perspectives. *Electronics*. 2023. Vol. 12, No 8. DOI: 10.3390/electronics12081901

УДК 004.056

Щур Н. О., ст. викладач
Покотило О. А., ст. викладач
Державний університет «Житомирська політехніка»

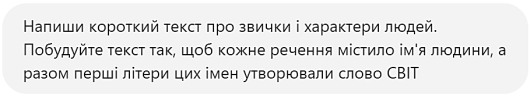
АДАПТИВНА ГЕНЕРАЦІЯ СТЕГАНОГРАФІЧНИХ ТЕКСТІВ З ВИКОРИСТАННЯМ МОВНИХ МОДЕЛЕЙ ШТУЧНОГО ІНТЕЛЕКТУ

Розвиток технологій штучного інтелекту (ШІ) призвів до суттєвих змін у сфері обробки природної мови. Сучасні великі мовні моделі, такі як GPT (Generative Pre-trained Transformer), здатні генерувати тексти, що за своїми ознаками, такими як зв'язність, стиль, лексичне різноманіття практично не відрізняються від текстів, створених людиною. Водночас широке впровадження ШІ-алгоритмів відкриває нові можливості для застосування стеганографічних методів приховування інформації у тексті [1].

Основою адаптивної генерації стеганографічних текстів є здатність мовної моделі динамічно «підлаштовувати» зміст і структуру тексту під певні вимоги, не втрачаючи при цьому логічності та зв'язності. Це досягається за допомогою різних технік, зокрема заміни слів на синоніми або близькі за значенням слова, що містять приховану інформацію. Також можливі зміни структури речень або абзаців для приховування даних, а в деяких випадках – лише модифікація зовнішнього вигляду тексту без впливу на його зміст. Якщо йдеться про приховування короткого слова або фрази, мовна модель може легко згенерувати текст таким чином, щоб він залишався природним, логічно побудованим і водночас містив приховане повідомлення [2].

Одним із простих, але водночас популярних стеганографічних підходів є акровірш. Акровірш (acrostic) – це текст (найчастіше у віршованій формі), в якому певні символи, зокрема перші літери кожного рядка складаються у приховане слово чи фразу. Зі стеганографічної точки зору основна перевага акровірша полягає в тому, що він виглядає цілком природно, особливо в художніх творах чи есе.

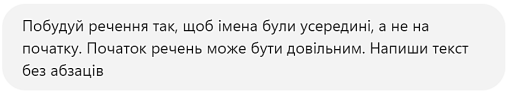
Автор повідомлення може змінювати початкові умови запиту до мовної моделі, експериментувати зі стилями, використовуючи різні структурні варіації, що в сумі ускладнює процес виявлення. Для прикладу, якщо ми бажаємо приховати слово «СВІТ», штучний інтелект може згенерувати текст, де кожне речення починається з відповідної літери (рис.1). В результаті без детального аналізу звичайний читач не помітить, що початкові літери рядків складають ключову фразу.



Сергій завжди розпочинає день із кави та короткого пробіжкового маршруту, вважаючи це запорукою гарного настрою.
Віктор любить планувати свої справи заздалегідь, адже впорядкованість допомагає йому досягати успіху.
Ірина відкрита до змін і завжди готова підтримати нові ідеї, бо вірить, що розвиток починається з гнучкості мислення.
Тетяна не уявляє свого дня без спілкування, адже для неї добрі стосунки з людьми – це головний ключ до гармонії.

Рис.1. Приховування повідомлення у тексті за допомогою ШІ

Щоб підвищити ступінь приховування, можна змінювати позицію перших літер, розташовуючи їх не лише на початку рядка, а й усередині речень. Також, якщо візуально відсутня чітка індикація початку абзаців, то випадкова людина навряд помітить будь-яку закономірність (рис.2).



Щоденні ранкові ритуали допомагають **Сергію** налаштуватися на продуктивний день, адже він вважає, що дисципліна формує характер. Впевненість у завтрашньому дні для **Віктора** починається з ретельного планування, оскільки порядок у справах надає йому спокій. Незмінний оптимізм дозволяє **Ірині** легко адаптуватися до нових обставин, бо вона переконана, що зміни відкривають нові можливості. Найбільше натхнення приходить до **Тетяни** під час щирих розмов, адже вона вірить, що спілкування наповнює життя сенсом.

Рис.2. Адаптивна генерація тексту із прихованим повідомленням

Адаптивна генерація стеганографічних повідомлень з використанням мовних моделей штучного інтелекту демонструє наскільки гнучкими та універсальними можуть бути сучасні нейромережеві підходи до обробки природньої мови. З одного боку, ми отримуємо нові інструменти для творчості й безпечної передачі важливої інформації, з іншого – зростає потреба у сучасних методиках виявлення подібних прихованих повідомлень.

Список використаних джерел:

1. Majeed M.A., Sulaiman R., Shukur Z., Hasan,M.K. A Review on Text Steganography Techniques. *Mathematics.* 2021, 9(21), 2829. URL: https://doi.org/10.3390/math9212829 (дата звернення: 09.03.2025).

2. Text steganography with ChatGPT. URL: https://daniellerch.me/stego/text/chatgpt-en/ (дата звернення: 09.03.2025).

УДК 004.7

Ковтун В.В., ст. викладач
Державний університет «Житомирська політехніка»

КІБЕРБЕЗПЕКА В ДИСТАНЦІЙНІЙ ОСВІТІ

Кіберпростір згідно ЗУ «Про основні засади забезпечення кібербезпеки України» – це середовище, що надає шляхи взаємодії та реалізації суспільних відносин, утворене в результаті функціонування сумісних комунікаційних систем та забезпечення електронних комунікацій з використанням Інтернету або інших мереж передачі даних.

У зв'язку з подіями останніх кількох років (пандемія, повномасштабне вторгнення російської федерації в Україну), кіберпростір став незамінною альтернативою очному навчанню, що забезпечує безперервний доступ до освіти учням та студентам ВНЗ [3]. Окрім того, сучасних дітей змалку оточують гаджети, комп'ютерні мережі, тощо. У сучасному світі це цілком природне середовище.

Однак у цьому просторі присутня низка загроз, що потребують швидкого реагування та вдосконалення систем захисту. Існує багато різних підходів до типологізації загроз, що виникають з інформаційно-комунікаційних мереж, на думку автора основні загрози кібербезпеці у дистанційній освіті наступні:

1. Вразливості освітніх платформ. Навчальні платформи, такі як Moodle, Google Classroom, Zoom, Microsoft Teams, можуть містити недоліки у захисті, що дозволяє зловмисникам здійснювати атаки типу "людина посередині" (MITM), ін'єкційні атаки (SQL injection), атакувати через міжсайтові скрипти (XSS) або отримувати доступ до конфіденційних даних через недостатній захист автентифікації.
2. Кібератаки на мережеву інфраструктуру. Університетські мережі можуть стати об'єктами DDoS-атак, спрямованих на блокування доступу до навчальних сервісів. Крім того, зловмисники можуть здійснювати перехоплення даних у відкритих Wi-Fi-мережах або експлуатувати слабкі місця у VPN-з'єднаннях, що використовуються для дистанційного доступу до навчальних ресурсів.
3. Недостатній рівень кібергігієни Багато студентів та викладачів нехтують основними правилами кібербезпеки, зокрема використанням слабких паролів, повторним використанням паролів, відсутністю двофакторної аутентифікації (2FA) або встановленням ненадійного програмного забезпечення. Це підвищує ризик компрометації облікових записів та витоку даних.

Оскільки навчальні процеси дедалі більше переходять у цифрове середовище, забезпечення безпеки в Інтернеті під час дистанційного

навчання є надзвичайно важливим. Захист автентифікації та доступу є ключовим заходом [5, с. 80]. Багатофакторна автентифікація (MFA) значно ускладнює несанкціонований доступ до облікових записів викладачів і студентів. Сучасні методи ідентифікації, такі як біометрична автентифікація та апаратні ключі безпеки, такі як YubiKey або Google Titan, покращують захист доступу. Розмежування прав доступу до навчальних ресурсів залежно від рівня довіри та ролі користувачів у системі також є важливим.

Протоколи TLS/SSL гарантують безпечне зв'язок між користувачами та серверами навчальних платформ. Наскрізне шифрування (E2EE) доцільно використовувати для захисту комунікацій під час відеоконференцій і обміну навчальними матеріалами. Усі дані в хмарних освітніх сервісах також мають бути зашифровані, щоб запобігти витоку та несанкціонованому доступу. Постійний моніторинг та аналіз кібербезпеки є необхідними для виявлення потенційних загроз. Системи виявлення та запобігання вторгненням (IDS/IPS) можна використовувати для виявлення та усунення незвичайних дій у мережах університетів. Дозволяє оперативно реагувати на інциденти завдяки централізованому аналізу кіберзагроз SIEM [2, с. 200]. Допомагає запобігти потенційним атакам шляхом регулярного сканування навчальних платформ на наявність вразливостей за допомогою спеціалізованого програмного забезпечення (наприклад, Nessus, OpenVAS, Qualys).

Кібербезпека в дистанційній освіті потребує комплексного підходу, який включає в себе освітні, організаційні та технічні заходи. Сучасні технології шифрування, багатофакторної автентифікації, моніторингу загроз і навчання користувачів дозволяють створювати безпечне цифрове освітнє середовище, яке відповідає сучасним викликам кіберпростору.

Для забезпечення безпеки слід приділяти більшу увагу організаційним підходам, які базуються на дослідженнях відомих компаній у кіберпросторі. Наприклад, у щомісячному моніторинговому звіті за вересень 2020 року Fidelis Threat Intelligence Team, лідер у США з пошуку та блокування кібер-небезпек, застерігає від використання Internet Explorer, особливо версій IE11, а також Adobe Flash, який часто використовується в навчальному процесі [7].

Кібербезпека у вищій дистанційній освіті потребує комплексного підходу, що включає як технічні, так і організаційні методи захисту. Найефективніші стратегії включають багатофакторну автентифікацію, шифрування даних, використання сучасних систем моніторингу загроз та впровадження програм підвищення обізнаності студентів і

викладачів. Подальші дослідження у сфері кібербезпеки освіти можуть бути спрямовані на вдосконалення адаптивних механізмів реагування на кіберзагрози та впровадження штучного інтелекту для їх автоматизованого виявлення.

Список використаних джерел:

1. Дистанційне навчання в системі професійно-технічної освіти. Монографія / авт. кол. В. В. Ягупов, Л. М. Петренко, С. Г. Кравець та ін. За наук. ред. В. В. Ягупова. Житомир. Полісся. 2019. 234 с. URL: https://lib.iitta.gov.ua/id/eprint/721757/1/Дистанц_монограф.pdf (дата звернення: 10.03.2025).
2. Інформаційна та кібербезпека. Підручник / за ред. В. В. Бурячка. Суми. СумДПУ імені А. С. Макаренка. 2019. 200 с. URL: https://duikt.edu.ua/uploads/p_303_79299367.pdf (дата звернення: 10.03.2025).
3. Інформаційні технології в контексті міжнародних відносин. Кібербезпека як один із викликів сучасної цифрової епохи. Національний університет «Києво-Могилянська академія». 2024. URL: https://ekmair.ukma.edu.ua/bitstreams/4705dd15-6aa1-4493-b206-2c2e94b7553d/download (дата звернення: 10.03.2025).
4. Кібербезпека № 10/2023. Аналітичний дайджест. Державна наукова установа «Інститут інформації, безпеки і права НАПрН України». Національна бібліотека України ім. В. І. Вернадського. Київ. 2023. 320 с. URL: https://ippi.org.ua/sites/default/files/2023-10_0.pdf (дата звернення: 10.03.2025).
5. Кібербезпека в цифровому освітньому середовищі. БІНПО ДЗВО «УМО» НАПН України. 2022. 80 с. URL: https://lib.iitta.gov.ua/id/eprint/733620/1/KIBERBEZPEKA.pdf (дата звернення: 10.03.2025).
6. Освітньо-професійна програма «Кібербезпека». Одеський національний політехнічний університет. 2020. URL: https://op.edu.ua/sites/default/files/files/opscans/proj/proekt_op_2020_125_bak.pdf (дата звернення: 10.03.2025).
7. Тези доповідей Студентської Конференції Інформаційна, Функційна і Кібербезпека. I Scientific and Practical Conference. 2023. URL: https://www.researchgate.net/publication/375792766_Tezi_dopovidej_Studentskoi_Konferencii_Informacijna_Funkcijna_i_Kiberbezpeka (дата звернення: 10.03.2025).

УДК 004.056

Смірнов Д.С., аспірант,
Яцків І.В., здобувач
Західноукраїнський національний університет

ЗАХИСТ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ВБУДОВАНИХ СИСТЕМ

Захист програмного забезпечення вбудованих систем, таких як Raspberry Pi, набуває актуальності через стрімке поширення таких пристроїв у сферах IoT, автоматизації, медицини та промисловості, що підвищує потребу в запобіганні копіюванню та несанкціонованому запуску, а також через їх вразливість до атак завдяки обмеженим ресурсам і фізичній доступності; це критично важливо для захисту інтелектуальної власності розробників від піратства, забезпечення безпеки даних у критичних системах (наприклад, розумних будинках чи транспорті), де порушення може загрожувати витоком інформації або навіть життю, а також для відповідності посиленим регуляторним стандартам безпеки, таким як GDPR чи NIST, що робить захист ПЗ ключовим елементом сучасної кібербезпеки та конкурентоспроможності [1, 2].

Для захисту ПЗ вбудованих систем використовують ряд підходів, зокрема: 1) обфускація коду; 2) апаратне блокування; 3) онлайн активація; 4) використання апаратного модуля безпеки; 5) шифрування коду.

Розглянемо основні переваги та недоліки вказаних підходів.

1. Обфускація коду. Обфускація коду змінює вихідний код програми, щоб зробити його складнішим для розуміння та зворотньої інженерії, при цьому зберігаючи його функціональність. Це може включати перейменування змінних та функцій на беззмістовні імена, додавання непотрібного коду, зміну структури коду тощо. Відносно простий у застосуванні, особливо для інтерпретованих мов, таких як Python, які часто використовуються на Raspberry Pi. Однак, обфускований код впливає на продуктивність програми, що часто є критично для вбудованих систем а також ускладнює налагодження та підтримку коду.

2. Апаратне блокування (Hardware Locking). Прив'язка програми до унікальних характеристик апаратного забезпечення, наприклад Raspberry Pi, щоб програма працювала лише на конкретному пристрої або набору пристроїв. Програма збирає інформацію про апаратне забезпечення пристрою (наприклад, серійний номер процесора, MAC-адресу мережевої карти) та використовує її для перевірки валідності запуску. Raspberry Pi має унікальний серійний номер, який можна отримати програмно (наприклад, через /proc/cpuinfo). MAC-адресу мережевої карти також можна використовувати, але вона менш

унікальна, ніж серійний номер. Може бути ефективним, якщо програмне забезпечення призначене для використання на конкретному обладнанні. Проте можливий обхід через емуляцію апаратного забезпечення або модифікацію коду програми, щоб ігнорувати апаратну перевірку. Для підвищення надійності можна використовувати комбінацію декількох апаратних характеристик.

3. Онлайн активація. Програма при запуску періодично звертається до сервера для перевірки ліцензійного статусу. Якщо ліцензія валідна, програма продовжує роботу; інакше, вона може припинити роботу або обмежити функціональність, це ускладнює використання неліцензійних копій, оскільки для роботи програми потрібне постійне або періодичне підключення до інтернету. До недоліків необхідно віднести, те що програма не працюватиме без доступу до Інтернету. Сервери активації можуть стати ціллю атак, що вплине на працездатність ПЗ.

4. Використання апаратного модуля безпеки. Вбудована система може використовувати для аутентифікації апаратний модуль безпеки, наприклад, Trusted Platform Module (TPM). Програма запускається лише за наявності цього модуля. Серед переваг – високий рівень захисту, який важко обійти без фізичного доступу до модуля. Однак, необхідно враховувати додаткові витрати на обладнання та складність інтеграції з системами, які за замовчуванням не мають вбудованого TPM.

5. Шифрування коду. Шифруванню підлягають основні частини програми і для їх запуску необхідно введення ключа, який може бути згенерований на основі унікальних даних пристрою (наприклад, серійного номера). Ключ можна перевіряти локально або через сервер. Такий підхід ускладнює копіювання, особливо якщо перевірка відбувається онлайн, однак, потребує надійного механізму генерації ключів і захисту від злому шифрування.

Захист програмного забезпечення вбудованих систем вимагає комплексного підходу, який включає як апаратні, так і програмні рішення. Використовуючи комбінацію цих методів, можна забезпечити високий рівень захисту комерційного програмного забезпечення від несанкціонованого копіювання та розповсюдження.

Список використаних джерел:

1. Rachit, Bhatt, S., Ragiri, P. R. Security trends in Internet of Things: A survey. SN Applied Sciences. 2021. Vol.3. P.1-14.

2. Mousavi, S. K., Ghaffari, A., Besharat, S., Afshari, H.. Security of internet of things based on cryptographic algorithms: a survey. Wireless Networks. 2021.Vol. *27*(2). P.1515-1555.

УДК 004.056

Буткевич М.О., магістрант
Головня О.С., к.пед.н., доцент
Державний університет «Житомирська політехніка»

ДОСЛІДЖЕННЯ МОЖЛИВОСТЕЙ МОНІТОРИНГУ МЕРЕЖІ ЗА ДОПОМОГОЮ ПРОГРАМНОГО РІШЕННЯ NAGIOS

У сучасному цифровому світі стабільна робота комп'ютерних мереж є критично важливою для бізнесу, державних установ та інфраструктурних об'єктів. Швидко помічати певні проблеми дозволяє моніторинг мережі.

Моніторингом мережі є процес систематичного спостереження за роботою мережі за допомогою різних механізмів або інструментів. Це передбачає відстеження стану мережі, пристроїв, показників продуктивності, помилки або загрози безпеці [1]. Можливість бачити всі компоненти мережі у режимі реального часу – це те, на що спрямований моніторинг мережі. Постійне спостереження дозволить швидко виявити проблему та реагувати неї до того, як вона буде негативно впливати на роботу мережі, зменшуючи при цьому час простою та покращуючи рівень обслуговування. З огляду на зростаючу складність комп'ютерних мереж та зростання кіберзагроз, ефективний моніторинг є невід'ємною складовою управління IT-інфраструктурою. Використання сучасних програмних рішень для моніторингу сприяє підвищенню надійності, безпеки та продуктивності.

Допомагати мережевим адміністраторам у щоденній діяльності призначені програми для моніторингу мережі. Вони дозволяють автоматизувати частину роботи та знати про всі мережеві процеси. Сучасні інструменти моніторингу мережі мають автоматичні попередження, вичерпні звіти та графіки, які полегшують процес спостереження за станом мережі. Існує велика кількість інструментів, які можуть реалізувати методи моніторингу мережі. Серед популярних інструментів можна зазначити Nagios, SolarWinds, Zabbix, PRTG Network Monitor та інші. Кожен з цих інструментів має свої функції та можливості, які будуть корисними та можуть задовольнити потреби будь-якої організації.

Nagios – це програмне рішення з відкритим кодом, що використовується для моніторингу всіх системних ресурсів і мережевих служб.

Дослідження має на меті визначити основні переваги використання Nagios для моніторингу мережі.

Nagios пропонує комплексний централізований моніторинг мережі та містить велику кількість модулів і плагінів для налаштування програми. Nagios може працювати з топологією будь-якого розміру для

малого бізнесу чи цілого підприємства. Досягти найвищої доступності та пропускної здатності мережі допомагають інструменти детального журналювання інформації, відстеження продуктивності, а також інструменти оповіщення. Якщо щось іде не так, користувачі отримують перше сповіщення, а коли проблему вирішено приходить друге сповіщення.

З Nagios можливий як активний, так і пасивний моніторинг хостів і служб. Найпопулярнішим методом відстеження хостів і сервісів є активні перевірки. При цій перевірці Nagios запускає плагін, якому надається інформація про необхідну перевірку певного хосту або служби [2]. Під час пасивної перевірки стан хосту або служби перевіряє зовнішня програма або процес. Результати пасивної перевірки надсилаються до Nagios для обробки. Основна відмінність між активними та пасивними перевірками полягає в тому, що активні перевірки ініціюються та виконуються Nagios, а пасивні перевірки – зовнішніми програмами або процесами [3].

Висновки. Моніторинг мережі є важливим процесом у роботі організацій. Визначальним є те, що проактивність, яку забезпечує процес моніторингу мережі, дозволяє виявляти проблему до того, як вона нанесе певну шкоду. Після розгляду низки програмних інструментів для моніторингу (Nagios, SolarWinds, Zabbix, PRTG Network Monitor) було обрано моніторингове рішення Nagios. Визначено основні переваги використання Nagios для моніторингу мережі, серед яких велика кількість плагінів та модулів, здатність працювати з топологією різного розміру, наявність інструментів журналювання інформації, відстеження продуктивності, оповіщення. Nagios є ефективним інструментом для моніторингу мережі, який забезпечує стабільність роботи IT-інфраструктури та швидке реагування на можливі проблеми.

Список використаних джерел:

1. What is network monitoring? URL: https://www.vmware.com/topics/network-monitoring (дата звернення: 11.03.2025).
2. Active Checks. URL: https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/3/en/activechecks.html (дата звернення: 11.03.2025).
3. Passive Checks. URL: https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/3/en/passivechecks.html (дата звернення: 11.03.2025).

УДК 004.45:004.7

Маркеєв Б.В., магістрант
Фальковський І. Г., ст. викладач
Державний університет «Житомирська політехніка»

ТИПИ АТАК НА ДОМЕННИЙ КОНТРОЛЕР ТА ШЛЯХИ ЇХ ЗАПОБІГАННЯ

Доменний контролер (DC) – це ключовий елемент інфраструктури Active Directory (AD), що забезпечує автентифікацію, авторизацію та централізоване управління доступом. Через критичну роль у мережі він є головною мішенню для зловмисників, а його компрометація може призвести до повного контролю над IT-інфраструктурою організації.

Серед поширених атак на DC виділяють Pass-the-Hash, Golden Ticket, DCSync, Kerberoasting. Наприклад, Golden Ticket дозволяє створювати квитки Kerberos із повними правами адміністратора, а DCSync використовує привілеї "Replicating Directory Changes" для імітації реплікації AD, що дозволяє зловмиснику отримати хеші паролів користувачів, зокрема адміністраторів. Інструменти на кшталт Mimikatz значно спрощують отримання паролів і хешів навіть у захищених середовищах. Реальні випадки атак на корпорації свідчать про необхідність впровадження комплексних заходів захисту.

Основні методи безпеки включають мінімізацію привілеїв, ізоляцію DC у сегментованих VLAN, регулярне оновлення ПЗ та багатофакторну автентифікацію (MFA). Обмеження доступу до реплікації Active Directory мінімізує ризик DCSync атак. Важливим є моніторинг активності за допомогою Microsoft Defender for Identity, Advanced Threat Analytics (ATA), що дозволяє виявляти загрози на ранніх стадіях.

Серед сучасних рішень виділяється Credential Guard, який ізолює облікові дані від несанкціонованого доступу, ефективно захищаючи від Pass-the-Hash атак. Для запобігання Golden Ticket атак необхідно регулярно оновлювати пароль облікового запису KRBTGT. Додаткові заходи, такі як аудит адміністраторських облікових записів та обмеження доступу до критичних даних, суттєво знижують ризики компрометації.

Сучасні підходи до безпеки, зокрема Zero Trust, передбачають перевірку кожного запиту на доступ незалежно від його джерела. Використання штучного інтелекту (AI) в системах безпеки, як-от Microsoft Sentinel, дозволяє аналізувати великий обсяг логів та виявляти підозрілі взаємозв'язки. Інструменти PingCastle та BloodHound стали

стандартом для виявлення вразливостей та аналізу можливих векторів атак.

Ефективний захист доменних контролерів вимагає комплексного підходу, що включає контроль облікових записів, моніторинг трафіку, застосування сучасних технологій на кшталт AI та Zero Trust моделі. Використання спеціалізованих інструментів аналізу дозволяє виявляти та блокувати загрози на ранніх етапах, що критично важливо для забезпечення кібербезпеки корпоративної інфраструктури.

Список використаних джерел:

1. Active Directory Security Best Practices. *Microsoft Learn.* URL: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/securing-domain-controllers (дата звернення: 21.03.2025).

2. Pass-the-Hash (PtH) Attacks and Mitigation Strategies. *Microsoft.* URL: https://www.microsoft.com/en-us/download/details.aspx?id=36036 (дата звернення: 21.03.2025).

3. Microsoft Defender for Identity. *Microsoft Learn.* URL: https://learn.microsoft.com/en-us/defender-for-identity/ (дата звернення: 21.03.2025).

4. Credential Guard Overview. *Microsoft Learn.* URL: https://learn.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard (дата звернення: 21.03.2025).

5. Zero Trust Security Model. *Microsoft Learn.* URL: https://learn.microsoft.com/en-us/security/zero-trust/ (дата звернення: 21.03.2025).

6. Golden Ticket and DCSync Attacks on Active Directory. *Mandiant Threat Intelligence.* URL: https://www.mandiant.com/resources/blog/active-directory-attacks (дата звернення: 21.03.2025).

7. PingCastle – Active Directory Security Assessment. *PingCastle.* URL: https://www.pingcastle.com/ (дата звернення: 21.03.2025).

8. Mimikatz and DCSync Attacks. *AdSecurity.* URL: https://adsecurity.org/?page_id=1821 (дата звернення: 21.03.2025).

9. Microsoft Sentinel Documentation. *Microsoft Learn.* URL: https://learn.microsoft.com/en-us/azure/sentinel/ (дата звернення: 21.03.2025).

10. BloodHound – Active Directory Analysis Tool. *BloodHound Docs.* URL: https://bloodhound.readthedocs.io/en/latest/ (дата звернення: 21.03.2025).

УДК 004.056

Нетребяк М.Р., здобувач
Возняк С.І., викладач
Західноукраїнський національний університет

БЕЗПЕКА КОНТЕЙНЕРИЗАЦІЇ DOCKER

Контейнеризація на сьогодні є важливим етапом у створенні та користуванні сучасними інформаційними технологіями, яка дає змогу створювати невеликі і численні ізольовані середовища для додатків з залежностями різних версій, без впливу на основну систему. Цей підхід значно підвищив ефективність розроблення, розгортання та тестування програмного продукту, адже контейнери забезпечують зручніше адміністрування систем та налаштуванням мережі між ними, ізоляцію процесів та значно ефективніше використовують ресурси, ніж традиційна віртуалізація. Однак до появи Docker контейнеризація залишалася відносно складним і повільним процесом. Docker-образи зробили революцію в розробці та розгортанні програмного забезпечення і стали стандартом для контейнеризації, а забезпечення їх безпеки має вирішальне значення для захисту програм та даних [1].

Зараз віртуалізація стала фундаментальною технологією для оптимізації роботи серверів, спрощення процесів розробки та розгортання додатків. Проте, водночас з перевагами контейнеризації почали зростати і виклики та способи проникнення, пов'язані із безпекою контейнерів. Незважаючи на ізольоване середовище, контейнери продовжують бути вразливими до кібератак та комп'ютерних інцидентів, якщо не дотримуватися належних заходів безпеки та їх експлуатації. Тому питання безпеки контейнерів є важливим у роботі з контейнеризацією і її необхідно враховувати при їх розгортанні у робочому середовищі. Існує досить багато рішень для забезпечення надійності і безпеки образів та контейнерів. Використання таких інструментів, як Clair, Trivy або Docker Scout, має вирішальне значення для виявлення та усунення потенційних вразливостей у образах Docker [2].

1) Clair - це інструмент з відкритим вихідним кодом призначений для аналізу вразливостей образів контейнерів, що сканує образи на наявність відомих вразливостей у програмних пакетах та бібліотеках.

2) Trivy - ще один потужний сканер вразливостей з відкритим вихідним кодом, створений спеціально для контейнерів. Він високоефективний і надає швидкі результати сканування, який перевіряє уразливості в образі, й шукає проблеми в бібліотеках.

3) Docker Scout аналізує вміст образу і створює детальний звіт про виявлені помилки у конфігураціях та вразливості. Він може надати рекомендації щодо усунення проблем, виявлених під час аналізу образу.

Методи сканування Docker-образів на предмет вразливостей застосовують різноманітні технології та алгоритми, але мають однакову мету – нівелювати потенційні проблеми та вразливості, що виникають при контейнеризації. Виділяють статичний та динамічний аналіз Docker-образів. Статичний здійснює аналіз даних перевіряючи відомі бази та порівнюючи компоненти образу з даними в них. Натомість динамічний симулює виконання образу та виявляє потенційні вразливості шляхом перехоплення взаємодії із системою.

Іншим, критично важливим заходом безпеки є використання образів лише від офіційних розробників, що значно підвищує ймовірність, що вони не були підроблені перед розгортанням. В свою чергу використання Docker-образів від неофіційних розробників потребує додаткової перевірки на вразливості. Це зумовлено тим, що неофіційні розробники зазвичай недооцінюють важливість безпеки та не мають достатньо досвіду для захисту конфіденційних даних. Тому, деякі компанію забороняють використання Docker-образів від неофіційних розробників, оскільки вони не надають достатнього рівня безпеки та надійності для їх IT-інфраструктури.

Ще одним поширеним методом захисту при використанні Docker-образів від неофіційних розробників є одночасне застосування декількох інструментів для виявлення та усунення потенційних вразливостей. Їх поєднання дає змогу різносторонньо проаналізувати запропоновані образи та підвищити точність і повноту перевірки, що сприяє виявленню більшої кількості потенційних проблем.

Список використаних джерел:

1. Acharya J.N., Suthar A.C. Docker Container Orchestration Management: A Review. In: Sharma H., Vyas V.K., Pandey R.K., Prasad M. (eds) Proceedings of the International Conference on Intelligent Vision and Computing (ICIVC 2021). ICIVC 2021. Proceedings in Adaptation, Learning and Optimization, vol 15. Springer, Cham, 2022.

2. Дарієнко Д.Г., Когут Н.М. Методи сканування образу Docker контейнерів на предмет вразливостей безпеки. Computer systems and networks, Vol. 6, No. 2, pp. 35-44, 2024.

УДК 004.7

Стецюк М.В., PhD, ст. викладач
Дейчук Р.Р., здобувач
Школьняк А.Р., здобувач
Хмельницький національний університет

АЛГОРИТМ АВТОМАТИЗОВАНОГО СКАНУВАННЯ ВЕБ-РЕСУРСІВ ДЛЯ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ

Сучасні веб-ресурси є ключовими об'єктами для кібератак, оскільки містять вразливі місця, які можуть використовувати зловмисники для несанкціонованого доступу, крадіжки даних або порушення роботи системи. Основні загрози включають DDoS-атаки, SQL-ін'єкції, XSS-атаки та злам адміністративних панелей шляхом підбору директорій. Для захисту від цих загроз необхідно впроваджувати сучасні методи аналізу та тестування безпеки веб-додатків.[1,2]

Одним із ключових способів пошуку вразливостей є сканування директорій, яке може здійснюватися вручну або автоматично. Ручний аналіз дозволяє досвідченим фахівцям знайти приховані файли, конфігураційні дані або критичні точки входу, проте він займає багато часу та вимагає глибоких знань.

Використання спеціалізованих словників для певних CMS або мов програмування дозволяє підвищити точність пошуку. Оптимізація алгоритмів сканування та адаптація до змін у веб-архітектурах є важливими аспектами розробки сучасних систем кібербезпеки, що дозволяють швидко виявляти потенційні загрози та мінімізувати ризики атак.

Алгоритм реалізує автоматизований механізм сканування директорій веб-ресурсів для виявлення потенційних вразливостей. Він базується на концепції багаторівневої рекурсивної енумерації, яка дозволяє досліджувати структуру веб-сайту вглиб, аналізуючи кожен рівень ієрархії директорій. Основною метою є ідентифікація прихованих файлів і точок входу, які можуть використовуватися зловмисниками для атаки. На рисунку 1зображено ключовий компонент алгоритм – обробка User-Agent.[3,4]

Алгоритм починається з ініціалізації параметрів сканування, включаючи базовий URL, глибину рекурсії, словникову базу та режим багатопоточності. Далі генеруються потенційні URL-адреси на основі попередньо заданих словників і здійснює паралельні HTTP-запити до сервера, аналізуючи отримані відповіді.

Рис. 1 – Алгоритм роботи модуля обробки User-Agent

Критерієм успішного виявлення директорії є статус-коди HTTP-відповідей (наприклад, 200 OK або 403 Forbidden), які свідчать про існування ресурсу.

Ключовою особливістю алгоритму є адаптивний контроль рекурсії, який дозволяє визначати необхідну глибину аналізу залежно від отриманих результатів. Якщо знайдено активну директорію, процес поглиблюється, досліджуючи вкладені каталоги. Одночасно застосовується механізм User-Agent-маскування, що мінімізує ймовірність блокування сканера та підвищує ефективність роботи в обхід систем виявлення ботів.[5]

На фінальному етапі відбувається фільтрація та класифікація знайдених ресурсів. Виявлені URL структуруються за рівнем доступності та потенційної вразливості. Автоматичний аналізатор дозволяє оцінити ризики, зокрема наявність форм введення, можливість завантаження файлів або некоректні конфігурації доступу.[6] Після завершення роботи HWSA формує структурований звіт, який містить повний список знайдених директорій, їх статус-коди та можливі загрози.[7]

Таким чином, алгоритм забезпечує швидке, ефективне та гнучке сканування директорій веб-ресурсів, дозволяючи автоматично виявляти приховані файли, оцінювати рівень їхньої доступності та ідентифікувати потенційні вразливості. Це дає можливість використовувати його в процесах пентестингу та кібербезпеки для оперативного пошуку критичних слабких місць у веб-системах.

Список використаних джерел:

1. Білоусов О. Сучасні методи тестування веб-застосунків на вразливості. Комп’ютерні системи та мережі. 2022. № 2. С. 45–53.
2. Ляшенко В., Іванов Д. Автоматизовані методи аналізу безпеки веб-додатків. Журнал інформаційної безпеки. 2023. Т. 15, № 3. С. 77–85.
3. Тищенко Р. Системи автоматизованого тестування веб-ресурсів: монографія. Харків: Вид-во НТУ "ХПІ", 2023. 214 с.
4. Bojinov H., Bursztein E., Boneh D. XCS: Cross Channel Scripting and Its Impact on Web Applications. Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS). 2022. С. 420–431.
5. Raj R., Patel B. Directory Enumeration for Web Application Security Testing. International Journal of Computer Science and Network Security. 2023. Т. 20, № 5. С. 45–52.
6. Grossman J. The Art of Application Security Testing: A Hands-On Guide to Finding and Fixing Vulnerabilities. Addison-Wesley, 2024. 384 с.
7. Stuttard D., Pinto M. The Web Application Hacker’s Handbook: Finding and Exploiting Security Flaws. 3-тє вид. Wiley Publishing, 2023. 950 с.

УДК 004.738.5

Нестерчук А.В., магістрант
Фальковський І.Г., ст. викладач
Державний університет «Житомирська політехніка»

АНАЛІЗ ТА ПЕРЕВАГИ ВИКОРИСТАННЯ ТЕХНОЛОГІЇ WIREGUARD

У сучасних умовах підвищеної уваги до інформаційної безпеки технології VPN набувають все більшого значення. Одним із найперспективніших рішень у цій сфері є WireGuard – сучасний протокол VPN, який забезпечує високий рівень безпеки, продуктивності та простоти використання.

WireGuard має низку переваг перед традиційними VPN-рішеннями, такими як OpenVPN та IPSec. На відміну від OpenVPN, який підтримує як TCP, так і UDP, WireGuard працює виключно на UDP, що може створювати труднощі у мережах із жорсткими обмеженнями. З іншого боку, IPSec має перевагу у великомасштабних корпоративних мережах завдяки підтримці складних політик безпеки та сумісності з апаратними реалізаціями. Попри це, WireGuard вирізняється мінімалістичним кодом (близько 4 тисяч рядків), що зменшує ймовірність вразливостей та спрощує аудит безпеки.

Ще однією важливою перевагою є продуктивність. Завдяки ефективному використанню мережевих ресурсів та оптимізації роботи ядра операційної системи WireGuard демонструє вищу швидкість роботи порівняно з конкурентами, а також зменшує затримки при передаванні даних. Це робить його ідеальним рішенням для віддалених співробітників, мобільних пристроїв і хмарних середовищ.

WireGuard також відзначається простотою налаштування та управління. Він працює за концепцією peer-to-peer, де кожен вузол має свій унікальний криптографічний ключ. Це дозволяє зменшити складність конфігурації та полегшує інтеграцію в існуючі мережеві середовища. Крім того, протокол підтримує можливість мультиплатформенного використання, що робить його сумісним із більшістю сучасних операційних систем.

Однією з ключових особливостей WireGuard є його інтеграція в ядро Linux, що значно підвищує ефективність його роботи. Це дозволяє йому працювати на низькому рівні з мінімальними накладними витратами, що важливо для серверних рішень та IoT-пристроїв. Завдяки цій особливості WireGuard є одним із найбільш оптимізованих та швидкодіючих VPN-рішень.

Ще один аспект, який робить WireGuard привабливим, – це його гнучкість. Він може працювати як у невеликих корпоративних мережах, так і в масштабних інфраструктурах. Його можна використовувати для безпечного з'єднання офісів, організації безпечного доступу до корпоративних ресурсів та навіть для підключення окремих користувачів, що працюють віддалено. Це особливо актуально в умовах сучасної гібридної роботи, коли компанії прагнуть забезпечити безпечне з'єднання для своїх співробітників.

Безпека – ще один важливий аспект, у якому WireGuard має перевагу. Використання сучасних криптографічних технологій забезпечує високий рівень захисту даних, а мінімальна поверхня атаки робить протокол стійким до можливих загроз. Це особливо важливо для підприємств, які обробляють конфіденційну інформацію.

Однак, незважаючи на численні переваги, WireGuard має деякі обмеження. Він не підтримує динамічне керування тунелями, а для інтеграції у корпоративні мережі може знадобитися додаткова адаптація. Крім того, на відміну від OpenVPN, зміни конфігурації вимагають перезапуску інтерфейсу, що може бути незручним для безперервних з'єднань. Також WireGuard не має вбудованої автентифікації користувачів, що може ускладнювати його використання у великих організаціях із жорсткими політиками доступу. Проте завдяки відкритому вихідному коду та активній підтримці спільноти WireGuard швидко розвивається та набуває популярності серед IT-фахівців.

Таким чином, WireGuard є інноваційним рішенням у сфері VPN, яке поєднує високий рівень безпеки, продуктивність та простоту налаштування. Його використання може значно підвищити ефективність та захищеність корпоративних і приватних мережевих середовищ. Завдяки своїм характеристикам він може стати стандартом VPN-рішень у майбутньому. Швидкість, безпека, гнучкість та простота налаштування роблять WireGuard перспективним вибором для багатьох компаній та індивідуальних користувачів.

Список використаних джерел:

1. Donenfeld J. WireGuard: Next Generation Kernel Network Tunnel. – 2020.
2. RFC 8999 – WireGuard Protocol Documentation. – IETF, 2021.
3. Офіційний сайт WireGuard – https://www.wireguard.com/
4. Linux Kernel Documentation: WireGuard – https://www.kernel.org/doc/html/latest/networking/wireguard.html

УДК 004.7

Стецюк М.В., PhD, ст. викладач
Заставна Я.В., здобувач
Тімош В.Л., здобувач
Хмельницький національний університет

СИСТЕМА ПОВЕДІНКОВОГО АНАЛІЗУ ДЛЯ ВИЯВЛЕННЯ ЗАГРОЗ В ІОТ-МЕРЕЖАХ

Інтернет речей (IoT) швидко змінює спосіб взаємодії людей із технікою, проте водночас стає вразливим до кіберзагроз, таких як DDoS-атаки, експлойти та брутфорс-атаки. Традиційні методи захисту, що базуються на статичних правилах, часто неефективні перед новими загрозами, тому ефективним рішенням є системи виявлення загроз на основі поведінкового аналізу. Вони здійснюють моніторинг активності пристроїв у реальному часі, дозволяючи виявляти аномалії, що можуть свідчити про атаку.[1]

Формування нормального профілю роботи пристроїв є важливим етапом у побудові ефективної системи поведінкового аналізу. Нормальний профіль визначає стандартні параметри функціонування IoT-пристрою та використовується для виявлення аномальних відхилень. Для кожного пристрою формується індивідуальний профіль, що включає його типову активність, середні значення мережевої взаємодії, рівень енергоспоживання, частоту обміну даними та інші показники. Це дозволяє системі адаптуватися до змін у роботі пристроїв без необхідності ручного налаштування для кожного окремого випадку.

Контролерна частина формує нормальний профіль підключеного пристрою, спостерігаючи за його роботою у звичайному режимі. Протягом певного періоду вона збирає дані та створює модель типової поведінки.[2] Ця модель включає такі параметри, як допустимий обсяг трафіку, інтенсивність запитів, рівень споживаної енергії та типові мережеві підключення. Після цього контролер починає порівнювати поточну активність пристрою з нормальним профілем. Якщо значення будь-якого показника виходить за встановлені межі, це вважається потенційною загрозою, і дані передаються на сервер для подальшого аналізу.

Серверна частина використовує отримані від контролера дані для перевірки аномалій і прийняття рішень щодо реагування. Сервер не лише перевіряє отримані показники на відповідність нормальному профілю, а й проводить аналіз за допомогою алгоритмів поведінкового моделювання.[4] Якщо аномалія підтверджується, сервер ініціює відповідні заходи безпеки, такі як генерація сповіщення, блокування підозрілого пристрою або оновлення політик контролера. Використання

серверних обчислень дозволяє швидко обробляти великі обсяги даних і виявляти складні загрози, які можуть залишатися непомітними на рівні окремих пристроїв.

Контролерна частина виконує первинний аналіз та передає підозрілі події на сервер. Її робота включає кілька основних етапів. Спочатку контролер здійснює збір параметрів пристрою, включаючи рівень енергоспоживання, мережеві підключення та структуру переданого трафіку. Далі отримані дані порівнюються з нормальним профілем пристрою. Якщо значення параметрів виходять за межі встановлених норм, система визначає рівень відхилень і оцінює, чи є вони критичними.[5] У разі виявлення підозрілої активності контролер передає відповідні дані на сервер для подальшого аналізу. Після завершення аналізу сервер надсилає оновлені політики безпеки, які контролер інтегрує у свою роботу. Це дозволяє забезпечити адаптивний захист та динамічне оновлення норм поведінки пристроїв. На рисунку 1 представлено алгоритм роботи контролерної частини

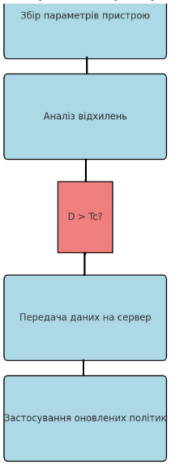


Рис. 1. Алгоритм роботи конролерної частини системи виявлення загроз

Серверна частина відповідає за глибший аналіз отриманих даних та прийняття рішень щодо можливих загроз. Після отримання інформації від контролера сервер застосовує алгоритми поведінкового аналізу для перевірки можливих аномалій. Якщо відхилення підтверджується, система генерує тривожний сигнал та ініціює заходи безпеки. Це може включати блокування пристрою, обмеження його мережевої активності або оновлення безпекових правил для всіх контролерів у системі.

Сервер також веде журнал загроз, що дозволяє проводити подальший аналіз атак та вдосконалювати алгоритми виявлення аномалій.

На рисунку 2 представлено блок-схему алгоритму роботи серверної частини.

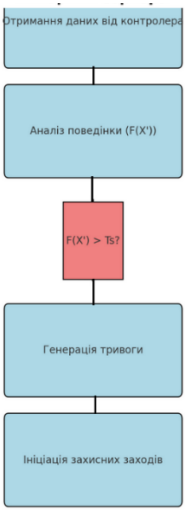


Рисунок 2 – Алгоритм роботи серверної частини системи виявлення загроз

Контролерна та серверна частини працюють у взаємодії через захищений канал зв’язку, що дозволяє здійснювати безперервний моніторинг і реагування на потенційні загрози. Контролери збирають дані та передають їх на сервер, який аналізує ситуацію і приймає рішення про необхідність втручання. Завдяки такій архітектурі система забезпечує виявлення та блокування загроз у режимі реального часу без необхідності попереднього знання про конкретний тип атак.

Список використаних джерел:

1. Булдаков О. В., Ковальов Г. П. Методи виявлення аномалій у трафіку IoT-пристроїв. *Комп’ютерні системи та мережі*. 2021. Т. 49, № 2. С. 112–121.

2. Anderson J., McCarthy B. Behavioral Analysis for IoT Security. *Journal of Cybersecurity Research*. 2020. Vol. 7, No. 1. P. 88–97.

3. Марченко Р. М., Коваленко А. А., Знайдюк В. Г. Аналіз методів виявлення аномального трафіку в мережах IoT. *Системи управління, навігації та зв'язку*. 2024. №1. С. 133–140.

4. IoT Analytics. State of IoT—Spring 2022. *IoT Analytics*. 2022. URL: https://iot-analytics.com/product/state-of-iot-spring-2022 (дата звернення: 10.03.2024).

УДК 004.056

Басістий В.П., аспірант,
Логош В.Д., магістрант
Західноукраїнський національний університет

АЛГОРИТМИ ГОМОМОРФНОГО ШИФРУВАННЯ

Алгоритми гомоморфного шифрування дозволяють виконувати обчислення над зашифрованими даними без їх розшифрування, отримуючи результат, який після розшифрування відповідає результату обчислень над відкритими даними. Ця технологія набуває дедалі більшої актуальності завдяки зростанню обсягів даних, потребі в конфіденційності та розвитку хмарних обчислень.

Алгоритм гомоморфного шифрування на основі "навчання з помилками" (Learning With Errors, LWE) є одним із широко досліджуваних підходів у сучасній криптографії, зокрема в контексті постквантової безпеки та гомоморфного шифрування. Він базується на математичній задачі, яка вважається стійкою навіть до атак квантових комп'ютерів.

LWE був запропонований Одедом Регевом у 2005 році і став основою для багатьох гомоморфних схем, включаючи частково гомоморфні (Partially Homomorphic Encryption, PHE) і повністю гомоморфні (Fully Homomorphic Encryption, FHE) системи [1, 2].

Основна ідея підходу "навчання з помилками" полягає в тому, щоб відрізнити випадкові лінійні рівняння від рівнянь, які мають невеликий "шум" (помилку), доданий до них. Ця складність використовується для створення криптосистем, які дозволяють шифрувати дані таким чином, що обчислення над ними (наприклад, додавання чи множення) можливі без розшифрування.

Алгоритми гомоморфного шифрування на основі LWE використовують математичні проблеми LWE для забезпечення безпеки і можливості виконання операцій над зашифрованими даними. Основні принципи роботи таких алгоритмів включають:

1) генерація ключів. Секретний ключ є випадковим вектором s. Відкритий ключ складається з множини пар (a, b), де $b = \langle a, s \rangle + e \bmod q$;

2) шифрування. Для шифрування повідомлення m, вибирається підмножина пар з відкритого ключа і комбінується їх з повідомленням. Результатом є зашифрований текст, який містить приховане повідомлення плюс невелику помилку;

3) розшифрування. Для розшифрування використовується секретний ключ для обчислення скалярного добутку, від якого потім віднімається

зашифрований текст, щоб отримати повідомлення плюс помилку. Якщо помилка достатньо мала, її можна видалити, щоб отримати оригінальне повідомлення;

4) гомоморфні операції. Алгебраїчна структура зашифрованого тексту дозволяє виконувати операції додавання та множення над зашифрованими даними, які перетворюються на відповідні операції над відкритими даними після розшифрування.

Математично, схеми гомоморфного шифрування на основі LWE зазвичай працюють над кільцями поліномів, що дозволяє ефективно представляти та маніпулювати зашифрованими даними. Популярний підхід полягає у використанні кільцевої версії LWE (Ring-LWE або RLWE), яка забезпечує кращу ефективність порівняно з оригінальною проблемою LWE.

Одним з ключових викликів у гомоморфному шифруванні є управління шумом. Кожна гомоморфна операція, особливо множення, збільшує рівень шуму у зашифрованому тексті. Якщо шум стає занадто великим, правильне розшифрування стає неможливим. На основі LWE розроблено ряд алгоритмів гомоморфного шифрування, зокрема [2]:

BGV (Brakerski-Gentry-Vaikuntanathan). Алгоритм підтримує довільну кількість додавань та обмежену кількість множень, з ефективними методами контролю шуму.

BFV (Brakerski/Fan-Vercauteren). Алгоритм оптимізований для ефективного множення, що широко використовується в практичних реалізаціях.

CKKS (Cheon-Kim-Kim-Song). Алгоритм призначений для обчислень з наближеними числами, що дозволяє ефективно виконувати обчислення з наближеними результатами.

GSW (Gentry-Sahai-Waters). Алгоритм використовує матричну версію LWE для досягнення компактності гомоморфного множення.

Базуючись на математичній проблемі LWE, алгоритми гомоморфного шифрування забезпечують безпеку навіть проти квантових обчислень.

Список використаних джерел:

1. Doan, T. V. T., Messai, M. L., Gavin, G., Darmont, J. A survey on implementations of homomorphic encryption schemes. The Journal of Supercomputing. 2023. Vol.79(13). P.15098-15139.

2. Mahato, G. K., Chakraborty, S. K. A comparative review on homomorphic encryption for cloud security. IETE Journal of Research. 2023. Vol. 69(8). P.5124-5133.

УДК 004.8

Сірик А. В., магістрант
Єфіменко А. А., к.т.н., доцент
Державний університет «Житомирська політехніка»

DEEPFAKE У ФІШИНГОВИХ АТАКАХ: АНАЛІЗ ЗАГРОЗ ТА ЗАСОБІВ ВИЯВЛЕННЯ

Сучасні технології штучного інтелекту суттєво змінюють ландшафт кібербезпеки, створюючи як нові можливості для захисту даних, так і загрози. Одним із найбільш небезпечних проявів цих загроз є використання deepfake – методів генерації підробленого аудіо, відео та зображень за допомогою нейронних мереж. Deepfake-технології, які спочатку розглядалися як інструменти для розваг та кіноіндустрії, сьогодні активно використовуються кіберзлочинцями у фішингових атаках для маніпуляції жертвами, обходу засобів автентифікації та компрометації корпоративних мереж.

Фішингові атаки, що використовують deepfake, можуть мати різні форми, зокрема:

– **Аудіофішинг** (voice phishing, vishing): Кіберзлочинці синтезують голос керівників компаній або знайомих осіб, щоб переконати жертву виконати певні дії, наприклад, здійснити грошовий переказ або передати конфіденційні дані.

– **Відеофішинг:** Використання підроблених відеозаписів, які створюють ілюзію реальної присутності людини. Такі відео можуть застосовуватися для обману співробітників або дискредитації осіб у суспільному та корпоративному середовищі.

– **Соціальна інженерія через фальшиві відеодзвінки:** Зловмисники можуть проводити відеоконференції, використовуючи deepfake, щоб видавати себе за керівників або працівників організацій та маніпулювати жертвами.

– **Компрометація особистих акаунтів:** Створення підроблених профілів у соціальних мережах із згенерованими зображеннями для отримання довіри та подальшого використання у шахрайських схемах.

Варто наголосити, що deepfake-фішинг становить значну загрозу, оскільки традиційні методи перевірки автентичності, такі як голосова ідентифікація чи відеозв'язок, стають ненадійними. Сучасні алгоритми deepfake дозволяють створювати надзвичайно реалістичні підробки, які важко відрізнити від справжніх навіть за допомогою професійних інструментів, що значно ускладнює їхнє виявлення. Окрім цього, автоматизація deepfake-застосувань сприяє розширенню масштабів атак, адже зловмисники швидко генерують великі обсяги

персоналізованого фішингового контенту, орієнтованого на конкретних осіб або організації. Такі атаки можуть мати далекосяжні наслідки не лише для корпоративної безпеки, а й для суспільства в цілому, оскільки deepfake активно використовуються у політичних маніпуляціях, дезінформаційних кампаніях та навіть у фінансових махінаціях, впливаючи на довіру до публічних осіб і ринків.

Ба більше, deepfake-фішинг є однією з найбільш витончених кіберзагроз, що вимагає комплексного підходу до виявлення та запобігання. Сучасні методи боротьби з такими атаками поєднують технологічні та організаційні заходи. Зокрема, ефективним способом є аналіз аномалій, коли алгоритми машинного навчання виявляють нестандартні рухи губ, невідповідність між звуком і відео, а також відхилення в тінях та освітленні. Важливу роль відіграє біометрична автентифікація, яка доповнює традиційні методи перевірки особи за допомогою аналізу мімічних мікровиразів обличчя та поведінкових особливостей голосу. Додатковий рівень безпеки забезпечують криптографічні методи перевірки контенту, що передбачають використання цифрових підписів для аудіо- та відеофайлів, дозволяючи підтвердити їхню автентичність. Не менш значущим є підвищення рівня обізнаності серед користувачів і співробітників компаній, що включає навчання методам розпізнавання deepfake-загроз і дотримання основних принципів інформаційної безпеки.

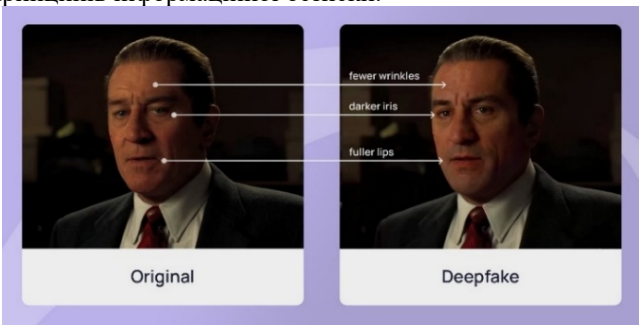


Рис 1. Порівняння оригінального зображення та deepfake

Таким чином, зосередимося на аналізі сучасних методів використання deepfake у фішингових атаках, їхній загрозі для інформаційної безпеки та ефективних способах протидії.

Список використаних джерел:

1. What is Deepfake Phishing: Deepfake Phishing Explained. - Keepnet. Keepnet Labs. URL: https://keepnetlabs.com/blog/what-is-deepfake-phishing.

2. Peters J. Deepfake phishing example: Protect your employees from deepfake scams. infosecinstitute. URL: https://www.infosecinstitute.com/resources/phishing/deepfake-phishing-example/.

УДК 004.02

Пирч О.В., асистент
Рак І.І., здобувач
Шемчук У.А., здобувач
Тітова В.Ю., к.т.н., доцент
Хмельницький національний університет

МЕТОД ПІДВИЩЕННЯ СТІЙКОСТІ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ ЗА РАХУНОК КОМБІНОВАНИХ СХЕМ АУТЕНТИФІКАЦІЇ

Електронний цифровий підпис (ЕЦП) є важливим інструментом забезпечення автентичності, цілісності та доступності електронних документів. Проте сучасні загрози у сфері кібербезпеки вимагають удосконалення методів захисту криптографічних ключів та підвищення надійності процесу аутентифікації користувачів [1].

У даному дослідженні запропоновано підхід до підвищення стійкості ЕЦП шляхом застосування комбінованих схем аутентифікації, зокрема контекстуальної аутентифікації у поєднанні із біометрією, та впровадження штучного інтелекту для порівняння біометричних даних користувачів.

Контекстуальна аутентифікація [2] передбачає аналіз факторів навколишнього середовища, зокрема місцезнаходження користувача, час входу у систему, поведінкові характеристики тощо. Додавання біометричної аутентифікації, яка включатиме у себе розпізнавання відбитків пальців, обличчя або голосу, в залежності від того що компанія вибере для своєї системи, забезпечує додатковий рівень захисту, ускладнюючи несанкціонований доступ до системи.

Для практичної реалізації методу підвищення стійкості ЕЦП був обраний програмний пакет на основі мови програмування Python із застосуванням криптографічної бібліотеки PyCryptodome.

Верифікація підпису виконується наступним чином (рис.1): після підписання документ може бути переданий іншій стороні для перевірки, тоді система використовує публічний ключ для верифікації підпису, при цьому використовуються додаткові перевірки на цілісність даних, що дозволяє виявити модифікацію даних після підписання.

Впровадження методу включало в себе тестування можливих векторів атак на криптографічні ключі та моделювання сценаріїв компрометації даних. Одним із запропонованих способів захисту є використання апаратних модулів безпеки (HSM) [3], які забезпечують ізольоване зберігання ключів, що в подальшому унеможливлює їх витік

навіть у разі компрометації серверного середовища на якому вони можуть зберігатися.

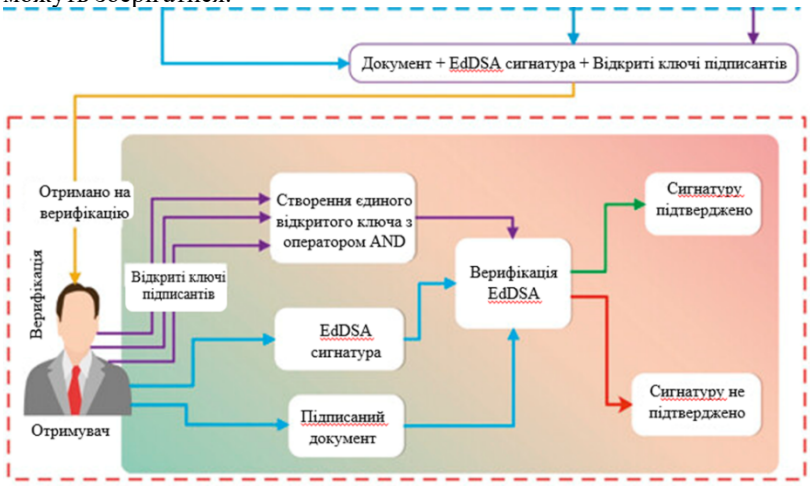


Рис.1. Процес перевірки ключів за даним методом

Відповідно запропонований метод підвищення стійкості ЕЦП складається з кількох важливих етапів: вибір нових криптографічних алгоритмів; інтеграція HSM для зберігання ключів; впровадження мультифакторної аутентифікації.

Практична цінність дослідження полягає у можливості впровадження запропонованого методу у корпоративних інформаційних системах, банківських установах та урядових структурах для підвищення рівня безпеки ЕЦП та аутентифікації користувачів. Запропонований підхід дозволяє зменшити ризики, пов'язані з компрометацією криптографічних ключів, що робить його ефективним рішенням у сфері інформаційної безпеки.

Список використаних джерел:

1. Albahadily, Hassan & Jabbar, Ismael & Altaay, Alaa & Ren, Xunhuan. (2023). Issuing Digital Signatures for Integrity and Authentication of Digital Documents. Al-Mustansiriyah Journal of Science. 34. 50-55. 10.23851/mjs.v34i3.1278.

2. Mahansaria, D., Roy, U.K. Contextual authentication of users and devices using machine learning. Computing 106, 4083–4107 (2024). https://doi.org/10.1007/s00607-024-01333-7.

3. Sommerhalder, M. (2023). Hardware Security Module. In: Mulder, V., Mermoud, A., Lenders, V., Tellenbach, B. (eds) Trends in Data Protection and Encryption Technologies . Springer, Cham. https://doi.org/10.1007/978-3-031-33386-6_16

УДК 004.75

Дмитрієв О.Г., магістрант
Державний університет «Житомирська політехніка»

ПОРІВНЯЛЬНИЙ АНАЛІЗ ЕФЕКТИВНОСТІ ОБЛАДНАННЯ MIKROTIK ТА CISCO У ЗАБЕЗПЕЧЕННІ БЕЗПЕКИ КОРПОРАТИВНИХ МЕРЕЖ

У сучасних умовах зростання кількості та складності кіберзагроз захист корпоративних мереж стає критичним завданням для будь-якої організації. Вибір обладнання для побудови мережевої інфраструктури впливає на рівень безпеки, продуктивності та загальні витрати на утримання мережі. Одними з найпоширеніших рішень у сфері мережевої безпеки є обладнання MikroTik та Cisco, які пропонують різні підходи до забезпечення захисту мереж. Ефективність використання цих рішень залежить від технічних можливостей, алгоритмів захисту та рівня стійкості до атак.

Метою дослідження є проведення порівняльного аналізу ефективності обладнання MikroTik та Cisco у забезпеченні безпеки корпоративних мереж. Дослідження охоплює аналіз алгоритмів захисту, продуктивності, масштабованості та вартості рішень MikroTik та Cisco у контексті забезпечення мережевої безпеки. Важливим аспектом є визначення переваг і недоліків кожного типу обладнання для формування оптимальної стратегії побудови захищеної мережі.

MikroTik забезпечує високу гнучкість і доступність для малого та середнього бізнесу. Невисока вартість, простота налаштування та широкий функціонал роблять це обладнання привабливим для використання у мережах невеликого масштабу. MikroTik пропонує вбудовані функції захисту, включаючи фільтрацію трафіку на рівні маршрутизації, міжмережеві екрани, захист від атак шляхом відключення невикористовуваних портів, а також шифрування трафіку за допомогою AES-256 [1]. VPN-рішення на базі MikroTik забезпечують безпечний віддалений доступ до мережі, що підвищує загальний рівень захисту. Однак, обладнання MikroTik має певні обмеження щодо масштабованості та продуктивності в умовах високого навантаження [2].

Cisco орієнтоване на забезпечення безпеки великих корпоративних мереж і надає більш складні та функціонально насичені рішення. Обладнання Cisco включає брандмауери нового покоління (NGFW) із глибокою інспекцією трафіку, VPN-рішення з використанням IPsec та SSL, інтеграцію з системами виявлення та запобігання атак (IDS/IPS), а також автоматизоване моніторинг трафіку з виявленням аномалій [3].

Високий рівень безпеки забезпечується за рахунок застосування складних алгоритмів шифрування та механізмів адаптивного реагування на інциденти безпеки. Основними перевагами Cisco є висока продуктивність, надійність і масштабованість, що робить це обладнання ідеальним для ядра мережі [4].

Інтеграція обладнання MikroTik та Cisco дозволяє створити ефективну багаторівневу систему захисту корпоративної мережі. MikroTik можна використовувати для управління доступом і фільтрації трафіку на периферійному рівні, тоді як Cisco ефективно забезпечує захист на рівні ядра мережі та обробку великого обсягу трафіку [5]. Такий підхід дозволяє оптимізувати витрати та досягти високого рівня безпеки за рахунок використання переваг обох платформ. Наприклад, використання MikroTik для побудови VPN-з'єднань і фільтрації трафіку в поєднанні з можливостями Cisco щодо централізованого управління безпекою забезпечує комплексний захист від зовнішніх і внутрішніх загроз [3].

У ході дослідження встановлено, що MikroTik забезпечує гнучкість, простоту налаштування та низьку вартість, що робить його ефективним рішенням для малих і середніх підприємств. Cisco надає більш складні та інноваційні рішення, орієнтовані на великі компанії з високими вимогами до безпеки та продуктивності [4]. Поєднання MikroTik і Cisco дозволяє створити масштабовану та захищену мережеву інфраструктуру, що відповідає вимогам сучасної кібербезпеки.

Висновки дослідження свідчать про те, що комбіноване використання обладнання MikroTik і Cisco дозволяє досягти оптимального балансу між гнучкістю, продуктивністю та рівнем безпеки. Рекомендується використовувати MikroTik для фільтрації трафіку та управління доступом на периферійному рівні, тоді як Cisco доцільно впроваджувати на рівні ядра мережі для забезпечення масштабованості та високого рівня захисту [5]. Такий підхід дозволяє створити ефективну та стійку до загроз корпоративну мережу з урахуванням особливостей функціонування обладнання MikroTik та Cisco.

Список використаних джерел:

1. MikroTik Wiki. Офіційна документація MikroTik. URL: https://wiki.mikrotik.com
2. Cisco. "Security solutions for small and medium businesses." Cisco.com, 2023. URL: https://www.cisco.com
3. Kent K., Souppaya M. NIST Special Publication 800-92, "Guide to Computer Security Log Management", 2006.
4. Ponemon Institute LLC. Exabeam SIEM Productivity Study, 2019.
5. Schneider M., Davies A., Ahlm E. Critical Capabilities for Security Information and Event Management, 2024.

УДК 004.056

Мариняк В.М., магістрант
Хмельницький національний університет

КІБЕРФІЗИЧНА СИСТЕМА ПАРКІНГУ

Кіберфізична система (КФС) - це багатовимірна складна система, яка інтегрує обчислення, зв'язок і фізичне середовище з важливими і широкими перспективами застосування [1]. Така система здатна здійснювати реальне спостереження, аналіз і вплив на фізичні процеси, часто через вбудовані датчики, виконавчі механізми та пристрої. КФС є основою для розвитку багатьох інноваційних технологій, від розумних будівель і транспортних систем до медичних пристроїв і промислових автоматизованих комплексів. Перспективи їхнього застосування значно зростають у різних сферах, таких як Інтернет речей (IoT), промислова автоматизація, охорона здоров'я, енергетика та транспорт, що дозволяє зробити ці технології надзвичайно важливими для забезпечення інтелектуальної взаємодії між машинами і людьми. Враховуючи складність і різноманітність компонентів таких систем, КФС потребують використання передових методів проектування, моделювання, аналізу та верифікації для досягнення високої надійності та ефективності в реальному часі.

Кіберфізичні системи дедалі більше проникають у повсякденне життя людини. Розвиток вбудованих контролерів, як основної складової КФС, повинен впоратися з впливом вбудованих контролерів, як основної складової КФС, а також із впливом постійного зростання складності, що спостерігається протягом останніх десятиліть. Стратегії розвитку на основі моделей, що підтримуються графічними формами та точною семантикою із інтерактивними інструментами, що дозволяють редагувати та компонувати моделі, проводити симуляції, верифікацію та автоматичну генерацію коду, можуть забезпечити високоефективний спосіб швидкого створення прототипів та надійної реалізації в різних галузях життєдіяльності людини.

Актуальність використання кіберфізичних систем (КФС), які іноді розглядаються як нове покоління мережевих вбудованих систем, значно зростає з точки зору видимості та важливості. До основних характеристик відноситься надійність, функціонування в надійний, безпечний і захищений спосіб, як стверджується в [2], яка визначає прогалини в дослідженнях та майбутні напрямки для різних фаз життєвого циклу системи життєвого циклу розробки.

В даному дослідженні показано практичну задачу, що включає реальний сценарій розгляду кіберфізичної системи із подальшим моделюванням її системи, включаючи усі виконавчі механізми.

Здійснено аналіз роботи контролера автостоянки, що включає в себе керування в'їзними та виїзними воротами, а також моніторинг місткості паркінгу. Найпростішою конфігурацією паркінгу є: один в'їзд та один виїзд, де на кожному в'їзді або виїзді встановлений датчик присутності на підлозі для виявлення прибуття автомобіля і кнопка, яку повинен активувати водій (щоб отримати талон на в'їзді, або вставити квиток (талон) після оплати на виїзді).

Доступність ресурсів також присутня, оскільки кількість вільних місць для паркування можна розглядати як ресурси, які на конкурентній основі розподіляються між користувачами, що приїжджають.

Однак, починаючи з цієї найпростішої конфігурації паркування, можна також припустити, що такий варіант буде не завжди і припустити різні умовні ускладнення, наприклад:

- наявність декількох в'їздів, де можуть виникати конфлікти, наприклад, коли кількість автомобілів, що намагаються в'їхати на парковку, перевищує кількість вільних місць на ній.
- включення декількох виїздів, а також декількох паркувальних зон або поверхів, враховуючи модульну структуру паркінгу (і там, де це можливо) структуру парковки.
- включаючи додаткові датчики на в'їздах і виїздах для покращення виявлення поведінки водія, наприклад, виїзд з в'їзду після спроби в'їзду і подальший рух заднім ходом.

Отже, можна розглядати як найпростіший випадок кіберфізичної системи паркування так і з точки зору згаданих ускладнень (сценаріїв), коли може бути прийнято кілька рівнів абстракції, починаючи від загального опису поведінки системи, до детального опису дій управління, що дозволяє безпосередньо пов'язати їх з активацією пропускних воріт чи шлагбауму.

Список використаних джерел:

1. L. Gomes, A. Costa, Model-driven development in hardware-software co-design of controllers for cyber-physical systems, in: ICELIE’2023 – 10th International Conference on E-Learning in Industrial Electronics; October 2023. P.16-19

2. R. Sinha, S. Patil, L. Gomes, V. Vyatkin, A survey of static formal methods for building dependable industrial automation systems, IEEE Transactions on Industrial Informatics 15. 2019. P. 3772–3783.

УДК 004.056

Мурсалов В. Р., здобувач
Головня О. С., к.пед.н., доцент
Державний університет «Житомирська політехніка»

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ В ДОДАТКАХ НА БАЗІ NODE.JS

Метою даного дослідження є аналіз основних методів та технологій забезпечення безпеки у додатках на базі Node.js.

Один із ключових принципів забезпечення безпеки в Node.js — регулярне оновлення як самого Node.js, так і залежностей проєкту [3]. Застарілі версії можуть містити відомі вразливості, тому використання команд на кшталт npm audit дозволяє оперативно виявити та виправити потенційні загрози. Крім того, слід уникати використання пакетів з низькою довірою або невідомими джерелами, що зменшує ризик шкідливого коду у вашому додатку.

Важливим аспектом є також правильне управління конфігурацією. Зберігати секрети, такі як API-ключі або паролі, у змінних середовища є обов'язковою практикою. Вони не повинні зберігатися у програмному коді або конфігураційних файлах, щоб уникнути їх витоку. Для додаткового рівня безпеки варто використовувати менеджери секретів або спеціалізовані інструменти на кшталт dotenv.

Обробка введених даних є ще одним критично важливим моментом. Node.js-додатки часто вразливі до атак типу SQL-ін'єкцій, XSS та командних ін'єкцій, тому слід завжди валідувати та санітизувати всі вхідні дані. Модулі на кшталт express-validator допомагають у забезпеченні цього захисту. [3]

Захист HTTP-заголовків також має велике значення. Бібліотека helmet дозволяє легко додати стандартний набір безпечних заголовків, що захищають від атак на основі маніпуляцій заголовками [1].

Обмеження рівня доступу є ще одним дієвим методом безпеки. Принцип найменших привілеїв повинен бути застосований як до додатка загалом, так і до окремих його частин. Наприклад, використання облікового запису з мінімальними правами для виконання Node.js-сервісу зменшує потенційний збиток у разі компрометації.

Регулярне логування і моніторинг подій у додатку дозволяють швидко виявляти спроби атак. Інструменти на кшталт winston чи morgan забезпечують ефективне ведення логів та допомагають у виявленні аномальних активностей.

Окрім того, використання механізмів захисту від DDoS-атак, таких як обмеження кількості запитів (rate limiting), захищає сервер від

перевантажень. Модулі на кшталт express-rate-limit є зручними засобами для цього.

Також варто подбати про безпеку сесій. У додатках на основі Express.js слід використовувати захищені кукі (secure cookies) з прапорцем HttpOnly, що унеможливлює доступ до них із JavaScript. [3]

Нарешті, слід регулярно тестувати додаток на наявність вразливостей за допомогою таких інструментів, як Snyk [3] або OWASP Dependency-Check [1], що дозволяють виявити та нейтралізувати потенційні загрози на ранніх стадіях розробки.

Дотримання цих рекомендацій дозволяє створювати надійні та захищені додатки на базі Node.js, мінімізуючи ризики як внутрішніх, так і зовнішніх атак.

У даній роботі було проаналізовано практики які дозволяють мінімізувати ризики та підвищити стійкість Node.js-додатків до атак. Регулярне оновлення залежностей, використання валідації введених даних, впровадження обмежень доступу, а також застосування інструментів моніторингу та тестування вразливостей є критично важливими заходами для безпечної роботи додатка. Комплексний підхід до безпеки допомагає захистити систему як від зовнішніх, так і від внутрішніх загроз.

Список використаних джерел:

1. Node.js Security Cheat Sheet - OWASP Cheat Sheet Series. (б. д.). OWASP Cheat Sheet Series. URL: https://cheatsheetseries.owasp.org/cheatsheets/Nodejs_Security_Cheat_Sheet.html (дата звернення: 21.03.2025).

2. Security Best Practices | Node.js. (б. д.). Node.js Documentation. URL: https://nodejs.org/en/learn/getting-started/security-best-practices (дата звернення: 21.03.2025).

3. Best Practice Security - Express. (б. д.). Express.js Documentation. URL: https://expressjs.com/en/advanced/best-practice-security.html (дата звернення: 21.03.2025).

УДК 004.056

Петренчук А.В., здобувач
Кулина С.В., к.т.н., доцент
Західноукраїнський національний університет

СИСТЕМИ АУТЕНТИФІКАЦІЇ НА ОСНОВІ БІОМЕТРИЧНИХ ДАНИХ

Системи аутентифікації на основі біометричних даних використовують унікальні фізіологічні та поведінкові характеристики, такі як відбитки пальців, риси обличчя або візерунки райдужної оболонки ока, для перевірки особи. Вони забезпечують вищий рівень безпеки порівняно з традиційними методами, як-от паролі, які легко втратити або викрасти. Аналізуючи унікальні маркери, такі системи дозволяють ефективно контролювати доступ у фінансовій, медичній та інших сферах, забезпечуючи надійність і зручність [1].

Сучасні системи аутентифікації – це комплекс технологій та методів, спрямованих на підтвердження особи користувача, який намагається отримати доступ до інформаційних ресурсів. Вони еволюціонували від простих паролів до складних біометричних систем, що враховують унікальні фізіологічні та поведінкові характеристики людини.

Основні типи сучасних систем аутентифікації:

• Парольна аутентифікація – найпоширеніший метод, але має ряд недоліків, таких як вразливість до зламу та необхідність запам'ятовувати складні паролі.

• Багатофакторна аутентифікація вимагає використання двох або більше факторів аутентифікації, що значно підвищує рівень безпеки.

• Біометрична аутентифікація використовує унікальні фізіологічні або поведінкові характеристики людини, такі як відбитки пальців, розпізнавання обличчя тощо.

• Аутентифікація на основі сертифікатів використовує цифрові сертифікати для підтвердження особи користувача.

• Аутентифікація на основі токенів використовує фізичні або програмні токени для генерації одноразових паролів.

Аналіз та порівняння існуючих біометричних систем є важливим етапом для розуміння їхніх можливостей, обмежень та сфери застосування.

Основні типи біометричних систем:

• Фізіологічні: відбитки пальців, розпізнавання обличчя, райдужна оболонка ока, геометрія руки.

• Поведінкові: розпізнавання голосу, динаміка підпису, натискання клавіш.

Критерії порівняння[2]:

• Точність – помилки хибного прийняття і хибного відхилення.
• Швидкість – час, необхідний для аутентифікації.
• Зручність – простота використання.
• Вартість – витрати на обладнання та впровадження.
• Безпека – стійкість до підробки.
• Прийнятність – сприйняття користувачами.

У таблиці 1 представлено порівняння існуючих типів біометричних систем за вище згаданими критеріями.

Таблиця 1

Порівняння існуючих типів біометричних систем

Характеристика	Відбитки пальців	Розпізнання обличчя	Райдужна оболонка ока	Розпізнання голосу
Точність	Висока	Середня	Висока	Середня
Швидкість	Висока	Висока	Висока	Середня
Зручність	Висока	Висока	Середня	Висока
Вартість	Низька	Середня	Висока	Низька
Безпека	Середня	Середня	Висока	Низька

Сучасні системи аутентифікації знаходяться на етапі трансформації, де традиційні методи поступово замінюються більш надійними та зручними рішеннями. Біометрична аутентифікація відіграє ключову роль у підвищенні рівня захисту, а багатофакторна біометрична аутентифікація є перспективним напрямком розвитку. Важливо враховувати етичні та юридичні аспекти використання біометричних даних, а також забезпечувати їхній захист від несанкціонованого доступу.

Список використаних джерел:

1. Tirfe D., Anand V.K. A Survey on Trends of Two-Factor Authentication. In: Sarma H.K.D., Balas V.E., Bhuyan B., Dutta N. (eds) Contemporary Issues in Communication, Cloud and Big Data Analytics. Lecture Notes in Networks and Systems, vol 281. Springer, Singapore, 2022.

2. Скорик Ю., Костромицький А., Копиця А. Порівняння видів біометричних пристроїв. Міжнародний науковий журнал інженерії та сільського господарства, 3 (5), 1–7, 2024.

УДК 004.7

Сініцина О.В., магістрантка
Бродський Ю.Б., к.т.н, доцент
Єфіменко А.А., к.т.н, доцент
Державний університет «Житомирська політехніка»

АНАЛІЗ НАЙПОШИРЕНІШИХ ЗАГРОЗ ДЛЯ LINUX-СИСТЕМ У 2024 РОЦІ

Операційна система Linux залишається однією з найбільш поширених платформ для серверів, хмарних інфраструктур і вбудованих систем завдяки її стабільності, безпеці та відкритому вихідному коду. Однак зростаюча популярність Linux-систем призводить до збільшення кількості кіберзагроз, спрямованих на їхню компрометацію.

Метою цього дослідження є аналіз найбільш поширених загроз для Linux-систем у 2024 році, а також вивчення ефективних методів їхньої нейтралізації. Дослідження базується на аналізі вразливостей, виявлених у 2024 році, та рекомендаціях з безпеки, спрямованих на мінімізацію ризиків для користувачів та організацій.

Згідно з дослідженням MITRE, проведеним на основі аналізу 31 770 CVE-записів, у 2024 році було виявлено критично важливі вразливості програмного забезпечення, які становлять загрозу безпеці Linux-систем. Найбільш небезпечними серед них стали помилки в архітектурі, програмному коді та механізмах реалізації. Особливу загрозу становлять вразливості нульового дня, кількість яких значно зросла порівняно з попередніми роками. Загальний збиток від хакерських атак у 2024 році досяг 2,3 мільярда доларів США, що на 40% більше, ніж у 2023 році.[1]

На основі аналізу вразливостей найбільш поширеними загрозами для Linux-систем стали:

1. **SQL Injection (CWE-89)** – виникає у випадку некоректної обробки введених користувачем даних, що дозволяє виконання довільних SQL-команд у базі даних. Це може призвести до несанкціонованого доступу, модифікації або видалення даних.
2. **Cross-Site Scripting – XSS (CWE-79)** – вразливість, що виникає через недостатню фільтрацію введених користувачем даних, що дозволяє виконання шкідливих скриптів у веб-браузерах інших користувачів. Наслідки включають компрометацію облікових записів та викрадення конфіденційної інформації.
3. **OS Command Injection (CWE-78)** – експлуатація неконтрольованого введення даних у командний інтерпретатор

операційної системи, що дозволяє виконувати довільні команди на сервері та призводить до повної компрометації системи.[2]

Окрім зазначених загроз, у 2024 році було виявлено численні вразливості з високим рейтингом CVSS, серед яких варто виокремити CVE-2024-42256 з рейтингом 9,8. Ця вразливість дозволяла несанкціонований віддалений доступ до системи через виконання довільного коду. Також значну небезпеку становили вразливості ядра Linux, які призводили до пошкодження пам’яті, збоїв у роботі системи та порушення її стабільності. Для мінімізації наслідків експлуатації таких вразливостей необхідно впроваджувати методи оновлення, які не потребують перезавантаження операційної системи.[3]

Для забезпечення належного рівня безпеки Linux-інфраструктури необхідно дотримуватись таких рекомендацій:

- Регулярне впровадження останніх патчів для ядра та програмного забезпечення дозволяє закрити відомі вразливості та зменшити ризик атак.
- Застосування технологій безперервного оновлення без перезавантаження мінімізує простої та підвищує рівень безпеки.
- Контроль доступу та моніторинг активності – багаторівнева аутентифікація, обмеження привілеїв користувачів та аналіз журналів доступу сприяють ранньому виявленню підозрілих дій.
- Проведення тренінгів щодо безпечних методів роботи з Linux-системами допомагає мінімізувати ризики, пов’язані з людським фактором.

Це дослідження дозволило визначити основні загрози для Linux-систем, серед яких SQL-ін’єкції, XSS-атаки, ін’єкції команд операційної системи, а також експлуатація вразливостей з високим рейтингом CVSS. Крім того, було розглянуто ефективні методи їхньої нейтралізації, включаючи регулярне оновлення програмного забезпечення, впровадження багаторівневої аутентифікації, моніторинг активності та навчання персоналу. Дотримання запропонованих рекомендацій сприятиме підвищенню безпеки Linux-інфраструктури та мінімізації кіберзагроз у майбутньому.

Список використаних джерел:

1. Дослідження MITRE. URL: https://www.bleepingcomputer.com/news/security/mitre-shares-2024s-top-25-most-dangerous-software-weaknesses/ (дата звернення: 21.03.2025).

2. Загальний перелік вразливостей (CWE). URL: https://cwe.mitre.org/ (дата звернення: 21.03.2025).

3. Перелік вразливостей NIST. URL: https://nvd.nist.gov/vuln (дата звернення: 21.03.2025).

УДК 004.056: 004.89

Лях І.М., магістрант

Державний університет «Житомирська політехніка»

СФЕРИ ЗАСТОСУВАННЯ OSINT У СУЧАСНИХ КІБЕРЗАГРОЗАХ

В епоху стрімкого розвитку цифрових технологій та зростання кіберзагроз важливу роль починає відігравати розвідка у відкритих джерелах (OSINT). Цей підхід дозволяє використовувати доступні інформаційні ресурси для моніторингу та аналізу загроз кібербезпеці як окремих осіб, так і великих корпорацій, державних установ або організацій.

Сучасний кіберпростір характеризується швидким зростанням обсягу даних і складністю кіберзагроз. У цьому контексті технології OSINT (розвідка у відкритих джерелах) стають важливим інструментом для виявлення, аналізу та протидії кіберзагрозам. OSINT дозволяє збирати та аналізувати дані з публічно доступних джерел, включаючи соціальні мережі, новинні ресурси, форуми, сайти організацій, що робить його ефективним засобом для моніторингу кіберризиків.

Основні сфери застосування OSINT в контексті завдань кібербезпеки включають :

1. **Моніторинг витоків даних**. OSINT дозволяє виявляти витоки конфіденційної інформації у відкритих джерелах, таких як форуми даркнету, соціальні мережі та онлайн-платформи обміну файлами. Наприклад, аналіз витоків даних, дозволяє здійснювати ідентифікацію осіб-зловмисників та військових злочинців.

Окремо слід зауважити, що OSINT-технології використовуються для так званого «doxing», коли без згоди особи, здійснюється збір персональної або конфіденційної інформації, з метою її подальшого несанкціонованого використання [1].

2. **Аналіз соціальної інженерії**. Використання OSINT допомагає досліджувати активність зловмисників у соціальних мережах та інших платформах для прогнозування можливих атак. Зокрема, аналіз активності допомагає передбачати потенційні атаки через методи соціальної інженерії, зокрема фішинг або шахрайські дії.

3. **Виявлення фішингових ресурсів**. Завдяки інструментам OSINT можливе автоматизоване виявлення шкідливих сайтів, які імітують легітимні ресурси, що забезпечує можливість блокування зловмисних ресурсів, ще до початку їх експлуатації та завдання шкоди користувачам.

Наразі спостерігається зростання кількості випадків, з використання тактики багатоетапного фішингу, яка заснована на

перенаправленні користувача від одного ресурсу до іншого, аби уникнути виявлення.

За таких умов, використання OSINT-технологій дозволяє прогнозувати атаки на ресурси, а також хдійснювати дослідження випадкві

4. **Кіберрозвідка щодо атакуючих груп**. Застосування OSINT дозволяє ідентифікувати активності та атрибуцію груп зловмисників шляхом збору відкритих даних про їх діяльність. Це дає змогу зрозуміти їхню тактику, методи та цілі, а також атрибутувати конкретні атаки до певних груп.

5. **Оцінка інформаційної безпеки компаній**. За допомогою OSINT можна визначати слабкі місця корпоративних ресурсів, які доступні через Інтернет. Це можуть бути неправильні налаштування серверів, незахищені API або витік технічної інформації.

6. **Протидія дезінформації та інформаційним операціям.** OSINT сприяє ідентифікації інформаційних кампаній, спрямованих на дискредитацію компаній або державних органів. Моніторинг інформаційних потоків дозволяє виявити та нейтралізувати фейки.

Враховуючи вищезазначене, можна виокремити наступні шляхи розвитку застосування OSINT-технологій в кібербезпеці, зокрема:

- Автоматизація процесів пошуку інформації у відкритих джерелах та використання штучного інтелекту;
- Розширене використання OSINT у військовій сфері;
- OSINT у боротьбі з фінансовими злочинами;
- Юридичні та етичні аспекти OSINT.

Таким чином, OSINT є важливим компонентом комплексної системи кіберзахисту, що дозволяє завчасно ідентифікувати та запобігати кіберзагрозам.

Список використаних джерел:

1. Івкова, В. і Опірський, І. 2024. Дослідження проблематики забезпечення безпеки персональних даних та конфіденційної інформації в контексті протидії OSINT. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*. 2, 26 (Груд 2024), 189–199. DOI:https://doi.org/10.28925/2663-4023.2024.26.682.

2. Брукс К. Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information. — 2020.

3. Коваленко О. А. Методи OSINT у задачах моніторингу кіберзагроз. Вісник кібербезпеки, 2022.

УДК 004.056.5

Басистий В. А., магістрант
Чешун О. В., здобувач
Чешун В. М., к.т.н., доцент
Хмельницький національний університет

ОРГАНІЗАЦІЯ КОМУТАЦІЙНИХ ПІДКЛЮЧЕНЬ МІКРОКОМП’ЮТЕРІВ В КОМЛЕКСІ МОНІТОРИНГУ І АНАЛІЗУ МЕРЕЖЕВОГО ТРАФІКУ ІОТ

Системи IoT відіграють все більшу роль в різних сферах життєдіяльності людини, але мають значний недолік – вразливість до кібератак [1]. Більшість пристроїв і систем IoT не здатні виконувати завдання захисту, зокрема, здійснювати моніторинг мережевого трафіку. Це пояснюється їхніми обмеженими ресурсами: низькою обчислювальною потужністю, невеликим обсягом пам’яті та обмеженою енергетичною ємністю. Через ці фактори встановлення засобів для постійного моніторингу та аналізу даних безпосередньо на IoT-пристроях стає неможливим.

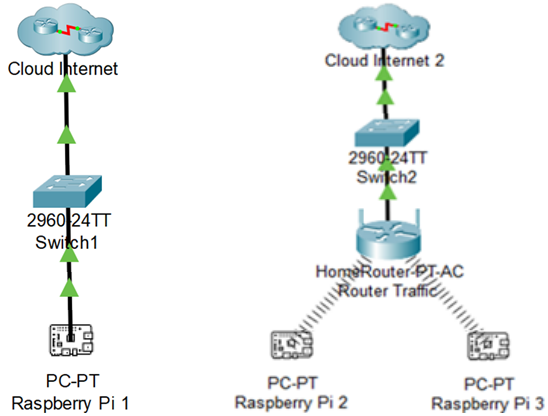
Внаслідок таких обмежень завдання з моніторингу часто передаються на централізовані сервери або хмарні платформи, які мають достатньо ресурсів для обробки великих обсягів даних [2]. Однак, безперервне передавання даних від великої кількості пристроїв до сервера може спричинити перевантаження мережі, а обробка даних на централізованих серверах може бути недостатньо швидкою для IoT-систем, які потребують миттєвої реакції на загрози.

В [3] авторами запропоноване рішення для створення комплексу моніторингу і аналізу мережевого трафіку IoT на одноплатних мікрокомп’ютерах.

Базовим елементом комплексу є мікрокомп’ютер Raspberry Pi (можлива реалізація на інших одноплатних мікрокомп’ютерах), на якому розгортається програма моніторингу. Для розробки програмної складової комплексу було обрано мову програмування Python з бібліотеками Psutil, Scapy, Pandas, що дає можливість отримувати детальну інформацію про активні процеси та підключені пристрої.

Сховищем інформації виступає сервер, який дозволяє користувачу збирати окремі пакети за стандартним протоколом від певного пристрою або від всіх одночасно. Аналіз проводиться на комп’ютері користувача без використання ресурсу основного пристрою.

Комплекс передбачає можливість підключень на основі кабельних з’єднань і через маршрутизатор з бездротовою точкою доступу (рис. 1).



а) б)

Рис. 1 – Організація комутаційних підключень в системі моніторингу: а) кабельне; б) з бездротовою точкою доступу

У випадку, коли немає можливості реалізувати безпровідне підключення, є можливість підключити IoT-пристрій через кабель (рис. 1.а). Використавши такий варіант підключення можна забезпечити надійний і стабільний зв'язок, який не обмежується перешкодами, але це робить підключення пристроїв обмеженим через кількість портів комутатора.

Бездротове підключення (рис. 1.б) вимагає використання маршрутизатора з функцією бездротової точки доступу для підключення до Інтернету. Цей варіант підключення надає можливість підключати велику кількість пристроїв, з високою швидкістю, тому воно є найкращим і обмежується тільки специфічним обладнанням і швидкістю передачі даних пристроїв.

Список використаних джерел:

1. Метод виявлення DDOS атак на IOT мережі / Нічепорук А.О. та ін. Вісник Хмельницького національного університету, Технічні науки. 2020. №1 (281). С.184-191.

2. Засоби моніторингу мережі в IoT інфраструктурі з гібридною архітектурою / Каплунов А. В., Гайдай А. Р., Гер В. М., Нікольський С. С. Телекомунікаційні та інформаційні технології. 2023. № 2(79). С.22-32.

3. Басистий В.А., Чешун О.В., Чешун В.М. Комлекс моніторингу і аналізу мережевого трафіку IOT на одноплатних мікрокомп'ютерах. Тези доповідей XXVII Всеукраїнської НПК «Могилянські читання – 2024», Технічні науки. С.103-108.

УДК 004.7

Годлевський О.О., здобувач
Фант М.О., к.філол.н., доцент
Державний університет «Житомирська політехніка»

БЕЗПЕЧНА АУТЕНТИФІКАЦІЯ ТА УПРАВЛІННЯ КОРИСТУВАЧАМИ У ВЕБДОДАТКАХ НА ОСНОВІ NEST.JS ТА NEXT.JS

У сьогоденному онлайн-світі важливо переконатися, що лише потрібні люди можуть отримати доступ до веб-сайтів. Щорічно кібер - ризики можуть спричинити порушення даних, несанкціоноване введення ресурсів або вразливості системи. Основна мета розробки сучасних веб -додатків - це не лише гарантування простоти для клієнтів, а й максимальна безпеки. Nest.js і Next.js дозволяє створювати безпечні системи з контролем доступу та управлінням ролями користувачів. Це дослідження аналізує стратегії аутентифікації, їхні переваги та недоліки, та рекомендує найкращу практику.

Існує декілька основних підходів до аутентифікації користувачів у веб-додатках, кожен із яких має свої особливості та сфери застосування. Перший спосіб JWT. Є одним із найбільш поширених методів аутентифікації. У цьому підході сервер генерує цифровий токен, який містить зашифровану інформацію про користувача. Токен може бути збережений у localStorage, sessionStorage або у HTTP-only cookie. Його переваги це безстейтова автентифікація (сервер не зберігає інформацію про сесію) та простота інтеграції з API. Також наявні і недоліки, а саме це, якщо access-token скомпрометовано, зловмисник отримує доступ до акаунту. Другий спосіб це використання NextAuth.js. Це бібліотека, що забезпечує інтеграцію OAuth. До переваг можна віднести легкість інтеграції з популярними постачальниками OAuth та гнучкості налаштування провайдерів. Щодо недоліків, то це менший контроль над внутрішньою логікою у порівнянні з власною реалізацією. І третій спосіб це за допомогою OAuth 2.0 та OpenID Connect. OAuth 2.0 – це протокол авторизації, який дозволяє користувачам входити через сторонні сервіси (Google, Facebook, GitHub тощо). OpenID Connect є розширенням OAuth 2.0 для ідентифікації користувачів. Головна перевага це додатковий рівень безпеки, оскільки пароль не передається додатку. Недоліки це залежність від сторінніх сервісів.

У роботі реалізовано систему аутентифікації на основі Nest.js для бекенду та Next.js для фронтенду з використанням наступних підходів:

- Реєстрація та аутентифікація користувачів реалізована через JWT з access та refresh-токенами; OAuth 2.0 використовується для входу через Google;
- База даних – Postgresql у поєднанні з Prisma для управління користувачами;
- HTTP-only cookies використанно для збереження токенів, щоб зменшити ризики XSS-атак.

Коли йдеться про автентифікацію користувачів та управління їхніми обліковими записами, то забезпечення безпеки є головним ключем до розробки веб-додатків. Можливі загрози, з якими можуть зіштовхнутися веб-додатки: несанкціонований доступ, витік персональних даних, DDoS-атаки та надмірне навантаження. Щоб запобігти цим загрозам, слід використовувати заходи безпеки, а саме: шифрування паролей, використання refresh-token для оновлення сесії, використання CAPTCHA для захисту від ботів та валідацію вхідних даних

Даний аналіз аутентифікації дозволяє забезпечити рівень безпеки завдки використанню JWT, bcrypt тощо. Гнучко масштабувати систему та додавати нові можливості. Надавати зручний інтерфейс користувачам через Next.js. Підтримувати вхід через Google, що спрощує аутентифікацію.

Можливі напрямки подальшого розвитку: додавання двофакторної автентифікації через SMS або TOTP. Інтеграція з GoogleFit для персоналізованого досвіду. Розширення логування для моніторингу активності користувачів.

Запропонована система є ефективним рішенням для сучасних веб-додатків, що потребують безпечної та масштабної автентифікації.

Список використаних джерел:

1. Nest.js Documentation: Introduction. Nest.js Documentation. URL: https://docs.nestjs.com (дата звернення: 21.03.2025).
2. Nest.js Documentation: Prisma. Nest.js Documentation. URL: https://docs.nestjs.com/recipes/prisma (дата звернення: 21.03.2025).
3. Next.js Documentation: Authentication. Next.js Documentation. URL: https://nextjs.org/docs/app/building-your-application/authentication (дата звернення: 21.03.2025).

УДК 004.89

Михайліченко О.В., аспірант
Національний університет «Полтавська політехніка ім. Юрія Кондратюка»

ЗАПОБІГАННЯ КІБЕРАТАКАМ ЗА ДОПОМОГОЮ НЕЙРОМЕРЕЖ

Сучасні телекомунікаційні мережі стикаються з дедалі витонченішими кібератаками, які можуть загрожувати як безпеці даних і конфіденційності користувачів, так і стабільності зв'язку. У світлі стрімкого зростання обсягів даних та швидкої еволюції новітніх технологій виникає гостра необхідність у впровадженні комплексних підходів до кібербезпеки. Згідно з даними Cybersecurity Ventures, до 2025 року глобальні економічні втрати від кіберзлочинів можуть досягти неймовірних $10,5 трлн на рік.

Одним із ключових інструментів у боротьбі з кіберзагрозами є нейронні мережі, здатні обробляти величезні обсяги інформації в реальному часі. Завдяки цій технології системи безпеки можуть ефективніше адаптуватися до нових типів атак, підвищуючи точність виявлення шкідливих дій. Особливо це важливо в умовах ускладнення атак, спрямованих на Інтернет речей (IoT) та хмарні платформи. [1]

З огляду на критичність кіберзагроз, лише у 2022 році середні витрати на ліквідацію наслідків витоку даних досягли 4,35 мільйона доларів, причому найбільша частка припала на DDoS-атаки. Ще однією небезпечною сферою використання шкідливих технологій штучного інтелекту є злам паролів або обхід двофакторної аутентифікації. [3]

Разом із цим існують численні успішні приклади використання нейронних мереж для захисту інформаційних систем - інтеграція в антивірусні програми. Завдяки впровадженню методів машинного навчання такі системи здатні виявляти не лише відомі шкідливі програми, а й зовсім нові загрози, які ще не внесені до відповідних баз даних. [1]

Для реалізації детекції кібератак у розподілених системах із застосуванням штучного інтелекту виконують аналіз різноманітних параметрів систем виявлення атак (IDS). До таких параметрів можуть належати характеристики пакетів даних, що включають заголовки, протоколи, методи кодування, тимчасові мітки передачі, інформацію про відправника та отримувача. Розглянуто запропоновану модель, яку автори визначають як багатоядерний алгоритм k-середніх із неповним ядром (MKKM-IC).

Ефективність запропонованого підходу була перевірена на трьох наборах даних: NSL-KDD, UNSW та AWID. Серед визначених загроз

виділяють DDoS-атаки, ін'єкції даних, несанкціоноване заволодіння адміністративним доступом та імітаційні дії. Результати експериментального порівняння точності (precision) виявлення кібератак показали, що найвищу ефективність продемонстрували моделі MKKM-IC і Змішана Модель Гаусса (GMM), досягнувши точності в діапазоні 71–88 %. У той же час найнижчі показники були зафіксовані для алгоритму пікових щільностей і k-середніх, які мали точність в межах 55–72 %. [2]

Для організацій, які бажають відповідати найвищим стандартам у сфері інформаційної безпеки у відношенні до нейромереж, стандарти ISO 27001 та ISO 27701 залишаються основними орієнтирами. [1]

Сучасні популярні інструменти для роботи з розподіленими системами включають вбудовані засоби для виявлення кібератак. Пропозиції таких компаній, як Oracle, AWS, Azure, DigitalOcean, Cisco та IBM, демонструють як подібність функцій, так і унікальні відмінності. Cisco зосереджується на мережевій безпеці, Oracle акцентує увагу на безпеці баз даних, тоді як IBM пропонує рішення, що базуються на аналізі та обробці даних із використанням штучного інтелекту. Azure та AWS пропонують широкий спектр різноманітних служб для покращення захищеності системи.

Аналізуючи існуючі рішеня від провідних компаній у сфері кібербезпеки, включаючи Cisco, Oracle, AWS, Azure та IBM. Зроблено висновок про важливість інтеграції методів штучного інтелекту для забезпечення адаптивного та проактивного захисту інформаційних систем.

Список використаних джерел:

1. Вплив нейронних мереж на розвиток кібербезпеки в умовах регуляторних змін. *THE INFLUENCE OF NEURAL NETWORKS ON THE DEVELOPMENT OF CYBER SECURITY IN THE CONDITIONS OF REGULATORY CHANGES*. 2024. Т. 30. С. 261–267. URL: https://doi.org/10.18372/2225-5036.30.19238.

2.ЧЕРЕВКО К. О. ШТУЧНИЙ ІНТЕЛЕКТ ЯК ІНСТРУМЕНТ ПРОТИДІЇ ЗЛОЧИННОСТІ. *Вісник Кримінологічної асоціації України*. 2023. Т. 28, № 1. С. 124–133. URL: https://doi.org/10.32631/vca.2023.1.10 .

3. Volokyta A., Melenchukov M. NEURAL NETWORKS IN DETECTING ATTACKS ON DISTRIBUTED SYSTEMS. *TECHNICAL SCIENCES AND TECHNOLOGIES*. 2024. No. 1(35). P. 135–145. URL: https://doi.org/10.25140/2411-5363-2024-1(35)-135-145.

УДК 004.7

Бобер Н.В., магістрантка
Воротніков В.В., д.т.н, професор
Державний університет «Житомирська політехніка»

АНАЛІЗ ВИКОРИСТАННЯ ChatGPT В СОЦІАЛЬНІЙ ІНЖЕНЕРІЇ: НОВІ ПІДХОДИ ДО КІБЕРЗАГРОЗ

У сучасному цифровому середовищі значення кібербезпеки різко зросло, ставши ключовим аспектом організаційної стратегії та національної безпеки. Ця ескалація насамперед пов'язана зі зростаючою залежністю від інформаційно-комунікаційних технологій у різних секторах.

Однією з найбільш значущих нових технологій, що впливають на кібербезпеку, є штучний інтелект (ШІ). Роль штучного інтелекту в кібербезпеці подвійна: він не тільки розширює можливості систем кібербезпеки, але й представляє нові вразливості, якими можуть скористатися кіберзлочинці.[1]

Ландшафт кібербезпеки, що розвивається, став свідком грізного супротивника у вигляді атак соціальної інженерії. Оскільки технології продовжують розвиватися, зловмисники соціальної інженерії все частіше використовують складні інструменти та методи, щоб обдурити своїх цілей. Одним з таких інструментів, який останніми роками привернув значну увагу, є генеративний штучний інтелект. [2]

ШІ відкриває нову еру в царині соціальної інженерії, надаючи суб'єктам загрози та кіберзлочинцям передові інструменти та тактики маніпулювання, обману та компроментації комп'ютерних систем. Ці технологічні досягнення відкривають зловмисникам кілька можливостей використовувати штучний інтелект для оркестрування атак соціальної інженерії.

В рамках дослідження розроблено: метод тестування здатності ChatGPT генерувати контент для атак соціальної інженерії; систему оцінки рівня довіри користувачів до згенерованих текстів; алгоритм аналізу лінгвістичних особливостей шкідливих повідомлень; методику перевірки вразливостей існуючих антифішингових систем перед контентом, створеним ШІ.

Запропонована система дослідження включає три основні компоненти:

- генерацію тестових даних, що створює різні типи шкідливих текстів (фішингові листи, маніпулятивні повідомлення, сценарії телефонного шахрайства);

- аналітичний модуль, що виконує лінгвістичний аналіз контенту, оцінюючи його маніпулятивні характеристики та схожість із реальними шахрайськими схемами;
- підсистему тестування безпеки, яка перевіряє ефективність антифішингових механізмів у виявленні контенту, створеного ChatGPT.

Попередні експерименти та теоретичний аналіз розробленої системи дослідження дозволяє прогнозувати високу ефективність її застосування для виявлення атак соціальної інженерії. Очікується, що система дослідження буде здатна:

- класифікувати згенеровані ChatGPT фішингові повідомлення;
- виявляти лінгвістичні патерни, характерні для маніпулятивних атак;
- аналізувати ефективність існуючих антифішингових систем та виявляти їх слабкі місця.

Для підтвердження ефективності запропонованого підходу планується проведення серії експериментів, у яких користувачам буде запропоновано оцінити достовірність згенерованих повідомлень [2], а також тестування зразків на сучасних антифішингових алгоритмах.

Попередні результати демонструють, що ChatGPT здатний генерувати контент, який може обійти деякі механізми захисту, що вказує на необхідність удосконалення методів кібербезпеки.

Практична цінність дослідження полягає у можливості вдосконалення існуючих антифішингових систем через врахування особливостей текстів, створених ШІ, дозволить підвищити рівень інформаційної безпеки та зменшити ризик атак соціальної інженерії.

Список використаних джерел:

1. Artificial Intelligence's Impact on Social Engineering Attacks. URL: https://opus.govst.edu/cgi/viewcontent.cgi?article=1521&context=capstones (дата звернення 24.02.2025)
2. Decoding the Threat Landscape : ChatGPT, FraudGPT, and WormGPT in Social Engineering Attacks. URL: https://www.researchgate.net/publication/374536568_Decoding_the_Threat_Landscape_ChatGPT_FraudGPT_and_WormGPT_in_Social_Engineering_Attacks (дата звернення 24.02.2025)
3. The Impact of Using ChatGPT on Cybersecurity & Social Engineering. URL: https://www.researchpublish.com/upload/book/The%20Impact%20of%20Using%20ChatGPT-16112023-4.pdf (дата звернення 24.02.2025)

УДК 004.056.5

Чернов С. В., здобувач
Жмурик І.М., здобувач
Чешун В. М., к.т.н., доцент
Хмельницький національний університет
Чешун Д. В., викладач
Хмельницький фаховий економіко-технологічний коледж

АРХІТЕКТУРА СИСТЕМИ ГЕНЕРАЦІЇ ЗАПИТІВ ДЛЯ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ ІНТЕРНЕТ-РЕСУРСІВ

Сучасні інформаційні технології відкривають широкі можливості для зберігання та передачі великих обсягів даних, однак разом із цим зростає загроза їхньої безпеки [1]. Вразливості в розподілених Інтернет-системах можуть призводити до витоків конфіденційної інформації, що створює ризики як для окремих користувачів, так і для організацій. Наслідки витоків даних можуть бути вкрай серйозними. Вони можуть включати фінансові втрати, реалізацію схем шахрайства, крадіжку особистих даних, репутаційні ризики для компаній та подальші юридичні санкції, а також викрадена інформація може бути використана для розгортання подальших атак або маніпуляцій [2].

Для зменшення ризиків витоків даних та експлуатації інших вразливостей в розподілених Інтернет-системах необхідно застосовувати багатоаспектні комплексні заходи безпеки [1].

Проведені дослідження присвячені генерації пошукових запитів для виявлення вразливостей або витоків даних Інтернет-ресурсів .

Запропонована система генерації пошукових запитів реалізована як сервісно-орієнтовна у поєднанні з архітектурою "Model View Controller". Сервіс-орієнтовна архітектура (SOA) дозволяє всім частинам системи, що представлені у виді незалежних сервісів, обмінюватись даними один з одним. Model View Controller (або ж MVC) є набором архітектурних принципів для побудови систем з інтерфейсом користувача, що в сумі ділиться на три основних складових: моделі – бізнес логіка програми; представлення – все що бачить користувач; контролер – займається обробкою дій користувача у взаємодії із системою.

Архітектура, що поєднує в собі сервісно-орієнтовний підхід та шаблон MVC, дозволяє ефективно розділити бізнес-логіку, шар представлення й механізми доступу до даних в задачах генерації пошукових запитів для виявлення вразливостей або витоків даних в інтернеті. Загалом, архітектуру використаних в системі технологій можна розділити на декілька шарів (рис. 1).

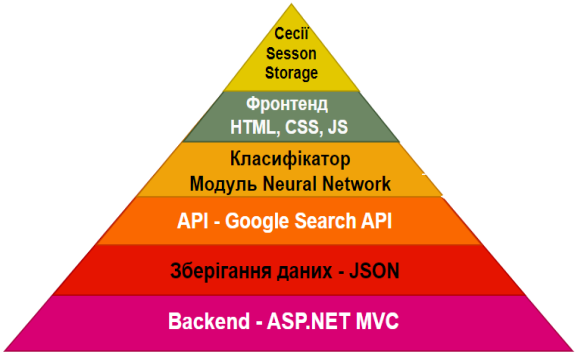


Рис. 1 – Набір технологій у вигляді архітектури

Основою розробленого додатку є сервіс “JsonDataService”, який виконує роль менеджера конфігурацій, відповідального за завантаження та обробку інформації з структурованих JSON-файлів, що містять конфігурацію модулів і операторів для запитів. Основна мета – забезпечення доступу до даних в JSON форматі, які зберігають в собі шаблони для генерації пошукових запитів. Сервіс дає можливість завантажувати шаблони пошукових запитів та їхні параметри. В коді сервіса зберігається шлях до JSON файлів, а також методи десеріалізації файлів з шаблонами для різних модулів та десеріалізації файлу з операторами пошуку. Такий підхід дозволяє легко додавати нові модулі та оператори без зміни основної логіки програми.

Сервіс “TagsService” управляє тегами, виконує аналітичну та категоризаційну функцію, дозволяючи витягувати унікальні теги, які прив’язані до конкретних модулів пошуку. Він допомагає класифікувати та фільтрувати пошукові запити, забезпечуючи швидкий доступ до ключових тегів, що характеризують певний модуль або групу запитів.

Ядро системи – сервіс “DorkGeneratorService”, який відповідає за генерацію пошукових запитів Google Dorks на основі заданих модулів, тегів чи параметрів. Він генерує пошукові запити, використовуючи шаблони та користувацькі параметри. Завдяки гнучкому підходу дозволяє формувати специфічні Dork-запити для пошуку інформації.

Список використаних джерел:

1. Захист критичних ресурсів веб-застосунку з оренди нерухомості / Корнієнко Богдан та ін. Інформаційні технології та суспільство. 2024. Випуск 4 (15). С.80-87.

2. Брижко В.М. Безпека інформаційної приватності: види та схеми шахрайства у сфері електронно-інформаційної взаємодії. Інформація і право. 2022. №3(42). С.65-79.

УДК 004.9

Козлов Д. О., магістрант
Бродський Ю. Б., к.т.н., доцент
Державний університет «Житомирська політехніка»

КОМП'ЮТЕРИЗОВАНА СИСТЕМА ПІДТРИМКИ ТА ПРИЙНЯТТЯ РІШЕНЬ ПРИ ВИНИКНЕННІ НАДЗВИЧАЙНИХ СИТУАЦІЙ

Сучасний розвиток технологій відбувається на тлі зростання кількості надзвичайних ситуацій (НС) природного та техногенного характеру. В умовах обмеженого часу для реагування на НС критично важливо приймати обґрунтовані управлінські рішення на основі повної та достовірної інформації про обстановку.

Традиційні підходи до оцінки ризиків і наслідків НС часто ґрунтуються на статистичних методах та імітаційному моделюванні, які є занадто обчислювально складними для застосування у режимі реального часу.

Налагоджена інформаційна взаємодія між службами екстреного реагування та використання комп'ютеризованих систем підтримки прийняття рішень (СППР) дозволяють суттєво зменшити затримки у зборі та обробці даних, мінімізувати людський фактор і підвищити ефективність заходів з ліквідації наслідків НС. Таким чином, розроблення комп'ютеризованої СППР для підтримки оперативного реагування є надзвичайно актуальним завданням, що спрямоване на збереження життя людей, зменшення матеріальних втрат та підвищення рівня безпеки в державі [1].

Метою роботи є розробка прототипу комп'ютеризованої системи підтримки та прийняття рішень при виникненні НС, що передбачає дослідження методів швидкого збирання, аналізу та інтерпретації даних про НС, а також алгоритмів оптимальних управлінських рішень. В процесі дослідження визначені принципи побудови СППР, які забезпечать інтеграцію різнорідних джерел інформації (сенсори, GIS, бази даних, прогностичні моделі) та підтримку роботи в реальному часі для потреб ситуаційних аналітичних центрів [2]. Структурно таку систему можна подати на рис.1.

Отже, об'єктом дослідження виступає процес прийняття рішень по виявленню, попередженню та ліквідації наслідків надзвичайних ситуацій та інформаційно-комунікаційні технології, що забезпечують його підтримку. Проаналізовані існуючі комп'ютеризовані системи та інтелектуальні технології, призначені для підготовки та прийняття рішень, що приймаються в умовах дефіциту часу та інформації.

Зокрема, проведений аналіз застосування геоінформаційних систем, систем моніторингу параметрів НС, моделей оцінки ризиків та збитків, експертних систем і штучного інтелекту для прогнозування розвитку ситуації, існуючі та перспективні підходи (наприклад, мультиагентні системи, технології великих даних, машинне навчання), що можуть бути інтегровані у СППР для НС.

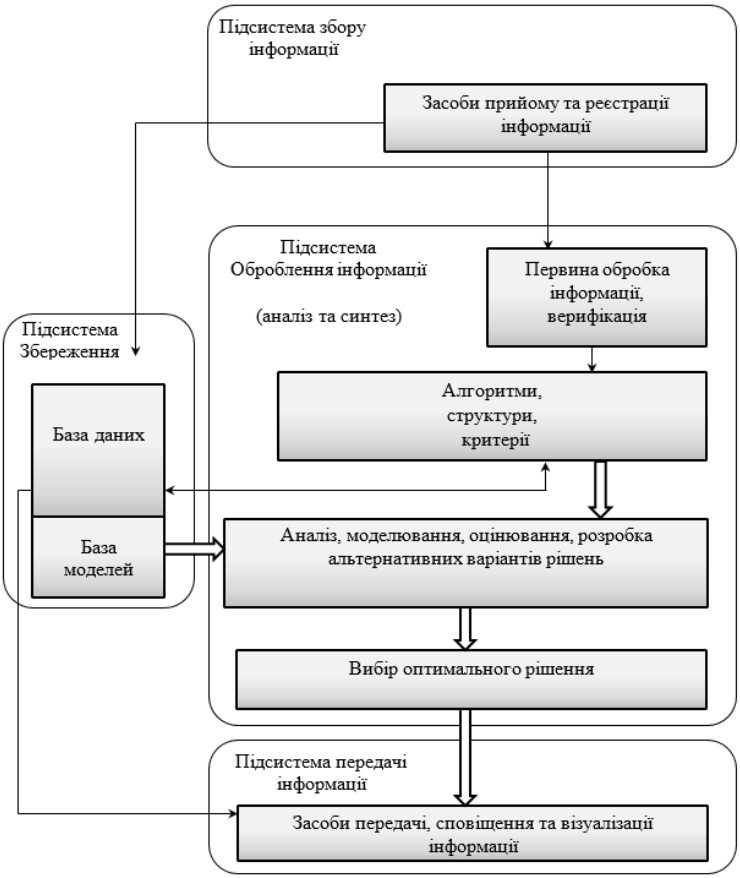


Рисунок 1. Система підтримки прийняття рішень

З світових аналітичних систем, призначених для підтримки прийняття рішень відома, наприклад, європейська комплексна система RODOS (Realtime Online Decision Support System), яка забезпечує підтримку рішень у реальному масштабі часу під час радіаційних аварій [3]. Дана система була впроваджена в Україні для раннього попередження та радіаційного моніторингу. Особливістю цієї системи є модульність та наявність підсистем аналізу і вибору рекомендованих рішень, стосовно виникнення надзвичайної радіаційної ситуації. У США федеральне агентство FEMA використовує програмний комплекс Hazus-MH для кількісної оцінки ризиків стихійних лих (повеней, ураганів, землетрусів тощо), що підтримує прийняття рішень на етапах планування, підготовки та реагування на виникнення НС [4]. Особливістю системи Hazus є стандартизовані моделі оцінювання втрат, інтегровані в ГІС, однак цей інструмент більше орієнтований на аналіз сценаріїв та планування, ніж на безпосереднє керування діями під час розвитку НС.

Аналіз відомих систем показав наявність вузької спеціалізації СППР, відсутність єдиних стандартів даних та інтерфейсів, а також необхідність залучення значних ресурсів, потрібних для їх впровадження та супроводження. Більшість існуючих СППР орієнтовані на окремі типи НС або потребують ручного внесення даних експертами, що може уповільнювати процес аналізу, оцінювання, моделювання та розробки альтернатив для оперативного прийняття ефективних рішень.

Таким чином, існує потреба в універсальній та гнучкій системі, здатній об'єднувати інформацію з різних джерел і формувати оптимальні рішення для різних видів надзвичайних ситуацій [5]. У ході виконання роботи запропоновано підхід до побудови СППР для надзвичайних ситуацій, який полягає в об'єднанні різнорідних даних про НС в єдиному інформаційному просторі та використанні інтелектуальних методів для генерування рекомендацій. Розроблено концептуальну модель системи, що включає підсистеми моніторингу (отримання даних від датчиків, повідомлень, моделей прогнозу погоди тощо), модуль ситуаційної оцінки на основі ГІС (візуалізація зони НС, розрахунок показників небезпеки), модуль експертного аналізу (правила та сценарії розвитку подій, база знань) та модуль підтримки рішення (алгоритми вибору оптимальних дій на основі критеріїв мінімізації втрат і часу реагування). Відмінністю запропонованого рішення є використання ризик-орієнтованого підходу: система в реальному часі оцінює потенційні ризики для населення і інфраструктури та ранжує альтернативні варіанти дій за ступенем

ефективності. Це дозволяє особам, що приймають рішення, зосередитися на критичних аспектах ситуації та отримати обґрунтовані поради щодо наступних кроків. У доповіді буде наведено результати розробки прототипу СППР. Впровадження такої системи, як складової Регіонального ситуаційного центру, метою якого є розробка концептуального підходу до НС через створення ефективного ситуаційного центру [6].

Крім того, будуть представлені перспективи подальшого дослідження щодо удосконалення прототипу системи, зокрема розширення бази знань, інтеграція з існуючими каналами зв’язку та проведення натурних випробувань. Отримані результати та запропоновані підходи можуть бути основою для створення інформаційно-комунікативної, комп’ютеризованої СППР, впровадження якої підвищить ефективність прийняття управлінських рішень при виникненні надзвичайних ситуацій.

Список використаних джерел:

1 Лахно В. А., Гусєв Б. С., Блозва А. І. та ін. Розробка системи підтримки прийняття рішень для аналізу надзвичайних ситуацій на міському транспорті // Кібербезпека: освіта, наука, техніка. – 2021. – №4(12). – С. 6–18.

2 Ноженкова Л. Ф., Ісаєв С. В., Нічепорчук В. В. та ін. Засоби побудови систем підтримки прийняття рішень з попередження і ліквідації НС // Проблеми безпеки та надзвичайних ситуацій. – 2008. – №4. – С. 46–55.

3 RODOS – Realtime Online Decision Support System for nuclear emergency management [Електронний ресурс]. – Режим доступу: http://www.rodos.fzk.de/ (дата звернення: 01.03.2025).

4 Federal Emergency Management Agency (FEMA) – Hazus Program [Електронний ресурс]. – Режим доступу: https://www.fema.gov/flood-maps/tools-resources/hazus (дата звернення: 01.03.2025).

5 Трофімова Н. В., Антамошкін О. О., Антамошкіна О. О., Нічепорчук В. В. Система підтримки прийняття рішень по реагуванню на надзвичайні ситуації і події на небезпечних виробничих об’єктах // Технології цивільної безпеки. – 2011. – №1. – С. 132–138

6 Бродський Ю. Б., Ковбасюк С. В. Концептуальний підхід до створення ситуаційного центру сталого розвитку регіону. Сучасні інформаційні технології у сфері безпеки та оборони. 2024. № 1 (49). С. 151–159. https://sit.nuou.org.ua/article/view/298451 .

УДК 004.7

Скалецький В.А., магістрант
Єфіменко А.А., к.т.н., доцент
Державний університет «Житомирська політехніка»

ЗАСТОСУВАННЯ НАВЧАННЯ З ПІДКРІПЛЕННЯМ У ТЕСТУВАННІ НА ПРОНИКНЕННЯ

Тестування на проникнення (або пентест) – це проактивний підхід до кібербезпеки, який імітує кібератаки, використовуючи спільні методи зі зловмисниками, що допомагає виявити вразливості до того, як вони будуть використані в реальних інцидентах. Інтеграція методів машинного навчання (ML) дозволяє автоматизувати рутинні процеси, покращує точність аналізу великих обсягів даних і швидкість реагування на нові загрози, в порівнянні з традиційними методами пентесту.

Відповідно до технік навчання, алгоритми ML розділять на кероване (supervised), некероване (unsupervised) і навчання з підкріпленням (reinforcement learning, RL). В контексті кібербезпеки, методи керованого і некерованого навчання частіше використовують для виявлення кіберінцидентів. Тоді як для тестування на проникнення обирають навчання з підкріпленням.

В RL пентестинг розглядається як задача послідовного прийняття рішень, середовище і завдання зазвичай моделюються як марковський процес вирішування (МПВ) або частково спостережуваний МПВ. В більш ранніх дослідженнях середовище моделювалося за допомогою графів атак або дерев рішень. А агент, взаємодіючи із середовищем, обирає дії для максимізації накопиченої винагороди.

Однією з ключових переваг навчання з підкріпленням є його здатність до самонавчання. Починаючи з мінімальних знань, агент вдосконалює свою стратегію протягом численних ітерацій, з часом набуваючи навичок і запам'ятовуючи найефективніші тактики. Такий підхід дозволяє динамічно адаптувати свою поведінку.

Агенти RL спроможні виявляти багатоетапні шляхи атаки, які можуть бути неочевидними при статичному аналізі. Такі інструменти, як DeepExploit, використовуючи глибоке навчання з підкріпленням, не лише виявляють вразливості, а й визначають найефективнішу послідовність атаки.

Основні переваги від інтеграції навчання з підкріпленням в процес пентесту:

- Адаптивність. Агенти RL здатні пристосовуватись до мінливого середовища, шляхом взаємодії з ціллю та оновленням своєї

стратегії на основі зворотного зв'язку (успіх або невдача атаки). Така гнучкість дозволяє конструювати вектори атак у більш реалістичний спосіб.

- Ефективність. Навчаючись на досвіді, агенти RL розробляють ефективні стратегії, які знаходять слабкі місця швидше ніж методи перебору. Такий підхід веде до більш дієвого виявлення вразливостей у великих, складних мережах.
- Економічна вигода. Автоматизація пентесту за допомогою RL може зменшити вартість і час операцій. На відміну від традиційних інструментів автоматизації, які часто тестують кожне корисне навантаження, агент глибокого навчання з підкріпленням здатен розумно визначати пріоритети ймовірних експлойтів.

Хоча тестування на проникнення на основі RL пропонує вагомі переваги, воно також має недоліки і обмеження:

- Високі обчислювальні вимоги. Агенту RL зазвичай потрібна велика кількість ітерацій проб і помилок, щоб вивчити ефективну стратегію, особливо в складних середовищах. У мережах з великою кількістю хостів, служб і можливих експлойтів, комбінація станів і дій зростає експоненційно, що значно збільшує час навчання. Таке навчання вимагає значних обчислювальних потужностей і часу.
- Етична та юридична невизначеність. Інструмент пентесту на основі RL в руках зловмисників може стати грізною зброєю. Тому розробка таких інструментів піднімає етичні питання. Також існує питання відповідальності. Автономна система тестування може не розпізнати ситуацію, коли потрібно зупинити атаку, яка може вивести з ладу цільову систему, тоді як людина експерт могла б проявити обережність.

Таким чином, впровадження методів навчання з підкріпленням у тестуванні на проникнення є цікавим та перспективним напрямком для досліджень. Вибір конкретного методу залежить від конкретної задачі, наявних даних та очікуваних результатів. Однак, для реалізації повного потенціалу потрібно вирішити відомі виклики та обмеження.

Список використаних джерел:

1. Ghanem M. C., Chen T. M. Reinforcement Learning for Efficient Network Penetration Testing. *Information*. 2020. Vol. 11, no. 1. P. 6. URL: https://doi.org/10.3390/info11010006.

2. Automated Vulnerability Exploitation Using Deep Reinforcement Learning / A. AlMajali et al. *Applied Sciences*. 2024. Vol. 14, no. 20. P. 9331. URL: https://doi.org/10.3390/app14209331.

УДК 004.7

Свіщо В.В., магістрант
Гнатчук Є.Г., д.т.н, доцент
Хмельницький національний університет

КІБЕРФІЗИЧНА СИСТЕМА СТЕЖЕННЯ ЗА СОНЦЕМ

Сучасні джерела енергії, зокрема сонячна енергетика, потребують систем стеження за положенням сонця для підвищення ефективності генерації енергії. Оптимальне налаштування сонячних панелей відповідно до руху сонця дозволяє максимізувати виробництво енергії протягом доби. Однак, існуючі методи й технології стеження за сонцем стикаються з низкою проблем, пов'язаних з точністю відстеження, енергоефективністю й надійністю систем у мінливих умовах зовнішнього середовища. Таким чином, розробка кіберфізичної системи, яка забезпечує надійне стеження за сонцем та адаптацію до змін погодних умов, є актуальною задачею [2].

Максимальна енергія виробляється сонячною фотоелектричною панеллю, коли вона розташована під прямим кутом до сонця. Одним із популярних типів трекерів є геліостат — рухоме дзеркало, яке спрямовує відбиток сонця на задану точку. Точність роботи сонячних трекерів залежить від сфери їхнього застосування. Для концентраторів, особливо тих, що використовуються у сонячних батареях, необхідна висока точність, аби зосереджене сонячне світло потрапляло безпосередньо на робочий елемент, який знаходиться близько до фокусної точки рефлектора або лінзи. Без відстеження система концентраторів не зможе функціонувати, тому навіть мінімальне одновісне відстеження є обов’язковим [3]. Вона включає датчик LDR (світлозалежний резистор) і двигун на постійному струмі. Arduino виступає головним елементом керування системою, яка слідкує за положенням сонця, забезпечуючи постійне перпендикулярне положення сонячної панелі до його променів і оптимізуючи, таким чином, потужність на виході [1].

LDR або світлозалежний резистор також відомий як фоторезистор, фотоелемент, фотопровідник. Це один з типів резисторів, опір якого змінюється залежно від кількості світла, що падає на його поверхню. Ці резистори часто використовуються в багатьох схемах, де потрібно перевірити присутність світла [4]. Наприклад, коли LDR знаходиться в темряві, його можна використовувати для ввімкнення світла або вимкнення світла. Типовий світлозалежний резистор має опір у темряві 1 МОм, а при світлі - кілька кілоом.

Структурна схема кіберфізичної системи стеження за сонцем представлена на рисунку 1.

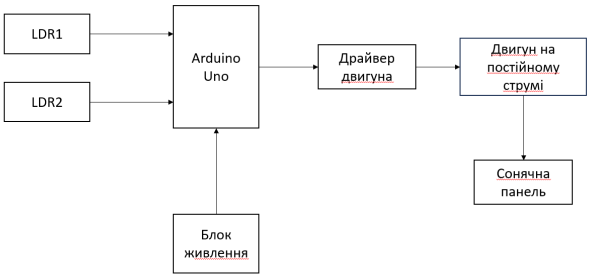


Рисунок 1 – Структурна схема кіберфізичної системи стеження за сонцем

Отже, представлена кіберфізична система стеження за положенням сонця, дозволяє автоматизувати процес стеження, оптимізуючи функціонування відповідного обладнання для максимальної енергоефективності та підвищення продуктивності в умовах змінного освітлення.

Список використаних джерел:

1. Embedded solar tracking system using arduino / Mouli Chandraa B et al. South Asian Journal of Engineering and Technology. 2022. Vol. 12, no. 2. P. 1–4. URL: https://doi.org/10.26524/sajet.2022.12.21 (date of access: 15.03.2025).

2. Design and Optimization of the Wall Climbing Robot for Magnetic Particle Detection of Ship Welds / X. Zhang et al. Journal of Marine Science and Engineering. 2024. Vol. 12, no. 4. P. 610. URL: https://doi.org/10.3390/jmse12040610 (date of access: 15.03.2025).

3. Singh A. K., Singh R. R. An Overview of Factors Influencing Solar Power Efficiency and Strategies for Enhancing. *2021 Innovations in Power and Advanced Computing Technologies (i-PACT)*, Kuala Lumpur, Malaysia, 27–29 November 2021. 2021. P. 3. URL: https://doi.org/10.1109/ipact52855.2021.9696845 (date of access: 15.03.2025).

4. Development of Smart (Light Dependent Resistor, LDR) Automatic Solar Tracker / I. A. Ayoade et al. *2022 5th Information Technology for Education and Development(ITED)*, Abuja, Nigeria, 1–3 November 2022. 2022. P.7.URL: https://doi.org/10.1109/ited56637.2022.10051239 (date of access: 15.03.2025).

УДК 004.7

Кльоц Ю.П., , к.т.н., доцент
Кукурудза Д.М., здобувач
Хмельницький національний університет

МЕТОДИ ВИЯВЛЕННЯ АТАК В КОМП'ЮТЕРНИХ МЕРЕЖАХ

Комп'ютерні мережі набули широкого розвитку паралельно з їх розвитком активно розвивається шкідливе програмне забезпечення та методи і засоби реалізації атак на та в комп'ютерних мережах. За методами атак також розвиваються і методи їх виявлення або недопущення.

Розвиток мереж та специфіка їх використання впливає і на особливості мережі. Серед відомих мереж можна виділити такі: корпоративні мережі, корпоративні мережі з BYOD, локальні мережі, публічні мережі з відкритим доступом.

Корпоративні мережі характеризуються високим рівнем контролю та управління, обмеженим доступом шляхом автентифікації та авторизації, використанням захищених сегментів VLAN, наявними засобами моніторингу та аналізу трафіку, політиками безпеки для користувачів та пристроїв, захистом від зовнішніх загроз (брандмауери, IDS/IPS), використанням централізованого управління (AD, SIEM, NAC).

Корпоративні мережі з BYOD характеризуються змішаним використання корпоративних та особистих пристроїв, динамічною IP-адресацією та ізоляцією пристроїв, використанням NAC для контролю доступу, високим ризиком зараження мережі через особисті пристрої, необхідністю обов'язкової сегментації та моніторингу трафіку, політиками безпеки на основі MDM, Zero Trust, контроль доступу, використанням VPN або контейнеризації даних.

Локальні мережі характеризуються висока швидкість передачі даних, відносно низьким рівнем безпеки, обмеженим будівлею або кампусом радіусом дії, центральним або децентралізованим контролем трафіку, використанням VLAN для поділу сегментів, основний фокус – продуктивність і стабільність.

Публічні мережі з відкритим доступом характеризуються відсутністю або мінімальним контролем доступу, високим ризиком атак (MITM, фішинг, підміна DNS), використанням загальних IP-адрес, відсутністю або слабким шифруванням трафіку, відкритим підключенням через Wi-Fi або Ethernet, високим рівнем анонімності користувачів, обмеженою пропускною здатність через велике навантаження.

Проведемо аналіз відомих методів та підходів до виявлення атак в комп'ютерних мережах.

Таблиця 1 Методи та підходи до виявлення атак в мережах.

Метод виявлення атак	Корпоративні мережі	Корпоративні з BYOD	Локальні мережі	Публічні мережі
Сигнатурний аналіз (IDS/IPS)	Добре	Середньо	Добре	Погано
Аналіз поведінки (UEBA)	Добре	Добре	Середньо	Погано
Моніторинг NetFlow/DPI	Добре	Добре	Добре	Погано
Моніторинг кінцевих пристроїв (EDR)	Добре	Добре	Середньо	Погано
Контроль доступу NAC	Добре	Добре	Середньо	Погано
Фільтрація DNS/блокування загроз	Добре	Добре	Добре	Добре
Аналіз логів (Syslog, SIEM)	Добре	Добре	Середньо	Погано
Виявлення DDoS-атак	Добре	Добре	Добре	Добре
Моніторинг Wi-Fi (WIPS/WIDS)	Середньо	Добре	Погано	Добре
Виявлення MITM-атак	Добре	Добре	Середньо	Добре

В комірках таблиці вказано наскільки ефективно використовувати розглянуті методи в різних типах мереж. Окрім цього при виборі методів виявлення атак необхідно враховувати вартість апаратного та програмного забезпечення, вимоги до мережевого обладнання, ресурсоємкість, скляність розгортання та підтримки системи.

Представлений в таблиці 1 аналіз методів вказує, що більшість з них орієнтовані на використання в корпоративних мережах. Сегменту локальних мереж приділена менша увага, оскільки здебільшого такі мережі є ізольованими від інтернету.

Методи виявлення атак зазвичай не орієнтовані на публічні мережі, оскільки вони будучи достатньо чисельним зазвичай не можуть використовувати дорогі програмно-апаратні комплекси та не мають можливості постійної підтримки та реакції на нові загрози.

Тому доцільним є розробка нових методів виявлення атак в публічних комп'ютерних мережах.

Список використаних джерел:

1. Scarfone, K., & Mell, P. Guide to Intrusion Detection and Prevention Systems (IDPS). NIST, 2007.

2. Chandola, V., Banerjee, A., & Kumar, V. Anomaly Detection: A Survey. ACM Computing Surveys, 2009.

УДК 004.7

Ставицький Я.О., магістрант
Гнатчук Є.Г., д.т.н, доцент
Хмельницький національний університет

КІБЕРФІЗИЧНА СИСТЕМА РОЗПІЗНАВАННЯ КВІТКОВИХ ВИДІВ РОСЛИН НА ОСНОВІ МЕТОДІВ ШТУЧНОГО ІНТЕЛЕКТУ

З розвитком сучасних технологій та зростанням інформатизації, проблема автоматичної класифікації та ідентифікації видів рослин стає все більш актуальною [3]. У сфері ботаніки та екології зростає потреба в ефективних інструментах для швидкого і точного розпізнавання квіткових видів.

Тому актуальним є створення кіберфізичної системи для класифікації квіткових видів, яка використовує штучний інтелект і методи комп'ютерного аналізу зображень[2]. Така система надає можливість візуалізації результатів, що дозволяє глибше аналізувати отримані дані з точністю вибраної моделі. Під час обробки і сортування великої кількості зображень штучний інтелект вивчає характеристики, такі як форма, колір та текстура [1].

На рисунку 1 представлено результати оцінки точності моделі машинного навчання, яка демонструє результати класифікації зображень квітів.

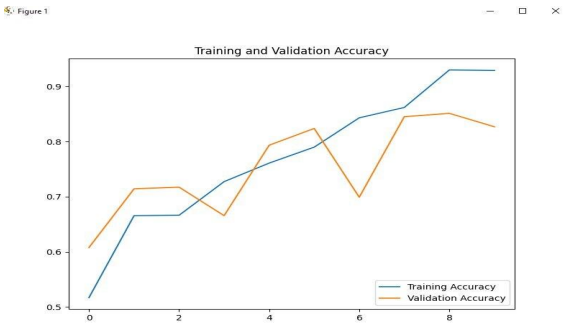


Рисунок 1 – Оцінка точності моделі машинного навчання

Був проведений ряд експериментів. Під час перших кроків, точність навчання зросла до 74%, що вказує на те, що модель успішно навчається на представлених даних. Водночас варіаційна точність досягла 79%, тобто змогла засвоїти знання на нових невідомих їй зображеннях. Це

свідчить про те, що модель не просто запам'ятовує дані, а дійсно розпізнає патерни, що є важливим для її ефективності визначення певних видів квіткових рослин.

Таким чином, модель показує результати, демонструючи потенціал для класифікації квітів на основі кількох відсортованих зображень. Це відкриває можливості для подальшого вдосконалення та покращення моделі. В подальшому вдосконалення можливе шляхом розширення набору даних та використання більш ефективної архітектури нейронних мереж. Одним із головних факторів є застосування оптимізації алгоритмів для мобільних пристроїв, що дозволить використовувати модель на практиці.

Отже, кіберфізична система на основі методів машинного навчання дозволяє ефективно класифікувати квіткові види з високою точністю. Використання бібліотек для обробки зображень значно підвищує продуктивність моделі. Отримані результати підтверджують ефективність підходу, на подальші дослідження. Система може бути спрямована на оптимізацію алгоритмів та розширення обсягу даних для покращення точності класифікації.

Список використаних джерел:

1. Lapkovskis, A., Nefedova, N., & Beikmohammadi, A. (2024). Automatic Fused Multimodal Deep Learning for Plant Identification. *arXiv preprint arXiv:2406.01455*. P.5-6. URL: https://arxiv.org/abs/2406.01455 date of access: 15.03.2025.Dosovitskiy A., Beyer L., Kolesnikov A. An Image Is Worth 16x16 Words: Transformers for Image Recognition at Scale. 2020.

2. Yao, J., Tran, S. N., Garg, S., & Sawyer, S. (2023). Deep Learning for Plant Identification and Disease Classification from Leaf Images: Multi-prediction Approaches. *arXiv preprint arXiv:2310.16273*. P.6-7. URL: https://arxiv.org/abs/2310.16273 (date of access: 15.03.2025).

3. Abdallah, H. B., Henry, C. J., & Ramanna, S. (2022). Plant Species Recognition with Optimized 3D Polynomial Neural Networks and Variably Overlapping Time-Coherent Sliding Window. *arXiv preprint arXiv:2203.02611*. P.25-26. URL: https://arxiv.org/abs/2203.02611 (date of access: 15.03.2025).

4. Beikmohammadi, A., Faez, K., & Motallebi, A. (2020). SWP-LeafNET: A novel multistage approach for plant leaf identification based on deep CNN. *arXivpreprintarXiv:2009.05139*.P.6.URL:https://arxiv.org/abs/2009.05139 (date of access: 15.03.2025).

УДК 004.5

Редчиць А.О. здобувач
Шелуха О.О. к.т.н. доцент
Державний університет «Житомирська політехніка»

ДОСЛІДЖЕННЯ НАПРЯМКІВ ЗАСТОСУВАННЯ AR ТА VR

У сучасному світі, коли стрімко розвиваються технології, мобільні мережі п’ятого покоління (5G), доповнена реальність (AR) та віртуальна реальність (VR) перетворюються на ключові інструменти, що змінюють наше повсякденне життя, роботу та розваги. Розвиток цих технологій відкриває нові можливості для трансформації різних сфер, таких як комунікації, освіта, медицина тощо. Завдяки швидкості та стабільності 5G, а також занурювальним можливостям AR і VR, виникають зміни, що роблять повсякденне життя зручнішим, ефективнішим та цікавішим. Розглянемо потенціал цих технологій, їхній вплив на сучасний світ і конкретні приклади їхнього застосування в різних галузях. П'яте покоління мобільних мереж, є значним кроком уперед у порівнянні з 4G, пропонуючи вищі швидкості, нижчу затримку та здатність підключати мільйони пристроїв на квадратний кілометр. Конкретні зміни життєдіяльності включають:

- Охорону здоров'я: 5G дозволяє проводити віддалені операції за допомогою роботів, забезпечуючи низьку затримку для реального часу, і покращує моніторинг пацієнтів через IoT-пристрої.

- Розумні міста: Технологія допомагає оптимізувати використання енергії, наприклад, через розумні лічильники, як у Empire State Building, де витрати на енергію зменшилися на 38%.

- Виробництво: 5G підтримує автоматизацію, дозволяючи реальний моніторинг виробничих ліній, що покращує ефективність.

- Користувацький досвід: 5G покращує AR і VR, наприклад, у геймінгу, забезпечуючи більш плавну взаємодію завдяки вищій пропускній здатності.

Ці зміни свідчать про те, що 5G не лише пришвидшує з'єднання, але й створює нові бізнес-моделі, такі як послуги доставки їжі чи спільного використання автомобілів, які з'явилися з 4G.

Щодо використання AR і VR, то ці технології вже інтегровані в численні сектори, надаючи інтерактивний та занурювальний досвід. Також ці технології не лише підвищують ефективність, але й створюють нові можливості для взаємодії з клієнтами та працівниками. Розглянемо потенціал VR і AR для освіти, розваг і медицини.

VR і AR мають великий потенціал для трансформації навчання. Дослідження показують, що навчання з використанням VR і AR перевищує традиційні методи на 50% за результатами. Конкретні

застосування включають: віртуальні екскурсії, наприклад, відвідування музеїв чи історичних місць, що робить освіту доступною для учнів, які не можуть подорожувати; симуляції наукових експериментів, що допомагає краще зрозуміти складні концепції; персоналізовані навчальні шляхи, особливо для учнів із особливими потребами, через інтерактивні платформи.

У сфері розваг VR і AR створюють нові форми взаємодії з контентом. VR забезпечує ігри, як "Beat Saber" чи "Half-Life: Alyx", де гравці повністю занурюються у віртуальний світ. AR, наприклад, у "Pokémon Go", додає цифрові елементи до реального світу, заохочуючи фізичну активність. До інших застосувань можна включити: віртуальні концерти, де користувачі можуть "бути" на шоу, навіть перебуваючи вдома; кінотеатри з AR, де глядачі можуть обирати ракурси чи взаємодіяти з персонажами, як у інтерактивних шоу; музеї з VR-галереями, як у ArtScience Museum у Сінгапурі, де відвідувачі досліджують мистецтво через VR-окуляри. Ці технології роблять розваги більш персоналізованими та доступними, але їх застосування викликає занепокоєння щодо залежності від екранів.

У медицині VR і AR теж змінюють підхід до лікування та навчання. За даними FDA, станом на 2024 рік було схвалено 69 медичних пристроїв із AR/VR. Конкретні застосування включають: симуляції операцій, де VR дозволяє хірургам тренуватися в безпечному середовищі, наприклад, для нейрохірургії, як у платформі Surgical Theater, реабілітацію, де VR використовується для фізичної терапії, наприклад, для пацієнтів після інсульту, покращуючи рухові навички, та лікування психічних розладів: VR застосовується для експозиційної терапії фобій і тривожності, створюючи контрольовані сценарії. Щодо AR, то, наприклад, під час операцій доповнена реальність надає 3D-візуалізацію анатомії, як у платформі SentiAR, що допомагає хірургам бачити органи в реальному часі під час процедур.

Отже, завдяки 5G, AR і VR стають важливими технологіями, які додають інтерактивність та розширюють можливості користувачів у багатьох галузях, від медицини до розваг. Їхній потенціал у освіті, розвагах і медицині обіцяє зробити ці сфери більш доступними, ефективними та персоналізованими.

Список використаних джерел:

1. The Impact of 5G: Creating New Value across Industries and Society URL: https://www.pwc.com/gx/en/about/contribution-to-debate/world-economic-forum/the-impact-of-5g.html

2. Augmented and Virtual Reality: The Future of Learning Experiences URL: https://virtualspeech.com/blog/augmented-virtual-reality-future-of-learning-experience

УДК 004.5

Примак В.В., здобувач
Шелуха О.О., к.т.н., доцент
Державний університет «Житомирська політехніка»

АНАЛІЗ ТЕХНОЛОГІЙ ВІДЕОСПОСТЕРЕЖЕННЯ ТА УПРАВЛІННЯ ДОСТУПОМ

В умовах зростаючих загроз кібербезпеки та необхідності захисту фізичних об'єктів, системи відеоспостереження та контролю і управління доступом (СКУД) стають важливими елементами комплексної безпеки підприємств, установ та критично важливої інфраструктури. Сучасні технологічні рішення дозволяють не тільки контролювати доступ у реальному часі, а й аналізувати поведінку користувачів, виявляти аномалії та запобігати загрозам безпеці.

Традиційні системи відеоспостереження та СКУД часто функціонують автономно, що обмежує їх ефективність та гнучкість. Їх модернізація передбачає інтеграцію з IoT-рішеннями, хмарними технологіями та штучним інтелектом (AI), що дозволяє реалізувати адаптивні механізми контролю доступу, автоматизований аналіз відеопотоків та централізоване управління безпекою. Розвиток цих технологій спрямований на розробку та впровадження сучасних методів забезпечення безпеки за допомогою відеоспостереження та систем контролю доступу, що базуються на концепції Індустріального Інтернету речей. Аналогові та цифрові системи відеоспостереження, а також IP-камери мають свої переваги та недоліки (табл.1), що визначає їхню ефективність залежно від сфери застосування.

Таблиця 1. Переваги та недоліки технологій відеоспостереження

Види систем	Переваги	Недоліки
Аналогові камери	- Низька вартість - Мінімальні вимоги до пропускної здатності мережі - Стабільна робота без затримок	- Обмежена роздільна здатність - Відсутність можливостей аналітики та інтеграції з AI - Складність масштабування
Цифрові камери	- Висока якість зображення - Сумісність із застарілими аналоговими системами - Легкість встановлення та налаштування	- Відсутність гнучких мережевих функцій - Обмежена можливість аналітики та інтеграції з хмарними сервісами - Потребує відеореєстратора для збереження записів
IP-камери	- Висока якість зображення - Інтелектуальні функції - Підтримка зберігання в хмарі та інтеграція з AI	- Вища вартість - Потребує якісної мережевої інфраструктури

	- Можливість віддаленого доступу через інтернет	- Можливі затримки через перевантаження мережі

Системи контролю доступу включають карткові зчитувачі, які працюють на основі RFID або MIFARE-технологій, біометричні системи, що використовують відбитки пальців, розпізнавання обличчя або вен, а також кодові панелі для автентифікації через введення PIN-коду. Інтеграція з відеоспостереженням дозволяє автоматично записувати відео кожної події доступу, контролювати переміщення людей та швидко реагувати на потенційні загрози. Розглянемо також переваги та недоліки систем контролю та управління доступом (табл.2), що визначає їхню ефективність залежно від сфери застосування.

Таблиця 2 Переваги та недоліки СКУД

Типи систем	Переваги	Недоліки
Карткові	Швидкість і зручність Низька вартість карток Можливість налаштування рівнів доступу	Картки можна втратити або скопіювати Не забезпечує верифікацію особи власника картки
Біометричні	Висока точність ідентифікації Неможливість підробки Не потребує носіння фізичних карток	Вища вартість впровадження Можливі помилки в розпізнаванні через зміну зовнішнього вигляду або пошкодження шкіри
Кодові панелі	Простота реалізації Не потребує носіння фізичних носіїв	Можливість передачі пароля третім особам Складність запам'ятовування паролів у великих організаціях

При інтеграції СКУД із відеонаглядом можна реалізувати такі функції, як: автоматичне фотографування користувача під час входу, розпізнавання обличчя для верифікації особи, фіксація спроб несанкціонованого доступу, підключення до систем безпеки для миттєвого блокування доступу в разі загрози

Також слід приділяти увагу інтеграції СКУД з системою відеоспостереження на базі контролерів доступу (HID, ZKTeco, Bosch, Axis та інші), зчитувачів (HID Global, Dahua, Bosch Security та інші) IP-відеокамер (Hikvision, Dahua та інші), відеореєстраторів (Hikvision, Dahua та інші).

Список використаних джерел:

1. Відеоспостереження. URL: https://rci-c.com/technology/videosposterezhennya/

2. Контроль доступу. URL: https://rci-c.com/technology/kontrol-i-upravlinnya-dostupom/

3. ACS 101: Understanding the Basics of Access Control Systems | 3Sixty Integrated. URL: https://www.3sixtyintegrated.com/blog/2024/01/03/access-control-systems/

УДК 004.45

Сімашко І.Б., здобувач,
Шелуха О.О., к.т.н. доцент
Державний університет «Житомирська політехніка»

SCADA-СИСТЕМИ: ПРИЗНАЧЕННЯ, ПРОБЛЕМИ ТА ЗАСТОСУВАННЯ НА ПРОМИСЛОВИХ ВИРОБНИЦТВАХ

Сучасне промислове виробництво потребує ефективного контролю та автоматизації технологічних процесів. Підприємства постають перед такими викликами, як необхідність постійного моніторингу виробничих ліній, оптимізація витрат на ресурси та зменшення впливу людського фактору в управлінні складними системами. Для вирішення цих проблем використовуються системи диспетчерського керування та збору даних (Supervisory Control and Data Acquisition, SCADA), що дозволяють в режимі реального часу отримувати інформацію про стан технологічних процесів, аналізувати її та приймати відповідні рішення. SCADA-системи являють собою програмно-апаратні комплекси, що забезпечують централізований моніторинг та управління виробничими процесами, основним принципом роботи якого є збір даних з датчиків та контролерів, їх передача через комунікаційні протоколи, аналіз отриманої інформації та керування обладнанням на основі зібраних даних.

Для реалізації такого управління SCADA-системи використовують широкий спектр промислових датчиків, які вимірюють параметри, такі як температура, тиск, рівень рідин, швидкість руху механізмів тощо. Отримані дані передаються до програмно-апаратних контролерів (наприклад, PLC – програмованих логічних контролерів), які здійснюють попередню обробку інформації та відправляють її до центральної SCADA-системи. Передача даних може здійснюватися за допомогою різних комунікаційних протоколів, серед яких одним із найбільш популярних є Profinet. Згідно з офіційною документацією "Siemens" [1], це високошвидкісний мережевий протокол, що дозволяє обмінюватися інформацією між контролерами та SCADA-системою в реальному часі з мінімальними затримками.

Використання SCADA-систем дозволяє підприємствам вирішувати низку важливих завдань: автоматизація виробничих процесів для зменшення необхідності у ручному управлінні; постійний моніторинг усіх виробничих параметрів, для швидкого реагування на відхилення від нормальних умов роботи обладнання та запобігання аваріям чи простою виробничих ліній; аналіз історичних даних для оптимізації споживання ресурсів та підвищення загальної продуктивності підприємства.

Однією з найважливіших проблем сучасних SCADA-систем є їхня

вразливість до кібератак. Промислові об'єкти, які використовують SCADA, часто стають ціллю для хакерів, оскільки їхня робота критично важлива для функціонування підприємства. Для запобігання кібератак на SCADA-системи використовуються різні механізми захисту.

По-перше, передача даних між датчиками, контролерами та центральною SCADA-системою шифрується за допомогою криптографічних протоколів (TLS/SSL або IPSec), щоб унеможливити їхнє перехоплення та модифікацію зловмисниками. По-друге, SCADA-системи забезпечують строгий контроль доступу до критичних функцій системи. Використовуються багаторівневі системи автентифікації, включаючи створення відповідних користувачів та паролі. По-третє, постійний моніторинг мережевої активності дозволяє виявляти підозрілі дії, такі як незвичайні спроби доступу або передачі даних, що може свідчити про кібератаку. Крім того, регулярне оновлення програмного забезпечення SCADA-системи та її компонентів допомагає закривати вразливості, які можуть бути використані зловмисниками. Нарешті, у разі успішної кібератаки важливо мати можливість швидкого відновлення системи. Тому SCADA-системи зазвичай включають механізми резервного копіювання даних та конфігурацій, що дозволяє відновити роботу системи в короткі терміни.

SCADA-системи мають величезний потенціал для подальшого розвитку, особливо з урахуванням впровадження штучного інтелекту (ШІ), який може значно покращити функціональність SCADA-систем, додавши їм можливості передбачення та адаптивного управління.

Однією з ключових переваг ШІ є передбачувальне обслуговування. Штучний інтелект може аналізувати дані з датчиків та виявляти ознаки майбутніх збоїв обладнання до того, як вони стануть критичними. Це дозволяє планувати обслуговування заздалегідь, уникнувши непередбачених простоїв. Крім того, ШІ може аналізувати великі обсяги даних у реальному часі та пропонувати оптимальні параметри роботи обладнання, що дозволяє знизити витрати енергії та сировини. Також використовуючи ШІ SCADA-системи можуть автоматично приймати рішення щодо управління виробничими процесами без участі людини. Це особливо корисно в умовах, де потрібна швидка реакція на зміни. Нарешті, штучний інтелект дозволяє аналізувати великі обсяги історичних даних, виявляючи закономірності та тенденції, які можуть бути використані для подальшого вдосконалення виробничих процесів.

Отже, SCADA-системи є невід'ємною частиною сучасної промислової автоматизації, оскільки вони забезпечують ефективний контроль та управління виробничими процесами.

Список використаних джерел:

1. Siemens AG. "SIMATIC WinCC: SCADA System." Офіційна документація.

УДК 004.056.53

Ожго Ю. А., здобувач
Дацюк Д. В., ст. викладач
Державний університет «Житомирська політехніка»

БЕЗПЕКА JSON WEB TOKEN (JWT): ВРАЗЛИВОСТІ ТА РЕКОМЕНДАЦІЇ ЩОДО ЗАХИСТУ

У сучасних інформаційних системах захист даних є критично важливим аспектом, особливо у веб-додатках, де автентифікація та авторизація забезпечують контроль доступу до ресурсів. Одним із поширених методів автентифікації є використання JSON Web Token (JWT) — відкритого стандарту для створення токенів доступу у форматі JSON, що зберігаються на стороні клієнта та забезпечують масштабовану авторизацію без необхідності підтримки сесійного стану на сервері. Незважаючи на ефективність і гнучкість цього механізму, його некоректне використання може призводити до численних загроз безпеці.

JWT складається з трьох основних компонентів: заголовка (header), корисного навантаження (payload) та підпису (signature). Заголовок містить алгоритм підпису (alg) і тип токена (typ). У корисному навантаженні зберігається інформація про користувача та метадані токена, зокрема iat (час створення), exp (час закінчення дії) [1], тощо. Підпис формується шляхом хешування заголовка і корисного навантаження за допомогою обраного алгоритму та секретного ключа. Оскільки криптографічний підпис є основним механізмом захисту JWT, його правильне використання має критичне значення, а помилки в реалізації можуть призвести до серйозних загроз безпеці.

Досить поширеною вразливістю є недостатня перевірка підпису. Деякі бібліотеки для роботи з токенами містять окремі функції для розкодування (decode()) та перевірки підпису (verify()). Якщо розробник помилково використовує лише функцію розкодування, система може прийняти змінений токен без перевірки його автентичності. Це дає змогу зловмиснику підробити токен, змінюючи, наприклад, ідентифікатор користувача або рівень доступу. У деяких випадках така вразливість виникає через тестові налаштування, коли перевірка підпису вимикається під час розробки, але після розгортання системи не активується знову. Щоб уникнути цього, необхідно гарантувати перевірку підпису для кожного отриманого токена перед його використанням.

Серйозну загрозу також становить можливість використання алгоритму None, що фактично означає відсутність підпису [2]. Якщо система дозволяє приймати токени з таким алгоритмом, зловмисник

може змінити значення alg на None, видалити підпис і отримати несанкціонований доступ. Це повністю обходить механізм перевірки автентичності токена, що може призвести до компрометації облікових записів або доступу до конфіденційної інформації. Щоб уникнути цієї вразливості, додатки повинні явно відхиляти JWT із алгоритмом None, незалежно від варіацій регістру (none, NONE, nOnE тощо). Додатково слід забезпечити використання надійних криптографічних алгоритмів і гарантувати, що всі токени підписуються та проходять перевірку перед використанням.

Ще одним критичним ризиком є можливість перехоплення JWT. Якщо токен передається через незахищене з'єднання або зберігається у локальному сховищі браузера (localStorage), зловмисник може викрасти його та повторно використати. Це створює загрозу replay-атаки, коли викрадений токен застосовується повторно навіть після виходу користувача з системи [3]. Для зменшення цього ризику слід використовувати лише захищені канали передачі (HTTPS), встановлювати обмежений термін дії токенів, застосовувати механізми оновлення (refresh tokens) і зберігати JWT у HttpOnly cookie. Останній підхід унеможливлює доступ до токена через JavaScript, що значно знижує ймовірність його викрадення через XSS-атаки.

JWT є ефективним механізмом автентифікації та авторизації у веб-додатках та розподілених системах, проте його некоректна реалізація може спричинити значні загрози безпеці, зокрема недостатню перевірку підпису, атаки із використанням алгоритму None та перехоплення токенів. Аналіз вразливостей цього механізму підтверджує необхідність дотримання принципів безпечної реалізації, оскільки навіть незначні помилки можуть призвести до компрометації даних і несанкціонованого доступу. Мінімізація цих ризиків вимагає використання криптографічно стійких алгоритмів, належної перевірки підпису та захищених методів зберігання і передачі токенів.

Список використаних джерел:

1. Introduction to JSON Web Tokens. URL: https://jwt.io/introduction (дата звернення: 14.03.2025).

2. Critical vulnerabilities in JSON Web Token libraries. URL: https://auth0.com/blog/critical-vulnerabilities-in-json-web-token-libraries (дата звернення: 14.03.2025).

3. Session hijacking attack. URL: https://owasp.org/www-community/attacks/Session_hijacking_attack (дата звернення: 14.03.2025).

Секція 3
КОМП'ЮТЕРНІ НАУКИ, ІНФОРМАЦІЙНІ СИСТЕМИ ТА ТЕХНОЛОГІЇ

УДК 004

Лук'яненко А.А., здобувач,
Українець М.О., асистент
Державний університет «Житомирська політехніка»

ПОРІВНЯННЯ ШВИДКОДІЇ ORM "ENTITY FRAMEWORK" ТА МІКРО-ORM "DAPPER" ДЛЯ .NET ДОДАТКІВ

Сучасна розробка програмного забезпечення потребує ефективного підходу до роботи з базами даних. У .NET популярними інструментами для взаємодії з реляційними базами даних є ORM (Object-Relational Mapping) фреймворки. Найбільш поширеним ORM є Entity Framework (EF), який автоматизує процес роботи з базою даних та дозволяє працювати з нею на рівні об'єктів. Альтернативним підходом є використання мікро-ORM систем, таких як Dapper, який надає розширені можливості взаємодії з SQL-запитами, тим самим, забезпечуючи високу продуктивність [3].

Метою дослідження є порівняння швидкодії ORM Entity Framework та мікро-ORM Dapper та опис доцільності їхнього використання у .NET додатках.

Entity Framework дозволяє розробникам працювати з базою даних, використовуючи об'єктно-орієнтований підхід, мінімізуючи необхідність написання SQL-запитів. Він підтримує запити LINQ, Change Tracking, міграції та автоматичну генерацію запитів, що спрощує розробку [1].

Dapper відноситься до сімейства інструментів, відомих як мікро-ORM. Dapper дозволяє контролювати запити SQL, зіставляти результати виконання запитів з об'єктами моделей, виконувати збережені процедури тощо. Він забезпечує високу продуктивність, що робить його ефективним рішенням для проєктів, де критично важлива швидкість виконання запитів [2].

Для проведення порівняння швидкодії цих фреймворків було розроблено тестовий програмний додаток на платформі .NET, який вимірює швидкість виконання основних операцій з базою даних, зокрема SELECT, INSERT, UPDATE, DELETE та SELECT + JOIN. Тестовий додаток працює з базою даних PostgreSQL. Для кожного тесту

виконується серія вимірювань, після чого обчислюється середнє арифметичне для часу виконання операцій. У якості тестових даних у базі даних було створено дві таблиці: records (поля: id, name, value) та orders (поля: id, recordId), у кожну з яких було додано значний обсяг записів (1.000.000 записів). Результати тестування зображено на рисунку 1.

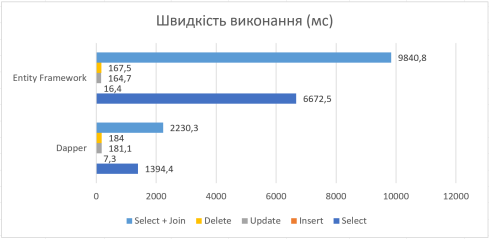


Рис. 1 Результати тестування ORM

Результати тестування швидкодії показали різницю між Entity Framework та Dapper. Dapper швидший за Entity Framework у виконанні запитів SELECT і SELECT + JOIN, але під час виконання запитів INSERT, UPDATE та DELETE різниця у швидкості виконання цих запитів майже непомітна.

Попри гіршу швидкодію порівняно з Dapper, використання Entity Framework залишається доцільним у проєктах зі складною схемою даних. Entity Framework допомагає автоматизувати роботу з базою даних, зменшуючи необхідність написання SQL-запитів вручну і забезпечуючи кращу підтримку та розширюваність коду. Крім того, автоматичне керування транзакціями та підтримка міграцій, значно спрощують розробку та обслуговування застосунку.

Таким чином, вибір між Dapper та Entity Framework залежить від конкретних вимог проєкту. Для систем, де критично важлива швидкість виконання запитів, доцільно використовувати Dapper, якщо ж система має складну схему даних і важлива простота розробки, то Entity Framework є кращим вибором.

Список використаних джерел:

1. Entity Framework documentation hub. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/ef/.

2. Welcome to learn dapper ORM - A dapper tutorial for C# and .NET core. Welcome To Learn Dapper ORM - A Dapper Tutorial for C# and .NET Core. URL: https://www.learndapper.com/.

3. Wiatrowski T. Comparative analysis of ORM systems for the .NET platform. Journal of computer sciences institute. 2024. Vol. 31. P. 97–102. URL: https://doi.org/10.35784/jcsi.6012.

УДК 004.925:004.94

Турлій А.О., магістрант,
Марчук Г.В., ст. викладач
Державний університет «Житомирська політехніка»

ВИКОРИСТАННЯ СУЧАСНИХ ТЕХНОЛОГІЙ ВІЗУАЛІЗАЦІЇ ПРИ РОЗРОБЦІ ІНТЕРАКТИВНИХ 3D-СВІТІВ

У сучасному процесі розробки відеоігор важливим є використання новітніх технологій візуалізації для створення високоякісних та ефективних інтерактивних 3D-світів. Поява нових інструментів та методів дозволяє розробникам досягати більшої глибини графічного зображення та покращувати користувацький досвід без значного навантаження на обчислювальні ресурси. Водночас, необхідно дотримуватися балансу між високою якістю візуальних ефектів та ефективністю їхнього виконання, що є особливо важливим для забезпечення стабільного ігрового процесу на пристроях з різним рівнем потужності.

Метою цього дослідження є оцінка впливу використання сучасних технологій візуалізації на створення інтерактивних 3D-світів, зокрема через впровадження таких технологій, як Shader Graph, VFX Graph, Level of Detail (LOD) та Global Illumination. Розглянуто вплив цих технологій на якість графіки, продуктивність ігрового процесу, а також їхню роль у забезпеченні адаптивності та ефективності ресурсів. Для досягнення мети дослідження було проведено поетапно.

Аналіз сучасних технологій візуалізації [1]. В ході дослідження були детально вивчені можливості Shader Graph і VFX Graph. Виявлено, що дані інструменти суттєво оптимізують процес створення візуальних ефектів, надаючи широкі можливості для їх налаштування.

Інтеграція та оптимізація рівнів деталізації. Використання технології LOD дозволяє знижувати рівень деталізації моделей залежно від відстані до камери, що значно знижує навантаження на процесор і графічну карту. Впровадження системи LOD дозволило зменшити кількість полігонів, що рендеряться на віддалених об'єктах, що безпосередньо вплинуло на продуктивність (Таблиця 1).

Таблиця 1.

Відстань до камери	Зменшення полігонів (%)	Збільшення FPS (%)
10-30 м	40%	15%

Продовження таблиці 1

30-50 м	50%	20%
50+ м	60%	25%

Моделювання освітлення та глобальної ілюмінації (Global Illumination). Було впроваджено техніку попередньо розрахованого (baked) глобального освітлення у статичних сценах, що знизило навантаження на графічний процесор у порівнянні з реальним часом обчислення. Динамічні джерела світла використовувалися вибірково, що дозволило покращити якість освітлення без значного зменшення продуктивності.

Тестування та оцінка ефективності [2]. Виконані стрес-тести показали, що впроваджені методи оптимізації дозволили зменшити середнє завантаження GPU на 30% та CPU на 15%, водночас зберігши стабільну частоту кадрів навіть у сценах з високою кількістю об'єктів та складними ефектами. Додатковий аналіз підтвердив, що використання LOD та оптимізованого освітлення мінімізує втрати продуктивності без помітного погіршення якості графіки.

Пропозиції щодо подальшого вдосконалення. Запропоновано інтеграцію технології адаптивного рендерингу, що дозволяє динамічно змінювати якість графіки залежно від продуктивності пристрою. Також можливість застосування DLSS (Deep Learning Super Sampling) для покращення деталізації без значного збільшення навантаження на систему. Додатково пропонується вдосконалення алгоритмів глобального освітлення, використання Screen Space Global Illumination (SSGI) у поєднанні з попередньо розрахованим освітленням.

Дослідження підтвердило, що використання Shader Graph, VFX Graph, LOD і Global Illumination значно покращує графічну якість і оптимізує ресурси в розробці інтерактивних 3D-світів. Shader Graph і VFX Graph спростили створення матеріалів та ефектів, дозволяючи розробляти складні візуальні елементи без ручного написання шейдерного коду. Завдяки LOD вдалося знизити навантаження на графічний процесор, покращивши продуктивність без втрати якості.

Список використаних джерел:

1. Alonso-Fernández C. Game Learning Analytics. // Journal of Learning Analytics. - 2022 -. URL: https://doi.org/10.18608/jla.2022.7633

2. Rosenfield Boeira J. N. Automated Testing with Unity. Lean Game Development. - Berkeley, CA, 2023.

УДК 378.6.004.4

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

ПЕРЕВАГИ ТА НЕДОЛІКИ ПАРСИНГУ САЙТІВ ЗАСОБАМИ POWER QUERY

Парсинг сайтів - це процес автоматичного збору інформації з веб-сторінок. Парсинг відіграє критичну роль у сучасному цифровому світі, де дані є ключовим активом, ставши невід'ємною частиною сучасного цифрового світу, надаючи можливість отримувати та аналізувати великі обсяги даних для різних цілей, таких як: бізнес, фінанси, інвестиції, наукові дослідження та багато інших [1].

Для отримання та перетворення даних доцільно скористатися потужним інструмент у Microsoft Excel та Power BI - Power Query. Він має інтуїтивно зрозумілий графічний інтерфейс, який дозволяє користувачам без навичок програмування легко створювати запити для парсингу веб-сайтів.

Метою дослідження є аналіз сильних та слабких сторін використання інструменту Power Query для парсингу вебсайтів.

Power Query дозволяє об'єднувати інформацію з різних джерел, наприклад об'єднати дані з сайту, з файлу Excel, та з бази даних, що забезпечує реалізацію комплексного аналізу даних.

Після імпорту даних редактор Power Query, дозволяє виконати різноманітні операції для обробки отриманої інформації: фільтрація рядків, редагування стовпців, перетворення типів даних, операції з текстом, числами і датами, видалення дублікатів, обробка HTML-розмітки, дозволяючи користувачу витягувати та структурувати дані у потрібному форматі без необхідності писати складний код

Power Query автоматично розпізнає всі таблиці, що є на веб-сторінці, і виведить їх список. На жаль, часто зустрічаються сайти, де при спробі такого завантаження Power Query "не бачить" таблиць. Найчастіше причина в тому, що веб-дизайнер при створенні таблиці використовував у HTML-коді сторінки не стандартну конструкцію з тегом <TABLE>, та її аналог - вкладені теги-контейнери <DIV>. В такому випадку після підключення до веб-джерела необхідно завантажувати інформацію у вигляді текстового файлу, що дозволить завантажити дані як простий текст, а не як веб-сторінку. В такому випадку при роботі в Power Query весь процес отримання необхідних

даних будується на використанні фільтрів, введені параметрів та вилученні зайвого контенту [2].

Слід зауважити, що надбудова Power Query - це інтерпретатор нової, скриптової, спеціалізованої для роботи з даними мови програмування M. Тому на кожну дію, яка виконується над даними у графічному інтерфейсі Power Query, у скрипт пишеться новий рядок коду. В результаті користувач отримує в панелі послідовність виконаних дій, що дозволяє маніпулювати виконаними кроками.

Після налаштування запиту Power Query може автоматично оновлювати дані з веб-сайту за розкладом або за запитом. Це значно спрощує процес збору даних та підвищує його ефективність, заощаджуючи час і зусилля. Висока продуктивність забезпечується використанням спеціальних алгоритмів для вилучення та трансформації даних [2].

В процесі аналізу парсингу сайтів за допомогою Power Query були виявлені деякі недоліки, а саме: обмежені можливості при роботі з динамічним контентом - складно парсити сайти, що використовують JavaScript, відсутність вбудованих інструментів для обходу захисту від парсингу, проблеми з сайтами, що мають CAPTCHA (автоматизований тест, який використовується для того, щоб відрізнити людину від комп'ютера) або обмеження доступу, можливі проблеми з продуктивністю при обробці дуже великих обсягів даних, обмежені можливості для паралельної обробки даних, складність налаштування парсингу складних структур даних та вкладених елементів, залежність від структури HTML, при зміні розмітки сайту потрібно переналаштовувати парсинг.

Незважаючи на виявлені недоліки можна з впевненістю стверджувати, що парсинг сайтів за допомогою Power Query є ефективним та зручним способом збору та аналізу веб-даних. Його переваги роблять використання Power Query особливо цінним для користувачів, які працюють з платформами Excel та Power BI і не мають глибоких знань в програмуванні.

Список використаних джерел:

1. Парсинг сайтів: що це і навіщо він потрібен URL: https://web-promo.ua/ua/blog/parsing-sajtov-chto-eto-i-zachem-nuzhen (дата звернення: 12.03.2025).

2. Равив Гил Power Query в Excel і Power BI: збирання, об'єднання та перетворення даних. Microsoft, 2021.378с.

УДК 004

Ковбасюк С.В., д.т.н., с.н.с.,
Українець М.О., аспірант
Державний університет «Житомирська політехніка»

ПЛАНУВАННЯ ТРАЄКТОРІЇ ПОЛЬОТУ БЕЗПІЛОТНОГО ПОВІТРЯНОГО СУДНА В НЕСПРИЯТЛИВИХ УМОВАХ

Застосування автономних безпілотних систем є однією з основних тенденцій оптимізації процесів в сферах життєдіяльності людства. Для підвищення якості виконання завдань моніторингу, збору даних, транспортування вантажів використовують автономні безпілотні повітряні судна (БПС).

Важливим завданням в контексті підвищення оперативності виконання завдань БПС є визначення маршруту руху БПС, який мінімізує ряд критеріїв, таких як час та відстань польоту, ймовірність пошкодження тощо з урахуванням умов середовища та характеристик БПС. Для підвищення ефективності та оперативності виконання завдань БПС в несприятливих умовах потребує рішення завдання планування траєкторії польоту БПС. Під несприятливими умовами маються на увазі такі умови польоту, в яких виконання завдань покладених на БПС ускладнене природними, техногенними чи інформаційними чинниками.

Актуальним питанням є визначення вимог до алгоритму планування траєкторії автономного БПС в несприятливих умовах.

Недостатня увага та відсутність алгоритмічного забезпечення для планування траєкторії БПС у несприятливих умовах призводить до протиріччя між вимогами до ефективності виконання завдань в несприятливих умовах і наявними алгоритмами планування траєкторії.

Метою дослідження є визначення вимог до алгоритму планування траєкторії автономного БПС в несприятливих умовах, проведення аналізу існуючих алгоритмів планування траєкторії та вироблення напрямків вирішення задачі планування траєкторії БПС в несприятливих умовах.

Для вироблення напрямків вирішення планування траєкторії польоту БПС в несприятливих умовах слід розглянути існуючі алгоритми планування траєкторії руху. Запропонована у [1] класифікація алгоритмів планування траєкторії виділяє дві основних категорії методів планування: методи глобального та локального планування траєкторії. Вирішення завдання планування траєкторії БПС в несприятливих умовах має включати в себе пошук оптимального глобального маршруту та коригування маршруту відповідно до виникнення динамічних перешкод в процесі польоту.

Планування глобального маршруту руху повинно забезпечувати пошук оптимального маршруту руху в умовах недостатності або відсутності інформаційного забезпечення про місцевість та перераховувати оптимальний маршрут після отримання нової інформації про місцевість. Для вирішення цього завдання доцільно використовувати алгоритм Rapidly exploring Random Tree Star (RRT*) та його модифікації. Перевагами цього алгоритму є те, що він працює в багатовимірних середовищах та дозволяє ефективно перераховувати оптимальний шлях з отриманням нової інформації. Недоліком даного алгоритму є те, що через випадкову природу, шлях отриманий з його допомогою має зигзагоподібний вигляд і потребує пост-обробки для його згладжування.

Для реагування на динамічні перешкоди слід застосувати алгоритми локального планування траєкторії. В контексті планування траєкторії БПС доцільно використати підхід Model Predictive Control (MPC) Він дозволяє оптимізувати траєкторію польоту БПС на основі його моделі руху в режимі реального часу з урахуванням динамічних перешкод. Перевагою використання цього підходу в поєднанні з RRT* є те, що він дозволяє зробити траєкторію гладкою. Недоліками MPC є повільний час реагування на швидкі перешкоди та потреба великої обчислювальної потужності.

В результаті аналізу алгоритмів планування траєкторії руху було визначено вимоги до алгоритму планування траєкторії польоту БПС в несприятливих умовах. Для вирішення цього завдання алгоритм повинен відповідати наступним вимогам:

– Забезпечувати планування траєкторії польоту в умовах недостатнього або відсутнього інформаційного забезпечення;

– Виконувати перерахунок глобальної траєкторії при отриманні нової інформації про середовище;

– Коригувати траєкторію відповідно до появи динамічних перешкод в середовищі;

Перспективним напрямком вирішення є розробка гібридного алгоритму планування траєкторії БПС в несприятливих умовах на основі RRT* алгоритму та MPC підходу. Подальші дослідження будуть спрямовані на розробку механізму формування оптимальної траєкторії на основі поєднання їхніх результатів.

Список використаних джерел:

1. Yang Y., Xiong X., Yan Y. UAV formation trajectory planning algorithms: a review. Drones. 2023. Vol. 7, no. 1. P. 62. URL: https://doi.org/10.3390/drones7010062 (date of access: 12.03.2025).

УДК 004

Граф М. С., Ph.D, зав. кафедри КН
Райковський В. А., магістрант
Державний університет «Житомирська політехніка»

ОБҐРУНТУВАННЯ ВИБОРУ АЛГОРИТМУ ПОБУДОВИ БЕЗПЕЧНИХ ВЕБ-ДОДАТКІВ ДЛЯ ОБМІНУ ПОВІДОМЛЕННЯМИ

Постановка задачі. Протягом останніх років цифрове листування стало основою сучасного спілкування, охоплюючи як особисті, так і професійні аспекти життя. Саме тому, безпека такого спілкування займає ключову позицію, адже від цього залежить захист особистих даних, конфіденційної інформації та ділових секретів.

Сьогодні бізнес активно прагне інтегрувати можливості обміну повідомленнями в корпоративні інформаційні системи, що використовуються в їхній роботі. Такі інтеграції дозволяють суттєво підвищити ефективність внутрішньої комунікації.

Розробка веб-додатка для обміну повідомленнями з можливістю інтеграції його в корпоративні інформаційні системи дозволить забезпечити ефективну комунікацію всередині компанії, а отже, підвищивши продуктивність роботи. Ключовим аспектом такої розробки є використання алгоритмів та інноваційних методів побудови безпечних веб-додатків для обміну повідомленнями, що гарантує надійний захист корпоративної інформації та конфіденційних даних.

Мета дослідження. Аналіз існуючих алгоритмів та методів розробки безпечних веб-додатків для обміну повідомленнями.

Огляд алгоритмів та методів забезпечення безпеки веб-додатків. При розробці веб-додатків особливо важливо забезпечити конфіденційність та безпеку даних користувачів, зокрема у програмних продуктах, що обробляють особисту інформацію [1]. Веб-додатки для обміну повідомленнями є прикладом таких продуктів.

На рисунку 1 зображена структурна схема, що являє комплекс дій необхідний щоб забезпечити надійність та безпеку веб-застосунків.

У цьому дослідженні акцентуємо увагу на шифруванні даних та його важливості для забезпечення безпеки веб-додатків для обміну повідомленнями. Розглянемо алгоритм End-to-End Encryption та особливості його застосування.

Рисунок 1 – Безпека веб-додатку

End-to-End Encryption (E2EE) — підхід, що передбачає доступ до повідомлень тільки відправнику та отримувачу, шляхом обміну публічними ключами шифрування. Прикладом використання данного алгоритму є Signal Protocol, який використовується в таких популярних месенджерах, як WhatsApp та Signal. Саме цей метод шифрування дозволяє захистити данні користувачів максимально якісно, адже ніхто крім відправника не може розшифрувати повідомлення, тобто будь-хто зі злочинними намірами не зможе отримати доступу до повідомлень.

Розглянемо алгоритм E2EE на прикладі обміну повідомленнями між двома користувачами. На початку кожен користувач генерує пару ключів: публічний (для обміну) і приватний (для розшифрування). Обмін ключами відбувається за допомогою серверу. Далі відбувається створення сесійного ключа, саме він використовується для шифрування повідомлення перед відправкою, користувачі обмінюються створеними ключами на основі алгоритму Диффі-Хелмана, за рахунок цього вони можуть створити спільний ключ не виконуючи при цьому передачу самого ключа через мережу. Відправник шифрує повідомлення використовуючи сесійний ключ та симетричне шифрування. Отримувач розшифровує повідомлення за допомогою сесійного ключа, який розшифрував використавши приватний ключ. Після кожного відправленого повідомлення сесійний ключ оновлюється, тим самим підвищуючи безпеку. Також є можливість підвищити безпеку алгоритму шляхом використання іншого протоколу узгодження двох раундів секретних ключів алгоритму Диффі-Хелмана [2], тому застосування цього підходу є оптимальним варіантом для підвищення надійності.

Використання алгоритмів та інноваційних методів безпеки, таких як End-to-End Encryption допоможе забезпечити безпеку та конфіденційність даних користувачів. Впровадження описаного алгоритму у веб-додаток для обміну повідомленнями дозволить гарантувати, що доступ до повідомлення отримає тільки відправник та отримувач.

Список використаних джерел:

1. Hoffman A. Web Application Security: Exploitation and Countermeasures for Modern Web. Gravenstein Highway North, Sebastopol: O’Reilly Media, Inc, 2024.

2. Pundir M., Kumar A., Choudhary S. Efficient Diffie Hellman Two Round Secret Key Agreement Protocol. 2023 1st International Conference on Innovations in High Speed Communication and Signal Processing (IHCSP). Bhopal, India, 2023. С. 7–10.

УДК: 004.8

Біємська А.С., магістрант,
Граф М.С., Ph.D, зав. кафедри КН,
Державний університет «Житомирська політехніка»

ОГЛЯД ПІДХОДІВ ДО АДАПТИВНОЇ СКЛАДНОСТІ У СУЧАСНИХ ВІДЕОІГРАХ

Сучасна ігрова індустрія постійно прагне підвищити рівень взаємодії з гравцями та забезпечити максимально комфортний і цікавий ігровий процес. Одним із ключових аспектів є адаптація складності гри відповідно до навичок та дій користувача.

В рамках дослідження було проведено огляд сучасних ігор, що використовують адаптивну складність. Виявлено три основні підходи:

− *Статична адаптація*: Використання попередньо визначених рівнів складності, що залежать від вибору гравця перед початком гри. Характеристики ворогів, кількість ресурсів та складність завдань залишаються незмінними протягом усього проходження Недоліком є обмежена гнучкість та нездатність підлаштовуватися під змінювані навички гравця.

− *Скриптована адаптація*: Застосування скриптів для зміни складності в залежності від виконаних дій гравця. Це дозволяє більш гнучко регулювати складність у порівнянні зі статичним підходом. Наприклад, в грі Resident Evil 4 використано систему, що змінює кількість та силу ворогів залежно від успішності гравця [1]. Водночас ми не можемо передбачати аномальні дії гравця, оскільки працюємо лише за наперед визначеними правилами.

− *Динамічна адаптація на основі ML*: Використання алгоритмів машинного навчання для прогнозування поведінки гравця в реальному часі та динамічної зміни складності. На відміну від статичної та скриптованої адаптації, алгоритми машинного навчання здатні навчатися на основі зібраних даних і самостійно приймати рішення про зміну складності [2]. Наприклад, у грі Left 4 Dead використовується «AI Director», що регулює кількість ворогів та ресурси на основі рівня стресу гравця. Такий підхід забезпечує максимально індивідуалізований та збалансований ігровий процес.

Підходи машинного навчання традиційно поділяють на три великі категорії, які відповідають парадигмам навчання, залежно від природи «сигналу» або «зворотного зв'язку», доступного системі навчання:

- *Supervised Learning*: Цей підхід передбачає навчання моделей на основі історичних даних про дії гравців. Мета — передбачити подальшу поведінку гравця та відповідно змінювати складність гри. Наприклад, у

грі Forza Motorsport використовуються алгоритми для аналізу стилю водіння гравця. Система збирає дані про швидкість, траєкторію та гальмування і на основі цього прогнозує можливості гравця. Завдяки цьому суперники підлаштовуються під рівень гравця.

- *Unsupervised Learning*: Використовується для виявлення патернів у поведінці гравців без попередньо визначених міток. Зокрема, алгоритми кластеризації, такі як K-means та DBSCAN, дозволяють розподілити гравців на групи за стилем гри: наприклад, агресивні, обережні чи тактичні гравці. У грі Tomb Raider цей підхід використовується для налаштування підказок і рівня складності головоломок. Якщо гравець часто затримується на розгадуванні головоломок, система може запропонувати додаткові підказки або спростити задачі.
- *Reinforcement Learning*: Навчання з підкріпленням передбачає, що система навчається на основі винагород та покарань за певні дії [3]. Алгоритми, такі як Q-Learning та Deep Q-Networks (DQN), дозволяють динамічно коригувати складність гри в залежності від успіхів гравця. Наприклад, у грі Alien: Isolation, якщо гравець часто використовує певні укриття або маршрути, вороги змінюють свою поведінку та знаходять нові шляхи атаки.

Реалізація алгоритмів машинного навчання для адаптації складності стикається з низкою викликів. Головні проблеми — це висока обчислювальна складність та ризик помилкової оцінки навичок гравця, що може призвести до втрати інтересу до гри. Подальші дослідження можуть бути спрямовані на оптимізацію ресурсів через спрощені моделі, гібридні підходи та покращення точності адаптації.

Список використаних джерел:

1. Weber B. G., Mateas M., Jhala A. *Using Data Mining to Model Player Experience*. Proceedings of the Fifth International Conference on the Foundations of Digital Games. 2011. URL: https://alumni.soe.ucsc.edu/~bweber/pubs/submission_3_epex_final.pdf (дата звернення: 10.03.2025).

2. Yannakakis G. N., Togelius J. Artificial Intelligence and Games. Springer. 2018. URL: https://link.springer.com/book/10.1007/978-3-319-63519-4 (дата звернення: 10.03.2025).

3. Silver D., Schrittwieser J., Simonyan K. et al. *Mastering the game of Go without human knowledge*. Nature. 2017. URL: https://www.nature.com/articles/nature24270 (дата звернення: 10.03.2025).

УДК 004.5

Богодвид О.В., магістрант,
Сугоняк І.І., к.т.н., доцент
Державний університет «Житомирська політехніка»

АНАЛІЗ ПІДХОДІВ ОПТИМІЗАЦІЇ ANDROID-ЗАСТОСУНКІВ

Оптимізація продуктивності Android-застосунків є важливим аспектом розробки мобільного програмного забезпечення, що дозволяє зменшити споживання ресурсів, підвищити швидкодію та покращити загальний користувацький досвід [1]. У сучасних умовах високої конкуренції серед мобільних застосунків ефективність їх роботи значною мірою визначає успіх продукту.

Метою аналізу є дослідження сучасних підходів до оптимізації Android-застосунків, які сприяють підвищенню продуктивності, зниженню використання енергоресурсів та покращенню інтерфейсу для користувачів [2].

Інтеграція сучасних технологій дозволяє значно покращити процес оптимізації мобільних застосунків. Завдяки інструментам моніторингу та аналізу продуктивності розробники можуть отримувати детальну інформацію про використання ресурсів, що допомагає визначати проблемні місця в коді та алгоритма

Одним з ключових підходів є оптимізація рендерингу інтерфейсу за допомогою **Jetpack Compose**, що дозволяє спрощувати розробку UI, зменшувати кількість викликів до основного потоку та підвищувати ефективність відтворення анімацій та складних візуальних елементів [3]. Це значно покращує швидкодію застосунку та користувацький досвід. На відміну від традиційного підходу з використанням XML-макетів, Jetpack Compose використовує декларативний стиль програмування та більш ефективний механізм перемальовування, який оновлює лише компоненти, що змінилися, замість повного перемальовування всього екрану. Це особливо важливо для сучасних застосунків з динамічними інтерфейсами та складними анімаціями.

Процес профілювання [4] передбачає використання інструментів, таких як **Android Profiler** та **Apptim,** які дозволяють аналізувати завантаженість CPU, використання пам’яті та продуктивність графічного рендерингу. Завдяки цьому можна швидко виявляти вузькі місця та підвищувати загальну ефективність роботи застосунку.

Важливу роль у зниженні навантаження на систему відіграє застосування сучасних бібліотек, таких як **Retrofit** для оптимізації роботи з мережею та **Glide** для ефективного завантаження й кешування

зображень [5]. Використання цих інструментів дозволяє мінімізувати затримки та підвищити продуктивність роботи застосунку.

Процес оптимізації потребує комплексного підходу, що включає різні аспекти, наприклад використання ефективних архітектурних патернів (MVVM, MVI), які дозволяють розділити логіку програми, зменшити навантаження на основний потік та покращити тестованість коду. Також варто згадати про грамотне керування ресурсами, управління потоками, ефективне кешування даних та зменшення використання пам’яті за допомогою механізмів утилізації об'єктів. Застосування найкращих практик розробки, таких як Lazy Loading, зменшення кількості необов’язкових викликів до бази даних та застосування багатопоточності для розподілу навантаження [6].

Розробка ефективних Android-застосунків потребує впровадження сучасних методів оптимізації, які дозволяють зменшити навантаження на систему, покращити продуктивність та забезпечити плавну взаємодію користувачів із програмою. Завдяки інтеграції передових підходів та інструментів розробники можуть створювати швидкі, стабільні та енергоефективні застосунки, що відповідають сучасним вимогам ринку.

Список використаних джерел:

1. Кузьма К.Т. *Програмування мобільних пристроїв: навчальний посібник для дистанційного навчання*. Миколаїв: СПД Румянцева Г.В., 2021. URL: https://files.znu.edu.ua/files/Bibliobooks/Inshi73/0053792.pdf (дата звернення: 03.03.2025).

2. Google Android Developers. *Best Practices for Performance Optimization.*2024. URL: https://developer.android.com/topic/performance/ (дата звернення: 03.03.2025).

3. Google Android Developers. *Jetpack Compose: Modern Toolkit for UI Development.* 2024. URL: https://developer.android.com/jetpack/compose (дата звернення: 03.03.2025).

4. Android Studio User Guide. *Profiling with Android Profiler*. 2024. URL: https://developer.android.com/studio/profile/android-profiler (дата звернення: 03.03.2025).

5. Square, Inc. *Retrofit: A type-safe HTTP client for Android and Java.* 2024. URL: https://square.github.io/retrofit/ (дата звернення: 03.03.2025).

6. *Google* Android Developers. *Memory* Management Best Practices. 2024. URL: https://developer.android.com/topic/performance/memory (дата звернення: 03.03.2025).

УДК 004:42

Дашкевич В.В., магістрант,
Граф М.С., Ph.D, зав. кафедри КН
Державний університет «Житомирська політехніка»

АНАЛІЗ СТРАТЕГІЙ РОЗГОРТАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Розгортання програмного забезпечення є важливим етапом у процесі розробки, оскільки саме на цьому етапі програмний продукт переходить від стадії розробки до стадії експлуатації. Від правильно обраної стратегії розгортання залежить не тільки успішність запуску проекту, але й його подальша ефективність та безпека.

Метою дослідження є аналіз та порівняння основних стратегій розгортання програмного забезпечення для визначення їхньої ефективності. Дослідження спрямоване на оцінку переваг і недоліків таких підходів, як Rolling Deployment, Canary Deployment та Blue-Green Deployment.

Rolling Deployment (Поступове Розгортання) - метод оновлення програмних систем, який дозволяє безперервно впроваджувати нові версії програмного забезпечення в продакшн-середовище за допомогою автоматизованих рішень, де окремі екземпляри системи оновлюються по черзі [1].

Canary Deployment (Канаркове Розгортання) - стратегія безперервного розгортання програмного забезпечення, яка дозволяє мінімізувати ризики, пов’язані з введенням нових версій системи в експлуатацію за допомогою спостереження її впливу на обмежену групу користувачів, перш ніж розгорнути її для загального використання [2].

Blue-Green Deployment (укр. Синьо-Зелене Розгортання) - метод встановлення змін для веб-сервера, додатка або сервера бази даних шляхом чергування робочих і проміжних серверів [3]. Даний підхід передбачає наявність двох ідентичних середовищ для розгортання: Blue (поточне середовище) та Green (нове середовище), що дозволяє в лічені секунди перемикатись між даними версіями або балансувати трафік між ними в залежності від налаштувань даного методу.

У результаті аналізу перелічених стратегій розгортання можна зробити наступні висновки.

Дані стратегії розгортання мають спільні недоліки:

- потребують ретельної перевірки сумісності версій перед початком розгортання, оскільки вони будуть існувати

паралельно протягом певного часу;
- потребують автоматизованої системи моніторингу роботи для прийняття рішення про подальше розгортання або відкат оновлень.

Незважаючи на перелічене, також можна виділити основні переваги та недоліки кожної з них:

Rolling Deployment. Перевага - більше підходить для систем що використовують мікросервісну архітектуру. Недолік - навантаження на систему може коливатись, оскільки інстанси що знаходяться в оновлені не можуть обробляти запити від клієнтів.

Canary Deployment. Перевага - дозволяє отримувати цінний зворотний зв'язок до того, як зміни будуть застосовані для всіх користувачів. Недолік - реалізація даного розгортання вимагає складного керування трафіком.

Blue-Green Deployment. Перевага - забезпечує швидке та безпечне розгортання з можливістю миттєвого відкату на попередню версію. Недолік - має високі витрати на керування та обслуговування двох продакшн-середовищ.

Отже, вибір оптимальної стратегії залежить від конкретних вимог проекту, наявних ресурсів та необхідних рівнів безпеки та стабільності. Кожен метод може бути ідеальним у своїх умовах, і вибір стратегії розгортання має враховувати такі фактори, як масштаб системи, вимоги до безперервної доступності, бюджет на інфраструктуру та необхідність швидкого реагування на збої.

Список використаних джерел:

1. Octopus Deploy. Rolling deployments: Pros, cons, and 4 critical best practices. 2025. URL: https://octopus.com/devops/software-deployments/rolling-deployment/ (дата звернення: 23.01.2025).
2. Octopus Deploy. Canary deployments: Pros, cons, and 5 critical best practices. 2025. URL: https://octopus.com/devops/software-deployments/canary-deployment/ (дата звернення: 23.01.2025).
3. Octopus Deploy. Blue/green deployments: how they work, pros and cons, and 8 critical best practices. 2025. URL: https://octopus.com/devops/software-deployments/blue-green-deployment/ (дата звернення: 23.01.2025).
4. CLOUD NATIVE COMPUTING FOUNDATION. Load balancing for blue-green, rolling, and canary deployment. 2025. URL: https://www.cncf.io/blog/2022/05/09/load-balancing-for-blue-green-rolling-and-canary-deployment/ (дата звернення: 23.01.2025).

УДК 004

Талько П.В., здобувач,
Українець М.О., асистент
Державний університет «Житомирська політехніка»

РЕЛЯЦІЙНІ ТА НЕРЕЛЯЦІЙНІ БАЗИ ДАНИХ У СИСТЕМАХ УПРАВЛІННЯ КУРСАМИ

Сучасні технології розвиваються з кожним днем, разом із цим змінюються потреби в зберіганні та обробці даних. Для забезпечення ефективної роботи інформаційної системи важливо вибрати правильну модель бази даних. Широко поширена реляційна модель бази даних має визначену схему, яка повинна бути розроблена перш ніж дані буде завантажено. З іншого боку, Google, Amazon, Facebook і LinkedIn були серед перших компаній, які виявили обмеження моделі реляційної бази даних в контексті нових вимог до програмних продуктів. Ці обмеження призвели до розвитку нереляційних баз даних, також відомих як NoSQL (Not Only SQL). Сучасні інформаційні системи використовують різні типи баз даних і їх вибір залежить від вимог конкретного проєкту [1].

Метою дослідження є опис реляційної та нереляційної моделі даних та визначення оптимального підходу до роботи з даними в системі керування курсами.

Реляційні бази даних використовують чітко визначену схему та забезпечують підтримку ACID-транзакцій (Atomicity, Consistency, Isolation, Durability). Це дозволяє ефективно керувати взаємопов'язаними даними, такими як: курси, дані користувачів, оцінки та результати. NoSQL бази даних забезпечують гнучкість і масштабованість, що робить їх корисними для зберігання великого обсягу неструктурованих даних (коментарі, файли, відео), аналізу поведінки користувачів (логи, історія активності). NoSQL підходить для систем, які повинні швидко адаптуватися до нових форматів даних.

Система керування курсами обробляє структуровані дані такі як облікові записи користувачів, реєстрація на курси. Водночас така система працює з неструктурованими даними, такими як активність користувача, персональні рекомендації та з сутностями, які мають між собою зв’язок «багато-до-багатьох». Для визначення оптимального підходу для збереження даних в системі управління курсами доцільно провести аналіз існуючих підходів до збереження даних.

SQL-бази даних забезпечують ACID-гарантії, що є критично важливим для фінансових операцій, реєстрації студентів та оцінювання. Завдяки визначеній структурі вони зберігають цілісність даних і запобігають дублюванню. Однак визначена схема ускладнює зміни у

структурі даних, а вертикальне масштабування може обмежувати продуктивність при значному збільшенні навантаження. Крім того, SQL менш ефективний при роботі з великими обсягами неструктурованої інформації, такої як активність користувача, персональні рекомендації. NoSQL-бази, навпаки, відзначаються гнучкою структурою, що дозволяє легко змінювати формат даних без необхідності оновлення всієї системи та ефективніше реалізовувати зв'язки типу «багато-до-багатьох». Вони демонструють високу продуктивність при роботі з великими потоками користувачів та ефективно масштабуються горизонтально. Проте рівень гарантій цілісності даних у NoSQL слабший у порівнянні з реляційними базами.

Комбінований підхід, що поєднує SQL і NoSQL, дозволяє використовувати реляційну базу для зберігання критично важливих структурованих даних, таких як курси, фінансові операції, дані студентів та їхні оцінки, а NoSQL – для обробки динамічної та неструктурованої інформації, зокрема логів активності, рекомендацій і мультимедіа. Це забезпечує баланс між надійністю та гнучкістю системи. Водночас такий підхід потребує складнішої архітектури інформаційної системи, додаткових ресурсів на адміністрування та оптимізацію запитів, а також роботи з різними моделями даних, що призведе до ускладнення розробки.

Вибір між реляційними та нереляційними базами даних у системах управління курсами залежить від специфіки вимог до роботи системи. Реляційні БД забезпечують цілісність, структурованість та ACID-транзакції, що важливо для збереження даних про навчальний процес та фінансові операції. NoSQL рішення відзначаються гнучкістю та масштабованістю, що зручно для роботи з великими обсягами неструктурованих даних, аналізу поведінки користувачів і персоналізації навчання. Перспективним рішенням може бути використання комбінованого підходу, що поєднує надійність SQL із продуктивністю NoSQL, дозволяючи адаптувати систему до вимог, які змінюються. Подальші дослідження будуть спрямовані на вироблення підходів роботи з комбінованою моделлю даних в системі керування курсами.

Список використаних джерел:

1. Băzăr C., Cosmin S. The transition from RDBMS to nosql. A comparative analysis of three popular non-relational solutions: cassandra, mongodb and couchbase. Database systems journal. 2014. Vol. V, no. 2. P. 49–59. URL: https://dbjournal.ro/archive/16/16_5.pdf.

УДК 004.8

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

ІНТЕГРАЦІЯ СУЧАСНИХ ТЕХНОЛОГІЙ У ДОДАТКИ ДЛЯ УПРАВЛІННЯ ОСОБИСТИМИ ФІНАНСАМИ

Останнім часом проблема управління фінансами стає все більш важливою в умовах цифровізації та технологічного прогресу, які кардинально змінюють традиційні підходи до цього процесу. Сучасні технології надають нові можливості для користувачів фінансових послуг, пропонуючи персоналізовані стратегії для ефективного планування, інвестування та зниження фінансових ризиків. Завдяки аналізу великих даних та машинному навчанню можна виявляти фінансові тенденції та автоматизувати процес прийняття рішень, що призводить до підвищення доходів і зменшення витрат.

Метою цього дослідження є вивчення впливу нових технологій на додатки для управління особистими фінансами. Завдання полягає в оцінці ефективності цих інструментів у прогнозуванні фінансових трендів, оптимізації процесу бюджетування та пошуку можливостей для економії, що, в свою чергу, сприяє кращому управлінню фінансами. Дослідження зосереджене на визначенні конкретних результатів впровадження таких технологій та пропонуванні рекомендацій для подальшого розвитку фінансових інструментів.

Фінансові додатки спрощують процес контролю за доходами, витратами та інвестиціями, автоматизуючи збір даних з різних джерел: банківських рахунків, кредитних карток і інвестиційних портфелів. Вони аналізують ці дані та надають користувачам інформацію, що допомагає приймати зважені рішення. Розробка таких додатків включає етапи планування функціональності, дизайну інтерфейсу, програмування та тестування, а також розробку систем захисту даних [1].

Впровадження новітніх технологій значно трансформує ці процеси, особливо в частині обробки великих даних і автоматизації рішень. Завдяки можливості створення алгоритмів, які вивчають фінансові звички користувачів і прогнозують майбутні витрати та доходи, додатки можуть надати персоналізовані рекомендації щодо управління бюджетом [2]. Це також вимагає адаптації додатків до змінюваних потреб користувачів і розробки складніших систем безпеки для захисту великих обсягів персональних даних.

Інтеграція таких технологій дозволяє значно розширити можливості фінансових додатків, перетворюючи їх із простих інструментів для відстеження доходів і витрат у комплексні системи для управління фінансовим плануванням.

Реалізація проекту додатку для фінансового управління, що включає інноваційні технології, починається з ідеї використання алгоритмів машинного навчання для оптимізації фінансових рішень. Ключовим моментом є те, що ці технології можуть адаптуватися до потреб користувачів, надаючи їм персоналізовані рекомендації. Визначення цілей проекту зосереджене на використанні великих даних для вдосконалення фінансових рішень, а також на розробці інтуїтивно зрозумілого інтерфейсу для зручності користувачів [3].

Розробка прототипу передбачає оцінку того, як нові технології можуть трансформувати фінансове управління через персоналізацію та автоматизацію процесів. Під час тестування проекту важливо забезпечити ефективність алгоритмів і належний захист даних користувачів.

Після запуску проекту важливим є моніторинг і оптимізація на основі відгуків користувачів, що дозволяє вдосконалювати алгоритми. Оновлення та підтримка продукту забезпечують його актуальність і відкривають нові можливості для інновацій.

Інтеграція нових технологій в додатки для управління фінансами дає користувачам низку переваг, серед яких: висока персоналізація, автоматизація процесів та прогнозування фінансових трендів. Завдяки цьому, користувачі отримують можливість більш ефективно управляти своїми фінансами, досягати фінансових цілей та підвищувати свою фінансову стабільність , сприяє оптимізації фінансових стратегій та забезпеченню більшої довгострокової економічної стійкості.

Список використаних джерел:

1. Stfalcon. Розробка фінтех-додатків: тенденції, особливості та перспективи. URL: https://stfalcon.com/uk/blog/post/fintech-app-development-trends-features-perspective

2. Domination over AI. ШІ у фінансах: 7 проривних застосувань. URL:https://dominion-overai.com/ai-in-finance-7-breakthrough applications/

3. Unite.ai. Штучний інтелект у фінансах: випадки використання, переваги та проблеми. URL: https://www.unite.ai/uk/Переваги-та-проблеми-використання-штучного-інтелекту-уфінансах/

УДК 004.4

Кондратюк О.В., магістрант,
Нічепорук А.О., к.т.н., доцент
кафедри комп'ютерної інженерії та
інформаційних систем
Хмельницький національний університет

ІНТЕЛЕКТУАЛЬНА СИСТЕМА КОНТРОЛЮ ТА БЕЗПЕКИ ДЛЯ СИСТЕМИ «РОЗУМНОГО БУДИНКУ»

На сьогоднішній день технології розумного будинку набувають все більшої популярності, оскільки дозволяють автоматизувати повсякденні процеси, підвищувати рівень комфорту мешканців та забезпечувати ефективний контроль безпеки житлових приміщень. З кожним роком зростає кількість розумних пристроїв, що взаємодіють між собою в межах єдиної екосистеми, створюючи складні розподілені системи управління. Одним із ключових завдань сучасних технологій є забезпечення надійного захисту таких систем від зовнішніх і внутрішніх загроз, що включає фізичну охорону, кібербезпеку, контроль доступу та аналіз поведінкових особливостей користувачів.

Безпека в концепції розумного будинку є складною та багатоаспектною задачею, яка включає в себе не тільки захист житла від фізичних проникнень, але й контроль доступу до приміщень, а також оперативне реагування на потенційні загрози, серед яких особливу увагу слід приділити таким, як витоки газу, води або виникнення пожежі [1]. Окремою важливою складовою є забезпечення конфіденційності та захисту персональних даних мешканців [2]. Варто зазначити, що традиційні підходи до забезпечення безпеки, зокрема використання механічних замків, класичних систем відеоспостереження чи ручних методів управління сигналізацією, стають менш ефективними [2]. Це пояснюється необхідністю постійного контролю з боку користувача, що є незручним у сучасних умовах, а також недостатнім рівнем інтеграції цих рішень у єдину екосистему домашньої автоматизації.

З огляду на ці виклики, сучасні тенденції в сфері домашньої безпеки орієнтовані на активне використання можливостей штучного інтелекту, глибокого аналізу великих масивів даних та автоматизації процесів з моніторингу і реагування на загрози у режимі реального часу [1; 4]. Істотний поштовх розвитку цього напряму дало поширення технологій Інтернету речей (IoT), завдяки яким стало можливим створення розподілених сенсорних мереж. Застосування алгоритмів машинного навчання дозволяє значно підвищити точність ідентифікації

потенційних загроз та дає системі можливість самостійно адаптуватись до змін у поведінці мешканців чи параметрів навколишнього середовища [4].

Основною метою даного дослідження є розробка комплексного підходу, що дозволяє створити надійну інтелектуальну систему безпеки для розумних будинків. Запропонована в дослідженні концепція передбачає використання аналітичних моделей для аналізу поведінки користувачів, автоматичне керування пристроями та багаторівневу систему захисту інформації. В межах цього дослідження також здійснюється аналіз існуючих рішень, визначаються їхні переваги та обмеження [1; 3].

В основу структури системи покладено три основні функціональні рівні: сенсорний, рівень аналітичної обробки інформації та рівень взаємодії з користувачем. Такий підхід дозволяє реалізувати ефективний процес збирання інформації, оперативного виявлення загроз та ухвалення відповідних рішень у режимі реального часу [1].

На першому, сенсорному рівні, здійснюється безперервний збір інформації про параметри внутрішнього середовища будинку та зовнішні фактори. До складу сенсорного рівня входять різноманітні датчики, зокрема датчики руху, температури, вологості, освітленості, а також сенсори, що реагують на дим, витоки газу та води. Другий рівень — це рівень обробки інформації, що відповідає за аналіз отриманих даних та ухвалення рішень. На цьому рівні реалізуються передові алгоритми машинного навчання, які дозволяють системі передбачати ймовірні загрози, своєчасно розпізнавати незвичні або небезпечні ситуації, а також контролювати доступ до приміщень [4].

Список використаних джерел:

1. Taiwo, O., Ezugwu, A. E., Ikotun, A. M., Oyelade, O. N., Almutairi, M. S. (2021). Internet of Things-Based Intelligent Smart Home Control and Security System. Security and Communication Networks, 2021, 1–17. DOI: 10.1155/2021/9928254.

2. Аніщенко, В. О. (2020). Технології Інтернету речей у сучасних розумних будинках: проблеми безпеки та захисту даних. Інформаційна безпека, 26(4), 345–352. DOI: 10.18372/2410-7840.26.15621.

3. Pacheco, J., & Hariri, S. (2021). IoT security framework for smart homes: An overview and research challenges. Journal of Network and Computer Applications, 174, 102867. DOI: 10.1016/j.jnca.2020.102867.

4. Kuzlu, M., Fair, C., & Guler, O. (2021). Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity. IEEE Internet of Things Journal, 8(21), 15833–15854. DOI: 10.1109/JIOT.2021.3079274.

УДК 004.056

Міщук В.С., магістрант,
Граф М.С., Ph.D, зав. кафедри КН
Державний університет «Житомирська політехніка»

ОПТИМІЗАЦІЯ ІНФОРМАЦІЙНИХ ПОТОКІВ У СИСТЕМАХ УПРАВЛІННЯ ПРОЕКТАМИ

Вступ. У сучасному управлінні проектами ефективний обмін інформацією відіграє ключову роль. Неконтрольований потік даних, дублювання повідомлень та нестача структурованої комунікації можуть призводити до зниження продуктивності команд. Системи управління проектами (СУП) забезпечують автоматизацію інформаційних потоків, проте їх ефективність залежить від правильної організації цих потоків. Оптимізація інформаційних потоків дозволяє зменшити перевантаження даними, підвищити швидкість прийняття рішень та покращити координацію команди.

Аналіз джерел. Проблематика управління інформаційними потоками у СУП широко досліджується в наукових і практичних джерелах. У роботах [1,2] розглядаються підходи до автоматизації обміну даними в проектах, а також аналізується вплив ефективної комунікації на продуктивність команд. Згідно з дослідженням McKinsey [3], лише 26% проєктів досягають успіху, що вказує на необхідність покращення процесів управління та аналізу даних у проектах.

Мета дослідження. Дослідити методи оптимізації інформаційних потоків у системах управління проектами та запропонувати шляхи їх покращення.

Виклад основного матеріалу. Одним із ключових аспектів оптимізації інформаційних потоків є правильна організація обміну даними між учасниками проекту. В межах СУП інформаційні потоки можна поділити на:

- **Вертикальні потоки** – передача завдань між рівнями управління (PM → Виконавець).
- **Горизонтальні потоки** – обмін інформацією між членами команди (Розробник ↔ Аналітик).
- **Зовнішні потоки** – взаємодія із замовниками, підрядниками та зовнішніми API-інтеграціями.

Основні проблеми інформаційних потоків у СУП:

1. **Дублювання повідомлень та інформаційне перевантаження.** Команда отримує багато несуттєвих сповіщень.

2. **Неструктуровані оновлення статусів задач.** Відсутність централізованого контролю змушує користувачів витрачати час на пошук актуальної інформації.
3. **Фрагментація каналів комунікації.** Використання декількох платформ (email, месенджери, Jira) призводить до втрати важливих деталей.

Методи оптимізації:

- **Централізація комунікації.** Використання єдиної СУП (наприклад, Jira, ClickUp) з інтеграцією всіх каналів комунікації.
- **Автоматизація оновлень статусів.** Використання правил автоматичного зміни статусів задач.
- **Фільтрація та пріоритезація інформації.** Впровадження рівнів доступу до інформації та налаштування персоналізованих сповіщень.
- **Використання AI та аналітики.** Алгоритми машинного навчання можуть аналізувати продуктивність команди та рекомендувати оптимальні стратегії розподілу інформації.

Висновки. Оптимізація інформаційних потоків у СУП дозволяє підвищити ефективність командної роботи, зменшити перевантаження інформацією та покращити швидкість прийняття рішень. Використання централізованих платформ, автоматизація рутинних процесів та впровадження інтелектуальних аналітичних систем є ключовими напрямками розвитку сучасних СУП. Подальші дослідження можуть бути зосереджені на інтеграції AI для прогнозування інформаційних потоків та оптимізації комунікацій у великих проектах.

Список використаних джерел:

1. Свінцицька О. М. Інформаційні технології в управлінні внутрішніми комунікаціями ІТ-проектів / О. М. Свінцицька // Збірник тез XI Міжнародної науково-технічної конференції «Інформаційно-комп'ютерні технології – 2020» (09–11 квітня 2020 р., м. Житомир). – Житомир : Житомирська політехніка, 2020. – С. 64–65.

2. Антоненко В. М. Сучасні інформаційні системи і технології: управління знаннями : навч. посібник / В. М. Антоненко, С. Д. Мамченко, Ю. В. Рогушина. – Ірпінь : Нац. університет ДПС України, 2016. – 212 с.

3. McKinsey. Unlocking success in digital transformations. [Електронний ресурс]. – Режим доступу: https://www.mckinsey.com/capabilities/people-and-organizational-performance/our-insights/unlocking-success-in-digital-transformations.

УДК 004.94:794.8:004.3

Матяш О.В., магістрант,
Марчук Г.В., ст. викладач
Державний університет «Житомирська політехніка»

ВПЛИВ ТЕХНОЛОГІЇ LUMEN НА ЯКІСТЬ ІГРОВОГО ПРОЦЕСУ

Все частіше ігри розробляють з використанням рушія Unreal Engine, який став стандартом у галузі завдяки своїй гнучкості та можливостям. Unreal Engine 5 використовується у відомих проектах, таких як Fortnite, The Matrix Awakens і Hellblade II, демонструючи потужність та реалізм нових технологій.

Lumen - це передова технологія динамічного глобального освітлення та відбиттів, яка вперше була представлена в Unreal Engine 5 компанією Epic Games [1]. Вона використовує поєднання Signed Distance Fields (SDF), voxel-технології та просунутих алгоритмів трасування освітлення в реальному часі. Головна перевага Lumen полягає у здатності забезпечувати реалістичне освітлення динамічних сцен без потреби у попередньо запечених (baked) джерелах світла чи відбиттях, що значно спрощує роботу розробників.

На відміну від технології RTX (Ray Tracing), яка вимагає спеціалізованих RT-ядер на відеокарті, Lumen працює на широкому спектрі пристроїв, включаючи консолі нового покоління (PlayStation 5, Xbox Series X) та середньопродуктивні ПК, що робить її більш доступною для масового використання.

Для аналізу було проведено тестування (Таблиця 1) гри Fortnite, яка була оновлена під Unreal Engine 5 та використовує Lumen для глобального освітлення. Дослідження проводилося на максимальних налаштуваннях графіки у роздільній здатності 1080p.

Таблиця 1

Режим	Середній FPS	Основні особливості
Lumen Off	120 FPS	Максимальна продуктивність, але менш реалістичне освітлення і прості тіні.
Lumen On(High)	80–90 FPS	Помітне покращення освітлення та тіней, реалістичні відбиття, проте втрата ~30% продуктивності.
Lumen On (Epic)	60–70 FPS	Високий рівень візуалізації: складні тіні, точні відбиття, глобальне освітлення, але втрата до 40% продуктивності.

Результати (рис.1) показують, що ввімкнення Lumen на високих або епічних налаштуваннях суттєво покращує якість зображення, забезпечуючи реалістичні ефекти освітлення та відбиттів, які критично важливі для створення занурення у віртуальне середовище. Наприклад, світлові джерела природно взаємодіють з об'єктами, тіні мають м'які краї та враховують вторинне освітлення, а поверхні точно відбивають довкілля.

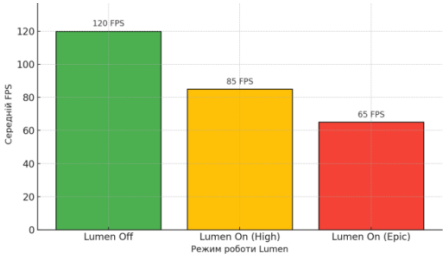


Рис.1. Вплив технології Lumen на продуктивність

Однак ці візуальні переваги супроводжуються зниженням продуктивності, що слід враховувати розробникам при балансуванні між графікою і плавністю ігрового процесу. У багатокористувацьких іграх, де продуктивність має критичне значення, доцільніше використовувати середні або низькі налаштування Lumen. У сюжетних та одиночних іграх, де важливіше враження від графіки, Lumen на «Епіс» забезпечує максимально реалістичний вигляд.

На відміну від RTX (Ray Tracing), який виконує трасування променів для створення освітлення та відбиттів, Lumen дозволяє отримати схожий рівень якості без необхідності мати дорогу відеокарту з RT-ядрами. Проте RTX має перевагу у складних сценах з великою кількістю дзеркальних поверхонь та точних відбиттів. Комбінація DLSS (Deep Learning Super Sampling) і RTX у конкурентних технологіях NVIDIA дозволяє частково компенсувати втрати продуктивності, аналогічно тому, як Lumen поєднується із Nanite (технологією мікрополігональної геометрії) для оптимізації роботи в Unreal Engine 5.

Технологія Lumen у Unreal Engine 5 демонструє новий рівень якості глобального освітлення, забезпечуючи реалістичне світлове середовище навіть у динамічних сценах. Незважаючи на вплив на продуктивність, Lumen відкриває нові горизонти для розробників.

Список використаних джерел:

1. T. W. Tan. Mastering Lumen Global Lighting in Unreal Engine 5 У: Game Development with Unreal Engine 5 Volume 1: Design Phase / T. W. Tan – Berkeley, California: Apress, 2024. – С. 223-275.

УДК 004:42

Левицький А.А., магістрант,
Левківський В.Л., Ph.D, доцент
Державний університет «Житомирська політехніка»

МЕТОДИ ІНТЕГРАЦІЇ НЕЙРОННИХ МЕРЕЖ В ІГРОВІ ДОДАТКИ НА БАЗІ РУШІЯ UNITY, ЇХ ПЕРЕВАГИ ТА НЕДОЛІКИ

Нейронні мережі є потужним інструментом для аналізу та генерування даних. Для ігрових додатків вони можуть надати великі можливості у створенні тексту діалогів, поведінки об’єктів або навіть кардинально нових шляхів побудови ігроладу. Однак стоїть питання правильно підібраного методу інтеграції нейронної мережі в конкретній ситуації, особливо якщо інструмент, на якому розробляється ігровий додаток, відстає в роботі зі складними мережами. До таких також відноситься мова програмування C#, яка застосовується у популярному серед розробників ігровому рушії Unity.

Існує три основні методи інтеграції нейронної мережі в ігровий додаток на обраному рушії, а саме:

1. Створити нейронну мережу всередині ігрового додатка за допомогою мови програмування C#;
2. Використати пакунок Sentis ігрового рушія Unity та за допомогою бібліотеки ONNX (Open Neural Network Exchange) інтегрувати модель нейронної мережі, створеної іншим інструментом;
3. Запустити окрему програму на віддаленому сервері з нейронною мережею, до якої буде звертатись ігровий додаток.

Перший метод передбачає створення, навчання та використання нейронної мережі в ігровому додатку, використовуючи мову програмування C# та її бібліотек. Метод реалізує мережу всередині ігрового додатка та дає повний контроль над нею, а саме змінювати структуру, перенавчати мережу за допомогою вдосконалених наборів даних тощо. Однак він не є оптимальним при роботі з величезними наборами даних та тренування глибоких нейронних мереж. Також бібліотеки обраної мови обмежено використовують переваги графічних процесорів, що сповільняє мережу в порівнянні з конкурентами.

Другий метод полягає у застосуванні бібліотеку ONNX [1], яка дозволяє експортувати будь-яку нейронну мережу в модель та імпортувати в інше середовище зі всіма перевагами. Це дозволяє використовувати як існуючі мережі, так і створювати власні за допомогою кращих інструментів для створення та навчання мереж, як от мова Python та її бібліотеки. Однак метод не дозволяє напряму

перенавчити імпортовану модель та обмежено може змінити її структуру, що не є гнучким у випадках, коли є намір динамічно доповнювати набір даних мережі. У випадку з ігровим рушієм Unity, пакунок Sentis [2] оптимізує використання такого методу.

Третій метод використовує сервер з нейронною мережею, до якого звертається додаток для отримання результату. Це дозволяє гравцям з непотужними системами грати в ігри зі складними нейронними мережами, а для розробників дає можливість їх вдосконалювати без потреби в змінах додатка. В такому разі мережу можна реалізувати за допомогою сторонніх інструментів та не виконувати імпорт для інтеграції в додаток. Однак метод потребує додаткових витрат та підтримки, що робить додаток актуальним лише певний проміжок часу, адже зазвичай сервери для подібних цілей підтримуються не довго.

В результаті було розглянуто три методи інтеграції нейронних мереж в ігрові додатки на базі рушія Unity та мови програмування C#. Після їх аналізу було зроблено наступні висновки щодо кожного з методів:

1. Створення нейронної мережі всередині додатка дає повний контроль над нею та не потребує додаткових інструментів, однак метод не підходить для глибокого навчання та обмежено використовує графічні процесори. Ним доречно інтегрувати прості мережі, а також проводити дослідження щодо їх роботи;
2. Використання пакунку Sentis та бібліотеки ONNX дають змогу створювати нейронні мережі за допомогою бажаних інструментів, а також використовувати існуючі моделі мереж, однак метод не дозволяє динамічно покращувати набори даних. Метод є універсальним та підходить для задач, де потрібні саме обчислювальні переваги мереж;
3. Сервер дає змогу вдосконалювати та керувати нейронною мережею без залежності до додатка, що дає змогу використовувати складні мережі з повним контролем та не навантажувати системи користувачів. Але метод потребує додаткових витрат та підтримки, а також він не довговічний. Він підходить для багатокористувацьких додатків, де результат обчислень повинен бути схожим у всіх, або в додатках зі складними нейронними мережами.

Список використаних джерел:

1. The Linux Foundation. Open Neural Network Exchange. 2019. URL: https://onnx.ai/ (дата звернення 19.02.2025).
2. Unity Manual. Sentis overview. 2025. URL: https://docs.unity3d.com/Packages/com.unity.sentis@2.1 (дата звернення: 19.02.2025).

УДК 004.7

Іванов Д.А., аспірант,
Єфіменко А.А., к.т.н., завідувач кафедри КІ та КБ
Державний університет «Житомирська політехніка»

ОГЛЯД ПІДХОДІВ ДО ОПТИМІЗАЦІЯ ВИБОРУ НАВЧАЛЬНИХ ДАНИХ У ПРОЦЕСІ САМОНАВЧАННЯ МОДЕЛЕЙ ІДЕНТИФІКАЦІЇ ОБ'ЄКТІВ

У задачах ідентифікації об'єктів глибокі нейронні мережі демонструють високу ефективність, проте їх самонавчання є обчислювально затратним процесом, що ускладнює їх оперативну адаптацію до нових даних. Одним із ключових чинників, що визначає швидкість і ефективність самонавчання, є стратегія відбору навчальних прикладів. Традиційні підходи, зокрема випадковий або рівномірний вибір даних, не забезпечують оптимального використання обчислювальних ресурсів. Водночас у контексті реальних застосувань систем ідентифікації об'єктів критично важливо забезпечити ефективне навчання моделі на обмеженій вибірці, фокусуючись на найбільш інформативних зразках.

Одним із способів оптимізації вибору навчальних даних є метод активного навчання. Даний підхід дозволяє зменшити необхідний обсяг анотованих даних шляхом вибору найбільш інформативних навчальних прикладів. Його основна концепція полягає в наданні моделі можливості самостійно визначати зразки з великого пулу неанотованих даних, які, згідно з її оцінкою, матимуть найбільший вплив на покращення її продуктивності. Такий підхід сприяє зниженню вимог до обсягу навчальної вибірки, скороченню витрат на процес маркування даних та підвищенню ефективності навчання моделі [1,2].

Є декілька підходів для реалізації методу активного навчання оптимізації вибору даних. Одним із найбільш поширених підходів є **метод невизначеного вибору,** який ґрунтується на принципі відбору зразків, для яких модель демонструє найменшу впевненість у прогнозах. Основна ідея цього підходу полягає в тому, що навчання на найбільш невизначених прикладах дозволяє суттєво покращити узагальнювальні властивості моделі, скорочуючи кількість необхідних анотованих даних.

Є декілька способів реалізації методу невизначеного вибору:

- **Entropy-based sampling** – вибір прикладів, для яких ентропія розподілу ймовірностей прогнозованих класів є максимальною.

- **Margin Sampling** – вибір прикладів, для яких різниця між ймовірностями двох найбільш ймовірних класів є мінімальною.
- **Least Confident Sampling** – вибір прикладів, для яких ймовірність найбільш ймовірного класу є мінімальною.

Метод невизначеного вибору ефективний у випадках, коли модель стикається з раніше невідомими класами або варіаціями об'єктів, що дозволяє зосередити ресурси на найкритичніших зразках [1,3].

Ще один популярний підхід - метод **комітетного запиту. Даний підхід** використовує ансамбль моделей (так званий "комітет") для оцінки невизначеності щодо нового зразка даних. Основна ідея даного методу полягає в тому, що якщо моделі в комітеті мають значні розбіжності у прогнозах щодо певного прикладу, цей зразок є інформативним і повинен бути включений у вибірку для анотації.

Основні принципи методу **комітетного запиту**:

- Формування комітету моделей.
- Оцінка невизначеності на основі розбіжностей між прогнозами.
- Вибір найбільш суперечливих прикладів для анотації.

Поєднання методу **комітетного запиту** із самонавчанням дозволяє ефективніше адаптувати моделі до нових даних, мінімізуючи витрати на анотацію.

Отже, активне навчання є потужним підходом до оптимізації процесу самонавчання моделей ідентифікації об’єктів, дозволяючи суттєво зменшити обсяг необхідних анотованих даних та прискорити процес навчання. Метод невизначеного вибору дозволяє моделі зосередитися на випадках, у яких вона демонструє найменшу впевненість, тоді як комітетний підхід використовує розбіжності в прогнозах різних моделей для виявлення суперечливих прикладів. Подальші дослідження будуть спрямовані на розробку гібридних методів, що комбінують переваги різних стратегій активного навчання для досягнення ще вищої ефективності самонавчання моделей.

Список використаних джерел:

1. Settles B. Active Learning // Synthesis Lectures on Artificial Intelligence and Machine Learning. – Morgan & Claypool, 2012. – 123 p.

2. Olsson F. A literature survey of active machine learning in the context of natural language processing. – Swedish Institute of Computer Science, 2009. – 47 p.

3. Wang K., Zhang D., Li Y. Cost-effective active learning for deep image classification // IEEE Transactions on Circuits and Systems for Video Technology, 2020. P. 1441–1452.

УДК 004.04: 004.78

Лукомський І.Ю., здобувач,
Марчук Г.В., ст. викладач
Державний університет «Житомирська політехніка»

МИНУЛЕ, СЬОГОДЕННЯ, МАЙБУТНЄ ІГРОВОЇ ІНДУСТРІЇ

Ігрова індустрія залишається однією з найдинамічніших сфер сучасної культури та економіки. З моменту появи перших відеоігор у 70-х роках, вона пройшла шлях від простих аркадних ігор до складних інтерактивних світів із передовими технологіями. Сьогодні це багатомільярдна галузь, яка об'єднує мистецтво, науку й технології.

Простежимо шлях, який пройшла ігрова індустрія, від своїх простих витоків до складних імерсивних досвідів, які маємо сьогодні. Початок ігрової індустрії припадає на 70-ті роки, коли з'явилися перші аркадні ігри, такі як Pong (1972). У 80-х роках популярність отримали домашні консолі, наприклад, Nintendo Entertainment System (NES), що зробило відеоігри доступними для широкої аудиторії. 90-ті роки стали періодом значного технічного прогресу. Перехід до 3D-графіки, поява таких класичних ігор, як Doom (1993) і Final Fantasy VII (1997), заклали фундамент для сучасних ігрових стандартів.

На сьогодні ігри стали частиною повсякденного життя мільйонів людей. Вони використовуються не лише для розваг, а й для освіти, тренувань і навіть терапії. Дослідження [1, 2, 3] доводить, що ігри можуть стати ефективним інструментом для покращення психічного здоров'я.

Інновації у графіці, штучному інтелекті та геймдизайні дозволяють створювати ігри з реалістичною графікою та складними сюжетами. Наприклад, віртуальна реальність (Virtual reality, VR) і доповнена реальність (Augmented reality, AR) відкривають нові горизонти для інтерактивного досвіду. Доповнена реальність має потенціал кардинально змінити освітній процес. Завдяки інтерактивності в режимі реального часу, різноманітним форматам візуалізації та поєднанню фізичного та цифрового світів, AR відкриває нові горизонти для викладання та навчання, роблячи їх більш захоплюючими та ефективними [4, 5, 6].

Інтернет дозволив розвивати онлайнігри та масові багатокористувацькі проєкти (World of Warcraft, Fortnite). Поява платформ для мобільних ігор, таких як App Store та Google Play, зробила відеоігри доступними для мільярдів людей. Станом на сьогодні відеоігри є одним із найбільших сегментів розважальної індустрії.

Гравці мають доступ до широкого спектра жанрів, від класичних платформерів і стратегій до багатокористувацьких онлайн-ігор (MMORPG) та інді-проектів. Інді-ігри, які створюються невеликими командами або навіть окремими розробниками, набули популярності завдяки платформам, як-от Steam і Epic Games Store. Вони дозволяють експериментувати з геймплеєм і сюжетами.

Індустрія відеоігор переживає епоху трансформації, зумовлену стрімким розвитком технологій. Мобільний геймінг, завдяки своїй доступності, захопив мільйони гравців по всьому світу. Кіберспорт став не просто розвагою, а повноцінною професійною сферою з величезними призовими фондами та мільйонами глядачів. Хмарні ігри стирають межі між платформами, дозволяючи запускати вимогливі проекти на будь-якому пристрої. Метавсесвіт, що поєднує ігри, соціальні мережі та віртуальну реальність, стає дедалі популярнішим. Штучний інтелект, у свою чергу, робить ігровий досвід більш реалістичним та адаптивним.

Список використаних джерел:

1. Dewhirst A., Laugharne R., Shankar R. Therapeutic use of serious games in mental health: scoping review //BJPsych open. – 2022. – Т. 8. – №. 2. – С. e37.

2. Thabrew H. et al. E-Health interventions for anxiety and depression in children and adolescents with long-term physical conditions //Cochrane Database of Systematic Reviews. – 2018. – №. 8.

3. Dewhirst A., Laugharne R., Shankar R. Therapeutic use of serious games in mental health: scoping review //BJPsych open. – 2022. – Т. 8. – №. 2. – С. e37.

4. Alfaro J. L. D., Puyvelde P. V. Mobile augmented reality apps in education: Exploring the user experience through large-scale public reviews //Augmented Reality, Virtual Reality, and Computer Graphics: 8th International Conference, AVR 2021, Virtual Event, September 7–10, 2021, Proceedings 8. – Springer International Publishing, 2021. – С. 428-450.

5. Vakaliuk, T. A., Marchuk, G. V., Levkivskyi, V. L., Morgun, A. M., & Kuznietsov, D. V. (2021, December). Development of AR Application to Promote the Historical Past of the Native Land. In Digital Humanities Workshop (pp. 125-131).

6. Lee J. Problem-based gaming via an augmented reality mobile game and a printed game in foreign language education //Education and Information Technologies. – 2022. – Т. 27. – №. 1. – С. 743-771.

УДК 004.932.72:004.932.4

Голенко М.Ю., аспірант,
Єфіменко А.А., к.т.н., доцент
Державний університет «Житомирська політехніка»

ОПТИМІЗАЦІЯ ВИЯВЛЕННЯ МАЛИХ ОБ'ЄКТІВ З БПЛА ЗА ДОПОМОГОЮ UPSCALE-МОДЕЛІ ESRGAN

Розпізнавання малих об'єктів на аерофотознімках, отриманих з безпілотних літальних апаратів (БПЛА), є складним завданням через низьку роздільну здатність та втрату важливих деталей. Традиційні методи обробки зображень часто не дають змогу досягти високої точності при ідентифікації об'єктів невеликого розміру. Один із можливих шляхів розв'язання цієї проблеми полягає у використанні алгоритмів підвищення роздільної здатності (super-resolution), зокрема ESRGAN (Enhanced Super-Resolution Generative Adversarial Network) [1].

ESRGAN – це покращена модель суперрезолюції на основі GAN, що підвищує деталізацію зображень. Використовуючи архітектуру RRDB та спеціальну функцію втрат, вона зберігає структуру об'єктів і усуває розмиття. На відміну від бікубічної інтерполяції, яка спричиняє втрату даних, ESRGAN відновлює деталі завдяки генеративному навчанню.

Підхід базується на використанні нейромережевої моделі Faster R-CNN для попереднього виявлення об'єктів на зображенні. Після цього фрагменти зображень, що містять потенційно важливі об'єкти, передаються у хмарне середовище, де виконується їх масштабування та покращення за допомогою ESRGAN. Це дозволяє зберегти текстури та структуру малих об'єктів, що покращує їх подальше розпізнавання.

Процес виявлення та покращення малих об'єктів із використанням ESRGAN включає кілька етапів:

1. БПЛА здійснює зйомку території, отримуючи аерофотознімки у режимі реального часу.
2. Faster R-CNN виконує початкову детекцію, визначаючи можливі об'єкти на знімку. Мережа ідентифікує об'єкти та визначає їх класову приналежність із певною ймовірністю.
3. Області з виявленими малими об'єктами вирізаються для подальшої обробки. Якщо об'єкт занадто малий для точного розпізнавання, відбувається фільтрація об'єкту для більш точного визначення.
4. Якщо рівень достовірності визначення об'єкта перевищує 90%, або присутні додаткові ознаки (контекст зображення, розмір об'єкта, умови освітлення), тоді фрагмент одразу передається на остаточну

класифікацію. Якщо ж значення ≤ 90%, дані передаються на додаткову обробку у хмарне середовище.

5. Виділені фрагменти надсилаються на хмарний сервер для обробки за допомогою ESRGAN. Для цього використовується оптимізований механізм передачі даних через мобільні мережі (4G/5G) або супутниковий зв'язок. Обробка у хмарі дозволяє уникнути обмежень на обчислювальні ресурси безпілотника.

6. Хмарний сервер виконує покращення роздільної здатності, підвищуючи деталізацію об'єкта без втрати ключових ознак. ESRGAN виконує upscale зображення, забезпечуючи реалістичне відновлення деталей.

7. Покращені зображення повертаються на обчислювальний модуль БПЛА або наземної станції для подальшого аналізу та остаточної класифікації.

8. У разі необхідності результати можуть бути тимчасово збережені у хмарному сховищі для подальшого.

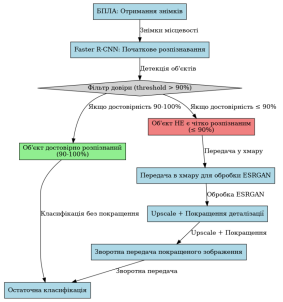


Рис. 1. Блок-схема роботи системи з використанням ESRGAN.

Комбіноване використання Faster R-CNN та ESRGAN дозволяє підвищити точність розпізнавання малих об'єктів на аерофотознімках, усуваючи проблему низької деталізації без необхідності зниження висоти польоту. Використання порогового значення достовірності детекції дозволяє мінімізувати витрати на передачу та обчислення, спрямовуючи ресурси лише на об'єкти, що потребують покращеної деталізації. Інтеграція хмарних обчислень забезпечує ефективне масштабування та швидку обробку великих обсягів даних.

Список використаних джерел:

1. Wang X., Yu K., Wu S., Gu J., Liu Y., Dong C., Loy C. C., Qiao Y., Tang X. ESRGAN: Enhanced Super-Resolution Generative Adversarial Networks // Proceedings of the European Conference on Computer Vision Workshops (ECCVW 2018). – Мюнхен, 2018. – С. 63–79.

УДК 004.925.8

Ганнущенко О.В., магістрант,
Марчук Г.В., ст. викладач
Державний університет «Житомирська політехніка»

АЛГОРИТМИ АДАПТИВНОЇ АНІМАЦІЇ ПЕРСОНАЖІВ ДЛЯ ДИНАМІЧНОГО СЕРЕДОВИЩА У ВІДЕОІГРАХ

Одним із важливих завдань сучасних відеоігор є забезпечення високого рівня реалістичності та якості ігрового процесу. У цьому контексті особливо важливою складовою є адаптивна анімація персонажів, яка дозволяє автоматично підлаштовувати рух до змінних умов середовища [1].

Особливого значення набуває така адаптивність у жанрі метроідванія, де персонаж часто взаємодіє зі складними, динамічними і багаторівневими локаціями і перебуває у постійних бойових ситуаціях. Це потребує створення ефективних алгоритмів, які дозволяють анімаційній системі швидко й точно пристосовуватися до змінних умов гри.

Сучасні ігри вимагають складної та динамічної взаємодії персонажів із середовищем. Традиційна анімація, яка базується на заздалегідь підготовлених анімаційних циклах, має низку недоліків: вона недостатньо адаптивна, вимагає великої кількості ресурсів для створення великої анімаційної бази і не завжди може забезпечити адекватну реакцію персонажа на мінливі ігрові ситуації. Тому виникає проблема пошуку алгоритмічних підходів для ефективної реалізації адаптивної анімації на основі процедурного та кінематичного контролю анімацій, який дозволить динамічно підлаштовувати рухи персонажів до реальних та змінних умов ігрового середовища.

Для вирішення виявленої наукової проблеми пропонується зосередитися на алгоритмічних підходах, зокрема на динамічному позиціюванні персонажів.

Для адаптивної анімації використовується алгоритм інверсної кінематики (ІК), що забезпечує динамічну корекцію позиції кінцівок і тіла персонажа в залежності від нахилу поверхонь, перепон, позиції ворогів та інших об'єктів [2].

Базовий алгоритм корекції руху складається з наступних етапів:

1. Визначення точок контакту у ігровому середовищі.
2. Визначення нормалей до поверхні.
3. За допомогою ІК, коригується положення кінцівок.

4. Для забезпечення стійкості персонажа, перераховується та балансується його загальна поза.

Математично це визначається наступним чином:

$$P_{new} = P_{old} + IK(N, \theta, L)$$

де P_{new}-скориговане, нове положення кінцівки; P_{old}- початкове положення; IK - інверсна кінематика; N - нормаль до поверхні; θ - кут нахилу; L - довжина сегменту кінцівки.

З метою оптимізації роботи системи планується впровадження буферизації та LOD-анімації. Ці інструменти забезпечать автоматичну адаптацію рівня деталізації анімації до відстані від камери та потужності пристрою.

Традиційні методи анімації передбачають статичні або заздалегідь записані рухи, що створює обмеження як у взаємодії персонажів, так і у продуктивності гри через суттєву ресурсомісткість великих об'ємів анімаційних наборів. Запропонований адаптивний підхід, що базується на процедурній побудові та алгоритмічній адаптації, суттєво зменшує необхідність великої кількості ручних анімацій, забезпечує візуальну якість та більш гнучкий і цікавий ігровий досвід.

Теоретична значущість дослідження полягає в його внеску в теорію розробки гнучких адаптивних анімаційних систем з використанням процедурних алгоритмів та машинного навчання. Практичною цінністю є безпосереднє впровадження представлених результатів у комерційні ігрові проєкти, що дозволяє покращити ігровий досвід з одночасною оптимізацією використання обчислювальних ресурсів.

У запропонованому методі процедурної адаптивної анімації, пропонуються алгоритмічно-кінематичні методи та елементи оптимізації через кадрову адаптацію (LOD-анімації).

Таким чином, розроблений метод створює основу для подальших досліджень у галузі створення розширених інтерактивних ігрових систем з погляду технологічних можливостей процедурної анімації.

Список використаних джерел:

1. Christo A. Procedural Creature Generation and Animation for Games. Bournemouth: Bournemouth University, 2022. URL:https://nccastaff.bournemouth.ac.uk/jmacey/MastersProject/MSc22/01/ProceduralCreatureGenerationandAnimationforGames.pdf

2. Cadevall Soto L. Procedural Generation of Animations with Inverse Kinematics. 2021. URL: https://hdl.handle.net/2445/182237

УДК 004.8

Бондар В.В., аспірант,
Бабенко В.Г., д.т.н., професор,
Черкаський державний технологічний університет

СУЧАСНІ ПІДХОДИ ПОКРАЩЕННЯ ЕФЕКТИВНОСТІ МЕХАНІЗМУ ЕМБЕДІНГІВ ТРАНСФОРМЕРІВ

Моделі трансформерів стали основою сучасних систем штучного інтелекту. Важливою частиною цієї архітектури є механізми ембедінгів, які перетворюють вхідні дані у високорозмірні вектори, придатні для self-attention операцій. Але ці шари ембедінгів часто займають значну частину параметрів моделі (35-40%), що зумовлює зниження ефективності в середовищах з обмеженими ресурсами. Tensor-train метод вирішує ці проблеми шляхом розкладання матриць ембедінгів, зменшуючи час обчислень, наприклад розкладаючи тензори розміром 512×768 на тензори розміром 4×16×12×6, зберігаючи при цьому 98,1% початкової перплексії в моделях BERT [1]. Ця факторизація використовує надлишковість параметрів, що особливо ефективно в задачах обробки природної мови [1, 2]. Підходи квантизації пропонують інший шлях до ефективності ембедінгів. SQ-Transformer запроваджує структурно квантовані ембедінги, які групують слова за синтаксичними ролями (наприклад, дієслова/іменники) використовуючи векторну квантизацію. У семантичному аналізі COGS, цей метод досягає 86,7% точності з 4-бітними ембедінгами проти 82,1% для стандартної 8-бітної квантизації [3]. Ключовою інновацією є Systematic Attention Layer, який застосовує однакові шаблони уваги до синтаксично еквівалентних структур, що архітектурно зменшує розмір ембедінгів у 4 рази, одночасно покращуючи композиційну генералізацію [2, 3]. Динамічне призначення бітової ширини базується на підходах квантизації, застосовуючи коригування точності на основі важливості, що включає обчислення значимості токенів через норми градієнтів, виділення 8 бітів для високозначимих токенів, таких як дієслова, і лише 4 бітів для менш значимих токенів, таких як артиклі, обраховуючи компенсації помилок через залишкові з'єднання від високоточних ембедінгів. Попередній аналіз на наборі даних GLUE показує, що цей метод зберігає 97,3% точності BERT-подібних моделей, зменшуючи при цьому середню бітову ширину до 5,2 бітів — на 35% краще стиснення порівняно зі статичною 8-бітною квантизацією [2, 3]. Міждоменне перенесення ембедінгів в роботі [5] з вирівнювання геномів та білків включає навчання універсального енкодера на мультимодальних даних (текст, послідовності білків, мовлення), отримання доменно-специфічних

ембедінгів через низькорангові адаптери (LoRA), та спільне використання основних параметрів ембедінгів для всіх модальностей. Цей метод дозволяє єдиному 768-вимірному простору ембедінгів обслуговувати декілька задач, використовуючи на 40% меншу кількістю параметрів [5, 6]. Розділені ембедінги пропонують покращення в систематичній генералізації шляхом розділення ембедінгів на інваріантні компоненти (синтаксичні ролі) та варіативні компоненти (семантичний зміст), що підвищує систематичність у тестах SCAN на 22% [3]. Сучасні методи покращення механізму ембедінгів балансують ефективність та виразність через квантизацію, декомпозицію та доменну адаптацію. Майбутні напрямки включають динамічні мережі ембедінгів, двостадійний обрахунок ембедінгів, квантизацію простору ембедінгів та інше розширять можливості застосування трансформерів у середовищах з обмеженими ресурсами, зберігаючи архітектурні переваги [1, 4, 3].

Список використаних джерел:

1. Y. Wang et al., "Characterization of MPC-based Private Inference for Transformer-based Models," 2022 IEEE International Symposium on Performance Analysis of Systems and Software (ISPASS), Singapore, 2022, pp. 187-197, doi: 10.1109/ISPASS55109.2022.00025.

2. Liu, Shih-yang, et al. "Llm-fp4: 4-bit floating-point quantized transformers." arXiv preprint arXiv:2310.16836 (2023). https://doi.org/10.18653/v1/2023.emnlp-main.39

3. Jiang, Yichen, Xiang Zhou, and Mohit Bansal. "Inducing systematicity in transformers by attending to structurally quantized embeddings." arXiv preprint arXiv:2402.06492 (2024). https://doi.org/10.48550/arXiv.2402.06492

4. Liang, Z., Wang, P., Zhang, R., Xu, N., Zhang, S., Xing, L., Bai, H., & Zhou, Z. (2024). MERGE: Fast Private Text Generation. Proceedings of the AAAI Conference on Artificial Intelligence, 38(18), 19884-19892. https://doi.org/10.1609/aaai.v38i18.29964

5. Nogin, Yevgeni, et al. "OM2Seq: Learning retrieval embeddings for optical genome mapping." Bioinformatics Advances, Volume 4, Issue 1, 2024, vbae079, https://doi.org/10.1093/bioadv/vbae079

6. Wu, Yueh-Kao, Ching-Yu Chiu, and Yi-Hsuan Yang. "JukeDrummer: Conditional beat-aware audio-domain drum accompaniment generation via Transformer VQ-VAE." arXiv preprint arXiv:2210.06007 (2022). https://doi.org/10.48550/arXiv.2210.06007

УДК 004.9

Валько В.О., магістрант,
Бродський Ю.Б., к.т.н, доцент
Державний університет «Житомирська політехніка»

ВИКЛИКИ ВПРОВАДЖЕННЯ ТЕХНОЛОГІЇ RPA У СУЧАСНІ БІЗНЕС – ПРОЦЕСИ

У сучасному світі автоматизація бізнес-процесів набуває дедалі більшого значення, стаючи ключовим фактором підвищення ефективності організаційної діяльності. Однією з провідних технологій у цій сфері є роботизована автоматизація процесів (RPA), яка дозволяє не лише оптимізувати виконання рутинних завдань, а й значно знизити операційні витрати, покращити точність обробки інформації та забезпечити безперебійну роботу цифрових систем. Однак, незважаючи на суттєві переваги, впровадження RPA супроводжується численними викликами, що потребують комплексного аналізу [1, 2].

Серед основних проблем варто виділити складність інтеграції з IT-інфраструктурою, оскільки у багатьох організаціях використовуються застарілі системи, які не підтримують гнучку автоматизацію через API або мають обмежені можливості взаємодії з програмними роботами. Недостатня готовність персоналу також є серйозним бар'єром, оскільки співробітники можуть сприймати RPA як загрозу для своїх робочих місць, що спричиняє опір змінам і саботаж. Проблеми масштабованості виникають через те, що багато компаній впроваджують RPA на локальному рівні, проте розширення автоматизації на всю організацію часто викликає труднощі, пов'язані з управлінням великим числом роботів [1, 2].

Сучасні підходи до впровадження RPA включають попередній аналіз процесів, вибір оптимальних рішень та їх адаптацію до потреб компанії. Розглянемо кілька популярних платформ для RPA: UiPath – одна з найпоширеніших платформ, що пропонує гнучкі можливості інтеграції, штучний інтелект для аналізу процесів та підтримку масштабованості [3]. Automation Anywhere спеціалізується на інтелектуальній автоматизації, включаючи розпізнавання тексту та обробку документів. Blue Prism орієнтована на корпоративний рівень автоматизації, забезпечує високий рівень безпеки та контрольованість процесів [4]. Окремо варто виділити Power Automate від Microsoft, який є гнучким інструментом для автоматизації бізнес-процесів у середовищі Microsoft 365 та інтеграції з іншими сервісами [5], що робить його ефективним рішенням для компаній, які вже використовують продукти Microsoft.

Для успішного впровадження RPA у бізнес-процеси варто дотримуватися наступних рекомендацій. Поетапне впровадження дозволяє починати автоматизацію з окремих процесів, оцінюючи їх ефективність, а потім масштабувати рішення на всю організацію. Використання аналітики та технологій процесного майнінгу (Process Mining) дозволяє оцінити ефективність процесів до та після впровадження автоматизації. Фокус на безпеці є критично важливим, оскільки програмні роботи працюють з чутливими даними, тому необхідно впроваджувати політики кібербезпеки та захисту інформації [2, 4].

Застосування RPA у різних галузях також має свої особливості. У фінансовому секторі автоматизація використовується для перевірки транзакцій, обробки платежів та управління кредитними заявками [1]. У сфері охорони здоров'я RPA допомагає в управлінні медичною документацією, реєстрації пацієнтів та обробці страхових виплат. Водночас у логістиці програмні роботи оптимізують управління ланцюгами постачання, відстеження вантажів та роботу складів.

Таким чином, технологія RPA є потужним інструментом для оптимізації сучасних бізнес-процесів. Проте її успішне впровадження потребує комплексного підходу, включаючи аналіз існуючих процесів, інтеграцію із сучасними технологіями та підготовку персоналу. Використання сучасних рішень, таких як UiPath, Automation Anywhere, Blue Prism та Power Automate, дозволяє гнучко адаптувати автоматизацію до потреб компанії, підвищуючи її конкурентоспроможність у цифровій економіці.

Список використаних джерел:

1. Муллакара Н., Асокан А. Robotic Process Automation Projects: Build real-world RPA solutions using UiPath and Automation Anywhere. Бірмінгем: Packt Publishing, 2020. – 388 с.

2. Тауллі Т. The Robotic Process Automation Handbook: A Guide to Implementing RPA Systems. Нью-Йорк: Apress, 2020. – 250 с.

3. UiPath Documentation URL: https://docs.uipath.com (дата звернення: 28.02.2025).

4. Blue Prism. Intelligent Automation Platform URL: https://www.blueprism.com (дата звернення: 02.03.2025).

5. Microsoft Power Automate documentation URL: https://learn.microsoft.com/en-us/power-automate/ (дата звернення: 03.03.2025).

УДК 004

Козлик С.О., здобувач,
Болотіна В.В., ст. викладач
Державний університет «Житомирська політехніка»

ТИПОЛОГІЯ СЛОГАНІВ ТА ЇХ РОЗРОБКА У ГРАФІЧНИХ РЕДАКТОРАХ

У сучасних маркетингових кампаніях часто використовується слоган як частина айдентики для формування впізнаваності бренду та комунікації з цільовою аудиторією. Слоган – це коротка та містка фраза, яка легко запам'ятовується та справляє незабутнє враження на споживача. Він повинен відображати ідею бренду, його філософію, місію та переваги для цільової аудиторії.

При створенні влучного слогана також необхідно враховувати те, які емоції бренд хоче викликати у споживачів. Залежно від цілей компанії розробляються слогани різних видів і стилів. Слогани можна поділити на 7 основних типів: імперативні, описові, провокаційні, переважаючі, питальні, конкретизуючі, далекоглядні [1]. Кожен з них має свої особливості взаємодії з аудиторією, змісту та графічному оформленні. Робота в Adobe Illustrator, Photoshop та Figma допомагає підсилювати їхнє ідейне навантаження та адаптувати для використання у різних макетах.

Імперативними є слогани, які містять заклик або наказ виконати певну дію. Вони мотивують споживачів діяти негайно та рішуче, формуючи сильний емоційний зв'язок з компанією. До даного типу можна віднести слоган компанії Nike – «Just Do It» (Просто зроби це).

Описові слогани пояснюють переваги бренду та його пропозиції. Вважаються найпростішим типом, однак демонструють високу ефективність у просуванні бренду на ринку. Прикладом є слоган компанії Subway – «Eat Fresh» (Їж свіже), який чітко відображає головну перевагу бренду – свіжість продуктів.

Провокаційні – викликають емоції та змушують замислитись аудиторію. Слоган компанії Adidas – «Impossible is Nothing» (Неможливе – ніщо) ідеально передає суть цього типу, оскільки кидає всім виклик та провокує споживачів на роздуми.

Переважаючими є слогани, які використовують найвищі ступені порівняння, щоб сформувати позитивне ставлення до бренду та викликати яскраві емоції. Наприклад, фраза «The Happiest Place on Earth» (Найщасливіше місце на Землі), яка є слоганом Disneyland.

Питальні – використовують питання, щоб зацікавити цільову аудиторію та змусити її задуматися. Наприклад, слогани компаній

Verizon – «Can You Hear Me Now?» (Чуєш мене зараз?) і California Milk Processor Board – «Got Milk?» (Є молоко?). Останній вважається одним з найвдаліших слоганів, який був запущений у найбільш тривалій рекламній кампанії для підвищення популярності молока і водночас здорового способу життя.

Конкретизуючі слогани зрозуміло розкривають специфіку бренду, інформацію про продукт чи послугу, яку він пропонує; часто за формою нагадують коротке оголошення. Для прикладу можна навести слогани брендів M&M's – «Melts in Your Mouth, Not in Your Hands» (Тануть у роті, а не в руках) та Olay – «Love the Skin You're In» (Люби шкіру, в якій ти є).

Далекоглядні слогани передають візію компанії та показують її місію. Таким є слоган компанії Microsoft – «Be What's Next!» (Стань наступним!), оскільки він не просто закликає до дії, а передає бачення майбутнього і бажання розвиватися.

Хоча дизайн слоганів залежить насамперед від стилю та концепції компанії, можна виділити особливості, пов'язані з його типом. Для імперативних, провокаційних, та конкретизуючих слоганів зазвичай використовуються чіткі та жирні шрифти в поєднанні з контрастними кольорами. Часто при їх створенні у Photoshop додають Drop Shadow (тінь) або Outer Glow (зовнішнє світло) для об'єму та глибини тексту. Описові, переважаючі та питальні слогани мають рукописні або курсивні шрифти з ніжними або нейтральними кольорами, інколи з використанням градієнту. Для далекоглядних можуть використовувати сучасні шрифти, наприклад, Futura і Roboto. Щоб створити справді красивий та вдалий слоган варто повною мірою використовувати можливості Photoshop, як-от робота з Layer Styles (стилями шару), сітками та направляючими (Guides), шарами та масками, різноманітними ефектами та фільтрами.

Отже, слоган є важливим інструментом, який допомагає брендам виділитися на ринку та ефективніше взаємодіяти зі споживачами. Залежно від типу, слоган може виконувати різні функції, від вмотивування до виконання дії до опису цінностей компанії. Завдяки використанню можливостей графічних редакторів підвищується ефективність слогану у залученні та утриманні уваги аудиторії.

Список використаних джерел:

1. Гальчинська О. С. Дизайн-проєктування основних компонентів айдентики бренду [Текст] / О. С. Гальчинська // Графічний дизайн в інформаційному та візуальному просторі : монографія / за заг. ред. М. В. Колосніченко. - Київ : КНУТД, 2022. - С. 149-169.

УДК 004.7

Лактіонов О.І., к.т.н., доцент
Національний університет «Полтавська політехніка імені Юрія Кондратюка»

ТЕОРЕТИЧНІ АСПЕКТИ РОЗРОБКИ СИСТЕМИ ПРИЙНЯТТЯ РІШЕНЬ ЩОДО ОБОРОНОЗДАТНОСТІ ДЕРЖАВИ

Результати існуючих напрацювань галузі інформаційних технологій зорієнтовані на розробку комплексних досліджень щодо узагальнення різної інформації [1]. Для цього розробляються нові інструменти, зокрема розширюється кількість параметрів моделі, котра зорієнтована на вирішення конкретного практичного завдання [2].

Оскільки методології зорієнтовані на комплексне об'єднання різної інформації у єдиний кейс, то за результатами експериментів з роботи [3], пропонують комплексний критерій, котрий об'єднує кілька альтернатив.

Результати попередніх напрацювань [4] містить один із варіантів методів. Попри позитивні результати практичного використання, результати напрацювань [4] не використовуються у системі прийняття рішень. Актуалізується питання створення системи прийняття рішень щодо обороноздатності держави.

Загальна структура системи прийняття рішень вивчалася у роботі [5], де одним з найважливіших її елементів є критерій відбору альтернатив на основі котрого ухвалюватимуться рішення. На відміну від існуючих, запропонована система повинна враховувати принципи масштабування, взаємодії, повного перебору оцінок, ансамблювання та бути адаптивною до невизначеності.

Загальна структура запропонованої схеми прийняття рішень щодо обороноздатності держави може бути представлена формально. Дано множина моделей з кількома результатами та стратегіями дій і рішеннями. Вихідний результат обирається залежно від обраної моделі із визначенням ризиків, наприклад за допомогою варіативності, табл. 1.

Таблиця 1

Схема прийняття рішень щодо обороноздатності держави

Модель	Результат	Стратегії дій	Рішення
Модель і	Вихідний результат моделі і	Множина стратегій дій	Множина рішень кожної стратегії дій

Наприклад вихідний результат моделі і на виході може мати п’ять діапазонів значень: 0,1-0,2; 0,21-0,4; 0,41-0,6; 0,61-0,8; 0,81-1,0, де кожен діапазон значень, це окрема стратегій дій та рішення.

Для відбору альтернатив й прийняття рішень пропонується розробити метод, котрому на вхід подаватимуться дані з попередніх робіт, наприклад [4] або інших. Оскільки дані мають різні діапазони значень, зокрема [0, 1], [1, n], то вивчатиметься нормування. Серед методів нормування досліджуватимуться лінійні й нелінійні. Це дозволить враховувати різні структуровані оцінки. Для перевірки надійності рішень розглядатимуться інструменти теорії автоматів.

Таким чином, запропонована ідея розробки системи прийняття рішень, на базі методів з попередніх напрацювань, дозволить поліпшити ефективність ухвалення рішень та скоротити час для корекції помилок, за їх наявності. Ефективність ухвалення рішень є фактором впливу на обороноздатність держави.

Наступні дослідження міститимуть практичні сценарії пропозицій, зокрема математичні й програмні представлення.

Список використаних джерел:

1. Ліп’яніна-Гончаренко Х. Узагальнений принцип синтезу інформаційної технології інтелектуального аналізу соціально-економічних даних ТГ. *Measuring and computing devices in technological processes*. 2024. № 1. С. 359–367. URL: https://doi.org/10.31891/2219-9365-2024-77-48

2. Mokin V. B., Losenko A. V., Yascholt A. R. Information Technology Analysis and Predicting a Multiwave Number of New COVID-19 Disease Based on Prophet Model. *Visnyk of Vinnytsia Politechnical Institute*. 2020. Vol. 153, no. 6. P. 65–75. URL: https://doi.org/10.31649/1997-9266-2020-153-6-65-75

3. Лях І. М. Методологічні основи інформаційної технології обробки даних експресії генів та їх застосування в галузі біоінформатики : автореф. дис. … д-ра техн. наук : 05.13.06. Львів, 2024. 44 с.

4. Implementation of unsupervised learning models for analyzing the state's security level / O. Laktionov et al. *Advanced Information Systems*. 2024. Vol. 8, no. 3. P. 85–91. URL: https://doi.org/10.20998/2522-9052.2024.3.10

5. Shefer A., Laktionov A., Mykhailenko O. Дослідження процесу прийняття рішень у складних технічних системах. *Системи управління, навігації та зв’язку. Збірник наукових праць*. 2022. Т. 1, № 67. С. 34–37. URL: https://doi.org/10.26906/sunz.2022.1.034

УДК 004.8

Гідлевський Д.В., магістрант,
Бродський Ю. Б., к.т.н., доцент,
Державний університет «Житомирська політехніка»

РОЗРОБКА ІНТЕЛЕКТУАЛЬНОЇ СИСТЕМИ УПРАВЛІННЯ РЕСТОРАННИМ ВЕБ-ДОДАТКОМ

У сучасних умовах розвитку ресторанного бізнесу веб-додатки є ключовим інструментом для оптимізації замовлень, управління меню, збору відгуків та підвищення задоволеності клієнтів загалом. Емануель Мелесе [1] у своїй статті підкреслює, що відгуки й коментарі клієнтів, а саме їхні оцінки, можна застосовувати для формування персоналізованих рекомендацій. Це стимулює гостей робити повторні замовлення, підвищує середній чек і формує довгострокову лояльність. Застосування технологій машинного навчання і статистичних моделей дає можливість аналізувати поведінку користувачів і попит на позиції меню. Одним із підходів до реалізації таких рекомендацій є колективна фільтрація за допомогою методу невід'ємної матричної факторизації (NMF), який дозволяє аналізувати вподобання, щоб запропонувати страви, що ймовірно їм сподобаються [2].

Суть цього підходу полягає в тому, що всі оцінки відвідувачів (наприклад, від 1 до 5 балів) представляються у вигляді великої матриці, елементи якої є невід’ємними. NMF «розкладає» цю матрицю на дві менші, кожна з яких містить приховані характеристики: одна відповідає за узагальнені «смаки» користувачів, а інша описує «властивості» страв. Зіставлення цих характеристик дає змогу передбачити, яку оцінку може поставити клієнт тій чи іншій позиції меню, навіть якщо він раніше її не замовляв. Таким чином, система персоналізованої рекомендації пропонує позиції, що потенційно сподобаються відвідувачам.

Для оптимізації операційних процесів ресторану важливо враховувати не лише рекомендації страв для клієнтів, але й сезонні та трендові зміни попиту[3]. Для цього використовують аналіз часових рядів за допомогою моделі ARIMA (AutoRegressive Integrated Moving Average). Це методика, призначена виявляти й описувати закономірності у часових рядах, де дані (наприклад, щоденні замовлення) фіксують на регулярних проміжках. ARIMA зазвичай описується трьома параметрами:

- AR (авторегресія) — показує, як минулі значення впливають на поточне;
- I (інтегрування) — віднімає сусідні спостереження, щоб

позбутися глобального тренду й отримати «більш рівний» ряд.

- MA (ковзне середнє) — нівелює випадкові коливання, згладжуючи шум у даних.

Для ресторану це означає, що, маючи історію замовлень (наприклад, за кожну годину чи день), можна навчити модель ARIMA, щоб вона виявляла приховані закономірності. На основі такої аналітики ресторан може заздалегідь визначати періоди зростання чи спаду попиту й заздалегідь планувати обсяги закупівель, кількість персоналу або інші ресурси. Це допомагає ресторану краще планувати запаси продуктів в пікові години.

Щоб правильно використати методики вище, важливо вибрати правильну архітектуру. Тоді у єдиній системі можливо забезпечити високу продуктивність оброблення замовлень, належну роботу з базою даних, простоту внесення змін у бізнес-логіку, а також можливість швидко оновлювати алгоритми машинного навчання.

Умовно систему можна поділити на дві основні частини:

1. Бекенд, реалізований на Java з використанням Spring Boot [4]. Цей фреймворк дає змогу швидко виконувати CRUD-операції, впроваджувати авторизацію, зручно взаємодіяти з базою даних і налаштовувати авторизацію та аутентифікацію. Окрім того, Spring Boot має розвинені засоби автоконфігурації, що полегшує розгортання веб-додатку.

2. Аналітичний модуль, який потрібно винести в окремий сервіс на Python. У ньому реалізовано методи NMF (для формування рекомендацій) і ARIMA (для прогнозування попиту). Така архітектура є кращою, завдяки можливості швидко змінювати алгоритми машинного навчання без ризику впливу на базову інфраструктуру обробки замовлень і керування меню, іншою перевагою є можливість використовувати Python окремо, що відкриває доступ до великої екосистеми бібліотек.

Також важливою причиною впровадження мікросервісної архітектури - зменшення ризику помилок при оновленні системи та можливість швидко впроваджувати зміни. Потрібно запровадити безперервну інтеграцію й розгортання (CI/CD). У межах цього підходу створюються автоматизовані процеси збірки й тестування коду, які підвищують якість розробки й знижують кількість збоїв. Контейнеризація (наприклад, використовуючи Docker) дає змогу запускати різні програми у відокремлених середовищах, а використання систем оркестрації (Kubernetes та подібних) забезпечує гнучке масштабування та оновлення окремих модулів.

Ресторан мусить дбати й про збереження даних клієнтів. Безпека є важливою. Уся інформація про замовлення та вподобання користувачів має бути захищеною від доступу сторонніх осіб. Розробка же має включати створення механізмів шифрування даних під час передачі між сервісами та зберігання, обмежувати доступ до критичних сервісів і вести моніторинг підозрілих запитів. Для шифрування даних під час передавання налаштовують протокол TLS (Transport Layer Security), щоб уникнути перехоплення даних, а також застосовують алгоритми шифрування на рівні бази даних.

Найкращим рішенням є заздалегідь передбачити резервне копіювання та відновлення БД, а також проводити регулярний аудит, щоб убезпечити систему від потенційних вразливостей. Використовуючи таке рішення, вдається уникнути витоків конфіденційних даних і втримувати довіру клієнтів, адже репутація є вирішальним фактором для будь-якого бізнесу.

Таким чином, формується мікросервісна архітектура, де кожен компонент розв'язує свій набір завдань. Для збереження інформації про замовлення, користувачів та оцінки слід використовувати реляційну СУБД (наприклад, PostgreSQL), яка забезпечить необхідний рівень консистентності даних. Взаємодія між сервісами буде здійснюватися через REST API, що спростить обмін даними у форматі JSON в зашифрованому форматі.

Отже, проєктування такої структури з окремими модулями для операційних завдань і алгоритмів машинного навчання відповідає вимогам інтелектуальної системи і дає змогу суттєво підвищити ефективність планування та обслуговування клієнтів.

Список використаних джерел:

1. Melese A. Food and restaurant recommendation system using hybrid filtering mechanism / A. Melese // North American Academic Research Journal. — 2021. — Т. 4, № 4. — С. 268-281.

2. Kim J. Restaurant recommender system based on customer preference and rating data / J. Kim, S. Lee // IEEE Access. — 2023. — Режим доступу: https://doi.org/10.1109/ACCESS.2023.3324971.

3. Schmidt A. Machine learning based restaurant sales forecasting / A. Schmidt, M. W. Ul Kabir, M. T. Hoque // Machine Learning and Knowledge Extraction. — 2022. — Т. 4, № 1. — С. 105-130

4.. Spring Boot: documentation [Електронний ресурс]. — Режим доступу: https://spring.io/projects/spring-boot (дата звернення: 25.02.2025).

Секція 4
СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ТЕЛЕКОМУНІКАЦІЯХ ТА БІОМЕДИЦИНІ

UDC 661.96

Vovk O.O., D.Sc., professor,
Kutsenko V.O., junior researcher,
PylypchukIe.V., Cand.Sc.,
Kovalenko O.M., junior researcher,
Martyniuk I.D., junior researcher
Center for Information-analytical and Technical Support of Nuclear Power Facilities Monitoring of the National Academy of Sciences of Ukraine

SEARCH AND EXTRACTION OF UNDERGROUND HYDROGEN DEPOSITS: MODERN TECHNOLOGIES AND ENVIRONMENTAL ASPECTS

Search and extraction of natural hydrogen became relevant in the context of alternative energy development. Studies of natural hydrogen as an energy source began relatively recently, but today this direction is topical. The search of hydrogen deposits and its efficient extraction can contribute to reducing dependence on fossil hydrocarbons and reducing greenhouse gas emissions. In addition, hydrogen can become an important element of the transition to renewable energy, as it is easy to store and transport. Various technologies are used to effectively detect hydrogen deposits. They include ground-penetrating radar systems, underwater vehicles and modern methods of patent analysis.

This paper is devoted to the main approaches to search and extraction of underground hydrogen, their prospects and challenges. One of the important stages of research is a patent search, which allows evaluating innovative solutions in the field of hydrogen extraction. The main resources for analysis include Google Patent Search [1], USPTO [2] and UKRNOIVI [3]. They contain detailed information on patented technologies. Analysis of key patents indicates the active development of methods for detecting industrial hydrogen deposits, including hydraulic fracturing, gas production from oil fields, and the use of underwater vehicles.

Among modern approaches to detecting underground hydrogen deposits, georadar technologies play an important role. Use of gradiometric georadars allows non-invasive mapping of deposits. It significantly improves the accuracy of research. In addition, remote seismic surveys using underwater

vehicles open up new opportunities for searching for hydrogen in deep-sea areas.

Fuel reforming technologiesarepromisingregarding innovative solutions in the field of hydrogen production.Laser systems are used to determine the depth of deposits. Such approaches contribute to increasing efficiency of production and reducing the environmental load.

Exploration and production of underground hydrogen have number of challengesdespite the great potential. Geology of hydrogen deposits requires further research for more accurate prediction of deposits and effective planning of production. It is necessary to develop effective production methods that will be competitive in the energy market. An important component is calculation of the costs for exploration, well construction and transportation of hydrogen.

Also, the development of new deposits should be accompanied by an assessment of the impact on the environment and minimizing negative consequences. For example, possible hydrogen leaks can affect gases balance of in the atmosphere. The development of production requires an appropriate legal basis and international cooperation. States should coordinate regulatory acts regulating environmental standards and rights to use subsoil.

The search and production of underground hydrogen is a promising direction for the energy industry development. Modern technologiesuse (likegeoradar systems), underwater vehicles and patent analysis allows significant increase of research and productionefficiency. Innovative approaches in this area open up opportunities for expanding sources of hydrogen and its widespread use in the future. Underground hydrogen could be an important part of the future energy system, offering a clean and efficient source of energy. However, its large-scale extraction requires further research, technical improvements and appropriate legislative framework.

The combination of modern detection methods, the latest extraction technologies and government support will make hydrogen energy more accessible and efficient on a global scale, contributing to sustainable energy development and reducing greenhouse gas emissions.

List of references

1. Patent base Google Patent. https://patents.google.com/ Date of access 10.03.2025.

2. Patent base USPTO. https://ppubs.uspto.gov/pubwebapp/ Date of access 10.03.2025.

3. Patent base UKRNOIVI. https://sis.nipo.gov.ua/uk/search/simple/ Date of access 10.03.2025.

УДК 621.396

Коваленко А. П., здобуач,
Залевський В. Й. с.н.с.,
Сидорчук О. Л., к.т.н., доцент , ст. викладач,
Житомирський військовий інститут імені С. П. Корольова

РОЗРАХУНОК ЕЛЕКТРОМАГНІТНОГО ПОЛЯ, РОЗСІЯНОГО РУПОРОМ ДЗЕРКАЛЬНОЇ АНТЕНИ РАДІОЛОКАЦІЙНОЇ СТАНЦІЇ

Особливості сучасних радіолокаційних станцій(РЛС) найчастіше визначають їх антенні системи. Параметри таких систем значною мірою впливають на якісні показники їх функціонування. Отже їх удосконалення здійснюється головним чином не шляхом створення принципово нових антенних систем, а шляхом покращення їх характеристик спрямованості, узгодження, поляризації тощо.

Для того, щоб покращити такі характеристики виникає необхідність у визначенні електромагнітного поля, розсіяного від антенної системи таких РЛС.У роботі це доведено на прикладі РЛС типу 1РЛ133.

Основною складовою РЛС типу 1РЛ133є однополяризаційна антенна система, яка має дзеркальний параболоїд обертання та опромінювач пірамідальної форми.

Провендено аналіз останніх досліджень і публікацій визначення розсіяного поля від рупорного опромінювача, розташованого у фокусі параболоїдного дзеркала а також аналіз відомих підходів до побудови антенних параболічних систем.Такі дослідження необхідні для удосконалення або проектування нової параболічної антени з покращенням її характеристик спрямованості, узгодженості, поляризаційних параметрів та зменшення ефективної поверхні розсіювання, що зумовлює необхідність оцінювання її розсіювальних властивостей.

Метою роботи є вирішення завдання визначення електромагнітного поля, розсіяного від рупорного опромінювача, розміщеного в площині фокуса параболоїда обертання, у разі довільного падіння на нього плоскої електромагнітної хвилі на прикладі антенних систем РЛС типу 1РЛ133.

Поставлене завдання має дві складові: визначення електромагнітного поля в площині фокуса параболоїда обертання в разі довільного падіння на нього плоскої електромагнітної хвилі та знаходження електромагнітного поля, розсіяного від рупорного опромінювача колової поляризації, розміщеного в площині фокуса параболоїда обертання за умови довільного падіння на нього плоскої

електромагнітної хвилі. Розглянуто два окремих випадки нормального падіння плоскої хвилі і проведено розрахунки для електромагнітного поля, розсіяного в точці фокуса дзеркальної антени і поля на осі дзеркала. Отримано інтегральні вирази для поля, що перевипромінюється рупорним опромінювачем в області параболоїда обертання.Для взяття інтегралу і з'ясування фізики процесу було використано наближений чисельний метод Перевалу.

Працездатність отриманих результатів перевіримо на прикладі антенної системи 1РЛ133 шляхом підстановки її параметрів у вираз для визначення поля, що перевипромінюється рупорним опромінювачем у двох площинах.Проведемо моделювання для амплітуд електромагнітного поля, які можна отримати із кінцевих виразів із застосуванням методу Гюйгенса-Кірхгофа, для хвилі типу H_{01} .

Таким чином, отриманий за чисельним методом вираз, для визначення електромагнітного поля, в області фокуса параболоїда обертання дзеркальної антенної системи, є хоча і наближеним, проте працездатним з досить великою точністю.

Розрахунки за новим методом дозволять оцінювати вплив різноманітних елементів, розміщених у площині фокуса, на розсіяння антенних систем в цілому за будь-якого випадку падіння хвилі на дзеркало.

Побудова РЛС на основі розрахованої за новим методом параболічної антени дозволить отримати значні переваги над традиційними, в разі виявлення об'єктів із малою ефективною поверхнею розсіювання і виділення їх інформативних ознак.

Список використаних джерел:

1. Hou Y.C, Liao W.J, Tsai C. C, Chen SH. Planarmultilayerstructureforbroadbandbroad-angle RCS reduction. IEEE TransactAntennasPropag. 2016. 1859–67. doi: 10.1109/TAP.2016.253516.

2. Sidorchuk O., Tofanchuk O., Kritenko O. Methodologyimprovmentoftheelectromagneticfieldamplitudestudyrelatedtot heantennasystemriskradio-solidstationofland-development "Credo-M1" // ScientificworksofKharkivNationalAirForceUniversity. 2017. № 5 (54). P.102–109.

3. Сидорчук О. Л., Залевський В. Й. Фриз С. П.Чисельний метод визначення електромагнітного поля в області фокуса параболоїда обертання дзеркальної антенної системи//Зб. наук. праць «Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем 2019. № 17. С.121–133.

УДК 004.72

Степанов В.І., здобувач,
Бура В.В., старший викладач
Державний університет «Житомирська політехніка»

ОПТИМІЗАЦІЯ ТА НАЛАШТУВАННЯ ЛОКАЛЬНОЇ МЕРЕЖІ В МЕДИЧНІЙ УСТАНОВІ НА ОСНОВІ ІСНУЮЧОЇ ІНФРАСТРУКТУРИ

В умовах цифрової трансформації медичної галузі ефективне функціонування локальних мереж стає критично важливим для забезпечення надійного доступу до інформаційних ресурсів. Впровадження електронних медичних карток, автоматизованих систем обробки даних, телемедицини та інших цифрових рішень вимагає стабільної, швидкої та безпечної мережевої інфраструктури. У медичних закладах, де щоденно обробляється великий обсяг чутливої інформації, навіть короткочасні збої в мережі можуть негативно вплинути на якість надання медичних послуг.

Аналіз та оптимізація локальної мережі є необхідними для забезпечення її високої продуктивності, масштабованості та безпеки. Це дозволяє не лише підвищити ефективність роботи персоналу, але й мінімізувати ризики витоку інформації та забезпечити відповідність вимогам сучасних стандартів кібербезпеки.

Актуальність даної роботи обумовлена стрімким зростанням вимог до мережевої інфраструктури медичних закладів. Основними викликами є недостатня пропускна здатність мереж, застаріле мережеве обладнання та відсутність комплексних рішень із захисту даних.

Метою дослідження є аналіз існуючої мережевої інфраструктури медичного закладу та розробка рекомендацій щодо її оптимізації для підвищення продуктивності та безпеки.

Предметом досліджень в роботі є медичний заклад (перинатальний центр), його інфраструктура та характеристики.

Для досягнення мети роботи передбачено вирішення таких завдань:

1. Аналіз існуючої мережевої топології та визначення її недоліків.
2. Оцінка пропускної здатності мережі та рівня її безпеки.
3. Розробка рекомендацій щодо оптимізації мережевого обладнання та впровадження засобів моніторингу.
4. Визначення заходів із підвищення кіберзахисту медичних даних.

Після аналізу існуючої топології мережі (рис.1) ми бачимо, що використовується змішана структура, з наявним з’єднанням типу лінія, що суттєво навантажує на один вузол та збільшує час відгуку дальніх робочих місць.

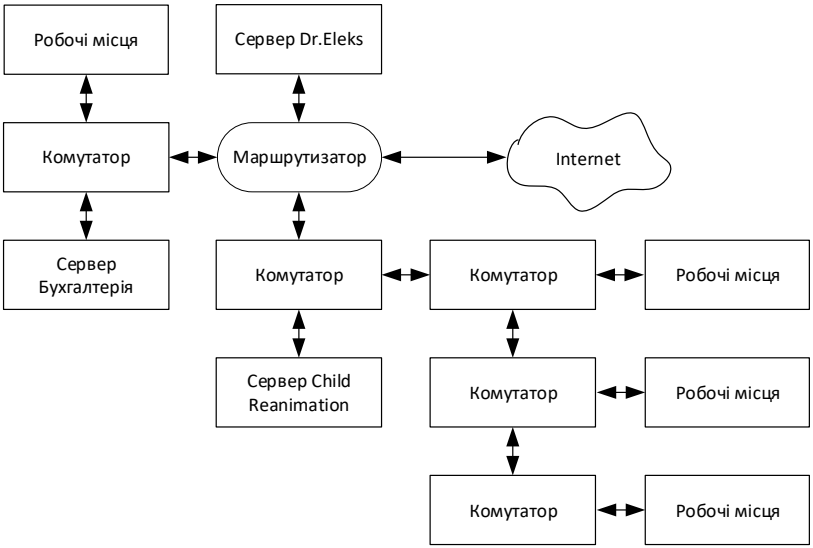


Рисунок 1. Топологія локальної мережі медичного закладу

Для підвищення надійності, відмовостійкості, можливості подальшого розширення мережі, покращення швидкості роботи окремих робочих місць та забезпечення неперервного функціонування було запропоновано і впроваджено:

1. Резервування основних з'єднань для забезпечення відмовостійкості.
2. Централізоване управління мережею через мережеві контролери.
3. Підтримка стандартів GigabitEthernet (1 Gbps) та 10-Gigabit Ethernet для основних комутаторів.
4. Забезпечення пропускної здатності не менше 110 Mbps для периферійних сегментів мережі.
5. Впровадження мережевих брандмауерів (NGFW) для захисту від зовнішніх атак.
6. Сегментація мережі за допомогою VLAN для ізоляції критичних сервісів.
7. Комутатори третього рівня з підтримкою VLAN та QoS.
8. Маршрутизатори із підтримкою VPN-з'єднань та брандмауера.
9. Впровадження системи моніторингу (Zabbix).
10. Збір аналітики про трафік та продуктивність мережі.
11. Резервування каналів виходу в інтернет, шляхом додавання провайдера.

Як бачимо структура замінена на колову, що підвищує надійність з'єднання, резервує канали та підвищує швидкість роботи мережі. Після реалізації запропонованих заходів аналіз відповіді у внутрішній мережі показав час менше 15 мс, при цьому до модернізації цей час перевищував 300 мс для окремих робочих місць.

Можемо зробити висновок, що оптимізація мережі виконана з врахуванням потреб медичного закладу.

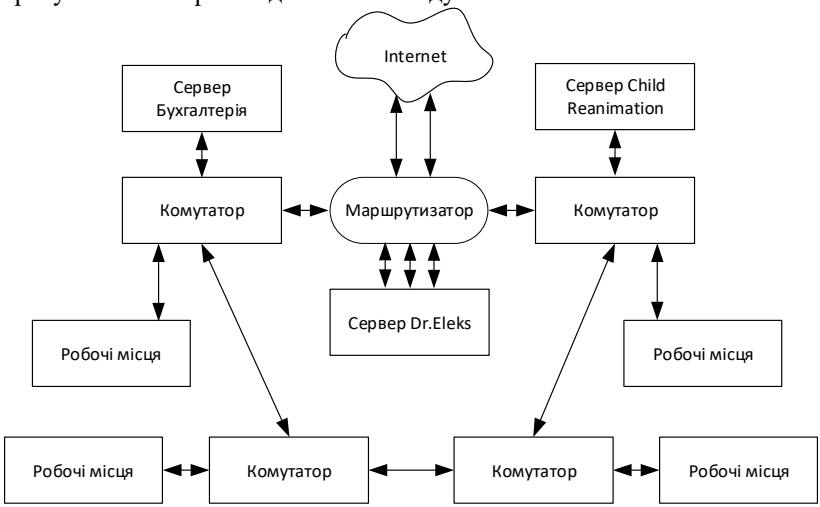


Рисунок 2. Топологія локальної мережі медичного закладупісля модернізації

Список використаних джерел

1. Євсеєв С.П., Дженюк Н.В. Комп'ютерні мережі. Книга 1. Технології комп'ютерних мереж, 2024. Видавництво Новий світ-2000.

2. DevOpsHandbook: HowtoCreateWorld-ClassAgility, Reliability, &SecurityinTechnologyOrganizationsbyGeneKim, PatrickDebois, JohnWillis, andJezHumble, 2023.

3. Бурячок В. Л. Технології забезпечення безпеки мережевої інфраструктури. [Підручник] / В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. – К.: КУБГ, 2019. – 218 с.

4. Кучернюк П.В. Технології моніторингу та трафік–інжинірингу в телекомунікаційних мережах: підручник для студ. спеціальності 172 «Телекомунікації та радіотехніка». Київ : КПІ ім. Ігоря Сікорського, 2021. 257 с. URL: https://ela.kpi.ua/handle/123456789/41500

УДК 621.391:621.37

Петраш С.В., к.т.н доцент,
Зелінський О.В., ст. викладач
Антонюк А.В., ст .викладач
СклярВ.В., здобувач, гр. 313 ТР
Житомирський військовий інститут імені С.П.Корольова

АЛГОРИТМ РОЗПІЗНАВАННЯ РАДІОТЕХНІЧНИХ ВИПРОМІНЮВАЛЬНИХ ОБ'ЄКТІВ

Збільшення кількості радіотехнічних випромінювальних засобів (РВЗ) збільшує навантаження частотного діапазону, в якому вони працюють. Для розділення сигналів таких засобів і забезпечення електромагнітної сумісності застосовуються сигнали спеціальних конструкцій. Зменшення різниці у параметрах сигналів призводить до погіршення якості їх виявлення та розпізнавання.

Задача розпізнавання є однією з ключових за здійснення радіомоніторингу. У такому випадку вона полягає у визначенні належності РВЗ до певного типу, а потім - екземпляру.

Розв'язання задачі розпізнавання реалізується шляхом віднесення вихідних даних до визначеного типу або екземпляру РВЗ за допомогою виділення істотних ознак, що характеризують ці дані.

Ознаки розпізнавання є сукупністю параметрів РВЗ та використовуються при розпізнаванні. Головними вимогами до ознак відносяться високі інформативність та стійкість.

У такому випадку процес розпізнавання зводиться до послідовного знаходження і порівняння з еталонами все нових і нових фрагментів інформації в умовах неперервної зміни режимів роботи та станів РВЗ на основі отриманих ознак (вимірів).

Процес розпізнавання за радіомоніторингу має імовірнісний характер та цілком визначені специфічні особливості:

- часткова апріорна невизначеність початкових даних про РВЗ;
- велика кількість РВЗ, що розпізнаються, точна кількість яких невідома;
- незнання точного часу приходу сигналів;
- вплив випадкових та організованих завад.

Проведений аналіз існуючих методів в умовах часткової або повної апріорної невизначеності появи сигналів в зоні відповідальності пасивних радіотехнічних засобів контролю дозволив вибрати групу статистичних методів розпізнавання.

В алгоритмі розпізнавання РВЗ за типами як ознаки пропонується використовувати виміри параметрів їх сигналів: тривалість сигналів, несуча частота, ширина спектра, період випромінення тощо.

Особливістю запропонованого алгоритму розпізнавання є визначення типу шляхом застосування різних наборів апріорних даних та критеріїв:

Байєса, який враховує наявність повного набору статистичних даних про ВЗ та вагу прийнятого рішення;

Зігерта – Котельнікова (ідеального спостерігача), в якому використовується наявність апріорної інформації;

Максимальної правдоподібності та Неймана – Пірсона, які не вимагають наявності апріорних даних.

Вибір критерію розпізнавання визначається наявністю апріорної інформації.

Як ознаки індивідуального розпізнавання пропонується використовувати особливості паразитної зміни параметрів випромінення, характерні до окремих екземплярів РВЗ: обвідні діаграм спрямованості антен, відхилення несучої частоти, тривалості тощо.

Для індивідуального розпізнавання пропонується використати кореляційний аналіз ознак (метод Ковалевського). Даний метод заснований на попередній статистичній обробці вхідних даних та використанні функцій кореляції. В алгоритмі розпізнавання використовується міра схожості ознак, якою виступає середня квадратична відстань між ними.

За наближенням функцій кореляції (коефіцієнтів кореляції) до максимальних значень відстань між еталонними описами та виміряними параметрами сигналів наближаються до мінімуму. Порівняння коефіцієнтів кореляції з порогом дозволяє прийняти рішення про належність прийнятих сигналів до певного екземпляру.

Для застосування методу вимагається наявність апріорних даних, які стосуються можливих щільностей розподілу ймовірностей значень ознак.

Список використаних джерел:

1. Бондаренко В. О. Методичний підхід до визначення доцільної кількості ознак моніторингу для ідентифікації стану об’єктів розвідки. / Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського.-К.: НУОУ, 2021. – вип. 3(73). – С. 97-101. doi: https://doi.org/10.33099/2304-2745/2021-3-73/97-101.

2. Bruce J. S. AutomaticTargetRecognition, FourthEdition.– Bellingham, Washington : SPIE Press, 2020.– 396 p. ISBN: 9781510631199.

УДК 621.37:621.391

Костін О.В., здобувач
Ципоренко В.В., к.т.н., доц.
ЦипоренкоВ.Г., к.т.н., доц.
Державний університет «Житомирська політехніка»

РОЗРОБКА ТА ДОСЛІДЖЕННЯБЕЗПІЛОТНОГО ПРИСТРОЮ ПЕЛЕНГУВАННЯ З ВИКОРИСТАННЯМ ТРЬОХЕЛЕМЕНТНОЇ АНТЕННОЇ РЕШІТКИ

На сьогодні радіомоніторинг радіоелектронних засобів повинен здійснюватися в умовах складної електромагнітної обстановки, великої апріорної невизначеності щодо параметрів радіовипромінювань, а також в умовах реального масштабу часу реалізації. Перспективним напрямком реалізації радіомоніторингу для вказаних умов є використання безпілотних широкосмугових радіопеленгаторів із застосуванням цифрової обробки радіовипромінювань.

Зазвичайширокосмугове пеленгування реалізується пошуковим кореляційним методом з визначенням такого значення компенсуючої затримки, яке забезпечує максимум взаємної кореляційної функції, недоліком якого є великі часові або апаратурні витрати. Тому дослідження по підвищенню швидкодії малогабаритних безпілотних кореляційно-інтерферометричних пеленгаторів при забезпеченні високої точності є актуальною задачею.

Проведений аналіз відомих швидкодіючих методів та пристроїв кореляційного пеленгування радіовипромінювань. Визначено, що основними їх недоліками є: неоднозначність виміру, що виникає за умови, якщо антенна база перевищує половину робочої довжини хвилі. З іншого боку відомі рішення даної проблеми призводять до значного погіршення точності виміру пеленгу. В результаті досліджень запропоновано використання для кореляційного пеленгатора малогабаритної 3-х елементної антенної решітки (АР), що забезпечує суттєве скорочення апаратурних витрат і зменшення методичної похибки пеленгування. Конфігурація 3-х елементної рівносторонньої решітки має вигляд зображений на рис.1. Три антенні пари АР (АР1 – 0 та 1, АР2 – 1 та 2, АР3 – 0 та 2) мають однакову величину антенної бази, що розташовані в просторі під кутом 60 градусів відносно одна одної.

Виконаний аналіз технічної реалізації пристрою наоснові малогабаритнихSDR-пристроях типу BladeRF 2.0 micro*A4 SDR .Показано, що запропоновані блоки представляють собою завершенні функціональні вузли, що виконуються на основі відомих і широко поширених радіотехнічних технологіях, що випускаються світовою

промисловістю. Виконано обґрунтування алгоритму оцінки напрямку на ДРВ. Основними етапами алгоритму є вибір режиму роботи антенних пар (АР1, АР2 та АР3) та усунення неоднозначності пеленгування.

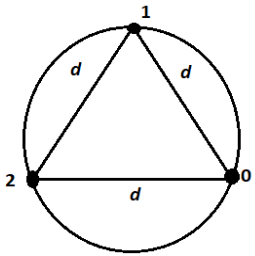


Рис.1 – Конфігурація 3-х елементної антенної решітки

Тому для умов одночасного пеленгування різних джерел радіовипромінювання для використання швидкого алгоритму пеленгування необхідна попередня селекція, наприклад, частотна, кодова або просторова з відповідним розділенням випромінювань окремих джерел. Вказані вимоги ефективно реалізуються при частотному цифровому кореляційному пеленгуванні завдяки використанню попереднього паралельного цифрового комплексного спектрального аналізу.

Розроблений цифровий метод радіопеленгування з використанням 3-х елементної АР забезпечує можливість суттєвого підвищення швидкодії пеленгування і скорочення апаратурних витрат у порівнянні з відомими часовими та спектральними кореляційно-інтерферометричними пошуковими методами пеленгування. Підвищення швидкодії забезпечується за рахунок використання дисперсійного перетворення комплексних взаємних спектрів сигналів та подальшого прямого визначення напрямку на ДРВ. Проведені дослідження методу та пристрою підтверджують ефективність запропонованих рішень, які забезпечують суттєве підвищення дальності та швидкодії пеленгування при незначних втратах точності.

Список використаних джерел:

1. Sabibolda, A., Tsyporenko, V., Tsyporenko, V., Smailov, N., Zhunussov, K., Abdykadyrov, A., Baigulbayeva, M., &Duisenov, N. (2022b). Improving the accuracy and performance speed of the digital spectral-correlation method for measuring delay in radio signals and direction finding. *Eastern-European Journal of Enterprise Technologies*, *1*(9(115)), 6–14.https://doi.org/10.15587/1729-4061.2022.252561

УДК 621.37

КозадаєвВ.В., здобувач
ЦипоренкоВ.Г., к.т.н., доц.
Державний університет «Житомирська політехніка»

РОЗРОБЛЕННЯ БЕЗДРОТОВОЇ СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ АВТОСТОЯНКИ

У процесі виконання курсової роботи було успішно розроблено систему бездротового відеоспостереження для автостоянки, яка включає п’ять камер Hikvision DS-2CD2043G0-I та маршрутизатор TP-Link Archer C6. Враховано всі аспекти, необхідні для ефективного функціонування системи: планування території, вибір обладнання, розрахунок покриття, економічна доцільність і тестування.

Результати показали, що запропонована система забезпечує високу якість відеозображення, надійність та енергоефективність. Завдяки оптимальному розташуванню камер вдалося досягти покриття 95% території автостоянки, що відповідає встановленим вимогам безпеки.

Мета роботи – розроблення бездротової системи відеоспостереження для автостоянки – досягнута. Система відповідає критеріям економічності, надійності та зручності експлуатації. Запропоновані рішення зменшують витрати на фізичну охорону та підвищують рівень безпеки на об'єкті.

Подальший розвиток системи може включати інтеграцію з розумними технологіями, наприклад, підключення до системи управління автостоянкою для автоматичного розпізнавання номерних знаків, а також розширення мережі за рахунок додаткових камер для охоплення 100% території. Доцільним є використання хмарного сховища для резервного копіювання даних та впровадження додаткових методів шифрування і моніторингу мережі з метою підвищення рівня кібербезпеки.

Таким чином, розроблена система відеоспостереження має значний потенціал для подальшого вдосконалення, що дозволить ще більше підвищити її ефективність та безпеку. Зв’язок системи відеоспостереження з аварійними службами або охоронними компаніями є важливим компонентом для забезпечення безпеки.

Сповіщення поліції: у разі виявлення підозрілої активності або порушення, система може автоматично передавати сигнал поліції з прикріпленням відеофрагмента для швидшого реагування.Співпраця з охоронними компаніями: система може бути інтегрована з центрами моніторингу охоронних компаній, які оперативно реагують на тривожні сигнали (наприклад, злом автомобіля або вандалізм).Смарт-

оповіщення: сповіщення можуть надходити у вигляді push-повідомлень на мобільні пристрої адміністратора автостоянки або відповідальних осіб, дозволяючи їм оперативно приймати рішення.

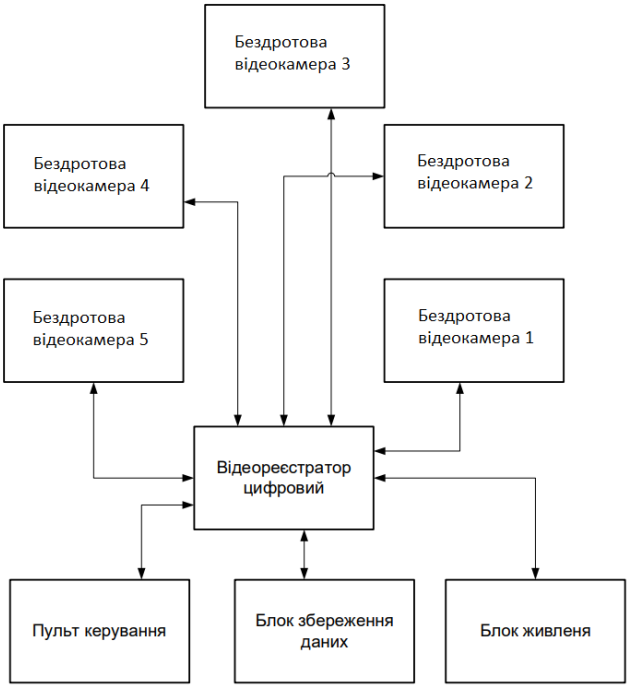


Рис.1 – Система відеоспостереження автостоянки. Схема електрична функціональна

Таким чином, інтеграція системи відеоспостереження з іншими автоматизованими системами, такими як управління паркуванням та аварійними службами, значно підвищує її функціональність та ефективність. Це дозволяє не лише покращити безпеку, але й забезпечити більш зручне та швидке обслуговування клієнтів.

Список використаних джерел:

1. Українські Інфосистеми — Системи відеоспостереження для різних об’єктів. [Електронний ресурс]. – Режим доступу:https://ukrinfosystems.com.ua

УДК 621.396.24

Андреєв О.В., к.т.н., доцент
Фещенко С.О., здобувач
Прокопенко В.В., здобувач
Державний університет «Житомирська політехніка»

ОЦІНКА ВПЛИВУ НЕНАВМИСНИХ ПЕРЕШКОД НА ДАЛЬНІСТЬ ДІЇ ШИРОКОСМУГОВОЇ РАДІОЛІНІЇ

У сучасних телекомунікаційних системах при передачі даних по радіоканалу НВЧ діапазону набули використання різноманітні технології розширення спектру сигналу. При цьому, потрібна швидкість передачі цифрових даних з необхідною якістю, забезпечується використанням достатньо широкої смуги радіоканалу. В умовах існуючих обмежень на потужність передавача, необхідна дальність радіолінії забезпечується шляхом адаптивної зміни тривалості передавання, що дозволяє суттєво збільшити значення бази радіосигналу. Однак, тривалість передачі у реальному часі сигналу мови обмежена значенням періоду дискретизації голосового сигналу. Тому збільшення бази радіосигналу у короткохвильовому діапазоні можливо через застосування широкосмугових сигналів із шириною спектру, що перевищує ширину радіоканалу існуючих вузькосмугових засобів зв'язку.

Під час проведення спеціальних операцій застосування засобів прихованого зв'язку, які використовують сигнали із зменшеною спектральною щільність потужності, є дуже важливим аспектом. У [1] розглянута можливість створення аналогової радіолінії з використанням широкосмугового сигналу з ЛЧМ несучої 30МГц та девіацією частоти 1 МГц із базою сигналу B, що дорівнює 54. Значення дискретних відліків голосового сигналу запропоновано передавати шляхом зміни часової позиції імпульсу ЛЧМ тривалістю 54 мкс на величину, що залежить від амплітуди сигналу на вході модулятора. Показано, що випромінення передавача ШЗР не порушує нормальну роботу вузькосмугових засобів радіозв'язку(ВЗР), що працюють на співпадаючих частотах, якщо передавач ШЗР знаходиться від приймача ВЗР далі ніж передавач ВЗР, із тією ж самою потужністю. Однак остаточні висновки щодо можливості одночасної роботи ШЗР із вузькосмуговими засобами короткохвильового діапазону можуть бути зроблені лише після проведення математичного моделювання сумісної роботи засобів, при умові їх частотно - територіального та часового рознесення.

Метою роботи є дослідження зміни дальності дії ШЗР, як при випадковій кількості ВЗР, що працюють на співпадаючих частотах з різними потужностями передавачів, так і випадковому розташуванні їх у просторі навколо ШЗР.

Оцінка можливості передачі мови із заданими показниками якості за допомогою ШЗР фактично зводиться до розрахунку відношенняпотужності корисного сигналу P_c до потужності шуму$P_{\text{Ш}}$для визначеної дальності зв'язку. Для оцінки погіршення відношення сигнал/шум на виході демодулятора ШЗР, при потраплянні у смугу пропускання приймача вузькосмугових перешкод, які створюються ВЗР, що працюють на співпадаючих частотах одночасно із ШЗР, необхідно зауважити наступне. У приймачі ШЗР низькочастотний голосовий сигнал виділяється на виході корелятора ЛЧМ-сигналу після проходження низькочастотного фільтру із смугою, що, як правило, не перевищує 25 кГц. Тому будь-яка перешкода, що потрапляє у смугу приймального пристрою стає широкосмуговою на виході корелятора, а у вузьку смугу низькочастотного фільтру потрапляє лише частина перешкоди. У цьому випадку відношення сигнал/шум *S/N,*на виході демодулятора ШЗР може бути розраховано згідно виразу [2]:

$$S/N = \frac{P_c \cdot B}{P_{\text{Ш}} + \sum_{i=1}^{N} \frac{\Delta f_c}{\Delta f_{\text{ШЗР}}} \cdot P_{\text{сВЗ}i}},$$

деΔf_c, $\Delta f_{\text{ШЗР}}$ - смуга радіоканалу ВЗР та ШЗР, відповідно;

$P_{\text{сВЗ}i}$ – потужність сигналу, що створюється на вході приймача ШЗР передавачем і-го ВЗР;

N– максимальна кількість сигналів ВЗР, що одночасно потрапляє у смугу пропускання приймача ШЗР.

У роботі проведена перевірка можливості суміщеноїроботи широкосмугової радіолінії з ВЗР, що працюють на співпадаючих частотах, при їх просторово – часовому рознесенні шляхом математичного моделювання.

Список використаних джерел:

1. Андреєв О.В., Мартинчук П.П., Полещук І.І. і Хоменко М.Ф. Широкосмуговий засіб радіозв'язку короткохвильового діапазону для передачі аналогових вузькосмугових сигналів, Вісник ЖДТУ. Серія "Технічні науки", 2016, 3(78), с. 49–55.

2. Андреєв О.В., Ципоренко В. В., Ципоренко В. Г., Андреєва Є.О.,Дубина О. Ф., Пулеко І. В. Електромагнітна сумісність широкосмугових та вузькосмугових короткохвильових засобів радіозв'язку, SciencesofEurope. 2025. Vol 1, № 158. P.78–86.

УДК 621.37

Іванов І.Г., здобувач, гр. ІВ-21-1
Ципоренко В.В., к.т.н., доцент
Державний університет «Житомирська політехніка»

ДОСЛІДЖЕННЯ СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ ТА КОНТРОЛЮ ДОСТУПУ ДЛЯ «ЖИТОМИРСЬКОЇ ПОЛІТЕХНІКИ»

Метою досліджень є розробка та впровадження системи відеоспостереження забезпечення безпеки на території та в будівлях є ключовим завданням сучасної інженерії. Одним із найефективніших засобів досягнення цієї мети є впровадження систем відеоспостереження. У контексті забезпечення безпеки на автостоянка Політехнічного університету, розробка дротової мережі відеоспостереження є важливим аспектом, що дозволить моніторити ситуацію в режимі реального часу, запобігати злочинам та швидко реагувати на надзвичайні ситуації.

Предметом дослідження в роботі є автостоянка Політехнічного університету, її інфраструктура та характеристики. Необхідно врахувати специфіку об'єкта, такі як розмір, форма, освітлення та інші фактори, що можуть вплинути на відповідність системи спостереження вимогам безпеки.За всіма характеристиками цифрові системи відеоспостереження, незважаючи на деякі недоліки, є більш перспективними, ніж аналогові системи. Цифрові системи легше інтегрувати в будь-які складні системи. Ціна мережевих камер може бути вищою, ніж у аналогових камер, але системи на базі мережевих камер мають більшу функціональність та гнучкість.

Розроблено структурну схему нашого проекту та визначили його основні компоненти. Також було проведено розрахунок показників камер для потрібних зон і зроблено вибір обладнання відповідно до цих показників. Було також здійснено розрахунок мережі (бітрейту), яка забезпечить стабільну передачу даних від камер до відеореєстратора, а також розрахунок системи відеозапису, щоб визначити мінімальний необхідний обсяг простору на записуючих пристроях протягом 30 днів.

Один із найважливіших параметрів, який має велике значення, є чутливість камери, оскільки вона визначає можливості розташування та використання камер. Це особливо важливо при розташуванні камер у зонах з низьким рівнем освітленості або для зйомки вночі. Монохромні камери вважаються лідерами у відношенні до найвищої чутливості, оскільки вони здатні підтримувати рівень чутливості навіть до 0,001 люкс, тоді як у кольорових камерах цей рівень значно нижчий. Проте,

для зйомки вночі зазвичай достатньо чутливості на рівні 0,01 люкс. Існує багато сучасних технологій, які дозволяють камерам перевищити можливості людського ока завдяки оптимізації напрямку фотонів, отриманих об'єктивом. Деякі з таких технологій наступні. Lightfinder – розроблена з метою виявлення низького рівня освітленості шляхом чутливості до навіть декількох фотонів видимого світла. Завдяки цій технології камери можуть розрізняти кольори навіть у ситуаціях обмеженого освітлення краще, ніж людське око. Цей результат було досягнуто завдяки використанню оптичних компонентів, таких як високоякісний об'єктив, спеціально підібраний датчик зображення та алгоритми цифрової обробки зображень, вбудованих у систему на кристалі. OptimizedIR – працює краще, ніж попередня, оскільки вона забезпечує зйомку в повній темряві.

У деяких випадках може виникати потреба у відповідній адаптації обладнання до ситуацій з яскравим освітленням, наприклад, коли вихід з підвалу на вулицю в ясну погоду. В таких випадках широкий динамічний діапазон може бути використаний для вирішення цієї проблеми. Він працює за допомогою застосування декількох рівнів експозиції, підвищення контрастності та використання розширених алгоритмів, які зменшують шум і збільшують сигнал зображення. Такий підхід дозволяє адаптувати зображення до засвітлених областей і забезпечує більш рівномірну видимість об'єктів у сцені.

У ході виконання роботи було досягнуто основних цілей проєкту. Проведено аналіз вимог до системи відеоспостереження, зокрема щодо технічних параметрів обладнання, зони покриття та мережевої інфраструктури. Розроблено оптимальну схему дротової мережі відеоспостереження, яка забезпечує ефективний моніторинг території стоянки та прилеглих зон. Вибрано відповідне обладнання для реалізації системи, враховуючи критерії якості, вартості, надійності та сумісності з іншими компонентами. Проведено розрахунок вартості проєкту, який відповідає бюджетним обмеженням.

Розроблена мережа відеоспостереження забезпечує високий рівень безпеки об'єкта, дозволяючи оперативно виявляти загрози, фіксувати події та створювати відеоархів для подальшого аналізу.

Список використаних джерел:

1. Управління інформаційною безпекою. [Електронний ресурс].https://uk.wikipedia.org/wiki/Система_управління_інформаційною_безпекою

2. Проектування системи відеоспостереження. [Електронний ресурс]. – Режим доступу: https://www.jvsg.com

УДК 621.37

Литвинчук А.С., здобувач
Макієвський О.А., здобувач
Ципоренко В.В., к.т.н., доц.
Державний університет «Житомирська політехніка»

РОЗРОБЛЕННЯ БЕЗДРОТОВОЇ МЕРЕЖІ ВІДЕОСПОСТЕРЕЖЕННЯ ПАРКОВКИ

У роботі розглянуто процес розроблення бездротової мережі відеоспостереження для об'єкта. Проект передбачає використання сучасних бездротових технологій, таких як Wi-Fi та IP-камери, для забезпечення ефективного моніторингу території без необхідності прокладання кабелів. У роботі детально аналізуються основні методи проектування систем відеоспостереження, переваги та недоліки бездротових рішень, а також технічні вимоги до системи.

Сучасні системи відеоспостереження набувають широкого застосування завдяки забезпеченню безпеки та контролю. Бездротові технології дозволяють спрощувати їх впровадження, знижувати вартість встановлення та експлуатації, а також забезпечують більшу гнучкість у використанні. У світлі зростаючої потреби у підвищенні рівня безпеки, розробка таких систем стає важливим завданням.Актуальні методи проектування систем відеоспостереження включають використання сучасних технологій, таких як штучний інтелект для аналізу відео, відеокамери з високою роздільною здатністю, а також інтеграцію з хмарними сервісами для зберігання і обробки даних. Важливим аспектом є вибір типу камер (аналогові чи IP) і методів зберігання відео (локальне зберігання або хмарне). Крім того, важливим є застосування алгоритмів для виявлення руху або аномалій, що дозволяють знизити навантаження на систему і збільшити ефективність використання ресурсів.

Розробка власної бездротової системи відеоспостереження вимагає ретельного планування, врахування характеристик місцевості, де буде встановлено обладнання, а також вимог до якості зображення і збереження даних. Вибір камер з високою роздільною здатністю, налаштування мережі для забезпечення стабільного сигналу, а також безпеки передачі даних є критично важливими аспектами. Окрім того, важливо розглянути можливості інтеграції з іншими системами безпеки та обробки даних в реальному часі для підвищення ефективності роботи системи.

Для проєктурозроблено симуляцію парковки з розташуванням бездротових камер.

Розглядаєтьсяствореннясистемивідеоспостереженнядля контролютериторії парковки, щозабезпечує:

- моніторинг руху автомобілів;
- запобігання правопорушенням (крадіжки, вандалізм);
- забезпечення безпеки майна водіїв та відвідувачів.

Мета системи – забезпечити повний огляд парковки, відсутність сліпих зон, високу якість зображення та оперативний доступ до відеозаписів.

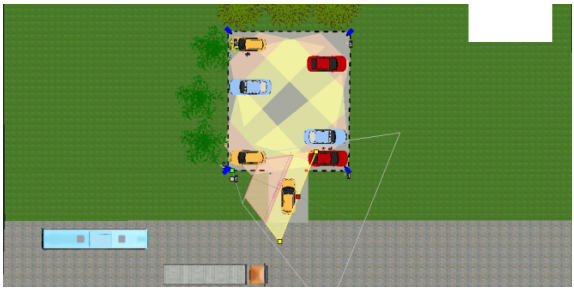


Рис.1 – Симуляція розташування камер на парковці

Розроблена система відеоспостереження, що складається з п’яти бездротових камер, маршрутизатора, мережевого відеореєстратора (NVR) та додаткових компонентів. Камери передають відеосигнал через Wi-Fi маршрутизатор до NVR.NVR записує відео та дозволяє перегляд записів через підключений монітор або мобільний додаток.Камери та маршрутизатор отримують живлення від електромережі, а в разі її відключення — від UPS.Хмарне сховище використовується для резервного копіювання даних (за наявності підключення до інтернету).Представлена схема демонструє оптимальний підхід до проектування бездротової системи відеоспостереження. Завдяки використанню сучасних технологій досягається висока якість зображення, стабільність системи та мінімізація витрат на встановлення.Отримані результати свідчать про практичність та ефективність запропонованого рішення. Використання бездротових технологій дозволяє знизити витрати на встановлення, забезпечуючи водночас високу мобільність і гнучкість у налаштуванні.

Список використаних джерел:

1. HikvisionLearning&Support Ресурс з технічними документами і прикладами використання IP-камер Hikvision у бездротових мережах. [Інтернет ресурс]. Режим доступу:https://www.hikvision.com/

УДК 004.7

Хрульов М.М., аспірант,
Миронюк Т.В., к.т.н., доцент кафедри комп'ютерної інженерії та інформаційної безпеки
Черкаський державний технологічний університет

ПЕРСОНАЛІЗОВАНІ ЦИФРОВІ МЕДИЧНІ СИСТЕМИ: ІНТЕГРАЦІЯ IOMT, ШІ ТА АНАЛІТИКИ ДАНИХ

Сучасна медицина активно впроваджує цифрові технології для покращення якості надання медичних послуг. Інтеграція IoMT, ШІ та аналітики даних дозволяє створювати персоналізовані системи, що сприяють ранньому виявленню захворювань та підвищенню ефективності лікування [3, 5]. Однак, існують виклики, пов'язані з безпекою даних та сумісністю різних систем [5].

Метою доповіді є виконання аналізу можливостей і переваг впровадження персоналізованих цифрових медичних систем, що поєднують IoMT, ШІ та аналітику даних, з метою покращення якості медичних послуг. Особливу увагу приділено дослідженню способів оптимізації діагностичних процесів, підвищенню точності прогнозування стану здоров'я пацієнтів та розробці підходів до безпечного обміну медичною інформацією. Також розглядаються перспективи адаптації таких систем у реальній клінічній практиці та визначення ключових викликів їх впровадження.

Впровадження IoMT-пристроїв дозволяє безперервно збирати життєво важливі показники пацієнтів, що сприяє ранньому виявленню відхилень та своєчасному втручанню лікарів [4, 5]. Поєднання цих даних з аналітикою ШІ забезпечує:

Дляпацієнтів:

- Раннє звернення до фахівців при виявленні перших ознак захворювання [3].
- Можливість вживати профілактичні заходи на основі персоналізованих рекомендацій [2].
- Покращення якості життя завдяки постійному моніторингу та своєчасному втручанню [5].

Длялікарів:

- Більш точну діагностику на основі детальних та актуальних даних пацієнта [4].
- Надання якісніших медичних послуг завдяки індивідуалізованому підходу [3].
- Зменшення часу прийому через попередній аналіз даних системою [1, 5].

Однак впровадження таких систем супроводжується викликами, зокрема щодо безпеки та конфіденційності даних пацієнтів, а також необхідності розробки стандартів для забезпечення сумісності різних систем [2, 5].

Виконанийаналіз дозволить:

- Визначити основні переваги персоналізованих цифрових медичних систем для покращення діагностики та лікування.
- Розробити рекомендації щодо впровадження IoMT та ШІ в медичну практику з урахуванням інформаційної безпеки та сумісності систем.
- Оцінити потенційний вплив таких технологій на медичну галузь у майбутньому та визначити ключові напрямки подальших досліджень.

Список використаних джерел:

1. Коротка В.О., Мокринський В.А. Технології штучного інтелекту в сучасній медицині: впровадження та проблематика // Український медичний часопис. 2024. № 3. С. 87–94. URL:https://umj.com.ua/uk/publikatsia-257497-tehnologiyi-shtuchnogo-intelektu-v-suchasnij-meditsini-vprovadzhennya-ta-problematika (дата звернення: 10.03.2025).

2. AIoT у 2024 році: приклади, технології, проблеми впровадження // DusunIoT. 2024. URL:https://www.dusuniot.com/uk/blog/aiot-artificial-intelligence-of-things/ (дата звернення: 10.03.2025).

3. Сучасні цифрові тенденції в галузі медичних технологій // Stfalcon. 2024. URL:https://stfalcon.com/uk/blog/post/healthcare-trends (дата звернення: 12.03.2025).

4. Висоцький А.А., Суріков О.О. Розвиток штучного інтелекту в сучасній медицині // Науковий вісник охорони здоров’я. 2023. № 2. С. 45–58. URL: https://example.com/ai-healthcare (дата звернення: 12.03.2025).// Матеріали конференції. 2021. URL:https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/37126/1/Тези_2021_Рябощук_Міца.pdf (дата звернення: 12.03.2025).

5. Штучний інтелект в охороні здоров'я: переваги та виклики // Pharmcare. 2024. URL:https://account.pharmcare.online/2024/01/31/310124-1/ (дата звернення: 12.03.2025).

УДК 004.8

Гідлевський Д.В., здобувач,
Державний університет «Житомирська політехніка»

РОЗРОБКА ІНТЕЛЕКТУАЛЬНОЇ СИСТЕМИ УПРАВЛІННЯ РЕСТОРАННИМ ВЕБ-ДОДАТКОМ

У сучасних умовах розвитку ресторанного бізнесу веб-додатки є ключовим інструментом для оптимізації замовлень, управління меню, збору відгуків та підвищення задоволеності клієнтів загалом. ЕмануельМелесе [1] у своїй статті підкреслює, що відгуки й коментарі клієнтів, а саме їхні оцінки, можна застосовувати для формування персоналізованих рекомендацій. Це стимулює гостей робити повторні замовлення, підвищує середній чек і формує довгострокову лояльність. Застосування технологій машинного навчання і статистичних моделей дає можливість аналізувати поведінку користувачів і попит на позиції меню. Одним із підходів до реалізації таких рекомендацій є колективна фільтрація за допомогою методу невід'ємної матричної факторизації (NMF), який дозволяє аналізувати вподобання, щоб запропонувати страви, що ймовірно їм сподобаються [2].

Суть цього підходу полягає в тому, що всі оцінки відвідувачів (наприклад, від 1 до 5 балів) представляються у вигляді великої матриці, елементи якої є невід'ємними. NMF «розкладає» цю матрицю на дві менші, кожна з яких містить приховані характеристики: одна відповідає за узагальнені «смаки» користувачів, а інша описує «властивості» страв. Зіставлення цих характеристик дає змогу передбачити, яку оцінку може поставити клієнт тій чи іншій позиції меню, навіть якщо він раніше її не замовляв. Таким чином, система персоналізованої рекомендації пропонує позиції, що потенційно сподобаються відвідувачам.

Для оптимізації операційних процесів ресторану важливо враховувати не лише рекомендації страв для клієнтів, але й сезонні та трендові зміни попиту[3]. Для цього використовують аналіз часових рядів за допомогою моделі ARIMA (AutoRegressiveIntegratedMovingAverage). Це методика, призначенавиявляти й описуватизакономірності у часових рядах, де дані (наприклад, щоденнізамовлення) фіксують на регулярнихпроміжках. ARIMA зазвичай описується трьома параметрами:

1. AR (авторегресія) — показує, як минулі значення впливають на поточне;
2. I (інтегрування) — віднімає сусідні спостереження, щоб позбутися глобального тренду й отримати «більш рівний» ряд.
3. MA (ковзне середнє) — нівелює випадкові коливання,

згладжуючи шум у даних.

Для ресторану це означає, що, маючи історію замовлень (наприклад, за кожну годину чи день), можна навчити модель ARIMA, щоб вона виявляла приховані закономірності. На основі такої аналітики ресторан може заздалегідь визначати періоди зростання чи спаду попиту й заздалегідь планувати обсяги закупівель, кількість персоналу або інші ресурси. Це допомагає ресторану краще планувати запаси продуктів в пікові години.

Щоб правильно використати методики вище, важливо вибрати правильну архітектуру. Тоді у єдиній системі можливо забезпечити високу продуктивність оброблення замовлень, належну роботу з базою даних, простоту внесення змін у бізнес-логіку, а також можливість швидко оновлювати алгоритми машинного навчання.

Умовно систему можна поділити на дві основні частини:

3. Бекенд, реалізований на Java з використанням SpringBoot [4]. Цей фреймворк дає змогу швидко виконувати CRUD-операції, впроваджувати авторизацію, зручно взаємодіяти з базою даних і налаштовувати авторизацію та аутентифікацію. Окрім того, SpringBoot має розвинені засоби автоконфігурації, що полегшує розгортання веб-додатку.

4. Аналітичний модуль, який потрібно винести в окремий сервіс на Python. У ньому реалізовано методи NMF (для формування рекомендацій) і ARIMA (для прогнозування попиту). Така архітектура є кращою, завдяки можливості швидко змінювати алгоритми машинного навчання без ризику впливу на базову інфраструктуру обробки замовлень і керування меню, іншою перевагою є можливість використовувати Python окремо, що відкриває доступ до великої екосистеми бібліотек.

Також важливою причиною впровадження мікросервісної архітектури - зменшення ризику помилок при оновленні системи та можливість швидко впроваджувати зміни. Потрібно запровадити безперервну інтеграцію й розгортання (CI/CD). У межах цього підходу створюються автоматизовані процеси збірки й тестування коду, які підвищують якість розробки й знижують кількість збоїв.

Контейнеризація (наприклад, використовуючи Docker) дає змогу запускати різні програми у відокремлених середовищах, а використання систем оркестрації (Kubernetes та подібних) забезпечує гнучке масштабування та оновлення окремих модулів.Завдяки цьому, можна додавати нові алгоритми або змінювати логіку бекенду без тривалої зупинки роботи ресторанного застосунку. Це має значення у ситуаціях, коли виникає необхідність швидко виправити критичні помилки.

Ресторан мусить дбати й про збереження даних клієнтів. Безпека є важливою. Уся інформація про замовлення та вподобання користувачів має бути захищеною від доступу сторонніх осіб. Розробка же має включати створення механізмів шифрування даних під час передачі між сервісами та зберігання, обмежувати доступ до критичних сервісів і вести моніторинг підозрілих запитів.

Для шифрування даних під час передавання налаштовують протокол TLS (TransportLayerSecurity), щоб уникнути перехоплення даних, а також застосовують алгоритми шифрування на рівні бази даних.

Найкращим рішенням є заздалегідь передбачити резервне копіювання та відновлення БД, а також проводити регулярний аудит, щоб убезпечити систему від потенційних вразливостей. Використовуючи таке рішення, вдається уникнути витоків конфіденційних даних і втримувати довіру клієнтів, адже репутація є вирішальним фактором для будь-якого бізнесу.

Таким чином, формується мікросервісна архітектура, де кожен компонент розв'язує свій набір завдань. Для збереження інформації про замовлення, користувачів та оцінки слід використовувати реляційну СУБД (наприклад, PostgreSQL), яка забезпечить необхідний рівень консистентності даних. Взаємодія між сервісами буде здійснюватися через REST API, що спростить обмін даними у форматі JSON в зашифрованому форматі.

Отже, проєктування такої структури з окремими модулями для операційних завдань і алгоритмів машинного навчання відповідає вимогам інтелектуальної системи і дає змогу суттєво підвищити ефективність планування та обслуговування клієнтів.

Список використаних джерел:

1. Melese A. Food and restaurant recommendation system using hybrid filtering mechanism / A. Melese // North American Academic Research Journal. — 2021. — Vol. 4, № 4. — С. 268-281.
2. Kim J. Restaurant recommender system based on customer preference and rating data / J. Kim, S. Lee // IEEE Access. — 2023. — DOI: 10.1109/ACCESS.2023.3324971.
3. Schmidt A. Machine learning based restaurant sales forecasting / A. Schmidt, M. W. Ul Kabir, M. T. Hoque // Machine Learning and Knowledge Extraction. — 2022. — Vol. 4, № 1. — С. 105-130.
4. Spring Boot: documentation [Електронний ресурс] – Режим доступу: https://spring.io/projects/spring-boot (дата звернення: 02.25.2025).

УДК 621.3:004.9

Соболенко С.О., к.т.н. доцент, начальник кафедри
Дубина О.Ф., к.т.н доцент, заступник начальника кафедри
Пулеко І.В., к.т.н доцент
Григор'єв І.С., ст. викладач
Житомирський військовий інститут імені С.П.Корольова

ПІДХІД ДО КЛАСИФІКАЦІЇ ОБ'ЄКТІВ ПО ЗОБРАЖЕННЯХ З IP-ВІДЕОКАМЕР З ВИКОРИСТАННЯМ ТЕОРІЇ НЕЧІТКОЇ ЛОГІКИ

Дослідження методів ідентифікації об'єктів на зображеннях являє собою недостатньо вивчену область технічних знань. Це пов'язано з неможливістю передбачення усіх факторів для формування зображення об'єкту на знімку, що пов'язані з певною невизначеністю.

Проведений аналіз показує, що показники ефективності стосовно інтегрованої системи охорони (ІСО) можуть бути представлені групою, що включає, з одного боку, показники, що характеризують комплекс технічних засобів (КТС) системи охорони, з другого — показники, що характеризують людський чинник.[1]

У загальному випадку при побудові систем охорони при використанні ймовірнісного підходу показник ефективності та надійності КТЗ можна записати в аналітичному вигляді як:

$$W_{\text{е}} = P_0, P_{\text{кл}}, P_{\text{св}}, P_{\text{н}}^{\text{сер}}, P_{\text{св}}^{\text{кз}},$$

де P_0 – ймовірність виявлення об'єкта датчиками;

$P_{\text{кл}}$– ймовірність правильної класифікації об'єктів датчиками;

$P_{\text{св}}$ – ймовірність, що характеризує своєчасність обробки інформації в тракті сигнального розпізнавання;

$P_{\text{н}}^{\text{д}}$– ймовірність безвідмовної роботи датчика,

$P_{\text{св}}^{\text{кз}}$– своєчасність видачі інформації по каналу зв'язку.

Найбільша ефективність функціонування сучасних систем безпеки й охорони забезпечується шляхом використання систем відеоспостереження.

Сучасні мережеві IP відеокамери охоплюють широкий діапазон розрізнень. Процентні співвідношення не використовуються; і тепер вимоги до роздільної здатності вказуються в пікселях та доповнено альтернативним параметром: кількістю міліметрів об'єкту знімання, що припадають на один піксель зображення, отриманого з камери відеоспостереження.

Практично це означає, що проектувальник та замовник повинні визначитися з метою встановлення кожної камери (розпізнавання

людей, ідентифікація, детектування, спостереження). При підборі зони огляду камери слід розрахувати, за яких параметрів камери та об'єктива в зоні огляду камери буде достатня щільність пікселів для виконання завдання.

Проведений аналіз показав, що для визначення реальної роздільної здатності зображення і, відповідно, ймовірності правильної класифікації об’єктів системами відеоспостереження, необхідно враховувати багато чинників, що знаходяться у певному протиріччі один з одним і цей процес не піддається аналітичному моделюванню. До основних таких чинників відносяться: розрізнення, освітленість під час знімання, дальність до об’єкта, глибина різкості.

Для ідеальних умовах знімання і, враховуючи технічні характеристики відеокамери, розрахунок щільності пікселів не представляє складності.

В умовах слабкої освітленості, що є притаманним для охоронних систем, роздільна здатність зображення погіршується. Ці зміни досить складно описати аналітично чи провести моделювання.

У цьому випадку, для оцінки характеристик і параметрів знімання пропонується застосовувати нечітку логіку (FuzzyLogic) із застосуванням експертних даних [2].

Нехай база нечітких правил прийняття рішень містить визначені експертами залежності рівня відповідності роздільної здатності вимогам європейського стандарту EN 50 132-7 для виявлення, розпізнавання та ідентифікації від рівня освітленості та значення діафрагми.Введемо лінгвістичні змінні: освітленість = (висока, низька); діафрагма = (велика, мала); відповідність = (висока, середня, низька).

Застосовуючи відомий алгоритм нечіткого виведення Мамдані, для заданих нечітких множинотримаємо, у скільки разів погіршується роздільна здатність відеокамери по відношенню до ідеальних умов.

Даний підхід можливо застосовувати при проектуванні охоронних систем відеоспостереження.

Список використаних джерел:

1. Vakaliuk T., Dubyna O., Nikitchuk T., Andreiev O. EvaluationoftheEffectivenessoftheIntegratedSecuritySystemasanInformationSystem. Proceedingsofthe 11-th InternationalConference "InformationControlSystems& Technologies", September 21–23, 2023. Odesa, Ukraine. CEUR WorkshopProceedings. 2023. Vol. 3513. pp. 16-26. – URL: https://ceur-ws.org/Vol-3513/paper02.pdf.

2. Carter, J., Chiclana, F., Khuman, A. S., &Chen, T. (Eds.) (2021). *FuzzyLogic: RecentApplicationsandDevelopments*. (1 ed.) SpringerNatureSwitzerland AG. https://doi.org/10.1007/978-3-030-66474-9

УДК 621.391

Шефер О.В., д.т.н., професор
Євдоченко О.І., аспірант
Національний університет
«Полтавська політехніка імені Юрія Кондратюка»

СУЧАСНІ АСПЕКТИ ВИКОРИСТАННЯ ТУРБО-КОДІВ В ЗАВАДОСТІЙКОМУ КОДУВАННІ

В системах передаванняданих для боротьбиіззавадамизастосовуєтьсязавадостійкекодування. Йоговикористовують для стисненняінформації і для захистуданих в пам'ятіобчислювального пристрою та накопичувачахінформації.

Турбо-код маєдоситьпотужний метод виправленняпомилок, буврозроблений в 1993 р. та описаний в науковихпрацях C. Berrou, A. Glavieux, P. Titimajshima. Вінмаєважливуперевагу в тому, щодозволяєзабезпечитинадійнийзв'язок з ефективністюдужеблизькою до теоретичноїграниці Клода Шенона. Турбо-коди є новимкласомметодів, щовизначаютьітеративнекодування з виправленнямпомилок. Турбо-код відноситься до блоковихкодів, але будується на основізгортковихкодів. Турбо-код посійноудосконалюється у напряміпідвищенняшвидкості та надійностіпередаванняданих. Це робить йогонайбільшперспективним в волоконно-оптичнихлініяхзв'язку, цифровому телебаченні, космічних та мобільних мережах зв'язку[1].

Використання турбо-кодів дозволяє працювати при значно більш низьких відношеннях сигнал/шум, ніж при використанні згорткового коду Вітербі або каскадних кодів Вітербі-Ріда-Соломона. Турбо-код забезпечує роботу при співвідношенні сигнал/шум приблизно 2 дБ в лініях, обмежених по доступній потужності [2].

Для турбо-кодової системи (рис.1) зі швидкістю $1/3$[3] доцільно використати верхній регістр для позначення двійкових чисел, а нижній регістр – для значень сигнал/символ.

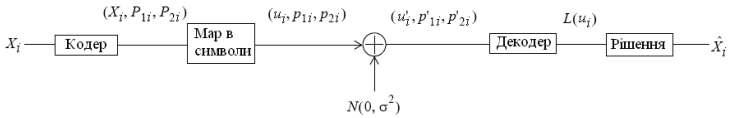


Рис. 1.Система турбо-коду

X_i – подана послідовність інформаційних битів; P_{1i} – дібіт з кодера 1; P_{2i} – дібіткодера 2; U_i – інформаційні символьні данні; p_{1i} – символи парності з декодера 1; p_{2i} – символи парності з декодера 2;σ^2 – дисперсія шуму; $u_i^{/}$– зашумовані інформаційні символьні дані; $p_{1k}^{/}$ –

зашумовані символи парності з декодера 1;p'_{2k} – зашумовані символи парності з декодера 2; $L(u_i)$ – «м'яке» рішення декодера; $\widehat{X}_i$ – «жорстке» рішення декодера.Схема турбо-кодера з двома загортковими ідентичними кодерами та перемежувачемP наведена на рис.2.Завданням перемежувача є перетворення вхідної інформаційної послідовності таким чином, щоб комбінації, що призводять до кодових слів з низькою вагою на виході першого кодера, були перетворені в комбінації, що породжують кодові слова з високою вагою на виході інших кодерів. Перемежувач є одним із способів боротьби з помилками.

Рис. 2.Схема турбо-кодера

Структура турбо-декодера (рис.3) складається з пари декодерів. Які працюють спільно для того, щоб уточнити оцінку бітів.

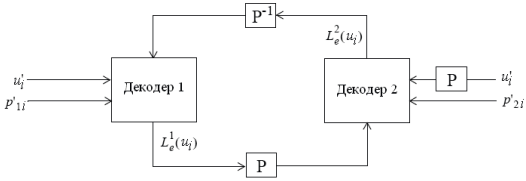


Рис. 3.Схема турбо-декодера

Декодерипрацюють на основі алгоритму декодування по максимуму апостеріорноїімовірності і випускаютьінформацію «м'якогорішення». Спочатку декодер № 1 починає роботу без ініціалізаціїінформації. У наступнихітераціяхінформація «м'якихрішень» використовується для активаціїіншого декодера. Інформація з декодера обертається петлею до того моменту, поки «м'які» рішення не сходяться на стабільномунаборізначень.

Список використаних джерел:

1. Breiling M. The Super-Trellis Structure of Turbo Codes / M. Breiling, L. Hanzo // IEEE Transactions on Information Theory. 2000. V. 46. № 6. P. 2212-2228.

2. БурачокР.А., КлимашМ.М., КовальБ.В. Телекомунікаційнісистемипередаванняінформації. Методикодування. Львів: ВидавництвоЛьвівськоїполітехніки. 2015.

3. BerrouC. NearShannonLimitError-CorrectingCodingandDecoding: Turbo-Codes / C. Berrou, A. Glavieux, P. Thitimajshima // IEEETransactionsonInformationTheory. 1996. V. 44. № 10. P. 1064-1070.

УДК 612.67

Сергійчук М.В., здобувач,
Галанзовська В.О., здобувач
Коренівська О.Л., к.т.н., доцент,
Бенедицький В.Б., ст. викладач
Державний університет «Житомирська політехніка»

СПОСОБИ КЕРУВАННЯ ПРОТЕЗОМ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

Розвиток штучного інтелекту (ШІ) суттєво змінює медичну галузь, і однією з найперспективніших сфер є створення інтелектуальних протезів. Розглянемо можливі варіанти керування протезами з використанням штучного інтелекту. Перспективними є способи керування через акселерометр, комп'ютерний зір, голосове керування та гібридні схеми керування з використанням нейросигналів.

1. Перспективним напрямком є розробка гібридної системи керування біонічним протезом руки на основі ШІ та ЕМГ (це міоелектричне керування, яке використовує електроміографічні (ЕМГ) сигнали м’язів пацієнта).

Принцип роботи наступний: на кінцівку встановлюються ЕМГ-датчики, які зчитують біоелектричні сигнали м’язів. ШІ аналізує та класифікує рухи, розпізнаючи, що хоче зробити користувач. Отримані дані передаються на сервомотори, які рухають штучну кінцівку. Протез стає природнішим у використанні та швидше реагує на команди.

2. Керування рухами протезу з використанням акселерометра.

Акселерометр – це сенсор, що вимірює прискорення по одній або кількох осях. У контексті протезування, акселерометр встановлюється на частину тіла (наприклад, плечовий м’яз), що збереглася, або безпосередньо в корпус протеза.

Під час руху кінцівки або частини тіла, акселерометр генерує аналогові або цифрові сигнали, які фіксують напрямок руху, швидкість (прискорення) руху, положення в просторі (при використанні гіроскопа – кутове положення).

Сигнали з акселерометра передаються до мікроконтролера, де фільтруються, розпізнаються шаблони рухів, за допомогою алгоритмів машинного навчання визначається команда для протеза. Наприклад: нахил уперед – стиснення кисті; поворот вправо – обертання протеза, підняття

Мікроконтролер подає сигнал на виконавчі механізми протеза (серводвигуни, електродвигуни), які імітують бажаний рух.

3. Керування рухами протезу за допомогою комп’ютерного зору.

Для початку встановлюється камера, яка спрямована на ділянку тіла користувача (наприклад, обличчя, залишену частину руки, очі або інші контрольні зони). Це може бути звичайна вебкамера, інфрачервона або 3D-камера, Камера вбудована в окуляри або шолом.

Зібране відео потрапляє на обробку комп'ютерним зором. Система використовує бібліотеки на кшталт OpenCV, MediaPipe, TensorFlow/Keras.

Алгоритм обробляє відео й визначає жест або керуючий рух. Виявлений жест інтерпретується як команда до дії. Оброблені команди передаються через мікроконтролер до електроприводів у протезі, які виконують відповідну дію.

Цей метод особливо корисний для людей, які втратили рухливість кінцівок, але зберегли рухливість голови, обличчя або очей.

4. Реалізація голосового управління біонічним протезом**.**

Для початку система потребує мікрофон або гарнітуру, які записують голос користувача. Записаний голос обробляється мовним інтерфейсом, наприклад Google Speech-to-Text API, Vosk або написаною програмою на Python з використанням бібліотек `speech_recognition`, `pyaudio`, `vosk`, `DeepSpeech`.

Після перетворення мови в текст, програма порівнює отриману команду з попередньо визначеним списком дій. Якщо команда знайдена, викликається відповідна дія. Команда надсилається до мікроконтролера який керує сервомоторами або актуаторами протезу. Мікроконтролер інтерпретує команду як електричний сигнал і керує елементами протеза.

Голосове керування особливо корисне для користувачів, які не можуть використовувати фізичні сенсори чи жести, але можуть чітко говорити. Такий підхід підвищує рівень автономності користувача.

Застосування штучного інтелекту в керуванні біонічними протезами кінцівок відкриває нові горизонти в реабілітаційній техніці, забезпечуючи більш природну, інтуїтивну та адаптивну взаємодію між людиною та пристроєм. Системи на базі ШІ здатні навчатися, адаптуватися до особливостей користувача, розпізнавати індивідуальні жести, інтонації та патерни руху. Це значно підвищує комфорт, швидкість реакції та ефективність управління протезом, роблячи повсякденне життя людей з втратою кінцівок більш незалежним та інтегрованим у соціальне середовище.

Список використаних джерел:

1. Савчук А.В., Попов А.О. Методи та засоби інтелектуального управління протезами верхніх кінцівок. *Електроніка та зв'язок*, *22*(2), 2017, с. 33 – 42.

УДК 612.67

Андреєв О.В., доцент
Нікітчук С.М., ст. викладач,
Возний О.А., аспірант
Нікітчук В.С., здобувач
Державний університет «Житомирська політехніка»

ТЕНДЕНЦІЇ ТА ВИКЛИКИ СУЧАСНИХ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ

Сучасне відеоспостереження – це інтелектуальна, гнучка та мережева технологія, яка продовжує активно розвиватися, надаючи користувачам все більше можливостей для забезпечення безпеки та отримання інформації в реальному часі. Відеоспостереження наразі перебуває на етапі стрімкого розвитку та глибокої інтеграції з іншими технологіями і вже давно перестало бути просто засобом запису відео і перетворилося на потужний інструмент для забезпечення безпеки, оптимізації бізнес-процесів та отримання цінних даних. В результаті аналізу, можна окреслити тенденції та характеристики сучасного відеоспостереження:

- перехід на IP-технології, адже аналогові системи поступово витісняються цифровими (IP) рішеннями, які забезпечують значно вищу якість зображення (HD, Full HD, 4K і вище), гнучкість, масштабованість та розширені функціональні можливості;

- розвиток відеоаналітики: сучасні системи відеоспостереження оснащуються потужними алгоритмами відеоаналітики, які дозволяють автоматично виявляти та реагувати на різні події: (детекція руху, перетину лінії, вторгнення в зону; розпізнавання обличь для ідентифікації осіб та контролю доступу; розпізнавання номерних знаків для контролю транспортних потоків; підрахунок людей та автомобілів для аналізу трафіку та завантаженості доріг; виявлення залишених або зниклих предметів; аналіз поведінки тощо;

- інтеграція зі штучним інтелектом (ШІ). ШІ стає ключовим елементом сучасних систем відеоспостереження, значно підвищуючи точність та ефективність відеоаналітики, зменшуючи кількість хибних спрацьовувань та забезпечуючи більш глибокий аналіз відеоданих;

- використання хмарних технологій, оскільки хмарне зберігання відеозаписів стає все більш популярним завдяки своїй зручності, надійності та можливості віддаленого доступу до архіву з будь-якої точки світу. Хмарні платформи також надають розширені можливості для аналізу відеоданих;

- бездротові технології: Wi-Fi та інші бездротові протоколи спрощують встановлення та розгортання систем відеоспостереження, особливо в домашніх умовах та малих офісах;

- мобільний доступ та керування - зручні мобільні додатки дозволяють користувачам переглядати відео в реальному часі, отримувати сповіщення про події, керувати налаштуваннями системи з будь-якого місця;

- розвиток IoT (Інтернету речей), адже відеокамери все частіше інтегруються з іншими пристроями «розумного дому» та промисловими системами, створюючи єдину екосистему безпеки та автоматизації;

- підвищення кібербезпеки. Зростання кількості кіберзагроз зумовлює підвищену увагу до безпеки систем відеоспостереження. Розробники впроваджують сучасні методи шифрування, аутентифікації та захисту від несанкціонованого доступу.

На ринку існує велика різноманітність систем відеоспостереження, які відрізняються за технологією, функціональністю, вартістю та призначенням. Основні типи можна класифікувати таблицею 1:

Тип	Принцип роботи
За технологією передачі сигналу	
Аналогові системи відеоспостереження	Передають відеосигнал по коаксіальному кабелю у нецифровому вигляді. Переваги: відносно проста установка, нижча вартість обладнання (у порівнянні з IP на момент їхнього розквіту). Недоліки: обмежена якість зображення (зазвичай SD), складнощі з масштабуванням, обмежена дальність передачі сигналу без підсилювачів, менша функціональність (відсутність вбудованої аналітики).
IP (цифрові) системи відеоспостереження	Передають відео та аудіо дані в цифровому вигляді по мережі Ethernet (часто використовуючи протокол TCP/IP). Переваги: висока якість зображення (HD, Full HD, 4K і вище), гнучкість та масштабованість, проста інтеграція з мережевою інфраструктурою, підтримка розширеної аналітики (розпізнавання обличь, детекція руху, перетин лінії тощо), можливість живлення по PoE (Power over Ethernet). Недоліки: вища вартість обладнання (зазвичай), складніша початкова настройка мережі, вищі вимоги до пропускної здатності мережі.
Гібридні системи відеоспостереження	Поєднують можливість підключення як аналогових, так і IP-камер до одного відеореєстратора (DVR/NVR).

	Переваги: гнучкість при модернізації існуючих аналогових систем, можливість поступового переходу на IP-технології Недоліки: компроміс між функціональністю аналогових та IP-систем, потенційні обмеження у кількості підключених камер кожного типу.
За призначенням та функціональністю	
Домашні системи відеоспостереження	Зазвичай прості в установці та використанні, часто бездротові (Wi-Fi), з можливістю перегляду відео через мобільний додаток, з функціями виявлення руху та надсилання сповіщень. Можуть включати хмарне зберігання даних.
Системи відеоспостереження для малого бізнесу:	Більш розширені функції, підтримка більшої кількості камер, можливість локального зберігання даних на мережевому відеореєстраторі (NVR), часто з елементами відеоаналітики.
Професійні системи відеоспостереження для великого бізнесу та промислових об'єктів:	Висока надійність, велика кількість камер, централізоване управління, розширена відеоаналітика, інтеграція з іншими системами безпеки (контроль доступу, охоронна сигналізація).
Системи відеоспостереження для громадських місць та міської інфраструктури:	Висока стійкість до вандалізму та погодних умов, велика кількість камер, інтелектуальні функції аналізу трафіку, розпізнавання номерних знаків, пошук об'єктів.
За типом камер	
Купольні камери	Компактні, непомітні, часто використовуються всередині приміщень
Циліндричні (bullet) камери	Мають витягнуту форму, часто використовуються на вулиці, можуть мати вбудоване ІЧ-підсвічування
PTZ (Pan-Tilt-Zoom) камери	Мають можливість дистанційного керування поворотом, нахилом та зумом об'єктива
Панорамні камери (риб'яче око)	Забезпечують огляд на 180 або 360 градусів
Приховані камери	Замасковані під різні предмети інтер'єру або екстер'єру
Тепловізійні камери	Виявляють об'єкти за їхнім тепловим випромінюванням

Системи відеоспостереження, хоча й є потужним інструментом для забезпечення безпеки, мають низку проблем, які можуть обмежувати їхню ефективність:

1. Технічні проблеми: якість зображення – недостатня роздільна здатність камер, особливо в умовах низької освітленості; спотворення

зображення через погодні умови (дощ, сніг, туман); проблеми з фокусуванням та налаштуванням камер;

2. Проблеми з підключенням: втрата сигналу через нестабільне Wi-Fi з'єднання або пошкодження кабелів; проблеми з живленням камер, що призводять до їх відключення; конфлікти IP-адрес при використанні мережевих камер;

3. Зберігання даних: недостатній обсяг пам'яті для зберігання великого обсягу відеозаписів; проблеми з доступом до архівних записів; ризик втрати даних через пошкодження носіїв інформації тощо;

4. Кібербезпека: вразливість систем до хакерських атак, що може призвести до несанкціонованого доступу до відеозаписів; ризик витоку конфіденційної інформації та ін..

Сучасне відеоспостереження є динамічною галуззю з великим потенціалом для підвищення рівня безпеки та ефективності різних сфер діяльності. Однак, для повноцінного використання всіх переваг цих технологій необхідно активно працювати над вирішенням існуючих викликів, особливо в галузі кібербезпеки, управління даними та дотримання етичних норм. Подальший розвиток штучного інтелекту, хмарних технологій та стандартизація протоколів обіцяють ще більше розширити можливості систем відеоспостереження в майбутньому.

Тому, в подальшому, буде приділено увагу конкретним стратегіям та інструментам для підвищення кібербезпеки систем відеоспостереження, ефективним методам зберігання та аналізу великих масивів відеоданих, а також правовим та етичним аспектам використання інтелектуальних систем відеоспостереження. Крім того, планується дослідження перспективних напрямків розвитку галузі, таких як подальша інтеграція ШІ, використання периферійних обчислень (Edge Computing) та розширення можливостей інтеграції з іншими системами безпеки та "розумного міста".

Список використаних джерел:

1. Відеоспостереження і охоронні системи.[Електронний ресурс]. – Режим доступу: URL: http:// https://secur.ua

2. Технології для відеоспостереження [Електронний ресурс]. – Режим доступу: URL: https://viatec.ua

3. Головні технологічні тренди розвитку відеоспостереження [Електронний ресурс]. – Режим доступу: URL: https://bezpeka.club/golovni-tehnologichni-trendy-rozvytku-videosposterezhennya

4. Особливості ринку відеоспостереження в 2023 року [Електронний ресурс]. – Режим доступу: URL: https://montageplus.cn.ua/

УДК 623.48

Сімчук А.Р., аспірант
Мацієвський В.А., аспірант
Нікітчук Т.М., к.т.н., доц.
Морозов Д.С., ст.викладач
Державний університет «Житомирська політехніка»

МАЙБУТНЄ ПЕРЕДАЧІ МЕДИЧНОЇ ІНФОРМАЦІЇ: НОВІ ТЕХНОЛОГІЇ ТА ПЕРСПЕКТИВИ

Як вже було зазначено в [1, 2] та згідно проведеного аналізу публікацій дослідників у галузі, сфера передачі медичної інформації в інформаційно-телекомунікаційних системах постійно еволюціонує. Сучасні тенденції, такі як цифровізація охорони здоров'я, розвиток Інтернету медичних речей (IoMT) та потреби у швидкому й безпечному обміні даними між медичними закладами та пацієнтами, стимулюють впровадження новітніх технологій зв'язку.

Одним із ключових напрямків розвитку є наскрізна передача даних від датчика до хмари**.** Це передбачає інтеграцію різноманітних медичних пристроїв, від простих фітнес-трекерів до складного діагностичного обладнання, в єдину мережу. Дані, зібрані цими пристроями, безперервно передаються через різні канали зв'язку до централізованих хмарних платформ для зберігання, обробки та аналізу.

Нові технології зв'язку, такі як TSN (Time-Sensitive Networking), SPE (Single Pair Ethernet), APL (Advanced Physical Layer) та 5G, відіграватимуть вирішальну роль у забезпеченні ефективної передачі зростаючих обсягів медичної інформації, а саме:

- TSN (Time-Sensitive Networking) – технологія забезпечує детерміновану передачу даних в мережах Ethernet, що є критично важливим для застосунків реального часу в медицині, таких як дистанційний моніторинг життєво важливих показників або керування медичним обладнанням. TSN гарантує передбачувану затримку та надійність передачі, що є неприпустимим для критичних медичних даних;
- SPE (Single Pair Ethernet) дозволяє передавати дані та живлення через одну скручену пару проводів, що значно спрощує підключення кінцевих пристроїв, особливо в обмежених просторах або у випадку великої кількості сенсорів. Це зменшує вартість та складність інфраструктури, роблячи підключення медичних датчиків більш гнучким та економічним.
- APL (Advanced Physical Layer) є стандартом для передачі даних та живлення через одну скручену пару проводів у вибухонебезпечних зонах, що є важливим для деяких промислових медичних застосунків,

наприклад, у фармацевтичному виробництві або при роботі з певним медичним обладнанням;

- 5G: мережі п’ятого покоління пропонують значно вищу пропускну здатність, меншу затримку та більшу щільність підключення пристроїв порівняно з попередніми поколіннями мобільного зв’язку. Це відкриває нові можливості для телемедицини, дистанційного моніторингу пацієнтів, передачі великих обсягів медичних зображень та відео в режимі реального часу, а також для розвитку мобільних медичних застосунків (mHealth).

Інтеграція цих нових технологій з існуючими методами передачі даних створить гібридні інформаційно-телекомунікаційні системи, які зможуть забезпечити високу пропускну здатність (для передачі великих обсягів медичних зображень, відеоконференцій під час телемедичних консультацій та інших ресурсомістких даних), низьку затримку (для застосунків реального часу, таких як дистанційне хірургічне втручання або моніторинг критичних станів пацієнтів), надійність та безпеку (забезпечення стабільної та захищеної передачі конфіденційної медичної інформації), масштабованість (можливість підключення великої кількості різноманітних медичних пристроїв та користувачів), економічну ефективність тощо.

У майбутньому можна очікувати подальшого розвитку та впровадження цих та інших новітніх технологій зв’язку в медичній галузі. Це сприятиме створенню більш ефективних, доступних та персоналізованих систем охорони здоров’я, покращуючи якість медичних послуг та підвищуючи рівень життя пацієнтів. Подальші дослідження будуть спрямовані на інтеграцію цих технологій з платформами штучного інтелекту для автоматизованого аналізу медичних даних та підтримки прийняття клінічних рішень.

Список використаних джерел:

1. Сімчук А.Р., Маційовський В.А., Нікітчук Т.М. Засоби передачі медичної інформації у інформаційно-телекомунікаційних системах. Тези Всеукраїнської науково-практичної on-line конференції здобувачів вищої освіти і молодих учених, присвяченої Дню науки, 13–17 травня 2024 року. Житомир : «Житомирська політехніка», 2024. С.67.

2. Нікітчук Т.М., Гулько А.О., Гулько Ю.О. Дослідження прийому та передачі біомедичних сигналів засобами IoT. Тези XIV Міжнародної науково-технічної конференції «Інформаційно-комп’ютерні технології – 2024», 28 – 29 березня 2024 р. Житомир; "Житомирська політехніка", 2024. С.159

Секція 5
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ В ОСВІТІ

УДК 004.4'275:7.02]-047.38:[37.016:004](06)

Тітова Л.О., викладач
Уманський державний педагогічний університет імені Павла Тичини

МОУШН-ДИЗАЙН НА УРОКАХ ІНФОРМАТИКИ: ОГЛЯД СУЧАСНИХ ПЛАТФОРМ

Для сучасних здобувачів освіти кліпове мислення стало нормою, а їхня увага вимірюється секундами, тому статичні презентації та монотонні пояснення давно втратили свою ефективність. Моушн-дизайн, що ще нещодавно був прерогативою професійних студій, сьогодні використовується у шкільній освіті, перетворюючи уроки інформатики на захоплюючі цифрові подорожі. За дослідженнями нейропсихологів, мозок опрацьовує візуальну інформацію набагато швидше, ніж текст, а додавання елементу руху створює ідеальні умови для засвоєння складного теоретичного матеріалу. Зважаючи на це, інтеграція інструментів моушн-дизайну в освітній процес стає не розкішшю, а необхідністю сучасної педагогіки інформатики.

М. Мурашко характеризує моушн-дизайн як «вид проектно-художньої діяльності, спрямований на створення аудіовізуальної продукції за допомогою засобів дизайну, аудіо й комп'ютерної анімації, де єдність форми та змісту зумовлена рухом, з яким пов'язані всі художньо-естетичні характеристики» [1]. Простими словами моушн-дизайн поєднує елементи графічного дизайну, анімації, 3D-моделювання, відеодизайну та ілюстрації. Він є частиною сучасного медіаарту та споріднений із відеоартом та цифровим мистецтвом [2].

В освітньому контексті моушн-дизайн включає створення анімованих презентацій та зображень, навчальних відеороликів, інтерактивних інфографік та інших динамічних елементів для візуалізації навчального матеріалу.

Моушн-дизайн як педагогічний інструмент дозволяє візуалізувати навчальний матеріал (особливо абстрактні та складні для сприйняття поняття), а також покращити його запам'ятовування через інтерактивність та динамічність, підвищити рівень залученості та мотивації здобувачів освіти до навчання. Важливою перевагою використання елементів моушн-дизайну під час вивчення інформатики є демонстрація процесів у часі, оскільки дозволяє показати роботу алгоритмів, процес виконання коду, функціонування баз даних тощо.

Застосування моушн-дизайну в освітньому процесі може здійснюватися через:

- створення учнями власних анімацій, анімованих презентацій, відеороликів;
- роботу з 3D-анімацією для візуалізації об'єктів, явищ та процесів;
- програмуванні об'єктів чи персонажів, наприклад при вивченні Scratch, Tinkercad Codeblocks тощо.
- використання динамічних конструкцій для пояснення навчальних матеріалів;
- розробку навчальних відео для подальшого використання у системах керування навчанням чи розміщенні на відеохостингах на кшталт Youtube;

На сьогодні існує широкий спектр платформ для моушн-дизайну. Серед яких можна виділити наступні:

- Canva (https://www.canva.com/) – онлайн-платформа для створення візуальної продукції із простим інтерфейсом, яка, зокрема, дозволяє створювати презентації, анімації та відео.
- Adobe After Effects – професійний інструмент від компанії Adobe для створення складної анімаційної графіки (включаючи 3D) та візуальних ефектів.
- Vyond (https://www.vyond.com/) – ШІ-платформа для створення різних видів відеоконтенту (анімаційних, з ШІ-аватарами тощо), які можуть бути використані в освітньому процесі для пояснення навчального матеріалу.
- Blender – безкоштовний редактор для створення 3D-графіки, зокрема й анімованої, що може бути використаний для створення складних проєктів.

Впровадження моушн-дизайну в освітній процес з інформатики відкриває нові горизонти для ефективного засвоєння складного матеріалу та розвитку інформаційно-цифрової компетентності учнів. Аналіз сучасних платформ для створення анімаційного контенту показує, що наразі існує широкий спектр інструментів різного рівня складності, які дозволяють педагогам інтегрувати динамічні візуалізації в освітній процес. Поєднання технічних можливостей цих платформ із продуманою методикою викладання дає змогу трансформувати традиційні уроки інформатики в інтерактивні та більш ефективні.

Список використаних джерел:

1. Мурашко М. В. Проектно-художній інструментарій моушн-дизайну (на прикладі рекламного ролику): автореф. дис. …канд. мистецтвознавства: 17.00.07 «Дизайн». Харків, 2017. 23 с.

2. Олійник В. Моушн-дизайн у контексті українського сучасного медіа-арту: зміст і перспективи. *Деміург: ідеї, технології, перспективи дизайну*. 2022. Т.5, № 2. С. 261–269. URL: https://doi.org/10.31866/2617-7951.5.2.2022.266917.

УДК 37.016:004.42]:004.8](045)

Медведєва М.О., к.пед.н., доц.
завідувач кафедри інформатики і інформаційно-комунікаційних технологій
Уманський державний педагогічний університет імені Павла Тичини

СУЧАСНІ МОЖЛИВОСТІ ШТУЧНОГО ІНТЕЛЕКТУ У НАВЧАННІ ПРОГРАМУВАННЮ

Штучний інтелект (ШІ) стає невід'ємною частиною освіти, зокрема у сфері навчання програмуванню. Інтеграція технологій ШІ дозволяє підвищити ефективність освітнього процесу, персоналізувати навчання та автоматизувати багато аспектів викладання. Завдяки інтелектуальним алгоритмам здобувачі освіти можуть отримувати індивідуальні рекомендації, автоматичний аналіз коду, інтерактивний зворотний зв'язок та доступ до адаптивних навчальних платформ.

Одним із ключових напрямів використання ШІ у навчанні програмуванню є розробка інтелектуальних систем підтримки кодування. Такі платформи, як GitHub Copilot, CodeT5, Tabnine та Amazon CodeWhisperer, використовують машинне навчання для автоматичного доповнення коду, що допомагає здобувачам освіти швидше розв'язувати завдання та вивчати нові синтаксичні конструкції. Ці системи аналізують контекст написаного коду та пропонують оптимальні варіанти його доповнення, зменшуючи кількість помилок та підвищуючи продуктивність навчання.

Ще одним важливим аспектом є інтерактивні навчальні платформи, що використовують ШІ для адаптації курсу під рівень знань здобувача освіти. Серед них можна виокремити Code.org, JetBrains Academy, Codecademy, Coursera та EdX, які застосовують алгоритми аналізу прогресу здобувача освіти, адаптивне тестування та рекомендаційні системи для персоналізованого навчання. Завдяки цьому здобувачі освіти можуть отримувати завдання відповідної складності, які поступово розвивають їхні навички програмування.

ШІ також активно використовується для автоматичного оцінювання коду. Інструменти на основі машинного навчання, такі як MOSS (Measure of Software Similarity), можуть порівнювати програми здобувачів освіти та визначати рівень унікальності їхніх рішень, що є важливим для виявлення плагіату та аналізу стилю програмування. Системи на кшталт Pythia та AutoGrader забезпечують автоматичне тестування коду, виявлення помилок та їх пояснення, що значно скорочує навантаження на викладачів.

Використання віртуальних асистентів та чат-ботів є ще одним перспективним напрямом інтеграції ШІ у навчання програмуванню. Чат-боти, такі як ChatGPT, Replika та CodePal, можуть допомагати здобувачам освіти у роз'ясненні складних концепцій, надавати підказки щодо синтаксису та структури коду, а також моделювати роботу реальних програмістських середовищ. Це сприяє створенню інтерактивного освітнього середовища, де здобувачі освіти можуть отримувати негайні відповіді на свої запитання.

Крім того, ШІ сприяє розвитку навчання через гейміфікацію та симуляційні середовища. Навчальні платформи, такі як Robocode, CodinGame та CodeCombat, використовують елементи гри та інтерактивні сценарії для залучення здобувачів освіти до освітнього процесу. Використання симуляцій дозволяє навчатися на основі практичного досвіду, що підвищує рівень засвоєння матеріалу та мотивацію здобувачів освіти.

Незважаючи на всі переваги, використання ШІ у навчанні програмуванню також постає перед певними викликами. Серед основних проблем можна виділити етичні аспекти, пов'язані з академічною доброчесністю, оскільки здобувачі освіти можуть зловживати автоматизованими засобами під час виконання завдань. Крім того, алгоритми ШІ можуть мати упередженість та обмеження в аналізі складних завдань, що вимагає залучення викладачів для перевірки критично важливих аспектів коду.

Таким чином, сучасні можливості штучного інтелекту значно розширюють потенціал навчання програмуванню, дозволяючи зробити його більш гнучким, адаптивним та ефективним. Використання інтелектуальних платформ, автоматизованих систем аналізу коду, віртуальних асистентів та гейміфікаційних технологій сприяє підвищенню якості освітнього процесу та підготовці майбутніх фахівців у сфері інформаційних технологій. Водночас важливо забезпечити баланс між використанням ШІ та традиційними методами навчання, щоб здобувачі освіти не лише отримували відповіді від алгоритмів, а й розвивали власні аналітичні та логічні здібності.

Список використаних джерел:

1. Медведєва М. О. Інноваційні AI-інструменти в освіті: трансформація освітнього процесу за допомогою штучного інтелекту // *New Horizons in Scientific Research: Challenges and Solutions:* матеріали міжнар. наук.-практ. конф., 21–23 жовтня 2024 р. Марсель. С. 137–140.

УДК 37.011.3-051:334.722-047.22-043.83]:004.946-049.7(06)

Кібаленко В.В., аспірант 1-го року навчання кафедри педагогіки та освітнього менеджменту
Уманський державний педагогічний університет імені Павла Тичини

ВИКОРИСТАННЯ EASYAR.COM ДЛЯ СТВОРЕННЯ НАВЧАЛЬНОГО КОНТЕНТУ, СПРЯМОВАНОГО НА ФОРМУВАННЯ ПІДПРИЄМНИЦЬКОЇ КОМПЕТЕНТНОСТІ ПЕДАГОГІВ

Доповнена реальність є однією з перспективних технологій у сфері освіти, що дозволяє інтегрувати цифрові об'єкти в реальне середовище. Зокрема, застосування AR в освітньому процесі сприяє підвищенню залученості педагогів у процес активного навчання, покращенню візуалізації складних концепцій, розвитку навичок ухвалення рішень у змодельованих ситуаціях, стимулюванню критичного мислення та креативності тощо.

Підприємницька компетентність педагогів передбачає не лише знання основ бізнесу та фінансової грамотності, але й здатність застосовувати інноваційні технології у професійній діяльності. Саме тут технології доповненої реальності можуть стати ефективним засобом навчання, оскільки забезпечують інтерактивний підхід до вивчення підприємництва через візуалізацію економічних моделей, бізнес-процесів та стратегій управління.

Цифровізація освітнього процесу та впровадження сучасних технологій відкривають нові можливості для формування ключових компетентностей педагогів, зокрема підприємницької. Одним із ефективних інструментів для створення інтерактивного навчального контенту є технологія доповненої реальності. Вона сприяє підвищенню зацікавленості у навчанні, активному засвоєнню знань та розвитку підприємницьких навичок через моделювання реальних бізнес-ситуацій. Одним із популярних сервісів для розробки AR-контенту є EasyAR.com, який надає можливість створювати інноваційні навчальні середовища без необхідності глибоких знань у програмуванні.

EasyAR – це платформа для розробки застосунків доповненої реальності, яка забезпечує простоту використання, широкі можливості інтеграції та підтримку різних форматів контенту. До основних переваг EasyAR можна віднести: доступність (можливість безкоштовного використання базових функцій та розширених можливостей у преміум-версії); інтуїтивний інтерфейс (користувачі можуть створювати AR-контент без глибоких знань у програмуванні); сумісність з мобільними

пристроями (створені моделі можуть відображатися на смартфонах і планшетах); гнучкість (підтримка 3D-об'єктів, інтерактивних відео, анімацій і текстових блоків); інтеграція з іншими платформами (можливість використання контенту в LMS-системах для дистанційного навчання).

Впровадження EasyAR у навчання для формування підприємницької компетентності педагогів може здійснюватися за кількома ключовими етапами. По-перше, визначення освітніх цілей, тобто окреслити навички, які необхідно сформувати, такі як управління ресурсами, фінансова грамотність, стратегічне планування тощо. По-друге, розробка AR-контенту, яка полягає у створені навчальних модулів, що включають: AR-моделі бізнес-процесів; інтерактивні кейси; симуляції. По-третє, інтеграція AR у навчальні програми, тобто включення доповненої реальності в навчальні дисципліни шляхом використання мобільних застосунків, інтерактивних дошок, LMS-платформ. І по-четверте, оцінка ефективності навчального контенту, а саме аналіз впливу AR-контенту на формування підприємницької компетентності педагогів за допомогою анкетування, тестування, моніторингу успішності.

Щодо застосування EasyAR у навчанні педагогів, то можна використовувати наступні активності як-от: моделювання стартапів у віртуальному середовищі, де педагоги можуть у реальному часі оцінювати стратегії запуску бізнесу, аналізувати ризики та ефективність інвестицій; використання AR-квестів для розвитку підприємницьких навичок, що містять інтерактивні навчальні маршрути, що включають завдання з економіки, менеджменту та маркетингу; гейміфіковані бізнес-сценарії, коли використовують віртуальні симуляції, де учасники приймають управлінські рішення в умовах змінного ринку.

Отже, використання EasyAR в освітньому процесі дозволяє ефективно формувати підприємницьку компетентність педагогів, поєднуючи інтерактивність, моделювання реальних ситуацій та практичний досвід. Інтеграція AR в освітні програми забезпечує нові можливості для персоналізації навчання, розвитку навичок критичного мислення та адаптації до сучасних економічних та професійних викликів.

Список використаних джерел:

1. Вакалюк Т. А., Медведєва М. О. Використання технологій доповненої реальності в освітньому процесі // *«Інформаційно-комп'ютерні технології – 2021 (ІКТ-2021)» :* тези доп. XII Міжнар. науково-техн. конф., м. Житомир, 1–3 квіт. 2021 р. С. 137–138.

УДК 681.3.07

Войтко В.В, к.т.н., доцент,
Вінницький національний технічний університет,
Бевз С.В., к.т.н., доцент,
Житомирський військовий інститут імені С.П. Корольова
Бурбело С.М., к.т.н.,
Житомирський військовий інститут імені С.П. Корольова
Юдін О.С., здобувач
Вінницький національний технічний університет

РОЗРОБКА МЕТОДІВ ТА ІНСТРУМЕНТІВ ВЕБСИСТЕМИ ВІЗУАЛІЗАЦІЇ, АНАЛІЗУ ТА ОЦІНЮВАННЯ СТАТИЧНИХ ЗОБРАЖЕНЬ

Обробка та аналіз зображень є важливими завданнями в багатьох сферах. Автоматизовані вебсистеми дозволяють значно спростити процес оцінювання візуальної інформації та забезпечують зручні інструменти для роботи з графічними даними [1].

Зі зростанням обсягів цифрових зображень виникає необхідність у швидких та ефективних методах їх обробки. Застосування алгоритмів машинного навчання, нейронних мереж та методів комп'ютерного зору відкриває можливості для автоматичного аналізу візуальних даних, їх класифікації та оцінювання якісних характеристик. Водночас інтеграція таких алгоритмів у вебсередовище дозволяє створювати доступні й масштабовані рішення для обробки зображень у режимі реального часу.

Важливим аспектом сучасних вебсистем є інтерактивність і персоналізація [2]. Користувачі не тільки переглядають контент, а й взаємодіють із ним через лайки, коментарі, пошук і системи рекомендацій. Це створює потребу у функціональній платформі, яка дозволяє не лише завантажувати та переглядати зображення, а й аналізувати їхні характеристики, оцінювати за певними критеріями, систематизувати за тегами та обмінюватися контентом між користувачами.

Вебсистема орієнтована на широке коло користувачів, включаючи науковців, дизайнерів, медичних спеціалістів та розробників, що працюють із цифровими зображеннями. Вона забезпечить інструменти для точного аналізу, обробки та візуалізації отриманих результатів, використовуючи сучасні стандарти веброзробки та бібліотеки для обробки графічних даних.

Розроблена вебсистема призначена для інтерактивного аналізу, оцінювання та обміну зображеннями. Вона дозволяє автоматизувати процеси взаємодії користувачів, проводити тематичні конкурси та ефективно організовувати цифровий контент.

Функціональні можливості системи охоплюють:

– можливість створювати пости із зображеннями та додавати до них теги;

– інтегрована система лайків, коментарів та обміну постами між користувачами;

– пошуковий механізм із фільтрацією за тегами та текстом у постах;

– персональні профілі користувачів з історією публікацій;

– система збережених постів для зручного доступу до вибраного контенту;

– конкурсне оцінювання зображень за заданими критеріями;

– можливість користувачам обмінюватися постами один з одним через спеціальний запит.

Отже, вебсистема орієнтована на створення динамічного середовища для взаємодії користувачів, де кожен може легко ділитися візуальним контентом та брати участь в оцінюванні творчих робіт. Інтуїтивний процес додавання зображень, пошук за ключовими словами та тегами, а також можливість коментування та обміну постами сприяють формуванню активної спільноти [3,4].

Гнучкість функціоналу дає змогу користувачам організовувати свій цифровий контент, швидко знаходити релевантні матеріали та зручно взаємодіяти з іншими учасниками платформи.

Головною перевагою розробленої системи є поєднання можливостей соціальної взаємодії, структурованого управління зображеннями та механізмів оцінювання, включаючи конкурси з гнучкими критеріями відбору. Це робить платформу привабливою для широкого кола користувачів.

Список використаних джерел:

1. ImgPost. URL: https://imgpost.net/?lang=uk (дата звернення: 10.03.2016).

2. Unsplash. URL: https://unsplash.com/ (дата звернення: 10.03.2016).

3. Pexels. URL: https://www.pexels.com/uk-ua/ (дата звернення: 10.03.2016).

4. Pixabay. URL: https://pixabay.com/ (дата звернення: 10.03.2016).

УДК 004.4

Сидорчук О.С., магістрант
Бейрак Д.Я., ст. викл. кафедри комп'ютерних наук
Державний університет «Житомирська політехніка»

АНАЛІЗ ЕФЕКТИВНОСТІ СЕРВІСІВ ОНЛАЙН-МЕНЕДЖМЕНТУ ОСВІТНІХ ПРОЦЕСІВ У ЗАКЛАДАХ ВИЩОЇ ОСВІТИ

Сучасна система вищої освіти стикається з низкою викликів, пов'язаних із необхідністю автоматизації управління освітніми процесами. Великі обсяги інформації про студентів, розклад занять, результати успішності, а також взаємодія між викладачами й адміністрацією потребують ефективного та інтегрованого підходу до управління даними. Існуючі проблеми включають надмірну паперову бюрократію, недостатню прозорість процесів, складнощі з відстеженням академічних успіхів студентів, а також необхідність постійного зв'язку з офіційним реєстром здобувачів освіти.

Запровадження онлайн-сервісів для менеджменту освітніх процесів здатне значно полегшити ці завдання. Ефективні системи онлайн-менеджменту сприяють економії часу, підвищенню точності даних та забезпечують доступ до актуальної інформації в режимі реального часу.

Було проведено аналіз існуючих сервісів онлайн-менеджменту, таких як Moodle, Anthology та АСУ «ВНЗ». Кожна з цих систем фокусується на певних задачах і відповідно має свої переваги та недоліки.

Moodle [1] є проектом з відкритим вихідним кодом, забезпечує широкий функціонал, включаючи основні його якості: можливість створення навчальних курсів, виставлення оцінок, ведення електронного журналу. Величезна кількість модулів та опцій дають можливість здійснити необхідне трансформування майбутньої системи навчального закладу, однак водночас створюють труднощі у налаштуванні. Разом зі збільшенням кількості модулів, експоненційно зростає і важкість подальшої підтримки, на що впливає й подекуди застарілий код проекту.

Anthology [2] — це одна з провідних платформ для онлайн-навчання, яка широко використовується у закладах вищої освіти завдяки своїм розширеним можливостям керування навчальним процесом. Основними перевагами Anthology є розвинена система аналітики, що дозволяє відстежувати успішність студентів, а також потужні засоби комунікації, включаючи форуми, відеочати та електронну пошту. Система інтегрується з популярними інструментами, такими як Microsoft 365 і Google Workspace, що

спрощує взаємодію викладачів і студентів. Водночас, основним недоліком Anthology є його складний інтерфейс, який може потребувати додаткового навчання для користувачів, а також вартість її використання.

АСУ «ВНЗ» [3] — це вітчизняна система управління навчальним процесом, орієнтована на автоматизацію освітніх та адміністративних процесів у закладах вищої освіти. Вона дозволяє ефективно керувати навчальними планами, обліковувати академічні успіхи студентів, автоматизувати розклад занять та забезпечувати документообіг. Головною перевагою АСУ «ВНЗ» є її адаптація до вимог української освітньої системи, що включає підтримку нормативних актів і державних стандартів. Крім того, система може працювати на локальних серверах, що забезпечує конфіденційність даних. Проте обмежена інтеграція з сучасними міжнародними освітніми платформами та менш зручний інтерфейс, вартість ліцензії, а також відносна застарілість та непопулярність системи серед університетів роблять її не надто надійним рішенням.

Таким чином, аналіз сервісів показує, що жоден із них не забезпечує повного набору можливостей для якісного та зручного управління процесами в університеті. Moodle є безкоштовним, відкритий код дозволяє вибудувати систему виходячи з індивідуальних потреб, але якість та подальше обслуговування роблять її не найкращим варіантом. Anthology надає інструменти аналітики, засоби комунікації та інтеграцію із сучасними сервісами, що є лише частиною із усіх необхідних модулів для управління освітніми процесами. АСУ «ВНЗ» відповідає нормам українського законодавства та дає повний функціонал для адміністрації, проте має високу ціну і низьку популярність, що призвело до зниження інтенсивності оновлень та її застарілості. Ці фактори спонукають до розробки нової системи, що враховуватиме усі вищезазначені недоліки та стане успішним додатком на ринку.

Список використаних джерел:

1. Moodle. URL: https://moodle.org (дата звернення: 12.03.2025).
2. Anthology. URL: https://www.anthology.com (дата звернення: 12.03.2025).
3. АСУ «ВНЗ». URL: https://vuz.osvita.net (дата звернення: 12.03.2025).

УДК 004.94:378

Цалко Я.В., здобувач,
Морозов А.В., к.т.н., доцент,
Плечистий Д.Д., к.т.н., доцент,
Державний університет «Житомирська політехніка»

МОДУЛЬ «ЗДОБУВАЧІ ОСВІТИ» ЯК СКЛАДОВА ІНФОРМАЦІЙНОЇ СИСТЕМИ «DIGITAL UNIVERSITY UA»

У сучасних умовах цифрової трансформації закладів вищої освіти (ЗВО) особливу увагу приділяють створенню та впровадженню інформаційних систем, які б забезпечували зручне, своєчасне й достовірне відображення даних. Питання розробки таких систем досліджувалося в роботах [1-3].

В Україні основним джерелом інформації про контингент студентів є Єдина державна електронна база з питань освіти (ЄДЕБО). Саме на її основі формується первинна інформація про вступників, які в подальшому стають здобувачами вищої освіти в ЗВО. Розроблений модуль «Здобувачі освіти» для інформаційної системи «Digital University UA» призначений для централізованого керування академічними групами, а також формування необхідних супровідних документів для кожного здобувача.

Початковим етапом функціонування модуля «Здобувачі освіти» є відображення даних про здобувачів вищої освіти. У меню «Здобувачі освіти - Усі здобувачі» користувачі із відповідними правами доступу можуть переглядати, фільтрувати та сортувати список здобувачів, які навчаються або навчалися у даному ЗВО. У таблиці для кожного здобувача вищої освіти відображається базова інформація, яка включає: прізвище, ім’я, по батькові; дату народження; унікальний ID картки (навчання) з ЄДЕБО; належність до академічної групи; курс; форму й основу фінансування (бюджет/контракт); освітній ступінь; спеціальність; освітню програму; факультет; дату початку та дату завершення навчання тощо. Користувачі можуть також переглядати детальну “картку здобувача” – індивідуальний профіль студента в ІС, де відображаються всі відомості з ЄДЕБО та додаткова інформація, яку вносять різні структурні підрозділи.

В ІС “Цифровий університет” реалізовано можливість централізованого додавання і зберігання супровідних документів, які стосуються перебігу навчання конкретного здобувача. Працівники деканатів та інших підрозділів, що мають відповідні права, можуть завантажувати додаткові файли до картки студента й при потребі

завантажувати типовий шаблон навчальної картки в редагованому форматі Word.

Важливою складовою діяльності деканатів у кожному ЗВО є формування, ведення та регулювання складу академічних груп.

Первинне створення академічних груп в ІС «Digital University UA» автоматизоване завдяки інтеграції із ЄДЕБО. Імпортування групи з ЄДЕБО дозволяє сформувати однойменну академічну групу в системі та прикріпити до неї здобувачів відповідного набору. У подальшому всі операції з переведення студентів між групами чи зміни їхнього курсу навчання виконуються лише в ІС «Digital University UA» і не потребують повторного ведення цих даних в ЄДЕБО.

Наступним аспектом, що часто постає в ЗВО, є переведення студентів на інший курс (наприклад, після успішної атестації, завершення академічної різниці чи виправлення технічних помилок). Для цього в ІС «Digital University UA» передбачено спеціальний розділ «Курси та статуси» у меню «Здобувачі освіти». У ньому доступні фільтри за назвою групи, освітнім ступенем, формою навчання, спеціальністю тощо. Вибравши потрібні групи, можна виконати групову операцію «Збільшити на 1 курс» або «Зменшити на 1 курс». Система автоматично оновить у своїй базі курс для всіх здобувачів цих груп і передасть зміни в ЄДЕБО. Це особливо зручно для масштабного переведення, яке відбувається наприкінці кожного навчального року.

Таким чином, ІС “Цифровий університет” у поєднанні з ЄДЕБО пропонує комплексне вирішення завдань, пов’язаних із керуванням контингентом здобувачів, формуванням академічних груп, а також генерацією навчальних документів.

Список використаних джерел:

1. Ostapchuk T., Orlova K., Morozov A. Management of digital educational environment: case of Zhytomyr Polytechnic State University // *Proceedings of the International Scientific Jean Monnet Conference: Building sustainable EU society for the future*. December 12-13, 2024, Zagreb, Croatia & online. University of Zagreb, Faculty of Economics & Business, 2025. P. 202-213.

2. Діденко О. В., Купрієнко Д. А. Електронний журнал обліку успішності слухачів (курсантів, студентів) як засіб раціоналізації навчально-виховного процесу // *Інформаційні технології і засоби навчання*. 2015. Т. 47, № 3. С. 110-123.

3. Триус Ю., Заспа Г., Кожем'якін О., Аширова А. Інформаційно-аналітична система підтримки освітньої діяльності структурних підрозділів закладів вищої освіти // *Вісник Черкаського державного технологічного університету*. 2020. С. 27-38.

УДК 004.94:378

Маслаков Д.Д., здобувач,
Морозов А.В., к.т.н., доцент,
Державний університет «Житомирська політехніка»

ІНФОРМАЦІЙНА СИСТЕМА «DIGITAL UNIVERSITY UA» ЯК ІНСТРУМЕНТ АВТОМАТИЗАЦІЇ ВСТУПНОЇ КАМПАНІЇ

Вступна кампанія є ключовим етапом у функціонуванні будь-якого університету, оскільки вона визначає кількісний та якісний склад майбутнього покоління студентів та безпосередньо впливає на штат викладачів у закладах вищої освіти, адже кількість студентів, які вступили на навчання визначає потребу у викладацькому складі та їхнє навантаження.

Питання автоматизації вступної кампанії закладів вищої освіти розглядалися в статтях [1-2].

В рамках інформаційної системи «Digital University UA» авторами тез розроблено модуль “Вступна кампанія”, який містить ряд функціональних сторінок та пунктів меню, кожна з яких відповідає певному набору дій чи відображає конкретний блок даних. До основних розділів належать:

1) «***Заклади освіти».*** Тут виводиться список закладів загальної середньої освіти, професійної (професійно-технічної) освіти, фахової передвищої освіти, випускники яких подали заяви на вступ за освітнім ступенем “бакалавр” на базі повної загальної середньої освіти (ПЗСО). Для кожного закладу фіксується кількість поданих заяв і кількість осіб, які виконали вимоги для зарахування. Цей розділ дає уявлення про географію вступників, дозволяє оцінити динаміку подань та передбачити можливі тенденції у формуванні контингенту студентів.

2) «***Бакалаври на базі ПЗСО»***, ***«Бакалаври на базі бакалаврів»***, «***Бакалаври на базі молодших бакалаврів»***, «***Магістри»***. Усі ці розділи спрямовані на відображення стану подачі заяв залежно від освітнього рівня та базової освіти абітурієнтів. Для кожного розділу відображається інформація про стан подачі заяв за статусами у вигляді діаграм та розширеної статистики за статусами ЄДЕБО. Нижче наводиться таблиця зі списком конкурсних пропозицій, закріплених за кожним факультетом. Для кожної конкурсної пропозиції відображається інформація про ліцензований обсяг, максимальний обсяг державного замовлення, загальна кількість поданих заяв та кількість заяв зі статусами 1, 2 та 3. Є можливість переглянути деталізовану інформацію за кожною конкурсною пропозицією. Для

кожної конкурсної пропозиції виводиться інформація, що наявна в ЄДЕБО та список поданих заяв, який включає інформацію про кожну заяву: ПІБ абітурієнта, фотографія, текст мотиваційного листа, конкурсний бал, пріоритетність, статус заяви, інформація про попередній документ про освіту, пільгові категорії та контактні дані. Для кожної заяви є можливість додавати інформацію про потребу у гуртожитку, адресу проживання, відомості про батьків абітурієнта тощо.

3) ***«Накази на зарахування»***. Цей розділ забезпечує відображення вже сформованих у ЄДЕБО наказів. Користувачі (співробітники приймальної комісії, деканатів тощо) можуть переглядати кожен наказ, переглядати список зарахованих осіб і, за потреби, переходити до індивідуальних "карток абітурієнта" чи "карток здобувача вищої освіти", якщо вступник уже набув такого статусу.

4) ***«Загальна статистика»***. Сюди потрапляють сукупні дані про кількість поданих заяв за всіма освітніми рівнями й усіма статусами заяв. Ця сторінка є корисною передовсім керівництву університету та відповідальним особам, оскільки надає можливість у режимі реального часу бачити динаміку вступу та приймати управлінські рішення про коригування планових показників.

5) ***«Вступні випробування»***. Цей пункт об'єднує кілька сторінок: "Екзаменаційні аркуші", "Екзаменаційні відомості", "Список заяв" та "Статистика заяв". Зокрема, університет отримує інструменти для обліку фахових іспитів, творчих конкурсів, вступних випробувань. Реалізовано функції формування та друку екзаменаційних аркушів, документів на отримання чи повернення письмових робіт, а також звітування про кількість учасників кожного випробування.

6) «***ЄВІ/ЄФВВ»***. Модуль містить механізми контролю і відстеження стану реєстрації на єдиний вступний іспит з іноземної мови (ЄВІ) та єдине фахове вступне випробування (ЄФВВ) для вступників на магістратуру.

Список використаних джерел:

1. Макоєдова В. О. Інформатизація процесів вступної кампанії в закладах вищої освіти // *Технічні науки та технології*. 2023. № 1 (31). С. 90-97.

2. Карашецький В. П., Яркун В. І. Автоматизована система моніторингу вступної кампанії закладу вищої освіти // *Information technology and computer engineering*. 2021. Т. 51, № 2. С. 12-16.

УДК 004.94:378

Джус І.О., здобувач,
Морозов А.В., к.т.н., доцент,
Державний університет «Житомирська політехніка»

ІНФОРМАЦІЙНА СИСТЕМА «DIGITAL UNIVERSITY UA» ДЛЯ ЦИФРОВІЗАЦІЇ ПРОВЕДЕННЯ СЕСІЇ У ЗАКЛАДІ ВИЩОЇ ОСВІТИ

Для закладів вищої освіти актуальною є необхідність автоматизації процесів обліку успішності студентів, зокрема у процесі виставлення оцінок за сесію. Питання функціонування електронних журналів та електронних кабінетів здобувачів висвітлювалися у роботах [1-2].

Впровадження модуля «Сесія» інформаційної системи «Digital University UA» для ведення електронних відомостей успішності є важливим кроком у цифровізації освітнього процесу, що надає такі переваги як:

а) зменшення корупційних ризиків;

б) прозорість процесу виставлення оцінок;

в) зменшення кількості помилок при виставленні оцінок;

г) використання результатів сесії для автоматизованого розрахунку стипендіальних рейтингів;

д) можливість аналізу результатів сесії за різними критеріями.

Модуль «Сесія» надає можливість автоматизовано генерувати електронні заліково-екзаменаційні відомості та надавати доступ до них викладачам, які здійснюють підсумковий контроль. Викладачі у встановлений у відомостях термін повинні заповнити доступні для них електронні відомості, виставивши оцінки усім здобувачам. Для вибіркових навчальних дисциплін передбачена можливість формувати у відомостях склад студентів, які вивчали дану навчальну дисципліну.

Модуль «Сесія» має можливість підписання електронних відомостей електронним підписом. Для цього було використано веб-плагін від АТ «ІІТ».

Передбачена можливість підписування електронних відомостей викладачем, який виставив оцінку, завідувачем кафедри та деканом факультету.

Реалізовано сторінку «Зведені відомості», на якій наводиться перелік усіх академічних груп, які навчалися у вибраному семестрі. Для кожної академічної групи можна подивитися успішність здобувачів за усіма освітніми компонентами, які викладалися у вибраному семестрі та, за необхідності, створити додаткові відомості для ліквідації академічних заборгованостей.

Для студентів реалізовано «Електронний кабінет здобувача», до якого мають доступ виключно студенти та аспіранти. Для доступу до електронного кабінету при першому вході здобувач повинен ввести у відповідні поля свій ID фізичної особи як логін та пароль. При першому вході в систему користувачу автоматично пропонується змінити пароль для забезпечення безпеки облікового запису.

У розділі «Сесія» відображається електронна залікова книжка здобувача. Цей розділ містить усі отримані оцінки, що дозволяє швидко переглядати результати навчання.

Для оцінок за екзамени реалізовано функцію погодження оцінок. Вона доступна тільки в тому випадку, якщо здобувач отримав 60 або більше балів. Якщо здобувач отримав менше 60 балів або оцінка є заліковою, кнопка погодження не відображається.

Після погодження оцінки здобувачем вона стає незмінною для викладача. При перегляді відомості викладачем погоджена оцінка забарвлюється зеленим кольором. Якщо здобувач обрав опцію «Йду на екзамен», оцінка в екзаменаційній відомості у викладача зафарбовується жовтим кольором та залишається доступною для редагування викладачем.

Здобувачі, які навчаються за декількома освітніми програмами одночасно, мають можливість перемикатися між ними в електронному кабінеті. Ліворуч відображається перелік доступних груп, з яких можна вибрати активну. Після вибору нової групи зміни набувають чинності, і вся інформація в кабінеті оновлюється відповідно до вибраної програми.

Ці функціональні можливості електронного кабінету значно покращують взаємодію здобувачів із навчальним процесом, забезпечуючи зручність та ефективність обліку академічних досягнень.

Список використаних джерел:

1. Ostapchuk T., Orlova K., Morozov A. Management of digital educational environment: case of Zhytomyr Polytechnic State University // *Proceedings of the International Scientific Jean Monnet Conference: Building sustainable EU society for the future*. December 12-13, 2024, Zagreb, Croatia & online. University of Zagreb, Faculty of Economics & Business, 2025. P. 202-213.

2. Діденко О. В., Купрієнко Д. А. Електронний журнал обліку успішності слухачів (курсантів, студентів) як засіб раціоналізації навчально-виховного процесу // *Інформаційні технології і засоби навчання*. 2015. Т. 47, № 3. С. 110-123.

УДК 004.77:004.223.3-043.83](06)

Ковтанюк І. І., викладач
Уманський державний педагогічний університет імені Павла Тичини
Ковтанюк М. С., вчитель
Уманський ліцей № 3 Уманської міської ради Черкаської області

СТВОРЕННЯ ЕМОДЗІ ЗА ДОПОМОГОЮ ОНЛАЙН-СЕРВІСІВ

Сучасний цифровий світ неможливо уявити без яскравих символів, які за секунди передають наші почуття та настрій. Маленькі віртуальні піктограми вже давно вийшли за межі простих усмішок і стали потужним комунікаційним інструментом у соціальних мережах, месенджерах та інших онлайн-платформах [1]. За допомогою них ми можемо виразити радість, смуток, здивування чи захоплення без єдиного слова. А з розвитком цифрових технологій з'явилась можливість не лише користуватися стандартним набором емодзі, але й створювати власні, які відображають індивідуальність.

Серед популярних онлайн-сервісів для створення емодзі варто відзначити **Bitmoji** – сервіс, який дозволяє створити власного аватара, який потім можна використовувати у різних ситуаціях. Він пропонує широкий вибір рис обличчя, зачісок, одягу та аксесуарів. Персонаж може виражати різні емоції та виконувати різноманітні дії.

Emoji Maker – ще один простий у використанні інструмент, який дозволяє створювати емодзі з нуля, комбінуючи різні елементи: форми обличчя, очі, рот, аксесуари тощо. Він має інтуїтивно зрозумілий інтерфейс, що робить процес створення швидким та приємним.

Emojify дозволяє перетворювати власні фотографії на емодзі. Потрібно лише завантажити фото, налаштувати стиль та отримати унікальний емодзі на основі вашого зображення. Emojify інтегрується з платформою Canva.

Хоча **Canva** відомий як інструмент для графічного дизайну [4], він також пропонує можливості для створення власних емодзі. Тут є шаблони, форми та елементи, які можна комбінувати для розробки унікальних емодзі.

Процес створення персоналізованого емодзі зазвичай розпочинається з вибору відповідного сервісу, який відповідає потребам та рівню навичок користувача. Після проходження реєстрації або авторизації (якщо це необхідно) користувач отримує можливість розпочати роботу з базової форми – обрати контур обличчя або стартовий шаблон. Далі додаються деталі, як-от очі, рот, ніс, брови та

інші елементи. Надається можливість налаштувати колір шкіри, зачіску та додаткові особливості відповідно до особистих уподобань. Для більшої виразності можна доповнити емодзі аксесуарами – окулярами, капелюхами, прикрасами тощо. Крім того, експериментування з мімікою дозволяє створювати виразні емоції. Готовий емодзі рекомендується зберігати у форматі PNG або SVG для подальшого використання.

При розробці ефективних емодзі важливо зберігати простоту, оскільки надмірна деталізація може призвести до втрати чіткості зображення при зменшенні його розміру. Використання яскравих кольорів сприяє кращому візуальному сприйняттю. Основна увага приділяється виразності – обличчя має чітко передавати емоцію. Крім того, створення універсальних емодзі сприяє їх розумінню широкою аудиторією. Додатковою перевагою є розробка тематичних наборів, що містять емодзі в єдиному стилі для різних емоцій.

Власні емодзі можна використовувати в месенджерах (WhatsApp, Telegram, Viber тощо), соціальних мережах, електронних листах, презентаціях та навіть для брендингу. Деякі платформи дозволяють завантажувати користувацькі емодзі як стікери чи наклейки.

Створення унікальних емодзі є чудовим способом виразити індивідуальність та передати емоції у цифровому середовищі. Завдяки сучасним онлайн-сервісам цей процес став доступним кожному, незалежно від рівня володіння дизайнерськими навичками [3]. Користувачі можуть експериментувати, створювати власні символи та збагачувати спілкування унікальними графічними елементами.

Список використаних джерел:

1. Криворучко І. І., Тітова Л. О. Хмарні та мобільні технології у підготовці майбутнього вчителя // *Педагогічна академія: наукові записки.* 2024. № 10. URL: https://doi.org/10.5281/zenodo.13924205.

2. Медведєва М. О., Жмурко О. І., Криворучко І. І., Ковтанюк М. С. Організація продуктивної взаємодії між учасниками освітнього процесу в умовах дистанційного навчання: аналіз сучасних додатків // *Науковий часопис.* 2021. Т. 1, № 80, С. 248–255. URL: https://dspace.udpu.edu.ua/handle/123456789/13778.

3. Криворучко І. І. Роль графічного дизайну в підготовці навчальних матеріалів майбутніми вчителями інформатики // *Наука і техніка сьогодні.* 2024. № 5(33), С. 677–687. DOI: https://doi.org/10.52058/ 2786-6025-2024-5(33)-677-687.

4. Тітова Л. О., Ковтанюк І. І. Цифрове портфоліо як елемент іміджу сучасного педагога // *Актуальні проблеми підготовки сучасного педагога: теорія, історія, практика :* XV Всеукраїнська науково-практична онлайн-конференція, м. Умань, 23 жовт. 2024 р. С. 355–358. URL: https://dspace.udpu.edu.ua/handle/123456789/17980.

УДК 004.7

Ковтун В. В., ст. викл.
кафедри інженерії програмного забезпечення
Державний університет «Житомирська політехніка»

АВТОМАТИЗОВАНІ СИСТЕМИ ОЦІНЮВАННЯ ЗНАНЬ СТУДЕНТІВ

Об'єктивне та адекватне оцінювання досягнень студентів завжди було дуже важливим і актуальним. Ця проблема стала особливо нагальною зараз, коли в Україні відбувається реформування системи освіти. Необхідність для зміни в системі оцінювання встановлюються на державному рівні. Це пов'язано з тим, що оцінювання знань студентів є важливою частиною навчального процесу в вищих навчальних закладах, оскільки це забезпечує високу якість освіти та формує конкурентоспроможних фахівців [5].

Оцінка є одним із важливих компонентів, які впливають на особистість студента під час навчання. Це регулятор, показник результативності та стимул для діяльності студентів. Практика показала, що немає ідеальних систем оцінювання, оскільки кожна система має свої сильні та слабкі сторони. Вочевидь, краще шукати найкращі системи, ніж створювати та використовувати ті, які мають найбільше переваг.

Сьогодні навчання передбачає кардинально інший погляд на те, як оцінювати знання, навички та навички учнів. Традиційна п'ятибальна система змінилася на систему накопичення балів, яка вимагає від студентів набрати від 60 балів (задовільно) до 100 балів (відмінно) протягом курсу. Студенти отримують кращі знання на певному курсі, коли вони отримують більше балів [2].

Мета впровадження стобальної системи оцінювання полягає в тому, щоб забезпечити об'єктивне визначення того, наскільки добре навчаються студенти. Незважаючи на це, існують деякі труднощі, щоб точно визначити рівень підготовки студентів під час оцінювання засвоєних знань, умінь і навичок студентів вищої освіти. Таким чином, кожен викладач намагається розробити ідеальну шкалу оцінювання, яка допоможе найкращим чином оцінити знання студентів [6].

Автоматизована система оцінювання знань — це програмно-технічний комплекс, призначений для автоматичного або напівавтоматичного визначення рівня знань студентів шляхом проведення тестів, контрольних завдань та їхньої обробки з подальшою статистичною та аналітичною обробкою результатів. Такі системи включають:

- Бази тестових завдань (банк тестів).
- Інтерфейси для студентів та викладачів.
- Алгоритми автоматичної перевірки та оцінювання.
- Засоби аналітики та звітності.

Автоматизовані системи оцінювання знань зробили організацію та проведення контрольних заходів, таких як тестування, самоконтроль і екзамени, більш простими. Ці системи дозволяють швидкий і ефективний збір і обробку результатів, що дозволяє викладачам швидко створювати аналітичні звіти та аналізувати якість знань студентів. Автоматизація процесів оцінювання гарантує об'єктивність оцінювання та виключає суб'єктивні елементи традиційного методу. Крім того, автоматизовані системи роблять процес перевірки знань зручним і доступним незалежно від місця перебування студента.

Автоматизовані системи оцінювання знань студентів значно розвинулися, інтегруючи штучний інтелект та освітні технології для забезпечення ефективного, персоналізованого і точного оцінювання. Одним із визначних підходів є комп'ютеризоване адаптивне тестування (КАТ), яке коригує складність тестових запитань у режимі реального часу на основі успішності студента, пропонуючи індивідуальний підхід до оцінювання [3].

Інтелектуальні системи навчання (ITS) використовують когнітивні моделі для відтворення експертних стратегій вирішення проблем, які дають учням миттєвий, контекстно-чутливий зворотний зв'язок і настанови. Наприклад, Університет Карнегі-Меллона розробив когнітивні репетитори, які використовуються для навчання математики, і показали, що вони ефективно покращують результати навчання студентів.

Accelerated Reader (AR) — це освітня програма, створена для того, щоб студенти могли відстежувати та контролювати своє самостійне читання та розуміння прочитаного. AR оцінює учнів за допомогою тестів і вікторин, заснованих на прочитаних книгах. Він також відстежує їхній прогрес у читанні та встановлює індивідуальні цілі щодо читання [1].

Структурно автоматизовані системи оцінювання знань зазвичай складаються з кількох модулів, які пов'язані один з одним. З них складається користувацький інтерфейс, який доступний у веб-додатках або мобільних додатках; модуль управління групами студентів; модуль формування та генерації тестів; модуль прав доступу до тестових завдань; і модуль автоматичної перевірки відповідей студентів [6]. Аналітичний модуль є особливо важливим, оскільки він забезпечує формування статистичних звітів, представлення результатів і

можливість оцінювати якість знань, отриманих на основі отриманих даних.

Докімологія, наукове дослідження освітніх методів тестування та оцінювання, допомагає в розробці та впровадженні оцінок, щоб переконатися, що вони справедливі, надійні та вартісні. Докімологія розширилася завдяки впровадженню штучного інтелекту та машинного навчання, що призвело до впровадження адаптивного тестування та автоматизованих систем оцінювання, які підвищують точність і ефективність оцінювання [7, с. 216].

Список використаних джерел:

1. Застосування системи автоматизованого опитування студентів // Матеріали науково-методичного семінару ВТЕІ КНТЕУ. 2015. С. 45–48. URL: https://www.vtei.com.ua/doc/materialuvebinary.pdf (дата звернення: 10.03.2025).
2. Лекція №4. Забезпечення якості вищої освіти / Житомирська політехніка. 2024. URL: https://learn.ztu.edu.ua/mod/resource/view.php?id=211278 (дата звернення: 10.03.2025).
3. Положення про електронне оцінювання залишкових знань студентів / Національний університет біоресурсів і природокористування України. 2015. URL: https://nubip.edu.ua/sites/default/files/u66/pro_electro_otcin_zalysh_znan.pdf (дата звернення: 10.03.2025).
4. Положення про контроль і оцінювання результатів навчання / Хмельницький національний університет. 2024. URL: https://khmnu.edu.ua/wp-content/uploads/normatyvni-dokumenty/polozhennya/pro-kontrol-i-oczinyuvannya-rezultativ-navchannya.pdf (дата звернення: 10.03.2025).
5. Положення про поточне і підсумкове оцінювання знань студентів / Тернопільський кооперативний фаховий коледж. 2024. URL: https://surl.li/vqtark (дата звернення: 10.03.2025).
6. Система оцінювання / Міжнародний науково-технічний університет імені академіка Юрія Бугая. URL: https://istu.edu.ua/studentam/systema-otsiniuvannia/ (дата звернення: 10.03.2025).
7. Системи оцінювання якості професійної освіти і навчання в країнах Європейського Союзу. Монографія / В. О. Радкевич, Л. П. Пуховська, О. В. Бородієнко та ін. Житомир. Полісся. 2018. 216 с. URL: https://surl.gd/akcdzx (дата звернення: 10.03.2025).

Секція 6
ЦИФРОВА ОБРОБКА СИГНАЛІВ ТА ЗОБРАЖЕНЬ В АВТОМАТИЗОВАНИХ ТА ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНИХ СИСТЕМАХ

УДК 621.317

Волинець Ю. Г., студент ІВТ-3м
Лугових О.О., старший викладач
Державний університет «Житомирська політехніка»

КОМП'ЮТЕРИЗОВАНА СИСТЕМА ВИМІРЮВАННЯ ВИТРАТ ТА КОНТРОЛЮ ВИТОКУ ПРИРОДНОГО ГАЗУ В ПОБУТОВОМУ СЕКТОРІ

У зв'язку з більш широким застосуванням природного газу в різних сферах промисловості і народного господарства загострюється необхідність повсюдного впровадження систем газової безпеки[1]. Невід'ємною частиною таких систем є пристрої, що перетворюють інформацію про витрату газу та його витоку в зрозумілу форму для користувача. Це пов'язано з тим, що звичайний метод зчитування показників не завжди є точним, а виявити невеликий витік газу дуже складно без спеціальних приладів.

Отже є мета для розробки пристрою для зчитування даних лічильника і витоку газу. Використання такого пристрою покращить процес зчитування показників, тобто зробить його автоматичним, а доповнення в вигляді датчику витоку газу допоможе виявити аварійні ситуації, що збільшить рівень безпеки для людей і навколишнього середовища.

Для виконання мети потрібно виконати такі задачі:

– Розглянути актуальність розробки такого пристрою;

– Побудувати структурну схему;

– Побудувати принципову схему;

– Обрати програмне забезпечення та написати відповідну програму.

Облік ресурсів вручну відходить у минуле: постачальники електроенергії в США, Китаї та Західній Європі вже понад десять років отримують показники автоматично. Для цього використовують розумні пристрої та бездротові способи передавання даних.

Більшість абонентів досі користуються моделями електронних та аналогових електролічильників без розумних функцій. Тому постачальникам доводиться вести облік даних вручну: залучати

контролерів і приймати показники користувачів телефоном або через інтернет.

Це завдає постачальникам низку незручностей:

– Несвоєчасне надходження показників. Абоненти забувають надіслати показники в установлений день.

– Утруднений доступ до лічильників. Користувачі можуть бути не вдома на час прибуття контролера чи не пустити його в оселю.

– Помилки. Іноді споживачі надсилають невірні дані, а оператор помиляється, вносячи показники в базу даних.

– Неточність. Старі лічильники класу точності «2» (особливо це стосується індукційних лічильників) менш чутливі до малих струмів, наприклад, зарядки телефона чи перебування електроприладу в режимі чекання. Тому такі облікові прилади можуть надсилати занижені дані про споживання, і постачальник, відповідно, отримає неповну оплату за надані ресурси.

– Розкрадання. Деякі моделі лічильників можна сповільнити, зупинити та навіть налаштувати на роботу у зворотному режимі[2].

Застосуємо сучасні елементи системи. В нашій системі неможливо обрати один датчик, що вимірюватиме усі параметри одночасно. Тому ми обираємо датчик Холла KY-035[3] для вимірювання кількості обертів ротора всередині лічильника та датчик для визначення наявності і концентрації окису вуглецю і метану в повітрі моделі MQ-9[4]. Для відображення результатів з двох датчиків обрано LCD екран, саме такий вибір зроблено через те, що його можна підключити через 2 дроти при нестачі виходів. «Мозком» пристрою обрано мікроконтролер ATmega328[5] через його переваги в роботі, наприклад: декілька режимів низького енергоспоживання, що дозволяє ефективно використовувати його в пристроях на батарейках; ATmega328 має 14 цифрових пінів введення/виведення, 6 з яких можуть використовуватися як ШІМ-виходи, і 6 аналогових входів, що забезпечує гнучкість у підключенні датчиків та інших компонентів; мікроконтролер має вбудований 10-бітний аналогово-цифровий перетворювач, який дозволяє точно зчитувати аналогові сигнали[6].

Структурна схема системи представлена на рис.1.

Складові системи наступні:

– Мікроконтролер;
– Датчик газу;
– Датчик Холла
– LCD екран
– Діод;
– Джерело живлення.

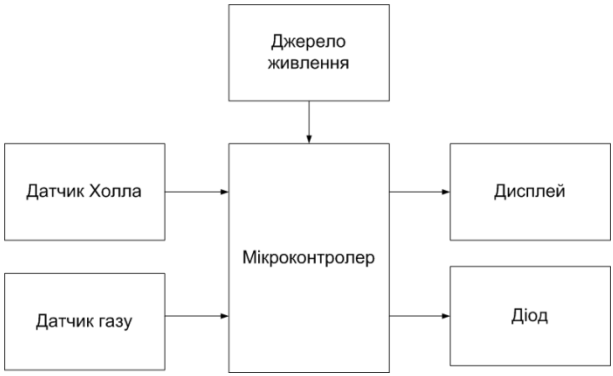


Рисунок 1. Структурна схема системи

Принципова схема пристрою представлена на рис.2

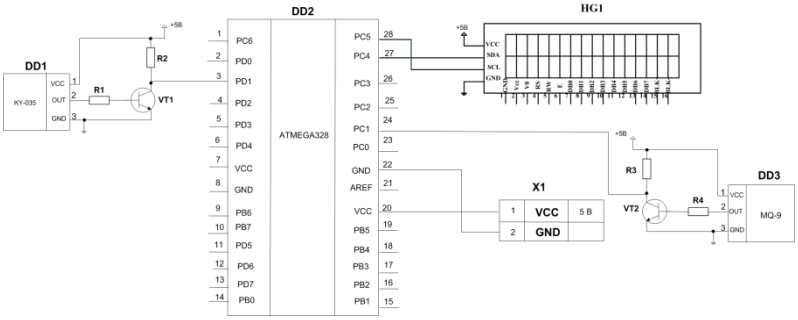


Рисунок 2. Принципова схема пристрою

В якості мови програмування для мікроконтролера ATmega328, датчиків обираємо мову програмування Сі та робоче середовище Arduino.IDE.

Виміряні дані виводяться на екран для візуалізації даних, що вимірюються в реальному часі Холла та датчиком газу.

Отже, створена система для моніторингу параметрів витрати і витоку газу дозволяє вимірювати кількість використаного газу споживачем, вміст окису вуглецю і метану в повітрі чадного газу. Створена система може бути використана для покращення контролю за

витратами газу, забезпечення своєчасного виявлення витоків та підвищення рівня безпеки споживачів природного газу.

Список використаних джерел:

1. Застосування детектору витоку побутового газу для моніторингу повітря [Електронний ресурс]. – Режим доступу: http://ecoj.dea.kiev.ua/archives/ 2023/1/16.pdf .

2. Як розумний електролічильник передає показники [Електронний ресурс]. – Режим доступу: https://jooby.eu/uk/blog/rozumnij-elektrolichilnik.

3. KY-035 Модуль датчика Холла [Електронний ресурс]. Режим доступу: https://artificer.com.ua/product/ky-035-modul-datchika-hollaю

4. Датчик газу MQ-9 модуль Python [Електронний ресурс]. – Режим доступу: https://www.mini-tech.com.ua/datchik-gaza-mq-9-modul.

5. Arduino UNO R3 [Електронний ресурс]. – Режим доступу: https://artificer.com.ua/product/arduino-uno-r3.

6. Мікропроцесорна техніка. Однокристальні мікроконтролери: навч. посібник / С.Р.Михайлов. - К.:, 2014. 123 с.

УДК 004.932, 681.518.3

Горшенін О. Є., к.т.н., доцент
Державний університет «Житомирська політехніка»

ФОРМУВАННЯ ВИМОГ ДО ХАРАКТЕРИСТИК БЕЗКОНТАКТНОГО ДАТЧИКА ПРОСТОРОВОГО ПОЛОЖЕННЯ ВИМІРЮВАЛЬНОЇ МІТКИ

В сучасних системах автоматичного управління механічними пристроями нерідко використовуються безконтактні датчики просторового положення фізичного об'єкта на основі сучасних ПЗЗ відеокамер. Просторове положення об'єкта управління (зсув, поворот тощо) оцінюється на основі положення спеціальних міток на кадрах відеопотоку за допомогою цифрових методів обробки зображень та фотограмметрії. Побудова таких датчиків для високоточних систем в заданих умовах вимагає висування певних вимог до конструкції і параметрів складових датчика: відеокамери, міток, а також до методів і алгоритмів обробки кадрів відеопотоку.

Вимоги до конструкції і параметрів складових датчика визначаються на основі вимог до його точнісних характеристик з боку системи автоматичного управління. Такими характеристиками за звичай є точність визначення векторів координат і швидкості переміщення вимірювальних міток. Для автоматизованої системи управління (АСУ) наземної антенної системи (АС) радіоканалу зв'язку з космічним апаратом (КА) в Х-діапазоні вимоги надаються в одиницях кутових хвилин. Тому основна увага дослідження була надана саме визначенню зв'язків точнісних характеристик датчиків з параметрами складових датчика та умовами його роботи.

Вважається, що параметри і характеристики такого датчика є сталими або керованими під час експлуатації. Тому постійними складовими похибок оцінювання в дослідженні знехтувано, бо постійні складові похибок просто усуваються шляхом калібрування та алгоритмічного оброблення після вимірювання. За оцінки точності в досліджуванні береться тільки СКВ оцінювання векторів координат і швидкості переміщення вимірювальних міток. Динамічні складові похибок не оцінювалися, бо в даних умовах частота кадрів відеокамери є надлишковою: часовий інтервал між сусідніми кадрами в десятки разів менший за час, коли об'єкт управління змінить свій стан на значиму частку.

Для відеокамери це кількість елементів в рядках і стовбцях ПЗЗ-матриці, фокусна відстань об'єктиву камери, кут захоплення об'єктиву, вхідний отвір об'єктиву, порогова чутливість та динамічний діапазон ПЗЗ-матриці, розрядність АЦП, частота кадрів, світловий потік, що створюють підсвічувальні світлодіоди в напрямку на мітку. Для

вимірювальних міток параметрами і характеристиками є фізичний розмір мітки, відбивні здатності фону і малюнка, детальність малюнка мітки, патерн мітки, який визначає кількість і форму піків автокорреляційної функції мітки. До характеристик умов роботи датчика відносяться відстань до об'єкта управління, характеристики середовища розповсюдження світла між об'єктом і відеокамерою (коефіцієнти прозорості та розсіювання, характеристики заломлення та турбулентності). Характеристиками методів і алгоритмів є обчислювальна складність та залишкова інструментальна похибка.

Дослідження проводилося для застосування результатів в конкретних умовах: безконтактний датчик на основі звичайної камери спостереження із з'єднанням по бездротової мережі WiFi, яка спостерігає лімб опорно-повертального пристрою (ОПП) наземної антенної системи (АС) радіоканалу зв'язку з космічним апаратом (КА), що здійснює орбітальний рух на низькій навколоземній орбіті. Камера встановлюються жорстко на кронштейні напроти лімбу обертання антени по азимуту або куту місця. Лімб є вимірювальною міткою і являє собою матовану алюмінієву смугу з чорненими вертикальними градусними мітками, товщиною 0,5 мм з кроком 4,3633мм. Між камерою та поверхнею лімбу повітряний шар без домішок та опадів. Камера встановлена так, щоб напрямок рядків на кадрах відеопотоку співпадав з напрямком пересування лімбу. Для контрастного зображення здійснюється підсвічування лімбів світлодіодами камер. Відеопотоки зображень вводяться в комп'ютер, де здійснюється виділення сусідніх кадрів потоку, усереднення значень пікселів за стовбцями у вікні аналізу, швидке обчислення взаємної кореляційної функції зображень з сусідніх кадрів, та знаходження відносного зсуву їх максимумів з наступним перерахунком в абсолютні значення кутового положення АС, відносний кутовий зсув. Обчислене кутове положення вводиться до алгоритму АСУ за виміряними значеннями.

В результаті дослідження виведені основні залежності між параметрами елементів датчика та СКВ похибок оцінювання векторів просторового положення та швидкості міток на об'єкті. Оцінений вплив кожного параметра. Для заданих умов застосування визначені основні вимоги до характеристик елементів датчика.

УДК 528.873:004.9

Даншина С. Ю., д.т.н., професор
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»

АНАЛІЗ МІСЬКОЇ ЗАБУДОВИ ЗА ДАНИМИ ДИСТАНЦІЙНОГО ЗОНДУВАННЯ ЗЕМЛІ

Розвиток технологій розумних міст спрямовано на використання передових технологій, що неможливо без сучасної доступної міської інфраструктури. Вимоги до її стану для розумного міста більш жорсткі, ніж для звичайних міст і регіонів [1]. Це потребує актуальних даних про міську забудову та тенденцій її розвитку.

Внаслідок урбанізації зростає чисельність міського населення, збільшується кількість будівництва, що призводить до перевантаження автошляхів, погіршення екологічного стану міського середовища тощо. Отже є необхідність у поєднанні класичних і нових способів керування міською забудовою, регулювання містобудівного процесу для забезпечення комфортних умов життя та нормального функціонування міських інфраструктур [1, 2].

Отже, актуальним завданням є удосконалення процесів аналізу наявної міської забудови, яка склалася внаслідок урбанізації, визначення проблем, викликаних збільшенням темпів будівництва міста, з урахуванням його територіально-планувальних особливостей і формування ґрунтовних Smart-рішень. Використання даних дистанційного зондування Землі (ДЗЗ) дає змогу вирішити частину проблем, пов’язаних з аналізом наявної міської забудови. При цьому зазначимо, що дані ДЗЗ мають великий обсяг, їх якість залежить від сукупності факторів, які не завжди можуть бути ідеальними, а їх оброблення займає значний час [1]. Тому виникає необхідність у створенні методу, якій максимально спростить процедуру оброблення даних ДЗЗ і надасть оцінки, придатні для подальшого аналізу та формування рішень щодо напрямів інтелектуалізації міста.

Перспективним варіантом вирішення складних просторових завдань є машинне навчання (МН), зокрема, глибоке навчання. В останні роки ці інструменти є основними компонентами просторового аналізу ГІС [2, 3].

Дослідження типового алгоритму МН при обробленні структурованих даних дало змогу сформувати метод аналізу міської забудови за даними ДЗЗ. Він поєднує таку послідовність етапів:

Eman 1. Завантаження супутникового знімку міської забудови для створення навчальної вибірки.

Eman 2. Формування навчальної вибірки з типових просторових

об’єктів міської забудови:

- ручне виділення полігонів типових об’єктів;
- автоматичне вилучення просторових фрагментів зображення з типовими об’єктами;
- збереження одержаних фрагментів у базу даних.

Eman 3. Отримання моделі Deep Learning:

- автоматичний циклічний пошук ознак у зображеннях навчальної вибірки;
- автоматична класифікація ознак за типовими об’єктами зображення.

Eman 4. Перевірка моделі Deep Learning на вихідному супутниковому знімку, а також її застосування на інших знімках для визначення можливості адаптації до інших вихідних даних.

Eman 5. Використання моделі Deep Learning для визначення об’єктів міської забудови по знімках.

Отримані результати стають основою для актуалізації даних генерального плану міста, для формування заходів з модернізації його інфраструктури, оптимізації вуличної мережі, будівництва вулиць, мостів і тунелів, транспортних розв'язок, поліпшення екологічного стану, а також формування напрямків інтелектуалізації.

Зазначимо, що для реалізації етапу 3 метода можна використовувати інструменти Image Analyst ArcGIS Pro 3.4, зокрема, модель Mask R-CNN для сегментації об’єктів з однаковими просторовими ознаками.

Список використаних джерел:

1. Wavelet Transform Cluster Analysis of UAV Images for Sustainable Development of Smart Regions Due to Inspecting Transport Infrastructure / Y. Zheng et al. *Sustainability*. 2025. Vol. 17(3), Article 927. DOI: https://doi.org/10.3390/su17030927.

2. Machine learning-enhanced assessment of urban sustainable development goals progress / F. Li et al. *Cities*. 2025. Vol. 158. Article 105718. DOI: https://doi.org/10.1016/j.cities.2025.105718.

3. Identifying influencing factors and characterizing key issues in urban sustainable development capacity through machine learning / H. Zhou et al. *Chinese Journal of Population, Resources and Environment*. 2024. Vol. 22, issue 3. P. 291 – 304. DOI: https://doi.org/10.1016/j.cjpre.2024.09.008.

УДК 621.317

Іщенко О.С., аспірант,
Подчашинський Ю.О., д.т.н., професор,
Чепюк Л.О., к.т.н., доцент
Державний університет «Житомирська політехніка»

МІКРОПРОЦЕСОРНА СИСТЕМА ВИМІРЮВАННЯ РІВНЯ ЗВУКОПРОЗОРИХ РІДИН У РЕЗЕРВУАРАХ

Процеси автоматичного вимірювання рівня звукопрозорих рідин у резервуарах шляхом локації рідини безконтактним методом крізь стінку резервуара за допомогою ультразвуку повинні керуватися законодавчими, нормативними документами, керівництвами, яким відповідають застосовувані програмно-технічні засоби, методи та процедури вимірювань [1–3].

Пропонується імпульсний метод вимірювання часу поширення акустичного сигналу в звукопрозорій рідині до її поверхні та перерахунок часу в відстань (рівень) за допомогою виміряного або заздалегідь відомого значення швидкості звуку в конкретній рідині за відомої температури. Тип вимірюваної рідини, калібрувальна таблиця, номер приладу в магістралі вводяться на етапі впровадження за допомогою спеціально передбачених для цього засобів.

Схема мікропроцесорної системи вимірювання рівня звукопрозорих рідин у резервуарі наведено на рис. 1.

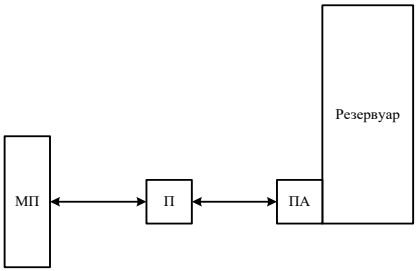


Рис. 1. Схема мікропроцесорної системи вимірювання рівня звукопрозорих рідин у резервуарі

Від мікропроцесора через підсилювач (канал вимірювання рівня) на акустичний перетворювач (ПА), встановлений у нижній точці резервуара, подається випромінюючий імпульс, який перетворюється в акустичний сигнал, що проникає крізь стінку резервуара і досягає поверхні рідини. Відбиті від поверхні рідини акустичні сигнали тим самим ПА перетворюються в електричні імпульси (ехо-сигнали) і через

підсилювач подаються на вхід мікропроцесора. Проводиться безперервне (1 раз на 1–5 секунд) вимірювання часу відгуку (до 33 ехо-сигналів в одному циклі вимірювань). Виміряний час відгуку перераховується у відстань (рівень) за виміряним або заздалегідь відомим значенням швидкості звуку (Сзв.) в конкретній рідині при певній температурі.

Для корекції швидкості звуку необхідно ввести в вимірювач рівня значення температури рідини, виміряне датчиками температури, які встановлені на резервуарі. Значення температури використовується для обчислення густини за швидкістю звуку, значення об'єму та густини парової фракції для зріджених пропан-бутану, хлору та аміаку, тиску насичених парів, процентного складу пропан-бутану.

На рис. 2 наведено приклад роботи програми вимірювання.

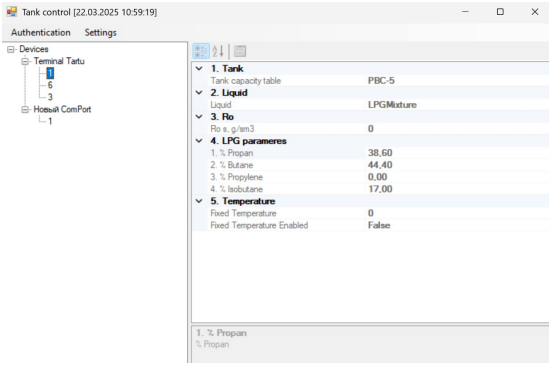


Рис. 2. Приклад роботи програми вимірювання

Список використаних джерел:

1. INTERNATIONAL STANDARD ISO 6578 Second edition 2017-10 Refrigerated hydrocarbon liquids – Static measurement – Calculation procedure.

2. INTERNATIONAL STANDARD ISO 8973:2013 Liquefied petroleum gases. Calculation method for the determination of density and vapour pressure (EN ISO 8973:1999, IDT).

3. INTERNATIONAL RECOMMENDATION OIML R 71 Edition 2008 (E) Fixed storage tanks. General requirements.

УДК 621.317

Лугових О.О., старший викладач
Молнар В.О., студент ІВТ-3м
Державний університет «Житомирська політехніка»

КОМП'ЮТЕРИЗОВАНА СИСТЕМА КОНТРОЛЮ ЯКОСТІ ПОВЕРХНІ ПРОМИСЛОВИХ ВИРОБІВ НА ОСНОВІ ФРАКТАЛЬНИХ МОДЕЛЕЙ

Забезпечення високої якості продукції є одним із ключових завдань сучасного виробництва. Виявлення та аналіз дефектів поверхні є важливим етапом у контролі якості промислових виробів. Використання комп'ютеризованих систем контролю, що базуються на фрактальних моделях, дозволяє автоматизувати процеси аналізу, підвищити точність і швидкість виявлення дефектів, а також зменшити вплив людського фактора.

Використання фрактальних моделей дозволяє аналізувати складні та нерегулярні структури поверхонь, що значно підвищує точність ідентифікації різних видів дефектів, таких як подряпини, тріщини, нерівності та інші пошкодження.

Основна ідея системи полягає у використанні математичних методів фрактального аналізу для дослідження текстур поверхні виробів. Завдяки цьому підходу можна не тільки ідентифікувати видимі дефекти, а й виявляти мікропошкодження, які не завжди помітні при використанні традиційних методів контролю. Фрактальна розмірність, як один із ключових параметрів аналізу, дозволяє визначити ступінь нерівності поверхні, що дає змогу більш точно оцінити якість виробу.

Розробка такої системи має важливе значення для автоматизації процесів контролю якості у промисловості. Автоматичний режим роботи системи забезпечує безперервний моніторинг якості виробів без необхідності ручного втручання, що підвищує продуктивність і зменшує ймовірність людської помилки.

Важливою частиною системи є камера високої роздільної здатності, яка забезпечує отримання чіткого зображення поверхні виробу. Це зображення передається на комп'ютер, де програмне забезпечення виконує його обробку, застосовує алгоритми фрактального аналізу та визначає наявність дефектів. У разі виявлення критичних відхилень система формує сигнал для оператора або автоматично фіксує виріб як бракований. Структурна схема **контролю якості поверхні промислових виробів представлена на рис.1**

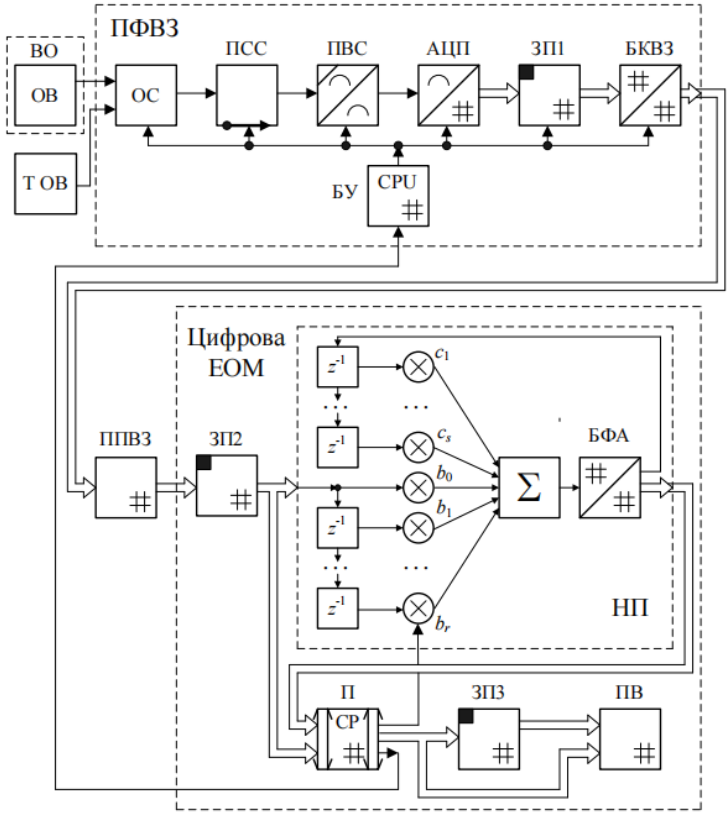


Рис.1.Структурна схема контролю якості поверхні промислових виробів

Розшифровка складових на рис. 1 наступна: ОВ – об’єкт вимірювань; ВО – виробниче обладнання; Т ОВ – тестовий ОВ для калібрування вимірювального каналу; ПФВЗ – пристрій формування відеозображень; ОС – оптична система ПФВЗ; ПСС – перетворювач «світло-сигнал»; ПВС – підсилювач відеосигналу; АЦП – аналого-цифровий перетворювач; ЗП1…ЗП3 – запам’ятовуючі пристрої для відеозображень; БКВЗ – блок кодування відеозображень; БУ – блок управління ПФВЗ; ППВЗ – пристрій передачі відеозображень у цифрову ЕОМ; НП – нейропроцесор у складі цифрової ЕОМ; БЗ – блок затримки; c1…cs, b0…br – вагові коефіцієнти штучної нейронної мережі, які настроюються відповідно до поточних умов вимірювань;

БФА – блок функції активації нейронної мережі; П – процесор цифрової ЕОМ; ПВ – пристрій візуалізації відеозображень і результатів вимірювання ГП об’єктів.

Однією з ключових особливостей системи є використання нейропроцесора, який забезпечує швидку обробку великої кількості даних і можливість адаптації алгоритмів до змінюваних умов. Швидка адаптація алгоритмів під різні типи поверхонь і виробничі умови робить систему універсальною та придатною для використання у різних галузях промисловості: каменеобробні, машинобудуванні, електроніці та інших сферах, де якість поверхні відіграє важливу роль.

Розроблена комп'ютеризована система контролю якості поверхні промислових виробів на основі фрактальних моделей забезпечує автоматизований аналіз зображень, виявлення дефектів та їх класифікацію. Розроблена система працює в автоматичному режимі, має високу точність (абсолютна похибка 1,5%, відносна похибка 3,2%) та надійність (14250 годин на відмову).

Список використаних джерел:

1. "Traditional Optical and Contact-Based Surface Inspection Methods" – порівняння традиційних методів контролю якості поверхні[Електронний ресурс]. – Режим доступу: https://www.sciencedirect.com/science/article/pii/S1474667017555810

2. ·Подчашинський Ю.О., Сагайдачний Є.В. "Автоматизована система контролю якості поверхні промислових виробів на основі фрактальних моделей[Електронний ресурс]. – Режим доступу: https://eztuir.ztu.edu.ua/jspui/bitstream/123456789/1260/1/84.pdf.com

3. Давидчук Н.С., Подчашинський Ю.О., Чепюк Л.О. "Дослідження якості поверхні виробів з природного каменю на основі фрактальних геометричних параметрів їх відеозображень".[Електронний ресурс]. – Режим доступу:https://conf.ztu.edu.ua/wp-content/uploads/2016/06/79-1.pdf.com.

4. Туз Ю.М., Самарцев Ю.М., Кокотенко Б.В., Козир О.В. "Система контролю якості поверхні промислових виробів з використанням фрактальних моделей". [Електронний ресурс]. – Режим доступу:https://asnk.kpi.ua/docs/pbf/confPB24/conf_pb_content_2024.pdf.com.

УДК 621.317

Магалецький Я.В., аспірант,
Подчашинський Ю.О., д.т.н., професор,
Чепюк Л.О., к.т.н., доцент
Державний університет «Житомирська політехніка»

АНАЛІЗ ВИМОГ ДО КОМП'ЮТЕРИЗОВАНОЇ ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНОЇ СИСТЕМИ МЕХАНІЧНИХ ХАРАКТЕРИСТИК АСИНХРОННОГО ЕЛЕКТРОПРИВОДА В НАСОСНОМУ ОБЛАДНАННІ

Для виконання вимірювань електричних характеристик електродвигунів відцентрових насосів (ЕДВН) використовують окремі вимірювальні прилади. Перевірку механічних характеристик ЕДВН виконують шляхом підключення гідравлічних частин насосів у тестовий режим перекачування рідини. У зв'язку з великою різноманітністю обладнання, яке надходить до сервісного відділення, виникає проблема проведення його попередньої діагностики та визначення характеристик, так подальшої діагностики після ремонту виникають [1,2].

Таким чином виникають наступні складнощі: вимірювальні прилади не поєднані у систему; недостатня точність вимірювання характеристик двигунів; процес вимірювання не є синхронізованими; вимірювання виконуються повільно; рівень кваліфікації персоналу впливає на якість діагностики.

Такий спосіб можна використовувати тільки для виконання перевірки працездатності і загального стану ЕДВН. В якості переваги даного методу проведення діагностики можна відзначити простоту реалізації і не значні витрати на обладнання та прилади для проведення вимірювань.

В результаті виконаного аналізу використання ЕДВН можна відзначити наступні вимоги до комп'ютеризованої інформаційно-вимірювальної системи (КІВС) механічних характеристик асинхронного електропривода в насосному обладнанні:

1) гнучка і адаптивна структура КІВС;

2) блоки для проведення вимірювань об'єднуються у єдину систему;

3) висока швидкість виконання вимірювань;

4) наявність відповідного програмного забезпечення для обробки результатів вимірювань;

5) результатів вимірювань можна представляти графічно;

6) можливість завантаження результатів вимірювань у зовнішню базу даних;

7) вимірювальні можливості системи можна розширити за рахунок підключення додаткових каналів вимірювання.

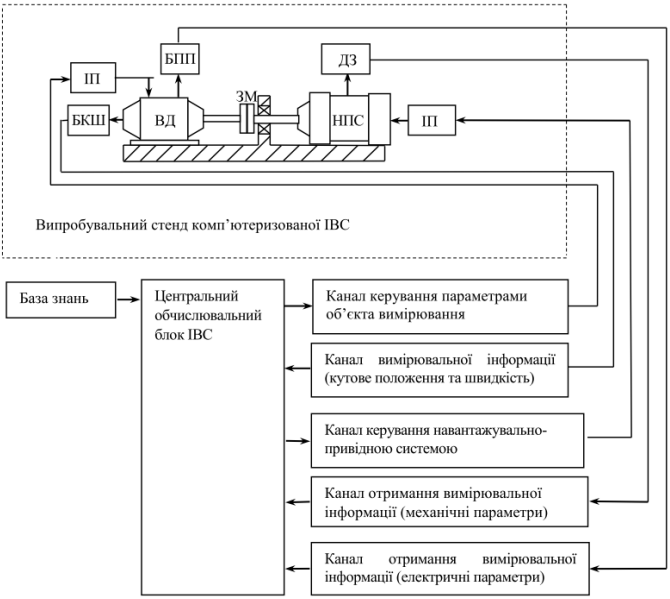


Рис. 1. Структурна схема КІВС механічних характеристик асинхронного електропривода в насосному обладнанні

Список використаних джерел:

1. Подчашинський, Ю.О., Магалецький, Я.В. (2024). Аналіз проблематики та розробка структури комп'ютеризованої інформаційно-вимірювальної системи механічних характеристик асинхронного електропривода в насосному обладнанні. Технічна інженерія, (1(93), 295–300.

2. Подчашинский Ю.О., Магалецький Я.В., Чепюк Л.О. Мікропроцесорна система вимірювання пускового моменту електродвигунів відцентрових насосів. Тези Сімнадцятої міжнародної науково-практичної конференції «Інтегровані інтелектуальні робототехнічні комплекси» (ІІРТК-2024), 21-22 травня 2024 р. К.: НАУ, 2024. 514 с. С. 242-244.

УДК 621.317

Лугових О.О., старший викладач
Невмержицький В. С., студент ІВТ-3м
Державний університет «Житомирська політехніка»

КОМП'ЮТЕРИЗОВАНА СИСТЕМА ВИМІРЮВАННЯ ГЕОМЕТРИЧНИХ ПАРАМЕТРІВ ВИРОБІВ НА МАШИНОБУДІВНОМУ ПІДПРИЄМСТВІ ЗА ЇХ ВІДЕОЗОБРАЖЕННЯМИ

Машинобудування – одна з найважливіших галузей української економіки. Серед основних негативних тенденцій розвитку галузі машинобудування можна відзначити зниження прибутковості підприємств і ефективності використання всіх видів виробничих ресурсів, застаріле обладнання, скорочення чисельності персоналу, низька якість кінцевої продукції.

Одним зі способів підвищення якості на виробництвах є впровадження в виробничий процес високоавтоматизованих оптичних систем контролю. В основі технології лежіть використання ЕОМ для імітації людської діяльності або людським зором: визначення геометричних розмірів та якості.

Впровадження технології машинного зору в геометричні вимірювання дозволяє досягти швидкості вимірювання розмірів, безконтактності, хорошої гнучкості та високої точності. Це економить час і енергію та дозволяє уникнути людських помилок у процесі вимірювання, а також може забезпечує безперервність виробництва та підвищує рівень автоматизації виробництва[1-3].

Прямими аналогами системи на міжнародному ринку є продукція компанії Keyence серія IM, компанії Sylvac серії Vision 200, а також промислові комплекси Nikon Inexiv.

Основними недоліками вище перерахованих систем є: висока ціна; складність інтегрування у вже існуюче виробництво; неможливість модифікації програмного забезпечення; послуги нав'язані виробником;

Тому розробка комп'ютеризованої системи вимірювання геометричних параметрів виробів на машинобудівному підприємстві за їх відео зображеннями є актуальною.

Система, що розроблюється передбачає використання таких основних компонентів: камера з CMOS матрицею, модуль обчислень та відображення. Об'єктами вимірювань будуть виступати деталі з прямими гранями.

Для розміщення об’єкту вимірювань потрібна робоча площина, камера повинна бути паралельно площині, для зменшення кількості спотворень. Вимірювальна система фіксує зображення, які відображають характеристики поверхні валу за допомогою CMOS-камери. Обробляючи зібрані дані зображення, комп’ютер може швидко й точно обчислити розмір деталі та видати результат безпосередньо на графічну карту, щоб показати його [4]. Схематично зображення системи представлено на рис. 3.1.

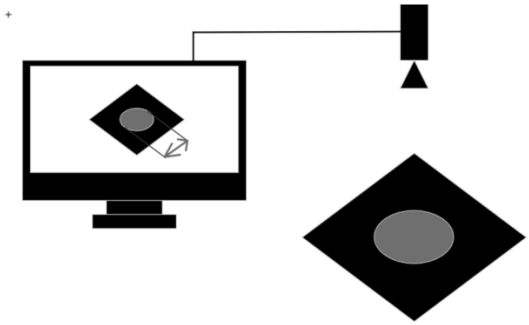


Рисунок 1. Схематичне зображення комп’ютеризованої системи вимірювання геометричних параметрів

Для визначення геометричним параметрів виробів на машинобудівному підприємстві була написана програма на мові Python та бібліотеки машинного зору OpenCV. За допомогою бібліотеки машинного зору OpenCV відбувається пошук об’єкту вимірювань і він виділяється прямокутником [5,6]. Робочий інтерфейс оператора представлений на рис.2.

Літери в програмі означають наступне: A – виділено червоним виведення джерела відеопотоку, кількість кадрів за секунду, а також роздільну здатність вхідного відео потоку; B – виділено жовтим виведення координати курсору, C – виділено зеленим інформація про обраховане значення довжини по вертикалі та горизонталі, а також діагональна довжина, D – фіолетовим кольором було виділено меню управління, в якому можна обрати режим роботи, E – виділено синім позначаються значення розмірів, J – багровим кольором обраховується площа тієї сукупності пікселів в яку входить зображення деталі, G – виділено салатовим позначає перехрестя в межі якого повинен попасти об’єкт вимірювання для більш точного визначення розмірів.

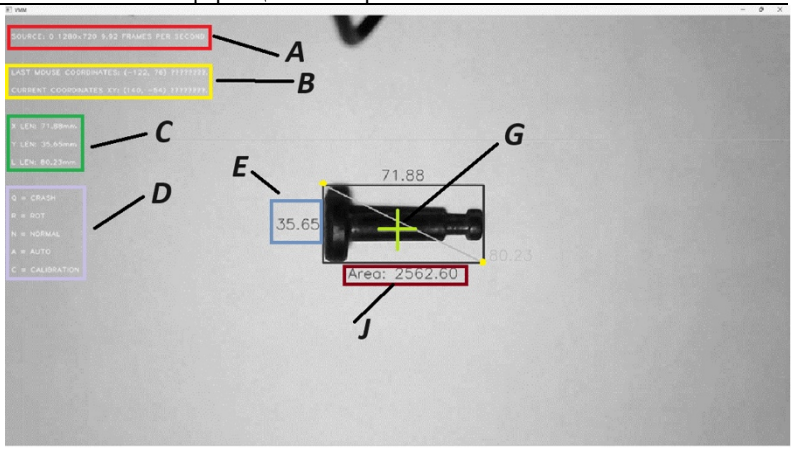


Рисунок 2. Демонстрація роботи програми

Розроблена система дозволяє безконтактно вимірювати лінійні розміри, за допомогою камери, з доволі високою точністю в ручному режимі, і дає уявлення про загальні розміри об’єкта вимірювань, якщо мова йде про автоматичний режим.

Список використаних джерел:

1. M. Brown, D.G. Lowe, Automatic panoramic image stitching using invariant features. Int. J. Comput. 2007.Vis. 74, 59–73.

2. G. Chen, K. Yang, R. Chen, et al., A gray-natural logarithm ratio bilateral filtering method for image processing. Chin. Opt. Lett.2008. 6(9), 648–650.

3.Gonzalez, R.C., and R. E. Woods, and S. L. Eddins. 2004. Digital Image Processing using MATLAB. 302 c.

4. Подчашинський Ю.О. Стиснення та перетворення цифрових відеозображень з вимірювальною інформацією про геометричні параметри об’єктів: Монографія. – Житомир: ЖДТУ, 2019. 200 с.

5. Мова програмування Python [Електронний ресурс]. – Режим доступу: https://wiki.python.org/moin/BeginnersGuide.

6. Бібліотека OpenCV [Електронний ресурс]. – Режим доступу: https://docs.opencv.org/4.x.

УДК 528.854:004.9

Подорожко К.Д., аспірант
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»

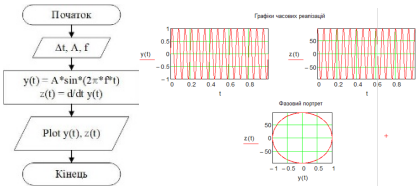
ЗАСТОСУВАННЯ КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ ДЛЯ ЦИФРОВОЇ ОБРОБКИ ГЕОПРОСТОРОВИХ ДАНИХ

Особливого розвитку в сучасних умовах набувають методи цифрової обробки зображень, оскільки вони є критично важливими для аналізу природних і техногенних процесів на Землі та в космосі. Завдяки сучасним комп'ютерним технологіям є можливість отримувати високоточні дані для моніторингу стану русла річок, ерозії берегів і впливу людської діяльності на екосистеми в цілому. Цифрова обробка супутникових даних дозволяє відстежувати зміни в реальному часі, що особливо важливо для запобігання екологічним катастрофам і планування водокористування. Запровадження та комбінування різноманітних комп'ютерних технологій підвищує ефективність аналізу геопросторових даних [1].

Важливим елементом цифрової обробки сигналів і зображень в автоматизованих та інформаційно-вимірювальних системах є дослідження алгоритмів, що дозволяють якісно та комплексно виконувати оброблення геопросторових даних. Дане дослідження присвячено опису цифрової обробки методом фрактального аналізу в програмі MathCad. Актуальність застосування фрактального аналізу як методу цифрової обробки, надзвичайно висока, адже він допомагає виявляти структурні особливості зображень, які важко помітити традиційними методами. Для застосування фрактального аналізу для дослідження динаміки стану русла річок важливу увагу варто приділити створенню коректного алгоритму, який дозволить програмно реалізувати побудову фазових портретів досліджуваної ріки та врахує всі особливості геопросторових даних [2]. На рис.1, а наведено приклад блок-схеми алгоритму програми цифрової обробки зображення русла річки. Основними вхідними даними алгоритму є: амплітуда показників, A; часовий крок ітерації отримання геопросторових гідрологічних даних, Δt,частота зміни даних, f.

Будемо розуміти під фазовою площиною площину, кожна точка якої однозначно визначає стан (фазу) гідрологічної системи. Оскільки площина має два параметра вимірювання y то z, то метод фазової площини придатний для аналізу руху систем, що описуються диференціальними рівнянням другого порядку [3]. Вивід графіків, реалізується функцією Plot, яка будує графіки фазових портретів і

часових реалізацій зміни стану річкової системи. Поведінку такої системи можна подати геометрично на площині у прямокутних декартових координатах.



а б

Рис 1. Алгоритм цифрової обробки зображення русла річки за фазовими портретами: а – блок-схема алгоритму; б – графіки часових реалізацій і фазовий портрет русла річки

На рис. 1,б наведено приклад реалізації запропонованого алгоритму в MathCad. Тут як вхідні данні прийнято: A=1, f=3, Δt = 0,001. Крива на фазовій площині складає фазову траєкторію і описує еволюцію системи. Фазовий портрет витягується зі зміною амплітуди сигналу. Після того, як фазовий портрет отримано, можна зазначити низку особливостей у формі та розташуванні фазових траєкторій. На фазовій площині зазвичай можуть бути такі типи фазових траєкторій: особливі точки, або положення рівноваги лінійної системи, ізольовані замкнуті траєкторії, що відповідають періодичним рухам та змінам стану русла річок у системі. Таким чином, цифрова обробка зображень дає змогу пришвидшити аналіз динаміки гідрологічних систем та отримати параметри змін, розв'язуючи диференціальні рівняння на площині з прямокутною системою координат.

Список використаних джерел:

1. John J. Qu, Wei Gao, Menas Kafatos, Robert E.Murphy, Vinsent V. Salomonson Earth Science Satellite Remote Sensing, Data, Computational Processing, and Tools. Tsinghua University Press, 2006.

2. Пащенко, Р. Е. Основи теорії формування фрактальних сигналів / Р. Е. Пащенко. – Харків : ЕкоПерспектива, 2005. – 296 с.

3. Пащенко, Р. Е. Сегментація зображень методом ранжування поля фрактальних розмірностей / Р. Е. Пащенко, А. В. Шаповалов // Системи обробки інформації. – 2004. – Вип. 8(36). – С. 103 – 107.

УДК 621.317

Подчашинський Ю.О., д.т.н., професор
Жураківський Я.Я., магістрант
Державний університет «Житомирська політехніка»

КОМП'ЮТЕРИЗОВАНА СИСТЕМА КОНТРОЛЮ ЯКОСТІ НА ВИРОБНИЦТВІ КОСМЕТИЧНОЇ ПРОДУКЦІЇ

Сучасне виробництво косметичної продукції вимагає високих стандартів якості, що обумовлено жорсткими вимогами споживачів та регуляторних органів. Впровадження комп'ютеризованої системи контролю якості дозволяє забезпечити точність, швидкість та автоматизацію вимірювань, що є ключовим фактором для підвищення конкурентоспроможності продукції на ринку. Тому з цього випливає, що актуальність розробки система контролю якості косметичної продукції є достатньо високої на даний час.

Для контролю якості косметичної продукції потрібно моніторити такі показники: рівень pH, концентрація газів (NH3, NOx, CO2, бензин) рівень спирту та колір.

Для вимірювання даних показників пропонується застосувати такі датчики: датчики якості повітря (MQ-135), датчик pH, датчик виявлення спирту(MQ-3), колірний датчик TCS3200. Відповідно для керування системою використовується мікроконтролер. Для живлення акумулятор. Для включення та виключення системи використовується кнопка. Для виведення виміряних показників якості використовується дисплей. Для звукового оповіщення застосовується динамік. Структурна схема комп'ютеризованої системи контролю якості на виробництві косметичної продукції представлена на рис.1

Було розроблено програмне забезпечення для мікроконтролера на мові Сі, яке забезпечує зчитування даних з датчиків, обробку інформації та виведення результатів на дисплей. Програма також передбачає звукове оповіщення у разі виявлення критичних значень якості. Проведено розрахунки похибок вимірювань для датчиків pH та спирту. Відносна похибка вимірювання pH становить 1,45%, а для вимірювання концентрації спирту — 1,65%. Це забезпечує достатню точність для контролю якості косметичної продукції.

Розрахунки показали, що середній наробіток системи до відмови становить 14186 годин, що свідчить про високу надійність розробленої системи.

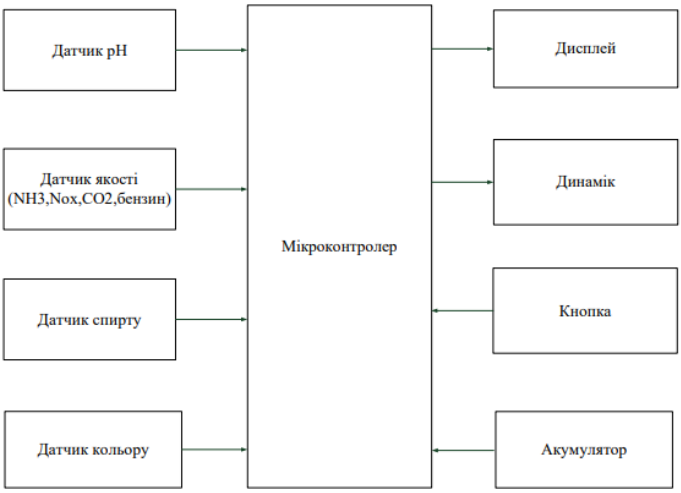


Рис. 1 Структурна схема комп'ютеризованої системи контролю якості на виробництві косметичної продукції

Складові системи наступні: мікроконтролер, OLED-дисплей, кнопка управління та динамік, акумулятор, датчик спирту, датчик рівня кислотності pH, датчик якості повітря, датчик кольору.

Розроблена система може бути впроваджена на виробництвах косметичної продукції для автоматизації контролю якості, що дозволить зменшити витрати на ручний контроль та підвищити точність вимірювань.

Список використаних джерел:

1. ДСТУ ISO 22716:2009 "Практика належного виробництва (GMP) для косметичних продуктів".

2. ДСТУ ISO 9001:2015 "Системи управління якістю. Вимоги".

3. Офіційний сайт Європейської комісії з питань косметики [Електронний ресурс]. – Режим доступу: https://single-market-economy.ec.europa.eu/sectors/cosmetics_en.

4. Arduino датчики і модулі. [Електронний ресурс]. – Режим доступу: Детальніше: https://arduinokit.com.ua/ua/g71152865-arduino-datchiki-moduli.

УДК 621.317

Подчашинський Ю.О., д.т.н., професор
Лук'яновець В.О., магістрант
Державний університет «Житомирська політехніка»

МЕТРОЛОГІЧНЕ ЗАБЕЗПЕЧЕННЯ ЗАСОБІВ ВИМІРЮВАННЯ ТЕМПЕРАТУРИ ТВЕРДИХ ТІЛ

Вимірювання температури твердих тіл є важливим елементом багатьох промислових процесів, наукових досліджень та побутових застосувань. Точність цих вимірювань впливає на якість продукції, безпеку обладнання та ефективність технологічних процесів. Метрологічне забезпечення забезпечує високу точність і надійність вимірювань, що є критичним для багатьох галузей, таких як металургія, енергетика, машинобудування та інші. Причини актуальності метрологічного забезпечення засобів вимірювання температури твердих тіл є наступними:

1. Вимірювання температури відіграє ключову роль у контролі якості продукції. У металургії, наприклад, точне вимірювання температури є критичним для забезпечення належних властивостей сплавів та сталі. Відхилення від необхідної температури може призвести до дефектів, що знижують міцність і довговічність виробів.

2. Підвищення технологічних процесів, таких як термічна обробка, зварювання, лиття та інші, температура є важливим параметром, що визначає ефективність процесу. Точні температурні вимірювання дозволяють оптимізувати процеси, зменшуючи витрати енергії та підвищуючи продуктивність.

В якості датчику температури використано платиновий терморезистор PT1000 [1]. Для точного вимірювання зміни опору використано мостову схему Уітстона, що дозволяє отримати невеликий аналоговий сигнал, пропорційний зміні температури.

Операційний підсилювач [2] OPA177, що забезпечує малий рівень шуму та високу стабільність сигналу, підсилює слабкий сигнал від мостової схеми до рівня, придатного для обробки мікроконтролером.

Фільтр низьких частот. використовується для усунення високочастотних шумів, що можуть виникати через електромагнітні завади.

Мікроконтролер ATmega328 [4] відповідає за обробку отриманих цифрових даних, виконання вимірювання та управління виведенням інформації.

OLED-дисплей 128x64 [5] використовується для виводу поточного значення температури у зручному форматі.

Блок живлення використано імпульсний перетворювач напруги MT3608, який забезпечує стабільну роботу системи, захист від перевантажень та короткого замикання.

Комп'ютеризована система вимірювання температури твердих тіл представлена на рис.1.

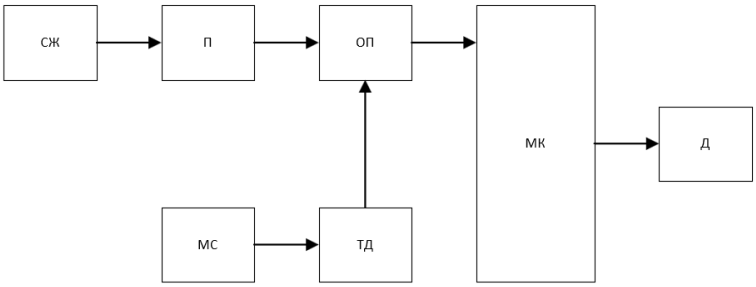


Рис.1 Структурна схема метрологічного забезпечення засобів вимірювання температури твердих тіл

Комп'ютеризована система вимірювання температури твердих тіл складається з наступних основних блоків: СЖ – система живлення; П – перемикач; ОП – операційний підсилювач; МС – мостова схема; ТД – температурний датчик; МК – мікроконтролер; Д – дисплей.

Ця схема забезпечує точне та стабільне вимірювання температури твердих тіл, з можливістю відображення даних у реальному часі.

Список використаних джерел:

1. Датчик температури PT1000 [Електронний ресурс] – Режим доступу до ресурсу: https://voron.ua/catalog/023278--datchik_temperatury_pt1000-2b_heraeus_termodatchik.

2. Операційний підилювач OPA177 [Електронний ресурс] – Режим доступу до ресурсу: https://imrad.com.ua/ua/opa177fp-6?srsltid.

3. Аналого цифровий перетворювач (ADC) [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Аналого-цифровий_перетворювач.

4. Мікроконтролер ATMEGA328 [Електронний ресурс] – Режим доступу до ресурсу: https://diylab.com.ua/p64493856-mikrokontroler-atmega328.html.

УДК 621.317

Подчашинський Ю.О., д.т.н., професор,
Рижук А.В., асистент,
Лугових О.О., ст. викладач
Державний університет «Житомирська політехніка»

СТВОРЕННЯ 3D СТРУКТУРИ НА ОСНОВІ 2D ЗНІМКІВ ЗРАЗКА БУРШТИНУ

Бурштин цінний ресурс який формувавсь 40-50 мільйонів років тому з хвойних дерев та який зберігся до сьогодення. Його цінність визначається своєю рідкістю. Найбільші залягання знаходяться на узбережжі Балтійського моря, України, Румунії, Білорусії, Росії, Мексиці та США [1].

Сам процес видобування досить непростий та завдає непоправної шкоди для навколишнього середовища, а саме зміна структури рельєфу, погіршення екологічного стану ґрунтів та зміни в режимі поверхневих та підземних вод, що веде за собою до знищення лісових масивів, яке може відновитись лише через сотні років[2].

Також свою найбільше цінність камінь здобуває після обробки. Під час усунення різноманітних дефектів каменю втрачається левова частка продукту. Бурштин застосовується в різних сферах, а саме в ювелірній справа, декор, медицина , промисловість (фарби, лаки), парфумерія. Існування великого попиту на бурштин унеможливлює повністю відмову від нього. Тому потрібно під час обробки, якомога зменшити втрату дорогоцінного матеріалу.

Для більш точного передбачення кроків що до обробки потрібно вдосконалювати комп'ютерні методи обробки зразків бурштину. А саме створення точної 3д моделі, що дасть змогу з більшою точністю планувати дії що до подальшої обробки.

Для створення 3д моделі буде використовуватись SFM(Structure from motion) алгоритм, який будує 3d – структуру сцени з набору 2D – зображень[3]. Ключовими кроками в 3д реконструкції є:

- Вилучення найважливіших (найстійкіших) ознак на зображені;
- Зіставлення знайдених контрольних точок;
- 3D реконструкція;
- Регулювання пучка;
- Отримання хмари точок та подальша генерація сітки поверхні об'єкта.

Першим та важливим етапом є детекція ключових точок. Автоматичний процес знаходження відповідності на зображаннях досить складний. Та і не можливо порівняти кожен піксель на одному

зображенні з відповідним пікселем на іншому зображені через комбінаторну складність. Та не всі точки підійдуть для зіставлення. Тому потрібно використовувати методи виокремлення та зіставлення. Так як наскільки точно буде визначено контрольні точки, залежить загальна точність 3D моделі. Серед існуючих методів пошуку та зіставлення контрольних точок найпопулярнішими є SIFT та ORB методи. Ці 2 методи потребують першочергового знаходження внутрішніх та зовнішніх параметрів камери. Після калібрування отримуємо данні про положення камери.

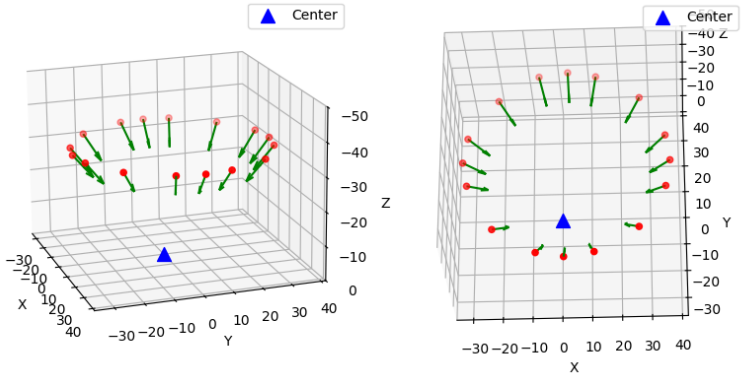


Рис.1 – Візуалізація внутрішніх та зовнішніх параметрів камери (положення камери в просторі)

На рис. 1 зображена сцена з колекції знімків зразка бурштину. Де вектори вказують на положення та напрямок камери. Та з синім центром де розташований сам зразок. Після того як визначено зовнішні та внутрішні параметри камери потрібно зіставити зображення на суміжних камерах котрі різняться положенням в 15º та 30º. Для цього буде використовуватись один з найпопулярніших алгоритмів зіставлення – SIFT[4] та ORB[5]. Для даного алгоритму буде застосовуватись SIFT так як показав кращі результати в швидкості, знаходженні контрольних точок та їх зіставлені.

SIFT(Scalse-Invariant Feature Transform) – алгоритм який використовується для виявлення ключових точок котрі є інваріантними відносно масштабу, обертання та зміни в освітлені. В основу цього алгоритму покладено функція L(x,y,σ), яка утворюється зі згортки Гауса(розмивання) в різних масштабах які між собою віднімаються та отримуються різниці Гауса. Кожен піксель на зображенні порівнюється з 8 сусідніми пікселями в тому ж масштабі, а також із 9 пікселями у

вищому масштабі та 9 пікселями у нижчому масштабі. У результаті виконується 26 перевірок. Якщо піксель який перевіряється є локальним екстремумом серед цих значень то він вважається потенційною ключовою точкою. Після чого навколо знайденого пікселю обертається околиця сусідніх пікселів(залежно від масштабу) та створюється орієнтаційна гістограма. Для обрахунку дескриптора для локальної області береться вікно 16x16 навколо точки поділене на 4x4 блоки. Для кожного блоку створюється гістограма орієнтації. Далі дескриптори порівнюються на основі ідентифікації їх найближчих сусідів за допомогою методу FLANN (Fast Library for Approximate Nearest Neighbors)[4].

Рис.2 – Хмара точок яка формує форму зразка бурштину

При отримані зіставлених точок обчислюється фундаментальна та істина матриця. Фундаментальна описує епіполярну геометрію між сусідніми зображеннями, а істина дає характеристику про положення та напрямок камери. Та на основі цих даних визначається 3d координата точки в просторі. Після цього застосовується регулювання пучка, щоб підвищити точність реконструкції. На виході SFM алгоритму маємо хмару точок 3д поверхні бурштину рис.2.

В результаті дослідження реконструкції на основі SFM алгоритму було зроблено 16 фото з різних ракурсів зразка бурштину, а саме через кожні 15º та 30º та з таких самих ракурсів було зроблено фото контрольної дощечки. Виконано калібрування камери та знайдено внутрішні і зовнішні параметри камери, використано метод SIFT для знаходження та зіставлення контрольних точок на зображені. Для кожного випадку було прораховано фундаментальну та істину матриця. Після чого сформовано хмару точок поверхні буршитну, яка в подальшому буде перероблена в поверхню. Отримана тривимірна

модель поверхні дає змогу не лише відображати зразок бурштину, а й проводити аналіз геометрії, оцінювати об'єм, ідентифікувати дефекти/вкраплення Це відкриває вікно можливостей для промислових потреб, а саме автоматичної класифікації зразків та моделювання подальших процесів та визначення оптимальних параметрів обробки.

Список використаних джерел:

1. Research of Methods for Determining Key Points for 3D Modeling of Amber Samples / Y. Podchashynskyi, A. Ryzhuk, O. Luhovykh, L. Chepiuk. Journal of Information Systems Engineering and Managemen. Vol. 10 No. 16s (2025), p. 784-801. DOI: https://doi.org/10.52783/jisem.v10i16s.2665.

2. Ковалевський С. С., Ковалевський С. Б. Бурштинові копалини: історія вивчення, методи добування та вплив на лісові екосистеми. Науковий вісник НЛТУ України. 2019. Т. 29. С. 56–59.

3. Lobo T. Understanding Structure From Motion Algorithms .Teresa Lobo. 2023. URL: https://medium.com/@loboateresa/understanding-structure-from-motion-algorithms-fc034875fd0c.

4. Deep. Introduction to SIFT(Scale Invariant Feature Transform). Medium. URL: https://medium.com/@deepanshut041/introduction-to-sift-scale-invariant-feature-transform-65d7f3a72d40.

5. Siromer. Detecting and Tracking Objects with ORB Algorithm using OpenCV. Medium. URL: https://medium.com/thedeephub/detecting-and-tracking-objects-with-orb-using-opencv-d228f4c9054e.

6. Науменко У. З., Мацуй В. М. Етапи геологічного розвитку та генетичний тип корінного першоджерела розсипів бурштину-сукциніту України. Геологічний журнал. 2020. № 4. С. 76-85. URL: http://jnas.nbuv.gov.ua/article/UJRN-0001245209.

УДК 621.317

Лугових О.О., старший викладач
Сай А. А., студент ІВТ-3м
Державний університет «Житомирська політехніка»

КОМП'ЮТЕРИЗОВАНА СИСТЕМА ДЛЯ ВИЗНАЧЕННЯ РІВНЯ РІДИНИ У РЕЗЕРВУАРАХ ХІМІЧНОГО ВИРОБНИЦТВА

Сучасні промислові процеси потребують високого рівня автоматизації для підвищення ефективності, безпеки та зниження витрат. Одним із критично важливих аспектів є моніторинг рівня рідин у резервуарах хімічного виробництва. Точне вимірювання рівня рідини дозволяє уникнути аварійних ситуацій, запобігти витокам та покращити контроль за використанням ресурсів.

Розробка комп'ютеризованої системи для визначення рівня рідини у резервуарах хімічного виробництва дозволить підвищити точність вимірювання, забезпечити безперервний моніторинг та своєчасне реагування на зміни рівня рідини.

Для створення системи визначення рівня рідини у резервуарах хімічного виробництва пропонується сучасний ультразвуковий датчик HC-SR04, який забезпечує точність до 3 мм та може працювати в широкому діапазоні температур. В якості обчислювального модуля використано мікроконтролер ATmega328, який забезпечує ефективну обробку даних та підтримує зв'язок із іншими компонентами системи. Візуалізація даних здійснюється за допомогою LCD дисплея 16x2, а звукове оповіщення про критичні рівні рідини реалізується через активний зумер.

Структурна схема системи представлена на рисунку 1.

Складові системи структурної схеми наступні:

- Мікроконтролер ATmega328;
- Ультразвуковий датчик HC-SR04;
- LCD дисплей 16x2;
- Активний зумер;
- Джерело живлення 5В;
- Додаткові модулі для розширення функціональності.

Рис. 1. Структурна схема комп'ютеризованої системи для визначення рівня рідини у резервуарах хімічного виробництва

Розроблена комп'ютеризована система дозволяє ефективно контролювати рівень рідини у резервуарах хімічного виробництва, своєчасно реагувати на зміну параметрів та забезпечувати безпеку виробничих процесів.

Список використаних джерел:

1. Використання ультразвукових датчиків у промислових системах [Електронний ресурс]. Режим доступу: http://ecoj.dea.kiev.ua/archives/2023/1/16.pdf .

2. Контроль рівня рідин у резервуарах хімічного виробництва [Електронний ресурс]. Режим доступу: https://jooby.eu/uk/blog/rozumnij-elektrolichilnik.

3. Технічні характеристики датчика HC-SR04 [Електронний ресурс]. Режим доступу: https://artificer.com.ua/product/ky-035-modul-datchika-hollaю

4. Програмування мікроконтролерів ATmega328 [Електронний ресурс]. Режим доступу: https://www.mini-tech.com.ua/datchik-gaza-mq-9-modul.

5. Arduino UNO R3 [Електронний ресурс]. Режим доступу: https://artificer.com.ua/product/arduino-uno-r3.

6. Мікропроцесорна техніка. Однокристальні мікроконтролери: навч. посібник / С.Р.Михайлов. – К.:, 2014. 123 с.

УДК 621.317

Ступак А.Г., аспірант,
Подчашинський Ю.О., д.т.н., професор,
Чепюк Л.О., к.т.н., доцент
Державний університет «Житомирська політехніка»

ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДІВ СТИСНЕННЯ МЕДИЧНИХ ЗОБРАЖЕНЬ З ВИМІРЮВАЛЬНОЮ ІНФОРМАЦІЄЮ БЕЗ ВТРАТ

Сучасні методи стиснення медичних зображень з вимірювальною інформацією нараховують велику кількість видів стиснення даних. Вони можуть відрізнятися як в основних принципах дії, так і мати подібні алгоритми з деякими відхиленнями, що удосконалюють кожен метод ще більше. Проблемою вибору методу є відбір найефективнішого у вирішенні поставленої задачі. Розглянемо кодування відеозображень без втрат методами імпульсно-кодовій модуляції (ІКМ) і диференційної імпульсно-кодової модуляції (ДІКМ).

При ІКМ сигнал зображення дискретизується, кожен відлік квантується і кодується двійковим кодом. На відміну від факсимільної передачі, де сигнали квантуються на два рівня: білий і чорний і кодується з точністю 1 біт на відлік (0 або1), кількість рівнів квантування напівтонових зображень встановлюється від 64 до 256, для кодування яких витрачається 6…8 біт. Кольорове зображення зазвичай являє собою комбінацію трьох кольорів: червоного (R), зеленого (G), синього (B). Кожен з цих кольорів обробляться незалежно від інших і для кодування кожного з них виділяється від 6 до 8 бітів на відлік. Кодування методом ІКМ являється свого роду еталоном кодування. Тому степінь зниження швидкості передачі за рахунок стиснення вихідного повідомлення одним із запропонованих методів, звичайно, оцінюється по відношенню до ІКМ. Зниження числа рівнів квантування при кодуванні методом ІКМ не доцільно, так як це викликає появу хибних контурів, які виникають за рахунок стрибкоподібних змін яскравості або кольору. В той же час ентропія напівтонового зображення складає 4 … 6 біт на пікселів, що свідчить про надлишковість кодування сигналів зображення методом ІКМ [1].

Для зменшення надлишковості сигналів зображення застосовують ДІКМ. При такому способі модуляції кодується не повне значення відліків, що представляють рівень яскравості елементів зображення (пікселей), а різниця між поточним і попереднім відліком сигналу. Ще у більшій степені зменшується надлишковість у системах з ДІКМ, в яких кодуванню підлягає різниця між попереднім відліком і прогнозованим значенням яскравості наступного піксела. Такий вид

обробки відеосигналів являється різновидом кодування з прогнозуванням, який найбільш широко використовується у сучасних системах передачі зображень. При цій модуляції використовується та обставина, що безперервно змінна яскравість зображення *B(x, y)* може бути прогнозована для різних *x*. Це використовується для стиснення повідомлення за рахунок передачі тільки цієї інформації, яка потрібна для корекції прогнозування. Оскільки прогнозоване значення кожного відліку обчислюється на основі тільки попередніх значень, то воно наявне як у кодері, так і в декодері. Відновлення відліків в декодері виконується шляхом сумування похибок прогнозу зі спрогнозованим значенням цього відліку. Структурна схема цифрової ДІКМ зображена на рис. 1.

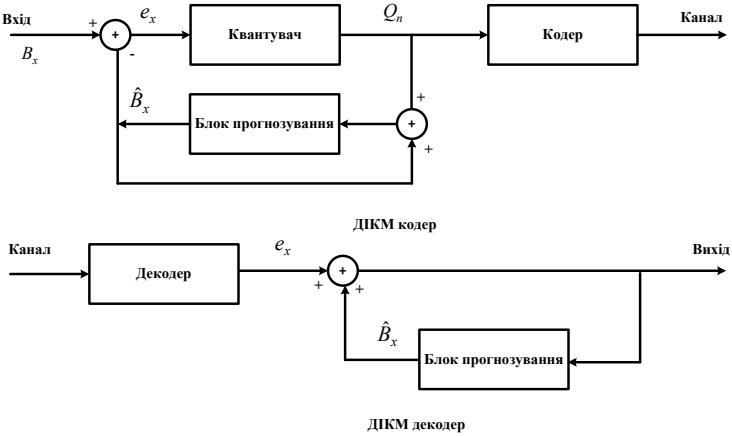


Рис. 1. Структурна схема цифрової ДІКМ

Список використаних джерел:

1. Stupak A.G., Podchashynskyi Yu.O., Chepiuk L.O. Comparative analysis of image compression methods with real-time measurement information. Topical aspects of modern scientific research. Proceedings of the 11th International scientific and practical conference. CPN Publishing Group. Tokyo, Japan. 2024. 425 p. P. 43-48. URL: https://sci-conf.com.ua/wp-content/uploads/2024/07/TOPICAL-ASPECTS-OF-MODERN-SCIENTIFIC-RESEARCH-11-13.07.24.pdf

УДК 621.317

Товстік С.О., аспірант,
Подчашинський Ю.О., д.т.н., професор,
Чепюк Л.О., к.т.н., доцент
Державний університет «Житомирська політехніка»

ЗАСТОСУВАННЯ СОНЯЧНОГО ТРЕКЕРУ У СИСТЕМІ ОРІЄНТАЦІЇ СОНЯЧНИХ БАТАРЕЙ

Сонячний трекер – це система, призначена для орієнтації на Сонці робочих поверхонь систем, що генерують електрику, або систем, що концентрують (генерують) теплову енергію, встановлених на трекері.

Робочою поверхнею виступають: батарея, що складається з сонячних фотоелектричних модулів (панелей); дзеркало параболічного відбивача, що фокусує сонячну енергію на двигуні Стірлінга, що виробляє електрику; дзеркало відбивача, що фокусує сонячну енергію на будь-який інший приймач сонячної енергії, яким може бути пристрій або теплоносій, залежно від типу системи, оптичні пристрої та ін. [1].

Точна орієнтація робочих поверхонь систем на Сонці необхідна для досягнення максимальної продуктивності. При цьому завдання трекерн – зменшити кут падіння сонця на робочу поверхню сонячних панелей (PV-модулів, CPV-концентрованих фотоелектричних модулів, CSP систем, HCPV систем, параболічних відбивачів та ін.).

Сонячний трекер у повній комплектації складається з несучої конструкції, що складається з фіксованої та рухомої частин, рухома частина має одну або дві осі обертання; системи орієнтації (позиціонування) рухомої частини трекера, що складається з актуаторів, та пристрої керування ними; системи безпеки для захисту від блискавк та від перевантажень; метеостанції для попередження системи про несприятливі погодні умови; стабілізаторів; системи управління; інтерфейсу для налаштування, контролю та обслуговування енергосистеми; системи віддаленого доступу для віддаленого моніторингу та управління системою; системи навігації для визначення географічного положення системи; інвертора для – перетворення корисного навантаження від трекера (PV-модулів та ін.) постійної напруги в змінну 220 В (110В) і передачі його споживачеві.

Рухлива частина трекера може змінювати своє положення за допомогою ручного приводу або за допомогою 1-2-х актуаторів – виконавчих пристроїв, виконаних на електродвигунах. Завдання трекера – встановити кути нахилу робочої поверхні навантаження, зорієнтувавши її суворо на сонце (сонячні промені повинні падати перпендикулярно площині сонячної батареї).

Такої орієнтації можна досягти кількома способами. У першому випадку пристрій управління актуаторами за допомогою декількох фотоприймачів аналізує освітленість при різних положеннях трекеру і передає сигнали управління на актуатори до моменту, коли потік світла на всіх фотоелементах буде однаковий. Розбалансування системи через рух сонця дає імпульс активації нового переміщення у бік сонцю. Схеми таких пристроїв нескладні та недорогі але у похмуру погоду, при опадах та забрудненні фотоприймачів система непрацездатна. Переорієнтувати систему можна вручну, або, керуючи актуаторами, подаючи сигнали управління за допомогою перемикачів. Такий спосіб прийнятний для сезонної орієнтації трекерів, коли на якийсь період часу виставляється відповідний кут нахилу. Для дешевих систем він цілком підходить. Управління рухом трекера по азимутальному та зенітному кутах можливе пристроєм управління, до складу якого входить таймер. При цьому актуатори розпочинають свою роботу за добовою програмою таймера (за потреби і за річною програмою). Точність орієнтації невелика, оскільки сонце протягом року постійно змінює час, місце сходу й заходу, зенітний кут.

Найбільш ефективний програмний спосіб управління актуаторами, якій у певні інтервали часу розраховує місце розташування сонця. По внутрішньому годиннику програма на блок управління буде видавати інформацію про значення азимутального (Azimuth) і зенітного (Zenith) кутів, з урахуванням розташування трекера. Після чого виконавчим пристроєм проводиться відповідна переорієнтація трекера. Дана програма для розрахунку розташування сонця має називу SPA.

Пристрої керування трекерами можуть бути виконані на захищених комп'ютерах, PLC – програмованих логічних контролерах, або у вигляді окремих закінчених пристроїв, що програмуються постачальником при постачанні трекера, з прив'язкою до місцевості свого виробу. Група трекерів може керуватися одним комп'ютером, що знижує собівартість електростанції.

Список використаних джерел:

1. Колонтаєвський Ю. П. Фотоенергетика:навч. посібник / Ю.П. Колонтаєвський, Д. В. Тугай, С. В. Котелевець ; Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова. – Харків : ХНУМГ ім. О. М. Бекетова, 2019. – 160 с.

УДК 004.093

Ячменьова С.О. здобувач,
Болотіна В.В. ст. викладач
Державний університет «Житомирська політехніка»

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В КОМП'ЮТЕРНІЙ ГРАФІЦІ

Останні роки зростає популярність штучного інтелекту та його використання у різних галузях, зокрема при роботі з обробкою зображень чи графічних системах. Використання інтелектуальних машин надає змогу швидше і якісніше опрацювати зображення чи створити ілюстрації, що дає змогу дизайнерам, архітекторам, контент створювачам мати кращі показники продуктивності.

Штучний інтелект або ж інтелектуальна машина - це нейронна мережа чи сукупність алгоритмів для виконання автоматизації процесу діяльності. Штучний інтелект широко застосовується у сферах, де є чітко побудована математична чи аналітична модель.

Однією з таких сфер є галузь комп'ютерної графіки. У цій сфері завданням діяльності є створення чи обробка зображення з використанням комп'ютера та його програмного забезпечення як основного інструментарію. Основними напрямами роботи поданого типу можна вважати наступні:

– Растрова графіка: робота з піксельними зображеннями, такими як фотографії;

– Векторна графіка: створення зображень із використанням форм, простих геометричних фігур;

– 3D-моделювання: формування тривимірних об'єктів та анімацій;

– Цифрове малювання: використання графічного планшета для створення мистецтва;

– Фоторетуш і маніпуляції: редагування фотографій для досягнення бажаного вигляду;

– Штучний інтелект: генерація або обробка зображень за допомогою інтелектуальної машини.

Останній перерахований спосіб діяльності, а саме використання штучного інтелекту для роботи із зображеннями, віднайшов не лише теротичне, а й практичне використання виробниками програмного забезпечення, як-от Adobe, Canva, Photopea, тощо, через автоматизування найбільш виснажливих процесів роботи.

Наприклад, у період до появи інструментів інтелектуального виділення, заміна фону зображення в Adobe Photoshop потребувала великого обсягу часу на ретельне окреслення об'єкта. Просто пошук і

виділення волосся людини могло тривати кілька годин. Але з появою функцій «Автоматичне виділення» та «Виділення об’єкта» цей процес тепер займає лише кілька хвилин (із незначними коригуваннями від користувача).

Альтернативний приклад використання інтелектуальної машини - це генерація колажів з існуючих об’єктів векторної графіки або ж повноцінної ілюстрації з простих геометричних фігур, у веб-ресурсі Canva. Це стає можливим, з використанням інструменту «Магічні дизайни», що потребує від користувача лише надання доступу до полотна для роботи та текстового опису побажання щодо майбутнього зображення.

MyHeritage InColor або DeOldify - ще один варіант застосування штучного інтелекту через здатність автоматично додавати кольори до старовинних чорно-білих фотографій або відео. Процес, який раніше вимагав значного ручного редагування, тепер, завдяки цим додаткам, здійснюється алгоритмами глибокого навчання, які аналізують зображення, враховують контекст, розпізнають об'єкти та відповідно обирають кольори, що робить історичні фото доступними для сучасного візуального сприйняття.

Отже, у сучасному світі комп’ютерна графіка широко використовує штучний інтелект з метою полегшення процесу обробки зображень чи їх створення. Подальші дослідження будуть спрямовані на вдосконалення існуючих методів використання інтелектуальних машин у цій сфері.

Список використаних джерел:

1. ШІ для графічних дизайнерів [Електронний ресурс] // Adobe. – 2024. – Режим доступу: https://www.adobe.com/ua/products/firefly/discover/ai-for-graphic-designers.html.

2. Цисарський В. Особливості, проблеми та перспективи використання штучного інтелекту в сучасному мистецькому просторі: письменництво, образотворче мистецтво, озвучування // Артпростір. – 2024. – № 1(4). – С. 154–182. – DOI: https://doi.org/10.28925/2519-4135.2024.49.

3. Миттєво створюйте унікальні дизайни за допомогою ШІ [Електронний ресурс] // Canva. – 2024. – Режим доступу: https://www.canva.com/uk_ua/help/using-magic-design.

Секція 7
КОМП'ЮТЕРНО-ІНТЕГРОВАНІ ТЕХНОЛОГІЇ. РОБОТОТЕХНІКА ТА ПРИЛАДОБУДУВАННЯ

УДК 623.746

Ткачук Д.Ю., асистентка кафедри РЕ та А ім. проф. Б.Б. Самотокіна,
Кравчук А.Р., доктор філософії, доцент кафедри РЕ та А ім. проф. Б.Б. Самотокіна,
Ткачук А.Г., к.т.н., доцент кафедри РЕ та А ім. проф. Б.Б. Самотокіна
Державний університет «Житомирська політехніка»

ВПЛИВ ОСВІТЛЕННЯ НА ЕФЕКТИВНІСТЬ ТА ТОЧНІСТЬ РОБОТИ ТЕХНІЧНОГО ЗОРУ

Системи машинного зору набувають все більшого значення в таких сферах, як автоматизація виробництва, контроль якості, робототехніка та медицина. Якість отриманих зображень безпосередньо впливає на ефективність алгоритмів комп'ютерного зору, при цьому освітлення відіграє ключову роль у формуванні високоякісних зображень [1,2]. Незважаючи на значний прогрес у розробці алгоритмів машинного зору, питання впливу різних типів освітлення на їх ефективність залишається недостатньо вивченим. Метою цієї роботи є кількісна оцінка впливу різних типів освітлення на точність розпізнавання об'єктів за допомогою систем машинного зору.

Вплив різних типів освітлення на точність розпізнавання об'єктів у системах машинного зору було оцінено через аналіз трьох основних типів освітлення: білого (дифузного та спрямованого), кольорового (монохроматичного освітлення різних довжин хвиль) та структурованого світла (проєкційні патерни).

Експериментальна установка включала камеру високої роздільної здатності (1920×1080 пікселів), змінні джерела освітлення (LED-панелі з регульованою інтенсивністю та спектром), набір тестових об'єктів різної форми, розміру, кольору та текстури, а також обчислювальну систему з алгоритмами машинного зору, заснованими на глибокому навчанні. Для кожного типу освітлення варіювалися такі параметри, як інтенсивність (від 100 до 1000 люкс), кут падіння світла (0°, 30°, 45°, 60°, 90°) та відстань між джерелом світла та об'єктом (0.5 м, 1 м, 2 м). Кожна конфігурація була протестована 100 повтореннями для забезпечення статистичної достовірності результатів.

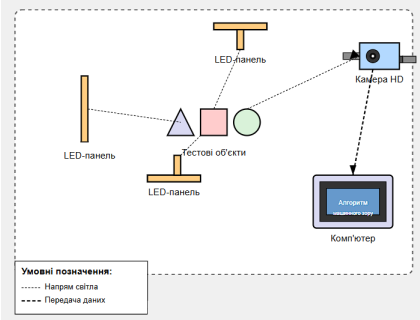


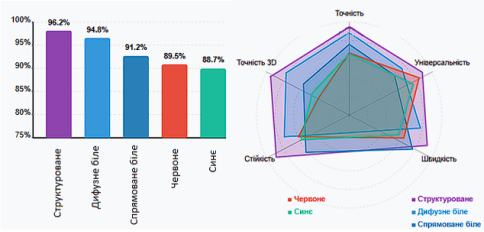
Рис. 1. Компоненти установки

Для кількісної оцінки ефективності використовувалися метрики, такі як точність розпізнавання (precision), повнота розпізнавання (recall), F1-міра [3], середньоквадратична похибка вимірювання розмірів об’єктів та час обробки зображення.

Таблиця 1

Порівняння ефективності різних типів освітлення

Тип освітлення	Точність розпізнавання	Стійкість до зовнішнього освітлення	Час обробки (мс)	Оптимальні сценарії використання
Дифузне біле	94.8%	Середня	42	Загальне розпізнавання об’єктів
Спрямоване біле	91.2%	Низька	45	Інспекція поверхонь і текстур
Червоне	89.5%	Висока	38	Розпізнавання контрастних об’єктів
Синє	88.7%	Висока	39	Біомедичні застосування
Структуроване	96.2%	Дуже висока	76	3D-реконструкція та вимірювання



а) б)

Рис. 2. Порівняльні діаграми впливу освітлення на машинний зір а) Стовпчаста діаграма точності розпізнавання; б) Радіальна діаграма характеристик.

Результати показали, що дифузне біле світло забезпечило найвищу точність розпізнавання (94.8%) при інтенсивності 500-700 люкс і куті падіння 45°, але на блискучих поверхнях ефективність знижувалась через відблиски. Спрямоване біле світло було ефективним для виявлення дефектів на текстурованих поверхнях, досягаючи точності 96.3% при куті 30°. Монохроматичне червоне світло (630-650 нм) дало найкращі результати при розпізнаванні синіх та зелених об'єктів (97.2%), а синє світло (450-470 нм) — для жовтих і червоних (96.5%). Однак воно знижувало точність до 78.3% для об'єктів подібного кольору. Структуроване світло у вигляді проєкційних патернів показало найкращі результати для тривимірної реконструкції та вимірювання розмірів об'єктів з похибкою менше 0.1 мм і високою стійкістю до змін зовнішнього освітлення.

Список використаних джерел:

1. Важливість освітлення для машинного зору URL: https://photonmission.com/blog/the-importance-of-lighting-in-machine-vision (дата звернення: 5.03.2025).

2. Важливість освітлення в машинному зорі URL: https://www.advancedillumination.com/a-practical-guide-to-machine-vision-lighting/ (дата звернення: 7.03.2025).

3. F1-міра URL: https://thetransmitted.com/adlucem/pokaznyk-f1-u-mashynnomu-navchanni/ (дата звернення: 8.03.2025).

4. Класифікація: точність, повнота, влучність і пов'язані показники URL: https://developers.google.com/machine-learning/crash-course/classification/accuracy-precision-recall?hl=uk (дата звернення: 10.03.2025).

УДК 004.7

Кравчук А.Р., доктор філософії, доцент
кафедри РЕ та А ім. проф. Б.Б. Самотокіна
Ткачук А.Г., к.т.н., декан ФКІТМР
Ткачук Д.Ю., асистент
кафедри РЕ та А ім. проф. Б.Б. Самотокіна
Державний університет «Житомирська політехніка»

ЗАСТОСУВАННЯ SBC В АВТОМАТИЗОВАНИХ СИСТЕМАХ IoT

Інтернет речей (IoT) є однією з ключових технологій сучасності, що сприяє інтеграції інтелектуальних пристроїв у різні сфери життєдіяльності, забезпечуючи автоматизацію процесів та ефективне керування ресурсами. Застосування автоматизованих IoT-систем потребує використання надійних, продуктивних і водночас енергоефективних обчислювальних платформ, здатних обробляти великі обсяги даних та взаємодіяти з хмарними сервісами. У цьому контексті одноплатні комп'ютери (Single Board Computers, SBC) відіграють важливу роль, оскільки поєднують високу обчислювальну потужність, компактність і підтримку різноманітних інтерфейсів та периферійних пристроїв.

У цій роботі здійснено аналіз технічних можливостей SBC у автоматизованих систем Інтернету речей (IoT). Виконано порівняльний аналіз продуктивності та енергоефективності найпоширеніших SBC-платформ.

Одноплатні комп'ютери являють собою компактні обчислювальні платформи, що містять на одній друкованій платі центральний процесор, оперативну пам'ять, інтерфейси введення-виведення та комунікаційні модулі [1]. Вони значно перевершують традиційні мікроконтролери за продуктивністю, підтримують повноцінні операційні системи (Linux, Android, Windows IoT тощо) та дозволяють реалізовувати складні алгоритми обробки даних, включаючи машинне навчання та аналіз потокової інформації в реальному часі. Завдяки цьому SBC стають незамінними для широкого спектра IoT-застосувань – від розумних будинків і промислової автоматизації до медичних діагностичних систем та сільськогосподарських моніторингових комплексів [2].

Дослідження SBC у контексті IoT передбачає оцінку їхніх технічних характеристик та функціональних можливостей для різних сфер застосування. Основними критеріями вибору є продуктивність (частота процесора, кількість ядер, обсяг оперативної пам'яті), енергоефективність (споживана потужність, можливість автономної

роботи від батарей), мережеві можливості (Wi-Fi, Bluetooth, Ethernet, LoRa, NB-IoT), а також підтримка відповідного програмного забезпечення та екосистеми розробки.

Методика порівняльного аналізі найпоширеніших SBC в автоматизованих системах IoT полягає у визначенні продуктивності та енергоефективності плат. Продуктивність визначається у синтетичному тесті, який визначає кількість виконаних операцій за секунду, в даному випадку використано тест Dhrystone (Dhrystone MIPS – Million Instructions per Second).

На основі отриманих результатів щодо продуктивності та енергоефективності, виконано аналіз який показав наступні результати. З точки зору енергоефективності найкращі результати показали плати Raspberry Pi Zero 2 W та Rock Pi S. Енергоспоживання даних плат на рівні 0.8-1.0 Вт. Середні показники продуктивності вищевказаних моделей 2000 – 3000 DMIPS, що є достатнім для виконання різних поширених завдань в IoT. Найвищу продуктивність демонструє плата Jetson Nano, яка має покази продуктивності на рівні 50000 DMIPS, проте має доволі високе енергоспоживання, приблизно 10 Вт. Така плата має наближені до сучасного ПК можливості та дозволяє використовувати штучний інтелект та системи технічного зору. З точки зору оптимального енергоспоживання та продуктивності добре показує себе плата Raspberry Pi 4 Model B, яка має середнє споживання 5 Вт та продуктивність на рівні 13000 DMIPS.

Отримані результати демонструють, що сучасні SBC забезпечують баланс між продуктивністю, енергоефективністю та функціональністю. Наявність інструкцій та інтерфейсів, які присутні в ПК робить їх ефективним рішенням для систем IoT. Подальші дослідження можуть бути зосереджені на оптимізації алгоритмів енергозбереження, інтеграції SBC із сучасними технологіями штучного інтелекту, а також розширенні їхніх комунікаційних можливостей за рахунок впровадження нових бездротових стандартів, зокрема 5G та LPWAN.

Список використаних джерел:

1. TensorFlow SSD MobileNet v1 [Електронний ресурс]. – https://kamleshs.medium.com/object-detection-using-ssd-mobilenet-with-tensorflow-1ee6e45a378b

2. Nanonets [Електронний ресурс]. – https://deepgram.com/ai-apps/nanonets

УДК 621.121

Горжий І. В., аспірант,
Писарець А. В., к.т.н., доцент,
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського

АВТОМАТИЗАЦІЯ ФУНКЦІОНУВАННЯ ГАЗОРОЗПОДІЛЬНИХ СТАНЦІЙ

Газова промисловість є стратегічно важливою галуззю, що забезпечує стабільне функціонування критично важливих об'єктів та енергетичну безпеку держави. Найважливішим етапом газопостачання є процес транспортування та розподілу газу. Для його переміщення країною використовуються основні магістральні трубопроводи, а для подальшого розподілу функціонують спеціальні об'єкти – газорозподільні станції (ГРС).

Газорозподільні станції включають в себе велику кількість елементів та вузлів, основними функціями яких є: очищення, підігрів та одоризація газу, запобігання утворенню гідратів, зниження тиску в трубопроводі, комерційний облік, визначення компонентного складу газу тощо [1]. Кожен з вузлів ГРС оснащений низкою вимірювальних приладів, перемикачів, сенсорів та інших механізмів, які зазвичай керуються вручну.

Необхідно регулярно перевіряти справність обладнання, дотримання необхідних параметрів експлуатації, проводити повірку вимірювальних приладів, а також калібрування у разі відхилення від певної норми. Усі ці заходи потребують значного ресурсу обслуговуючого персоналу ГРС, оскільки це надзвичайно відповідальна на важлива робота.

Процеси та функції цієї складної системи можна частково або повністю автоматизувати за допомогою систем автоматичного керування (САК). Система автоматичного керування – сукупність пристроїв та елементів зв'язку, за допомогою яких здійснюється певна взаємодія людини з допоміжними виконавчими механізмами будь-якого обладнання відповідно до програми керування, розробленої на підґрунті прийнятого технологічного процесу.

При цьому ручне керування є більш універсальним, проте обмежує можливість підвищення продуктивності. При використанні САК контроль та керування обладнанням відбувається на основі попередньо обробленої програми, що представляє собою набір послідовних команд, які забезпечують певне функціонування робочих елементів обладнання.

Застосування САК передбачає постійний автоматичний моніторинг основних параметрів станції, виключає потреби у постійному контролі

та присутності обслуговуючого персоналу, за винятком планової перевірки або технічного обслуговування обладнання.

Зокрема, застосування САК сприяє контролю виникнення та запобіганню аварійних ситуацій та позаштатної роботи станції, а також дистанційному контролю функціонування усіх складових ГРС.

Типова САК ГРС містить: джерела живлення; реле керування, призначене для контролю сигналізації та діями в аварійній ситуації; плати для контролю запірної арматури; аналогові плати, призначені для перетворення сигналів з перетворювачів та вимірювальних приладів; вхідні та вихідні дискретні плати; контролер, який організовує роботу всіх модулів.

САК ГРС реалізує широкий спектр завдань, виконання яких у ручному режимі вимагає залучення великої кількості фахівців, а саме: збір та обробка даних з первинних перетворювачів та вимірювальних приладів; спостереження та контроль стану кожного з вузлів станції; формування інформації про стан робочого процесу в режимі реального часу; автоматичні керування обладнанням, вентиляція та регулювання температури в приміщеннях з обладнанням, автоматична аварійна зупинка ГРС, захист від несанкціонованого втручання в експлуатацію станції та некоректних дій працівників станції [2] тощо.

Застосування систем автоматичного керування активно впроваджується в газовій промисловості України, що дозволяє підвищити точність контролю споживання газу, полегшити керування технологічним процесом ГРС та зробити його більш безпечним

Список використаних джерел:

1. Федоришин Р. М. Моделювання системи підігріву природного газу на автоматизованих газорозподільних станціях. *Вісник Національного університету "Львівська політехніка". Теплоенергетика. Інженерія довкілля. Автоматизація*. 2007. № 581. С. 22–34.

2. Ободянська О. І., Блеянюк А. О. Автоматизація та диспетчеризація газорозподільних систем. Матеріали LIII наук.-техн. конф. підрозділів ВНТУ, 20-22 березня 2024 р. Вінниця. 2024. Електрон. текст. дані. URI: https://conferences.vntu.edu.ua/index.php/all-fbtegp/all-fbtegp-2024/paper/view/20591.

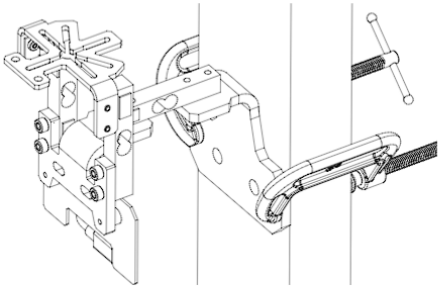
УДК 62-8

Кочук С.Б., к. т. н, доцент,
Шувалов Д.О., аспірант,
Дюділов Є.А., магістрант
Національний аерокосмічний університет ім. М.Є. Жуковського, «Харківський авіаційний інститут»

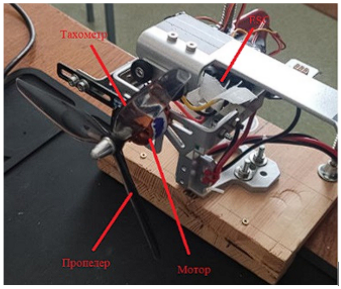
СТЕНД ДЛЯ ВИПРОБУВАННЯ BLDC-МОТОРІВ

Установка RCbenchmark (рис.1(а)) є універсальним малогабаритним стендом для перевірки не тільки моторів радіокерованих моделей та безпілотних літальних апаратів (БПЛА), але і ESC-регуляторів й акумуляторів [1]. Робота стенду підтримується спеціалізованим софтом фірми Tytorobotics RCbenchmark.com – GUI [2], що є у відкритому доступі та може бути встановлений на комп'ютер або ноутбук.

Сумісно з програмним забезпеченням стенд дозволяє виміряти та відобразити на моніторі комп'ютера багато параметрів як самого двигуна, так і гвинта, ESC-регулятора та акумулятора (рис.1(б)).



а) загальний вигляд установки



б) закріплений мотор з гвинтом

Рис. 1. Стенд

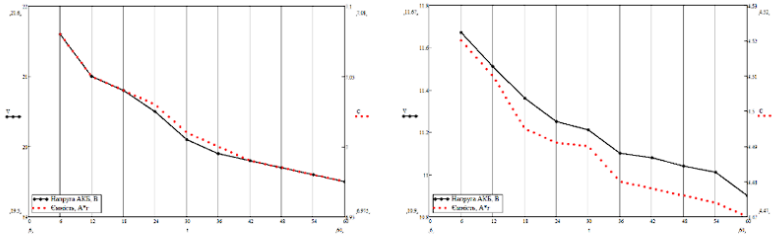
Дослідженню можуть підлягати: оберти мотора, тяга, крутний момент, електрорушійна сила (EPC), механічна та електрична потужності, рівень вібрацій та струми в обмотках BLDC, ємність, напруга та струм розрядження акумулятора. Установка використовується для отримання емпіричних даних випробування BLDC-моторів та пропелерів перед встановленням на БПЛА, особливо вперше створених або скомпонованих.

Стенд застосовувався для випробування мотору A2212/15T 930KV з дво- та трилопатевими гвинтами 7'' та ESC-регулятором на 60A (рис.1(б)), також оцінювалися втрати напруги та ємності двох акумуляторних батарей (АКБ) 6S Li-Ion і 3S Li-Po протягом певного часу роботи мотору.

Тестування мотору показало досягнення максимальних обертів 13700 та 9520 об/хв для АКБ 6S Li-Ion і 3S Li-Po відповідно, які мали початкові напруги 21,6 В і 11,6 В. Це свідчить про суттєве невиконання показника EPC мотору з АКБ 6S Li-Ion, оберти повинні досягати 18000.

Дослідження акумуляторів проводилося терміном 60 хв на середніх обертах мотору при вхідному ШІМ-сигналі 1500 мс.

При початковій напрузі 21,6 В Li-Ion 6S АКБ показав падіння на 2,04 В або 9, 4% (рис.2(а)), Li-Po 3S – падіння у 0,77 В або 6,6% (рис.2(б)).



а) Li-Ion 6S б) Li-Po 3S

Рис. 2. АКБ

Трилопатевий гвинт забезпечує на 30% більшу тягу по зрівнянню з дволопатевим, але спричиняє на 8,19% вищий рівень вібрацій.

Акумулятори з високою напругою та більшою ємністю дозволяють зменшити втрати енергії на 15%, що критично для тривалої та стабільної роботи електродвигунів БПЛА.

Список використаних джерел:

1. Thrust Stands for Brushless Motors and Propellers [Електронний ресурс]. – Режим доступу: https://www.tytorobotics.com/.

2. RCbenchmark Software. RCbenchmark.com – GUI [Електронний ресурс]. – Режим доступу: http:// www.tytorobotics.com /.

УДК 644.1+681.5

Здоренко С.С., аспірант,
Черепанська І.Ю., д.т.н., професор
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»

СИСТЕМА ЕНЕРГОЕФЕКТИВНОГО КЕРУВАННЯ ТЕМПЕРАТУРОЮ ПОВІТРЯ В БУДІВЛЯХ З АВТОНОМНИМ ОПАЛЕННЯМ

Зростання світових цін на енергетичні ресурси стимулює пошук ефективних технічних рішень щодо забезпечення енергоефективного керування температурою повітря у будівлях з автономним опаленням. Одними із перспективних напрямків вирішення даної проблеми є застосування прогнозних моделей (Model Predictive Control - MPC) [1], технологій штучного інтелекту та побудова на їх основі систем автоматичного керування.

Ключовою особливістю при енергоефективному керуванні температурою повітря в будівлях з автономним опаленням на основі MPC-алгоритму є визначення математичної моделі об'єкта керування (ОК), яка є основою роботи алгоритму керування. Структурна схема запропонованої системи енергоефективного керування температурою повітря у будівлях з автономним опаленням на основі MPC-регулятора зображена на рис. 1.

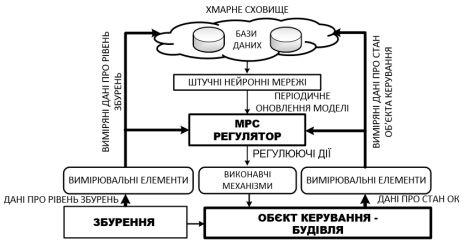


Рис. 1. Структурна схема запропонованої системи енергоефективного керування температурою повітря у будівлях з автономним опаленням на основі MPC-регулятора

Запропонована система енергоефективного керування температурою повітря передбачає застосування підходу, який дозволяє здійснювати коригування параметрів математичної моделі в режимі реального часу з урахуванням так званих історичних даних про стан ОК, а також збурюючих впливів, що мають стохастичний характер. Для визначення моделі ОК даний підхід передбачає застосування white-box методу, який описаний у роботі [2] та data-driven методу, який

наведений у роботі [3]. White-box метод використовується на підготовчих етапах для розрахунків параметрів моделі ОК у відповідності до характеристик конкретної будівлі (теплоізолюючі та теплоакумулюючі властивості стін та підлоги, її інерційність). Data-driven метод застосовується для збору в реальному часі так званих історичних даних про ОК за допомогою технології IoT. Зокрема, збираються поточні значення збурюючих факторів, що діють на ОК, значення температури повітря, яка підлягає регулюванню, а також значення інших параметрів стану ОК, наприклад, температури стін, підлоги тощо. Ці дані використовуються для визначення поточних параметрів математичної моделі ОК і їх порівняння із попередніми, так званими історичними значеннями, за допомогою штучної нейронної мережі. У разі необхідності в режимі реального часу здійснюється коригування параметрів математичної моделі за множиною відповідних логічних правил, що зберігаються у відповідній базі знань (БЗ) у хмарному середовищі. В іншому випадку параметри математичної моделі залишаються без змін. Процес коригування параметрів математичної моделі ОК здійснюється безперервно із заданими інтервалами часу.

Таким чином, застосування запропонованої системи керування дозволяє здійснювати енергоефективне керування температурою повітря в будівлях з автономним опаленням шляхом коригування параметрів попередньо визначеної математичної моделі ОК на основі накопичених історичних даних. Це забезпечує своєчасну зміну температури приміщення, яка корелює із витратами енергетичних ресурсів. У результаті досягається економія енергетичних ресурсів та підтримка необхідного рівня температури у будівлях для комфортного перебування людей.

Список використаних джерел:

1. Захарченко А., Степанець О. Особливості використання модельно-прогнозуючого керування в автоматизації будівель. *Вчені записки ТНУ імені В.І. Вернадського. Серія: технічні науки*. 2020. Т.31, Ч. 1. С. 70–77. URL:https://doi.org/10.32838/TNU-2663-5941/2020.6-1/12

2. Jorissen, F., Picard, D., Boydens, W., Helsen, L. White-box Model Predictive Control: Optimal Control and System Integration of Heat Pumps. *HPT Magazine*. 2022. Vol. 40, No 2. P. 28-31.

3. Joe, J., & Karava, P. A model predictive control strategy to optimize the performance of radiant floor heating and cooling systems in office buildings. *Applied Energy*. 2019. Vol. 245. P. 65-77. URL: https://doi.org/10.1016/j.apenergy.2019.03.209 (date of access: 09.03.2025).

УДК 629.3

Пулеко І. В., канд. тех. наук, доц.
Чумакевич В. О., канд. тех. наук, доц.
Оніщенко О. О., ст. викладач
Свистунович І. В., ст. викладач
Житомирський військовий інститут ім. С. П. Корольова, Державний університет «Житомирська політехніка», Національний університет «Львівська політехніка»

ПЕРСПЕКТИВИ ВИКОРИСТАННЯ ЕЛЕКТРОДВИГУНІВ В ЕЛЕКТРОПРИВОДАХ НАЗЕМНИХ РОБОТИЗОВАНИХ СИСТЕМ

Використання наземних роботизованих систем (НРС) в сучасному світі набуло нового значного розвитку. В XX сторіччі, через свою значну вартість, вони використовувались для заміни людей в монотонних операціях у складських приміщеннях та в місцях, де перебування людини було небезпечним для її життя і здоров'я. На території України такі НРС використовувались для ліквідації наслідків аварії на Чорнобильській АЕС. Ще на початку XXI сторіччі ця тенденція зберігалась і НРС використовували, наприклад, для дослідження геотехнічних умов в районі екологічного лиха в районі Солотвино Закарпатської області, де провалля ґрунту відбуваються через порушення правил видобування корисних копалин. Останніми роками широке застосування НРС розповсюдилось не лише на військову сферу, а й у сільське господарство, логістичні завдання, в ряді країн в тестовому режимі запустили безпілотні транспортні системи для перевезення пасажирів тощо.

Важливе місце в НРС займають силові приводи, які дозволяють пересуватись або керують маніпуляторами чи спеціальним обладнанням, наприклад, засобами спостереження та фіксації.

Для рушійних силових приводі використовуються двигуни внутрішнього згорання, різноманітні електричні двигуни, гідро- та пневмомашини, гібридні двигуни.

На даному етапі розвитку автомобільної техніки з гібридними силовими агрегатами є декілька різних напрямків. Кожна розробка по-своєму унікальна але вже зараз отримані основні типи та принципи побудови автомобілів з гібридним силовим агрегатом. У своїй основі, за прийнятою схемою побудови, вони поділяються на гібридні автомобілі:

– послідовним з'єднанням силового агрегату;

– паралельним з'єднанням силового агрегату;

– послідовно-паралельним з'єднанням силового агрегату;

– можливістю підзарядки АКБ від зовнішнього джерела електроенергії.

В наших дослідженнях розглянемо перспективи використання електричних приводів для НРС.

Застосування електроприводів для приведення в рух транспортних засобів не є новою ідеєю. Саме електромобіль першим подолав бар'єр швидкості у 100 км/год. Також широко використовується електротранспорт – метро, трамваї, тролейбуси, електровози, кар'єрні самоскиди БелАЗ, крокуючі екскаватори тощо. Для місячної програми в СРСР на місяцеходах також використовували електродвигуни. Але основна проблема полягає в забезпеченні живлення електродвигунів. Один з найпоширеніших варіантів сьогодні у світі – рух електротранспорту вздовж спеціально обладнаних шляхів – електровози, трамваї, тролейбуси, метро, крокуючі екскаватори. Другий підхід полягає у використанні потужного джерела енергії на борту транспортного засобу. Наприклад, потужного двигуна внутрішнього згорання для приведення в дію бортового генератора, бортові хімічні джерела напруги тощо. Доволі часто в якості джерела енергії для електроприводу рушія використовується постійний струм. Поруч із цим складність регулювання швидкості та моменту електродвигунів змінного струму до останнього часу також перешкоджала застосуванню таких двигунів.

Однак розвиток силової електроніки призвів, з одного боку, до підвищення статичних систем перетворення постійного струму в змінний, а з іншого – до значного спрощення процесів запуску та зміни швидкості обертання для двигунів змінного струму, особливо асинхронних. Слід відмітити, що двигуни змінного струму, особливо асинхронні, мають досить добрі масо-габаритні характеристики на одиницю потужності. Також значний прогрес досягнуто в збільшенні пускового та обертального моменту двигунів змінного струму. Тож обмеження в їх використанні на НРС перестають бути суттєвими.

Дослідження по використанню асинхронних двигунів на НРС планується проводити за наступними напрямками:

дослідження різних типів джерел електроживлення (використання бортових електростанцій, хімічних джерел струму тощо):

дослідження статичних систем перетворення постійного струму в змінний та об'єднання її із системою керування електродвигунами;

дослідження конструктивних особливостей електродвигунів, які дозволяють їх використовувати як приводи до рушійних систем тощо.

УДК 621.317

Ткачук А.Г., к.т.н, доцент
Безвесільна О.М., д.т.н., професор
Державний університет «Житомирська політехніка»
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»

МЕТОД ОПТИМІЗАЦІЇ ЕНЕРГОСПОЖИВАННЯ СТАБІЛІЗАТОРА ОЗБРОЄННЯ БМП-2

Основним озброєнням бойової машини піхоти БМП-2 є 30-мм автоматична гармата 2А42. Ця дрібнокаліберна швидкострільна гармата встановлена у башті і стабілізована у двох площинах, що дозволяє вести прицільний вогонь під час руху [1]. Ефективна дальність вогню гармати по наземних цілях становить до 1500–2000 м (броньовані цілі), а максимальна дальність по малозахищених цілях – до 4000 м. Основна гармата 2А42 і спарений кулемет стабілізовані у двох площинах, що дає змогу вести вогонь по цілях під час руху машини пересіченою місцевістю. Це значно підвищує влучність і реакцію вогню на ходу. БМП-2 оснащена прицільними приладами для стрільби вдень і вночі.

Електрогідравлічний стабілізатор БМП-2 забезпечує середню похибку стабілізації гармати на рівні 1 мрад на дистанції 1 км при швидкості руху машини до 25–35 км/год.

Стабілізатори озброєння споживають електроенергію від бортової мережі машини для роботи електричних та гідравлічних приводів. Енергоефективність таких систем залежить від конструкції, технологій, що використовуються, та стану технічного обслуговування.

Виявлено основні джерела втрат енергії, серед яких [2]:

– динамічні режими роботи приводу стабілізатора;

– перевитрати енергії під час компенсації вібрацій та швидких маневрів;

– неоптимальні режими роботи електродвигунів та елементів системи управління.

Запропоновано алгоритм, який регулює споживану потужність електродвигунів стабілізатора озброєння БМП-2 у залежності від поточних умов роботи. Алгоритм дозволяє знижувати енергоспоживання в моменти, коли система не потребує високої потужності (наприклад, під час повільного руху або відсутності зовнішніх збурень).

Адаптивне управління двигунами стабілізатора БМП-2 будується на основі теорії оптимального управління і враховує змінні умови

роботи, такі як швидкість, вібрації, зовнішні збурення та поточний стан енергоспоживання.

Система стабілізації описується рівнянням руху з врахуванням моментів і сил, що діють на стабілізатор озброєння:

$$J\ddot{\theta} + b\dot{\theta} + \zeta\theta = M_u + M_d,$$

де J - момент інерції системи; θ - кут повороту стабілізатора озброєння; $\ddot{\theta}, \dot{\theta}$ - прискорення і швидкість кутового руху відповідно; b - коефіцієнт в'язкого тертя у системі; ζ - коефіцієнт жорсткості; M_u - момент від двигуна стабілізатора (керуючий сигнал); M_d - момент від зовнішніх збурень.

Дане рівняння є базовим рівнянням динаміки обертального руху, що виводиться на основі другого закону Ньютона у кутовій формі. Його використання в системах стабілізації поширене у літературі з механіки, автоматичного керування та систем стабілізації.

Мета адаптивного управління — мінімізувати споживання енергії, забезпечуючи задану точність стабілізації. Функціонал оптимізації:

$$J = \int_0^T (q_1(\theta - \theta_{зад})^2 + q_2\dot{\theta}^2 + q_3 {M_u}^2)dt,$$

де $\theta_{зад}$ - заданий кут стабілізації; q_1, q_2, q_3 - вагові коефіцієнти, що визначають важливість точності, плавності руху і мінімізації енергоспоживання відповідно.

Такий функціонал часто використовується в задачах оптимального керування для мінімізації відхилення від заданого положення, швидкості змін та енергоспоживання системи. Адаптивний підхід передбачає налаштування коефіцієнтів q_1, q_2, q_3 залежно від умов роботи системи. Для мінімізації функціоналу J використовується закон управління у вигляді ПІД регулятора з адаптивними коефіцієнтами.

Список використаних джерел:

1. Бойова машина піхоти БМП-2. Загальна будова: навчальний посібник / В.В. Близнюк, В.Б. Добровольський, Д.В. Зайцев – К.: ВД «СКІФ». 2022. – 212 с.

2. Дії механізованого відділення при озброєнні бойової машини піхоти БМП-2: навчальний посібник / Д.В. Зайцев, В.Б. Добровольський, О.С. Дем'янюк, А.П. Наконечний – К.: ВД «СКІФ». 2022. – 120 с.

УДК 621.9

Богдановський М.В., ст. викладач,
Горбік Д.П., здобувач
Державний університет «Житомирська політехніка»

ВИКОРИСТАННЯ CAD/CAM СИСТЕМ ДЛЯ РОБОТИЗОВАНОЇ ОБРОБКИ ДЕТАЛЕЙ ІЗ СКЛАДНОЮ ПОВЕРХНЕЮ

В сучасному, гнучкому виробництві підвищення ефективності, скорочення термінів запуску та переналагодження обладнання знаходяться в переліку основних завдань. При обробці складних поверхонь деталей активно використовуються передові технології автоматизованого проектування та виготовлення CAD/CAM для верстатів з числовим програмним керуванням (ЧПК) та промислових роботів (ПР). В лабораторних умовах використання ПР та CAD/CAM систем дозволяють реалізувати швидке протипіювання фізичних зразків та створюють альтернативу у матеріалах виготовлення популярним технологіям тривимірного друку.

На сьогодні існує велика кількість програмних комплексів, що реалізують продуктивну технологію CAD/CAM. Наприклад, Autodesk Inventor, Autodesk Fusion 360, Creo Parametric, CATIA, T-FLEX CAD, SolidWorks та багато інших. За навчальних умов використання вищими навчальними закладами для реалізації налаштування тривимірної обробки поверхні було обрано Autodesk Fusion 360. ПР на якому виконувались налаштування та випробовування CAD/CAM: KUKA KR 6 R900-2 / KR C-4.

Модель поверхні для подальшої трансляції в CAM систему може бути створена штатними інструментами Autodesk Fusion 360 чи імпортована. В нашому випадку була імпортована двовимірна векторна модель зображення із подальшим, вибірковим екструдуванням окремих ділянок. Далі була створена технологія обробки, що включає 4 стадії обробки: вирівнювання поверхні, адаптивна обробка фрезеруванням крупних, торцевих елементів поверхні кінцевою фрезою 8 мм, адаптивна та контурна обробка фрезеруванням дрібних торцевих елементів кінцевою фрезою 2 мм.

Для можливості транслювання створених даних CAM системи в управляючу систему ПР обов'язковими є задача системи номеру налаштованої прив'язки «робот-поверхня обробки» у глобальній системі координат WNC offset. Формування коду керуючої програми ПР реалізується за допомогою пост-процесора KUKA у складі Fusion360. Для уникання проблем сингулярності, у налаштуваннях зазначаються параметри вихідної конфігурації ПР із дотримуванням

порад щодо прив'язки системи координат робочої поверхні та зони сервісу в межах одного квадранта базової системи координат ПР.

Вигляд деталі із трасировкою руху інструменту 4 стадії обробки та параметри налаштування пост-процесора представлено на рис.1.

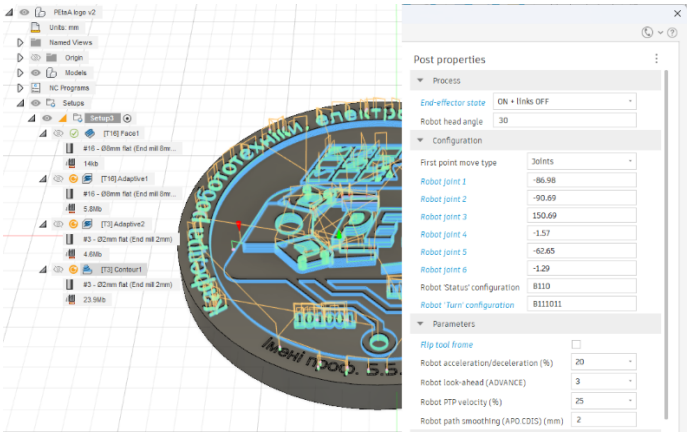


Рис.1. Екранні форми програмного комплексу Autodesk Fusion 360 трасировка руху інструменту на 4 стадії обробки та налаштування пост-процесора KUKA

З боку системи управління KR C-4 необхідно виконати прив'язку системи координат ПР до робочої поверхні обробки. Для цього спочатку потрібно провести калібрування інструменту (доступно до 16 позицій налаштувань) через головне меню системи управління ПР: Calibrate/Tool/XYZ 4 points (опція калібрування за чотирма підходами до точки обробки з довільних сторін). Після калібрування інструменту стає доступним калібрування системи координат (доступно до 32 позиції налаштувань) робочої поверхні: Calibrate/Tool/Indirect (опція калібрування за двома послідовними рухами у площині). Створена позиція налаштування має бути занесена в параметр WNC offset програмного комплексу Autodesk Fusion 360.

Список використаних джерел:

1. KUKA System Software 8.3. Operating and Programming Instructions for System Integrators. / KUKA Roboter GmbH Zugspitzstraße 140 D-86165 Augsburg, Germany, 2013.

УДК 681.5.01

Санін В.В., магістрант,
Литвяк О.М., д.т.н., доцент
Національний аерокосмічний університет М. Є. Жуковського «Харківський авіаційний інститут»

ДОСЛІДЖЕННЯ РОЗГІННИХ ХАРАКТЕРИСТИК ТЕПЛООБМІННОГО АПАРАТУ

Теплообмінні апарати займають важливе місце в хімічному виробництві та теплотехніці, що пов'язано з необхідністю забезпечення ефективного теплообміну при різноманітних умовах роботи. Постійне вдосконалення конструкцій і технологій таких апаратів спричиняє зростання вимог до математичного моделювання їх динамічних процесів. Вивчення динаміки теплообмінних апаратів висвітлене у науковій та навчальній літературі, проте існуючі математичні моделі часто не дають повної інформації для проектування сучасних систем автоматизованого керування (АСУ). У дослідженнях [3] і [4] були запропоновані нелінійні моделі для опису процесів теплообміну, проте в цих роботах не розглянуто вплив навантаження та транспортних затримок, що є важливими для забезпечення стабільної роботи АСУ.

Метою даної роботи є розробка лінійної зосередженої математичної моделі динамічних процесів теплообмінного апарату, яка дозволить підвищити якість регулювання температури продукту в технологічному процесі та забезпечити задані параметри якості автоматизованих систем управління під час зміни навантаження та зовнішніх впливів.

Теплообмінні апарати призначені для підігріву або охолодження продукту шляхом передачі тепла між теплоносієм та продуктом. Конструктивна схема теплообмінного апарату включає два основні потоки: продукт з температурою ТП1 та теплоносій з температурою ТТ1, які протікають через теплообмінні трубки, розділені перегородками. Це забезпечує ефективний теплообмін, оскільки тепло передається через стінки трубок з високим коефіцієнтом теплопровідності. У даній роботі було використано модель зосереджених параметрів, яка описується звичайними диференціальними рівняннями, що дозволяє спростити аналіз процесів, зокрема врахувати зміни температури теплоносія та продукту у часі. Модель передбачає, що температура теплоносія та продукту однакова в кожній точці відповідної порожнини апарату, що відповідає ідеальному перемішуванню. Крім того, передбачається відсутність теплових втрат у навколишнє середовище і незначність теплоємності матеріалу стінок.

Розглянуто два основних об'єми теплообмінного апарату: порожнина продукту, що підігрівається, і порожнина теплоносія. Час транспортного запізнення в кожній порожнині визначається часом перебування елементарної частки в об'ємі апарату, що відповідає

ідеальному витісненню. Для аналізу кількості теплоти, яку отримує продукт, було використано рівняння енергетичного балансу, яке враховує зміну температури продукту за час dt. Перехідні процеси теплообміну були моделювані за допомогою структурно-динамічної схеми апарату в середовищі VisSim, що дозволяє візуалізувати та аналізувати динамічні характеристики.

Розроблена модель дозволяє прогнозувати зміну температури продукту та теплоносія при різних режимах роботи теплообмінного апарату, зокрема при ступінчастій зміні витрати теплоносія. Зміни температури продукту та теплоносія внаслідок цієї зміни витрати демонструють типову розгінну характеристику для теплообмінних апаратів, що відповідає фізичним уявленням і попереднім дослідженням [2]. Врахування транспортного запізнення в моделях дозволяє отримати точнішу картину динаміки процесу теплообміну, що важливо для налаштування систем автоматизованого керування.

Структурно-динамічна схема теплообмінного апарату в середовищі VisSim продемонструвала свою ефективність для моделювання та синтезу систем управління, що здатні підтримувати оптимальні температурні режими в процесі теплообміну при змінах навантаження. Результати моделювання відповідають фізичним уявленням про процеси теплообміну, зокрема щодо впливу витрат теплоносія на температуру продукту на виході.

Список використаних джерел:

1. Касаткіна А. Г. Основні процеси та апарати хімічної технології: посібник з проектування / А. Г. Касаткіна. – М.: Хімія, 1973.
2. Ліпатов Л.М. Типові процеси хімічної технології, як об'єкти управління / Л.М. Ліпатів. – М.: Хімія, 1973.
3. Чернишов Н.М. Математичний опис процесу теплообміну у протиточних теплообмінних апаратах / Н.М. Чернишов, В.В. Турупалов, А.А. Прядко. – Донецьк: ДонНТУ, 2011.
4. Гаврилів В. І., Король О. С., Зімоха І. О. Математичні моделі теплообміну в елементах турбогенераторів // Український журнал інформаційних технологій, 2022.
5. Муравйова Є.А. Розробка системи адаптивного нечіткого керування пластинчастими теплообмінниками // Вісник ПНДПУ. 2020. № 4.
6. Офіційний сайт компанії Visual Solution Inc. – Режим доступу: http://www.vissim.com

УДК 621.9

Василевський Д.В., здобувач,
Біленький І.О., здобувач
Державний університет «Житомирська політехніка»

ВИКОРИСТАННЯ АДИТИВНИХ ТЕХНОЛОГІЙ 3D ДРУКУ ПРИ ВИГОТОВЛЕННІ УНІВЕРСАЛЬНИХ ЗАХВАТІВ ДЛЯ КОЛАБОРАТИВНИХ РОБОТІВ

Сучасні тенденції у виробництві вимагають гнучких та ефективних рішень, зокрема у створенні універсальних захватів для колаборативних роботів (КР). Однією з передових технологій, що забезпечує швидке виготовлення та адаптацію захватів під різні завдання, є адитивне виробництво, зокрема 3D друк.

Використання 3D друку дозволяє суттєво зменшити терміни виготовлення, здешевити процес виготовлення прототипу та виробництво захвату. Однією з ключових переваг є можливість швидкої модифікації конструкції захвату, враховуючи особливості об’єкту, над яким здійснюють маніпуляцію, та специфіку виробництва.

Для реалізації процесу виготовлення захвату можна використати програмне забезпечення Solidworks, це дозволить створити детальну 3D модель захвату з урахуванням ергономічності, міцності та функціональності.

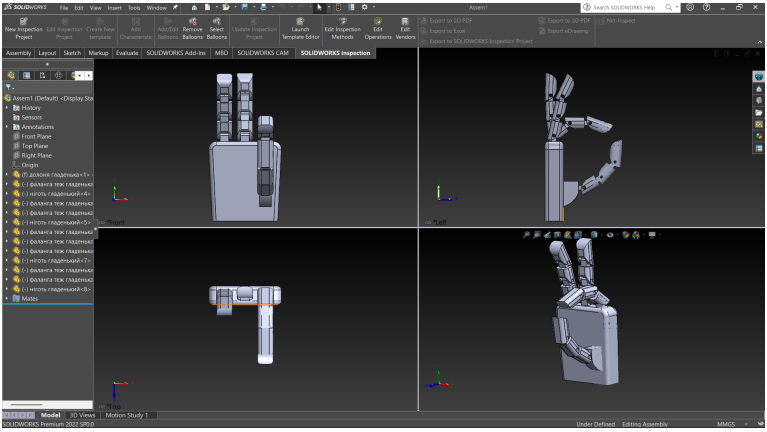


Рис.1. Екранні форми програмного забезпечення Solidworks при моделюванні прототипу захвату

В процесі проектування вищезгаданої моделі авторами розглядалась конструкція та конфігурація пальців із урахуванням типових елементів інфраструктури, з якими відбувається взаємодія та зменшення кількості

сервоприводів. Це в свою чергу дозволило спростити конструкцію, зменшити кількість сигналів та спростити закони управління.

Важливим аспектом при виготовленні захвату є вибір матеріалів. Для виготовлення прототипу та тестування окремих модулів захвату, можна обрати пластик PLA, найбільш популярний та легкий у друці філамент, який можна використати для перевірки захвату на збірність та зовнішній вигляд. Пластик PETG підійде для виготовлення самого захвату, так як він відрізняється своєю високою механічною міцністю, стійкістю до рідин, а також до високих температур. Таким чином, використання адитивних технологій у процесі створення захватних пристроїв для колаборативних роботів відкриває широкі можливості не лише щодо гнучкого проєктування конструкцій різної складності, а й у виборі матеріалів, що відповідають фізичним вимогам. Це, у свою чергу, сприяє підвищенню ефективності виробничих процесів та розширенню функціональних можливостей роботизованих систем.

Процес виготовлення захвату складається з наступних етапів:

1. Проєктування 3D моделі із врахуванням особливостей конструкції КР та параметрів об'єкта захоплення.
2. Підбір електронної апаратної бази відповідно до вимог.
3. Підготовка до друку: налаштування параметрів друку, типу матеріалу (PLA, PETG, TPU, ABS).
4. 3D друк елементів захвату.
5. Пост-обробка: видалення підтримок, шліфування, тестування на міцність та функціональність.
6. Збірка та програмування захватного пристрою.
7. Випробування захвату у виробничих умовах з колаборативним роботом.

Для забезпечення сумісності захвату з КР важливим етапом є калібрування системи координат та налаштування параметрів керування у системі управління ПР. Особливу увагу варто приділити ергономіці захвату, оскільки він має відповідати вимогам безпеки та ефективності роботи в колаборативному середовищі.

Список використаних джерел:

1. Gibson, I., Rosen, D., Stucker, B. Additive Manufacturing Technologies. 3D Printing, Rapid Prototyping, and Direct Digital Manufacturing. Springer, 2021.

УДК 004.383

Лукашенко В.А., к.т.н.
Гардер Д.А., к.т.н.
Лукашенко А.Г., д.т.н.,
Лукашенко В.М., д.т.н., професор,
Лукашенко Г.А., здобувач вищої освіти
Інститут електрозварювання ім. Є.О. Патона НАН України,
Черкаський державний технологічний університет

ПОРІВНЯЛЬНИЙ АНАЛІЗ БАГАТОПАРАМЕТРИЧНИХ КОМПОНЕНТІВ ПРОБЛЕМНО-ОРІЄНТОВАНИХ СИСТЕМ ЧЕРЕЗ ВІЗУАЛІЗАЦІЮ УЗАГАЛЬНЕНОГО КРИТЕРІЮ ВИДАЧІ РЕЛЕВАНТНОЇ ІНФОРМАЦІЇ

Відомо, що підвищення ефективності компонентів приводить до адекватного підвищення якості функціонуючих в реальному часі проблемно-орієнтованих систем [1]. Важливим завданням аналізу є визначення найкращого компоненту з множини існуючих, враховуючи цілий спектр техніко-економічних показників (ТЕП).

Основна проблемна задача полягає в тому, що між параметрами повністю відсутній математичний опис закономірності. Потужним засобом у цих умовах є моделювання умовне [2], на базі якого створюються умовні критерії видачі релевантної інформації (УКВРІ), що використовуються для кількісного об'єктивного оцінювання за багатьма параметрами одночасно. УКВРІ - це безрозмірні величини, які створюються на основі властивостей евристики, теорії розмірності, методу нульових степеневих комплексів, математичної логіки та формалізації.

Враховуючи пораду Ньютона, що при науковому досліджені – приклади іноді корисніше правил, тому в роботі пропонується показати вирішення поставленої задачі на прикладу дослідження сучасних лазерних випромінювачів. На основі евристики запропоновано таки лазери: №1 – волоконні; №2 – діодні; **№**3 –YAG-Nd з діодним накачуванням; №4 – YAG-Nd з ламповим накачуванням. Визначено (табл.1) їх основні параметри: P – вихідна потужність, кВт; η – ККД, %; D – дальність доставки випромінювання волокном, м; причому в умовних одиницях пропонуються таки параметри: M – займана площа, B – вартість обслуговування. На їх основі створюється узагальнена інформаційна модель (УІМ) такого вигляду

$$\varphi\left(\mathrm{P}_{max}, \mathrm{P}_{min,}\mathrm{B}_{max}, \mathrm{B}_{min}, \eta_{max}, \eta_{min}, \mathrm{M},\ \mathrm{D}_{max}, \mathrm{D}_{min}\right) \qquad (1)$$

Через відсутність взаємозв'язку між параметрами УІМ (1), формуються математично структуровані моделі наступних критеріїв:

$$K_D = \frac{D_{max}-D_{min}}{D_{max}} \to max;\ Км \to min,\ K_{\text{р}} = \frac{P_{max}-P_{min}}{P_{max}} \to max;$$
$$K_{\text{В}} = \frac{\text{В}_{max}-\text{В}_{min}}{\text{В}_{max}} \to min;\ K_\eta = \frac{\eta_{max}-\eta_{min}}{\eta_{max}} \to max. \quad (2)$$

Оскільки відповідні УКВРІ є безрозмірні величини, фізичне тлумачення цих критеріїв, що характеризує: $\boldsymbol{K}_{\text{р}}$ – вихідну потужність; $\boldsymbol{K}_{\eta}$ – ККД; $\boldsymbol{K_D}$ – дальність доставки випромінювання волокном; $\boldsymbol{K_M}$ – займану площу; $\boldsymbol{K_B}$ – вартість обслуговування; $\boldsymbol{K}_{\text{Н}}$ – ненадійність лазерних випромінювачів. Рівняння для кількісного оцінювання запропонованих лазерних випромінювачів через синтез УКВРІ, яке має такий вигляд:

$$\text{К}_\Sigma = \sum_{i=1}^{k} \text{К}_{imax} + \sum_{j=1}^{m} \frac{1}{\text{К}_{min.}} \text{[2]} \quad (3)$$

Візуалізація узагальненого УКВРІ, що об'єктивно оцінює представлена на рис.1.

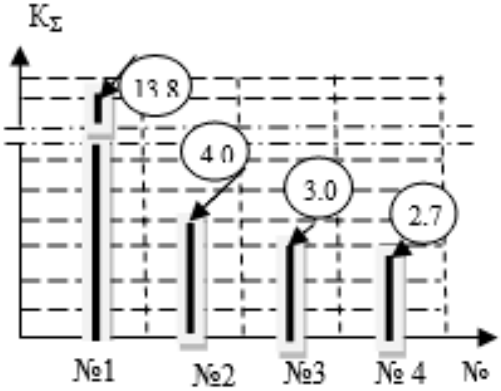


Рис. 1. Гістограма узагальнених **У**КВРІ лазерних випромінювачів

Таблиця 1

Реляційна модель основних параметрів лазерних випромінювачів

№ П	№1	№2	№3	№ 4
D	10..300	10...50	20...40	20...40
M	1,0	8	18	22
P	1...30	1..4	1...4	1...5
B	0,1	4...10	4...12	1
η	2...25	25...30	4...6	2...3

Примітка: №1,…, №4 відповідають типу лазерів.

За результатами порівняльного аналізу узагальнених УКВРІ (рис.1) виявлено, що найкращим за багатьма параметрами є №1 волоконний лазер. Отже, візуалізація запропонованого результату забезпечує по-перше високу швидкість процесу порівняльного аналізу, а по-друге процедура оцінювання забезпечує об'єктивність значень показників.

Список використаних джерел:

1. Grygor O. et al. (2021) "Formation of an effective model of the knowledge base through metallographic images of laser welding microstructures in the conditions of small-series production", ITEST 2024, LNDECT 221, pp. 1–18, 2024, doi: 978-3-031-71801-4-23.

2. Гардер Д. А., та ін. (2021) "Інформаційна технологія багатокритеріального кількісного об'єктивного оцінювання моделей волоконних лазерних модулів",Nauka i studia, Przemysl, 2021. № 5, pp. 39-45.

Секція 1. МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ТА РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Секція 2. КОМП'ЮТЕРНА ІНЖЕНЕРІЯ ТА КІБЕРБЕЗПЕКА

Секція 3. КОМП'ЮТЕРНІ НАУКИ, ІНФОРМАЦІЙНІ СИСТЕМИ ТА ТЕХНОЛОГІЇ

Секція 4. СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ТЕЛЕКОМУНІКАЦІЯХ ТА БІОМЕДИЦИНІ

Секція 5. ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ В ОСВІТІ

Секція 6. ЦИФРОВА ОБРОБКА СИГНАЛІВ ТА ЗОБРАЖЕНЬ В АВТОМАТИЗОВАНИХ ТА ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНИХ СИСТЕМАХ

Секція 7. КОМП'ЮТЕРНО-ІНТЕГРОВАНІ ТЕХНОЛОГІЇ. ПРИЛАДОБУДУВАННЯ.

Наукове видання

Тези XV міжнародної науково-технічної конференції «Інформаційно-комп’ютерні технології»

Житомир, 28-29 березня 2025 р.

Відповідальний за випуск: В.В. Болотіна