Міністерство освіти і науки України

Державний вищий навчальний заклад
«Донецький національний технічний університет»

Кафедра автоматики і телекомунікацій

Донецький науковий центр НАН України і МОН України

«ТАК»

Телекомунікації, автоматизація, комп'ютерно-інтегровані та інформаційні технології

Збірка доповідей Всеукраїнської науково-практичної конференції молодих учених
(Дрогобич, 12 грудня 2024 р.)

Дрогобич
ДВНЗ «ДонНТУ»
2024

УДК 621.39+681+004
Т 15

Т 15 **«ТАК»**: телекомунікації, автоматика, комп'ютерно-інтегровані технології: зб. доповідей Всеукр. наук.-практ. конф. молодих вчених, 12 грудня 2024 р. / ДВНЗ «ДонНТУ; відп. ред. Г.В. Ступак. – Дрогобич: ДВНЗ «ДонНТУ», 2024. – 215 с.

До збірника увійшли матеріали доповідей, представлених на Всеукраїнській науково-практичній конференції молодих учених «ТАК»: телекомунікації, автоматика, комп'ютерно-інтегровані технології. Конференція проводилася кафедрой автоматики та телекомунікацій (АТ) ДВНЗ «Донецький національний технічний університет».

У збірнику представлені результати досліджень та розробок молодих вчених із технічних вузів та наукових закладів України.

Збірник призначений для викладачів, аспірантів і студентів вищих технічних навчальних закладів, а також фахівців з телекомунікацій, автоматизації, інформаційних та комп'ютерно-інтегрованих технологій, електротехніки та електромеханіки.

УДК 621.39+681+004

СЕКЦІЯ 1

«Інформаційні технології, телекомунікації та кібербезпека»

ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ПРЕВЕНТИВНОГО ВИЯВЛЕННЯ ТА НЕЙТРАЛІЗАЦІЇ ШКІДЛИВОГО ПЗ

Ковалевич І.О., студент, ivan.kovalevych.kita@donntu.edu.ua;
Нікітенко А.О., асис. кафедри ПМІ, andrii.nikitenko@donntu.edu.ua
ДВНЗ «Донецький національний технічний університет», м. Дрогобич, Україна

На сьогоднішній день шкідливе програмне забезпечення (~~Ш~~ПЗ) становить серйозну загрозу кібербезпеці, зачіпаючи як звичайних користувачів, так і великі компанії, хакери постійно вдосконалюють шкідливе ПЗ, що стає серйозною проблемою для безпеки. Щороку виявляють мільйони нових зразків, які використовують обфускацію та метаморфізм, що ускладнює їхнє виявлення. Для захисту необхідне своєчасне та автономне виявлення загроз. Еволюція ШПЗ розпочалася з Creeper у 1970-х і досягає по сьогоднійній день свого піку. Гарним прикладом досить впливових вірусів є: Stuxnet, [1] WannaCry, Petya та NotPetya, які демонструють небезпеку сучасних вірусів [2].

Віруси – це один із видів шкідливого ПЗ, здатне до самовідтворення, яке поширюється через Інтернет, USB-накопичувачі та електронну пошту, завдаючи шкоди файлам і системам. Можна назвати деякі типи ШПЗ: макровіруси (у документах або коді програм), віруси електронної пошти (активуються через макроси у вкладеннях), поліморфні віруси (змінюють копії для уникнення виявлення) і трояни (маскуються під легальне ПЗ).

Ботнети – це мережі автоматизованих програм (ботів), які виконують завдання без втручання користувача і є значною загрозою для Інтернету.

На рис. 1 продемонстровано знаходження і аналіз шкідливого ПЗ традиційним методом.

Аналіз шкідливих програм – це процес перевірки виконуваних файлів з метою отримання максимальної кількості інформації. Основна мета – запобігання кібератакам на інформаційні системи.

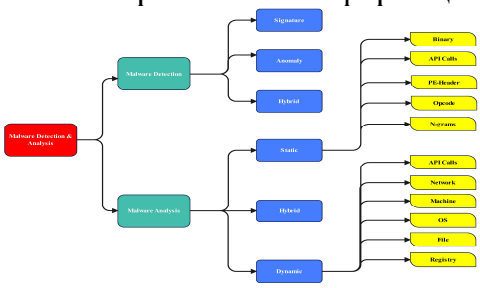


Рисунок 1 – Методи виявлення шкідливого ПЗ

Статичний аналіз дозволяє досліджувати шкідливе програмне забезпечення без його виконання, зосереджуючись на метаданих. Цей метод ефективний для ідентифікації відомих зразків, однак має обмеження при роботі з новими загрозами [3].

Динамічний аналіз досліджує поведінку шкідливого ПЗ під час його виконання. Основна мета — зрозуміти, як саме діє ПЗ, збираючи дані про його активність у реальному часі. Цей метод

дозволяє спостерігати за функціями шкідливого коду та взаємодією з оточенням у віртуальному середовищі, що забезпечує безпеку. Динамічний аналіз ефективніший за статичний, оскільки навіть при зміні структури коду поведінка залишається незмінною, що полегшує виявлення загроз [4].

Також є гібридний аналіз котрий поєднує статичний і динамічний методи аналізу шкідливого ПЗ.

Сигнатура – це послідовність даних, яка ідентифікує конкретне шкідливе ПЗ. Цей підхід швидкий і ефективний для виявлення відомих загроз, але неефективний для нових або модифікованих зразків. Зловмисники змінюють код, щоб уникнути виявлення за попередніми сигнатурами [5]. Виявлення шкідливих програм на основі поведінки аналізує дії програми під час виконання для визначення її шкідливості. Процес включає збір інформації (API-дзвінки, зміни файлової системи, мережні запити), створення поведінкової моделі та порівняння з відомими патернами шкідливого ПЗ для виявлення загрози [6].

Кіберпростір є вразливим до нових видів шкідливого ПЗ що може впливати на життя людей, безпеку та бізнес. Проведено низку досліджень для виявлення шкідливого ПЗ у Windows, Android, iOS, IoT та APT.

Jerlin et al. [7] реалізували систему виявлення шкідливого ПЗ на основі наївного алгоритму Байєса, аналізуючи PE-файли. Автори [8] досліджували зразки ПЗ через пари джерело-приймач, отримані FlowDroid. Catak et al. [9] запропонували підхід із LSTM для виявлення троянів, руткітів, вірусів, бекдорів і черв'яків. Автори [10] розробили систему на основі глибокого навчання для аналізу процесора, пам'яті та використання батареї. Pajouh et al. [11] представили рекурентну нейронну мережу для аналізу шкідливих програм Android. Karbaba et al. [12] запропонували систему з моделлю bag-of-words (BOW) для аналізу функцій Android-додатків, таких як дозволи, мережеві адреси та виклики API. Huan et al. [13] створили систему на основі CNN, яка перетворює файли на зображення RGB. Zhu et al. [14] запропонували MSerNetDroid, що використовує залишкову мережу для аналізу дозволів файлів. Seraj et al. [15] представили MLP для виявлення Android-загроз, в аналогічному дослідженн [16] використали приховану марковську модель для аналізу.

Аналіз наукових джерел демонструє, що основними підходами до виявлення шкідливого ПЗ є методи, засновані на машинному навчанні, зокрема наївний байєсівський класифікатор, LSTM, CNN та глибокі рекурентні нейронні мережі. Зазначені підходи забезпечують високу ефективність обробки даних, отриманих як в результаті статичного, так і динамічного аналізу. Вони особливо ефективні для виявлення складних та нових кіберзагроз, таких як атаки типу APT та програми-вимагачі. У подальшій роботі, спираючись на отримані результати аналізу, буде здійснено оцінку переваг і недоліків існуючих методів, а також виконано спробу розробки та навчання власної моделі для превентивного виявлення загроз.

Література

1. Debnath P., Mohiuddine S.A. Soft Computing Techniques in Engineering, Health, Mathematical and Social Sciences. — 1st ed. — Boca Raton : CRC Press, 2021. — 232 c.

2. Greenberg A. The untold story of NotPetya, the most devastating cyberattack in history // Wired. — 2018. — No. 22. — P. 1–14.

3. Прищепа О., Доценко О. Огляд статичних методів аналізу зловмисного програмного забезпечення // ScienceRise. — 2020. — URL: https://journals.indexcopernicus.com/api/file/viewByFileId/1179859.

4. Kiachidis I.G., Baltatzis D.A. Comparative review of malware analysis methodologies // International Journal of Network Security & Its Applications. — 2021. — Vol. 13, No. 6. — P. 103–116. — URL: https://aircconline.com/ijnsa/V13N6/13621ijnsa08.pdf.

5. Nigam P. Malware detection and signature generation // International Journal of Emerging Technologies and Applications in Engineering, Technology and Sciences. — 2020. — Vol. 7, No. 5. — P. 20–30. — URL: https://www.ijetajournal.org/volume-7/issue-5/IJETA-V7I5P3.pdf.

6. Liang G., Pang J., Dai C. A behavior-based malware variant classification technique // International Journal of Information and Education Technology. — 2016. — Vol. 6, No. 2. — P. 702–710. — URL: https://www.ijiet.org/vol6/702-IT060.pdf.

7. Jerlin M.A., Marimuthu K. A new malware detection system using machine learning techniques for API call sequences // Journal of Applied Security Research. — 2018. — Vol. 13. — P. 45–62.

8. Zhu D., Jin H., Yang Y., Wu D., Chen W. DeepFlow: Deep learning-based malware detection by mining Android application for abnormal usage of sensitive data // Proceedings of the IEEE Symposium on Computers and Communications. — Heraklion, Greece, 3–6 July 2017. — P. 515–520.

9. Catak F.O., Yazı A.F., Elezaj O., Ahmed J. Deep learning-based sequential model for malware analysis using Windows exe API Calls // PeerJ Computer Science. — 2020. — Vol. 6. — Article e285.

10. Milosevic N., Huang J. Deep learning guided Android malware and anomaly detection // arXiv preprint. — 2019. — arXiv:1910.10660.

11. HaddadPajouh H., Dehghantanha A., Khayami R., Choo K.K.R. A deep recurrent neural network-based approach for Internet of Things malware threat hunting // Future Generation Computer Systems. — 2018. — Vol. 85. — P. 88–96.

12. Karbab E.B., Debbabi M. MalDy: Portable, data-driven malware detection using natural language processing and machine learning techniques on behavioral analysis reports // Digital Investigation. — 2019. — Vol. 28. — P. S77–S87.

13. Huang Y.P., Basanta H. Bird image retrieval and recognition using a deep learning platform // IEEE Access. — 2019. — Vol. 7. — P. 66980–66989.

14. Zhu H.J., Gu W., Wang L.M., Xu Z.C., Sheng V.S. Android malware detection based on multi-head squeeze and excitation residual network // Expert Systems with Applications. — 2023. — Vol. 212. — Article 118705.

15. Seraj S., Khodambashi S., Pavlidis M., Polatidis N. MVDroid: An Android malicious VPN detector using neural networks // Research Square. — 2022. — P. 1–14.

16. Sasidharan S.K., Thomas C. ProDroid—An Android malware detection framework based on profile hidden Markov model // Pervasive and Mobile Computing. — 2021. — Vol. 72. — Article 101336.

Анотація

З розвитком технологій виявлення та аналізу шкідливого програмного забезпечення стає все більш актуальним завданням, оскільки сучасне зловмисне ПЗ може обходити традиційні захисні системи. У статті розглядаються різні методи виявлення шкідливого ПЗ, зокрема на основі машинного навчання (LSTM, CNN, Naive Bayes), які демонструють високу ефективність у розпізнаванні як відомих, так і нових загроз.

Ключові слова: шкідливе програмне забезпечення, машинне навчання, статичний аналіз, динамічний аналіз, сигнатурний метод, нейронна мережа.

Abstract

With the development of technologies for detection and analysis of malicious software, it is becoming an increasingly urgent task, as modern malicious software can bypass traditional protection systems. The article discusses various methods of detecting malicious software, in particular, based on machine learning (LSTM, CNN, Naive Bayes), which demonstrate high efficiency in recognizing both known and new threats.

Keywords: malware, machine learning, static analysis, dynamic analysis, signature method, neural network.

ДОСЛІДЖЕННЯ ТА ВДОСКОНАЛЕННЯ ТЕХНОЛОГІЙ НЕЙРОННОГО РЕНДЕРИНГУ В ГРАФІЧНИХ СИСТЕМАХ

Дмитрів Ю.П. студент, магістр, molfar.glitch@gmail.com
Прикарпатський національний університет імені Василя Стефаника, м. Івано-Франківськ, Україна

Терміни та абревіатури

1) Нейронний рендеринг (НР, англ. Neural Rendering) – сучасний підхід до створення та обробки зображень і відео за допомогою глибоких нейронних мереж. Використовується для оптимізації візуалізації та зниження обчислювальних витрат.
2) AMD FSR (FidelityFX Super Resolution) – технологія від компанії AMD для масштабування зображень із підвищенням їх роздільної здатності за допомогою просторових алгоритмів.
3) DLSS (Deep Learning Super Sampling) – метод NVIDIA, що базується на використанні згорткових нейронних мереж для покращення якості рендерингу при низькій роздільній здатності.
4) Intel XeSS (Xe Super Sampling) – технологія Intel для масштабування зображень на основі нейронних мереж, що оптимізує якість візуалізації.
5) PSNR (Peak Signal-to-Noise Ratio**)** – метрика для оцінки якості зображень на основі співвідношення сигналу до шуму.
6) SSIM (Structural Similarity Index Measure) – метрика для оцінки структурної схожості між двома зображеннями.

Актуальність питання

Нейронний рендеринг (НР) є сучасним підходом до створення та обробки зображень і відео, що базується на використанні нейронних мереж. Його застосування дозволяє значно підвищити якість візуалізації, знизити обчислювальні витрати та розширити можливості використання в галузях, таких як кіноіндустрія, ігровий девелопмент, медицина та військова справа. Актуальність дослідження зумовлена потребою в оптимізації існуючих алгоритмів для збереження якості при обмежених ресурсах.

Відомі дослідження та публікації

Попередні дослідження підтверджують ефективність технологій AMD FSR, NVIDIA DLSS та Intel XeSS у підвищенні роздільної здатності зображень із мінімальними втратами якості. Роботи Ledig C. та ін. висвітлюють переваги використання глибокого навчання у відновленні деталізації. Однак питання інтеграції цих технологій у реальні додатки залишається відкритим.

Постановка задачі та методи

Мета дослідження полягає в аналізі ефективності існуючих методів масштабування зображень, таких як AMD FSR, DLSS та XeSS, а також у вдосконаленні алгоритмів для покращення їх застосування в реальному часі. Основні завдання включають:

- Порівняння існуючих методів за допомогою метрик PSNR та SSIM.
- Дослідження впливу параметрів вхідного контенту на результати масштабування.
- Розробка алгоритму для створення навчальних баз даних.

Також були проаналізовані та використанні для роботи наступні алгоритми:

Метрика PSNR для оцінки якості зображень, для вимірювання якості зображення застосовується:

$$PSNR = 10 \cdot \log\left(\frac{MAX_I}{MSE}\right), \quad (1)$$

де $M\ A\ X_I$ - максимальне можливе значення інтенсивності пікселів (наприклад, 255 для 8-бітних зображень), MSE— середньоквадратична похибка між оригінальним та масштабованим зображеннями.

Метрика SSIM для порівняння зображень, для оцінки схожості зображень використовується спрощення формула SSIM:

$$SSIM(x, y) = [l(x, y)]^{\alpha} \cdot [c(x, y)]^{\beta} \cdot [s(x, y)]^{\gamma}, \quad (2)$$

де $l(x, y), c(x, y), s(x, y)$— функції, що відповідають за порівняння яскравості, контрасту та структури відповідно.

Для кращого маштабування зображень використовується інтерполяція Ланцоша:

$$f(x) = \sum_{k=-n}^{n} f(k) \cdot Lanczos(x - k), \quad (3)$$

де $f(x)$ — інтерпольоване значення в точці x, $f(k)$ — значення оригінальної функції в сусідніх точках k, n — параметр фільтра Ланцоша, що визначає ширину вікна (рекомендоване значення зазвичай становить $n = 3$). Це дозволяє зменшити артефакти при збільшенні зображень.

Основний матеріал та результати дослідження

У дослідженні було проаналізовано популярні методи масштабування зображень. Метод DLSS показав найвищу якість при низькій роздільній здатності завдяки використанню згорткових нейронних мереж. Метод AMD FSR, зосереджений на просторових алгоритмах, демонструє кращу продуктивність для пристроїв із обмеженими ресурсами. Розроблений алгоритм-програма дозволяє аналізувати відеоматеріали, визначати вектори руху та створювати кадри для подальшого навчання моделей.

Висновки та подальші дослідження

Дослідження підтвердило ефективність використання нейронних мереж для покращення візуалізації. Подальші роботи будуть спрямовані на інтеграцію цих технологій у системи доповненої реальності та оптимізацію їх

для пристроїв із обмеженими обчислювальними ресурсами. Також розроблений алгоритм-програма для зчитування зображень, що дозволяє аналізувати відео та фотоматеріали, визначати вектор руху та знаходити межі кадру. Ці дані можна використовувати для подальшого вдосконалення методів нейронного рендерингу та для використання в інших сферах.

Розроблені методи та алгоритми сприяють удосконаленню технологій нейронного рендерингу, їх інтеграції в різні галузі, включаючи обробку відео та зображень, що значно покращує якість кінцевих результатів. Розвиток таких технологій відкриває нові можливості для створення більш реалістичних та якісних зображень у різних додатках, таких як віртуальна реальність, відеоігри, та візуалізація для наукових та військових цілей.

Література

1. NeRF: Representing Scenes as Neural Radiance Fields for View Synthesis. [Електронний ресурс] URL: https://arxiv.org/pdf/2003.08934 (дата звернення: травень 2024р.)
2. DeepVoxels: Learning Persistent 3D Feature Embeddings. [Електронний ресурс] URL: https://arxiv.org/pdf/1812.01024 (дата звернення: травень 2024р.)
3. Ledig, C., et al. Photo-Realistic Single Image Super-Resolution Using a Generative Adversarial Network. [Електронний ресурс] URL: https://arxiv.org/pdf/1609.04802.pdf (дата звернення: вересень 2024р.).

Анотація

Дослідження присвячене вдосконаленню технологій нейронного рендерингу для графічних систем. Розглянуто методи масштабування зображень AMD FSR, NVIDIA DLSS та Intel XeSS. Показано, що DLSS забезпечує найвищу якість при низькій роздільній здатності, а AMD FSR підходить для пристроїв із обмеженими ресурсами. Розроблено алгоритм-програму для створення навчальних баз даних, що сприяє покращенню якості масштабування.

Ключові слова: нейронний рендеринг, масштабування зображень, нейронні мережі, DLSS, AMD FSR, Intel XeSS, PSNR, SSIM.

Abstract

The study focuses on improving neural rendering technologies for graphic systems. Methods such as AMD FSR, NVIDIA DLSS, and Intel XeSS image scaling are analyzed. DLSS demonstrated the highest quality at low resolutions, while AMD FSR proved effective for devices with limited resources. A program algorithm for creating training datasets was developed, improving scaling quality.

Keywords**:** neural rendering, image scaling, neural networks, DLSS, AMD FSR, Intel XeSS, PSNR, SSIM.

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЖИТТІ ЗДОБУВАЧА ОСВІТИ

Івахненко В.О., студент
Корнєва В.Р., викладач viktoriia.kornieva@ptfc.ukr.education
Прилуцький технічний фаховий коледж, Прилуки, Україна

У XXI столітті інформаційні технології стали невід'ємною частиною життя кожної людини, і особливо помітний їхній вплив у сфері освіти. Вони відкривають перед здобувачами освіти нові можливості, змінюють способи отримання знань, організацію навчального процесу та впливають на їхній розвиток. У цій статті розглянемо, як сучасні інформаційні технології впливають на навчання, які можливості вони надають здобувачам освіти та які виклики стоять перед ними.

Роль інформаційних технологій у навчальному процесі

Інформаційні технології радикально змінюють підходи до навчання, забезпечуючи інтерактивність, гнучкість і доступність освіти. Зокрема, вони сприяють персоналізації навчання, коли кожен учень може обирати зручний темп і стиль роботи. Використання електронних ресурсів, таких як інтерактивні підручники, освітні платформи та відеоуроки, дозволяє розширити доступ до інформації, яка раніше була недоступною або вимагала значних зусиль для її отримання.

Також сучасні технології допомагають створювати нові формати навчання, наприклад, дистанційні курси, онлайн-лекції, вебінари, відеоконференції тощо. Ці інструменти особливо стали актуальними під час пандемії COVID-19, коли навчальні заклади у всьому світі перейшли на дистанційний формат.

Виклики впровадження інформаційних технологій

Використання інформаційних технологій у навчанні студентів супроводжується низкою викликів, які потребують уваги. Один із головних викликів — цифрова нерівність. Не всі студенти мають рівний доступ до сучасних пристроїв і швидкісного інтернету, особливо у віддалених регіонах або серед соціально незахищених груп. Це обмежує можливості для участі у дистанційному навчанні та використання сучасних освітніх платформ.

Іншою проблемою є перевантаження інформацією. У цифровому середовищі студенти стикаються з величезними потоками даних, серед яких важко відрізнити корисну та достовірну інформацію від хибної або неактуальної. Брак навичок інформаційної гігієни й медіаграмотності посилює цю проблему.

Важливим аспектом є проблема втрати мотивації. Дистанційне навчання, яке широко впроваджується завдяки інформаційним технологіям, може знижувати залученість студентів через відсутність безпосереднього

контакту з викладачами та одногрупниками. Це може призводити до ізоляції, зменшення взаємодії та погіршення емоційної підтримки.

Кібербезпека також є значним викликом. Недостатнє знання правил безпеки в інтернеті може призвести до витоку персональних даних, шахрайства чи втрати доступу до акаунтів. Студенти часто стають мішенню для хакерів або фішингових атак через недосвідченість у питаннях цифрового захисту.

Тривале використання гаджетів і комп'ютерів негативно позначається на фізичному здоров'ї студентів. Виникають проблеми із зором, поставою, а також підвищується рівень психологічної напруги та втоми. Це потребує запровадження правил щодо збалансованого використання технологій.

Таким чином, незважаючи на численні переваги інформаційних технологій, студенти стикаються з серйозними викликами, які потребують комплексного підходу для їх подолання.

Як здобувачам освіти ефективно використовувати інформаційні технології?

1. Використовувати надійні ресурси

Здобувачам освіти слід обирати перевірені освітні платформи, такі як Coursera, EdX, Prometheus, Duolingo, Khan Academy тощо. Це допоможе отримати якісні знання та уникнути дезінформації.

2. Розвивати цифрову грамотність

Знання основ програмування, роботи з текстовими редакторами, електронними таблицями та презентаціями є базовими навичками для сучасної людини. Опанування цих інструментів сприяє успішності як у навчанні, так і в майбутній професійній діяльності.

3. Дотримуватись кібербезпеки

Здобувачам освіти важливо знати, як захистити свої персональні дані, уникати фішингових атак і створювати надійні паролі для облікових записів.

4. Дотримуватись балансу

Навчання за допомогою інформаційних технологій має бути збалансованим: не забувайте про фізичну активність, прогулянки на свіжому повітрі та живе спілкування.

5. Брати участь у проєктах

Групові онлайн-проєкти та спільна робота над завданнями допомагають розвивати навички співпраці та креативність. Такі сервіси, як Google Документи чи Miro, сприяють ефективній взаємодії між здобувачами освіти.

Перспективи використання інформаційних технологій в освіті

Майбутнє освіти безпосередньо пов'язане з інформаційними технологіями. Використання штучного інтелекту (AI), віртуальної та доповненої реальності (VR/AR), аналізу великих даних (Big Data) і блокчейну у навчальному процесі відкриває величезний потенціал.

Наприклад:

Штучний інтелект може створювати персоналізовані навчальні плани.

Віртуальна реальність дозволяє проводити інтерактивні уроки з хімії чи біології, а також досліджувати історичні місця.

Блокчейн-технології можуть забезпечувати захист дипломів та сертифікатів.

Здобувачі освіти, які активно використовують ці технології, мають більше можливостей для саморозвитку та професійного зростання.

Література

1. Гуржій А.М. Інформаційні технології в освіті: проблеми і перспективи / А.М. Гуржій, О.В. Спірін // Інформаційні технології і засоби навчання. – 2015. – №4. – С. 12–19.

2. Згуровський М.З. Інформаційні технології та системи управління знаннями у сучасній освіті / М.З. Згуровський // Вища освіта України. – 2012. – №3. – С. 15–20.

3. Морзе Н.В. Використання сучасних інформаційних технологій у навчальному процесі: досвід і перспективи / Н.В. Морзе // Інноваційні підходи в освіті. – 2018. – №1. – С. 45–52.

Анотація

Сучасні інформаційні технології є потужним інструментом для здобувачів освіти. Вони розширюють можливості навчання, сприяють інтерактивності та забезпечують доступ до якісних знань. Водночас важливо враховувати виклики, які супроводжують їх використання, і знаходити способи їх подолання.

Розумне використання технологій допоможе кожному здобувачеві освіти не лише досягти успіхів у навчанні, а й стати підготовленим до викликів майбутнього цифрового світу.

Ключові слова: інформаційні технології, освіта, персоналізоване навчання.

Abstract

Modern information technologies are a powerful tool for learners. They expand learning opportunities, promote interactivity, and provide access to quality knowledge. At the same time, it is important to consider the challenges that accompany their use and find ways to overcome them.

The intelligent use of technology will help every learner not only achieve success in their studies, but also become prepared for the challenges of the future digital world.

Keywords: information technologies, education, personalized learning.

МОДЕЛЬ ЗАХИЩЕНОГО AI- АСИСТЕНТА ДЛЯ СИСТЕМ ЕЛЕКТРОННОГО НАВЧАННЯ

Кузіков Б. О., к.т.н., доцент, b.kuzikov@dl.sumdu.edu.ua;
Шовкопляс С.Р. s.shovkoplyas@student.sumdu.edu.ua,
Сумський державний університет, Суми, Україна

Застосування систем на основі штучного інтелекту може надати поштовх у впровадженні персонально-орієнтованого навчання. Наприклад, використання інтелектуальних асистентів на основі великих мовних моделей (LLM) дозволяє розвантажити викладача при асинхронному форматі взаємодії із здобувачем. При цьому застосування стандартних компонентів має ряд критичних недоліків:

– інтелектуальні асистенти на основі LLM не мають інформації, пов'язаної із предметом та умовами навчання. Збагачення контексту у цьому випадку значно здорожчує використання;

– інтелектуальні асистенти типу "чат із сторінкою/pdf" не занурені в контекст навчання;

– використання pre-trained LLM стикається із необхідністю постійного їх оновлення через зсув горизонту знань (data cut-off);

– застосування RAG стикається із відсутністю оперативної інформації щодо процесу навчання (оцінки, коментарі, виконані завдання).

Виходячи з наявних протиріч, у роботі [1] запропонована модель інтелектуального асистента із використанням великих мовних моделей, Retrieval Augmented Generation (RAG) та гібридних джерел інформації. Модель використовує векторну базу даних для збереження навчальних матеріалів, що дозволяє швидко знаходити релевантну інформацію. За допомогою агрегації даних із Learning Management System (LMS) забезпечується актуалізація відповідей залежно від індивідуальних досягнень студента. Це дає можливість надавати контекстуально обґрунтовані й персоналізовані відповіді. Принципова схема запропонованого рішення наведена на рисунку 1, де синім відмічено елементи, що пропонувались в оригінальному дослідженні.

Проте застосування подібних систем пов'язане з певними ризиками, зокрема кібербезпековими загрозами. До основних можна віднести неавторизований доступ до LMS API та доступ до сторонніх персональних даних засобами генеративної мережі. Вирішення подібних проблем вимагає комплексного підходу. В основу рішення, що пропонується, покладена аутентифікація на основі JWT токенів, використання Access Control List (ACL) на основі векторної БД, розробка ACL для LMS.

У наведеній схемі запит до інтелектуального агента збагачується токеном для читання даних з LMS. Персональні дані користувача при цьому не розкриваються. Токен використовується для отримання даних щодо прав на

доступ користувача. Отримані дані використовуються як фасет пошуку у БД, слугуючи частиною авторизації. Фасет обмежує видимість документів, тож дані інших користувачів не можуть бути розкриті через зловмисним чином сконструйований промпт. Інформацію щодо користувача та доступні йому набори документів має лише LMS, розголошуючи їх лише у вигляді UUID для авторизованих запитів. А ні RAG, а ні вектрона БД такої інформації не має. Ключем на рисунку позначені запити, які містять ключ як засіб аутентифікації. Емітером ключа при цьому є LMS.

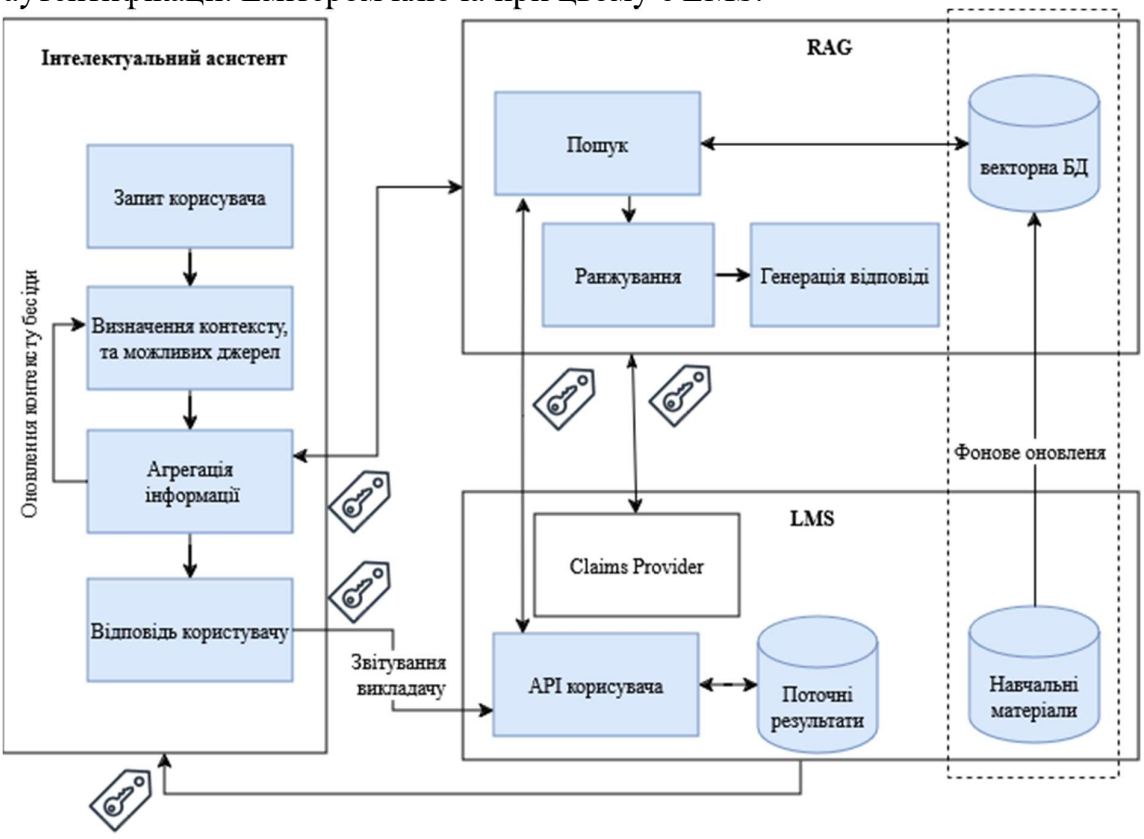


Рисунок 1. Модель інтелектуального асистента, із урахуванням кіберзагроз

Варто зазначити, що наведена схема вимагає використання таких баз даних як Elastic Search [2], SQLite (розшиення sqlite-vss / sqlite-vec), PostgreSQL (TsVector) на противагу більш спеціалізованим векторним базам даних, у яких функціонал ACL / Role-based access control (RBAC) / Attribute-based access control (ABAC) не підтримується [3-5].

Інтелектуальні системи на базі LLM та RAG можуть суттєво покращити навчальний процес, забезпечуючи персоналізовані відповіді на основі релевантних матеріалів і даних про прогрес студентів. Однак їх впровадження пов'язане зі значними кібер-загрозами, такими як атаки на векторні бази даних, несанкціонований доступ до API та отруєння даних. Для мінімізації цих загроз необхідно впроваджувати багаторівневі стратегії захисту, що включають шифрування даних, захист API, інтеграцію систем виявлення загроз та механізмів валідації даних. Використання комплексних засобів захисту

дозволить зменшити ризики, забезпечуючи надійність і безпеку інтелектуальної системи.

Робота виконана в рамках НДР "Інтелектуальні технології в кібербезпеці" (№ДР 0121U109466, Міністерство освіти та науки України)..

Література

1. Шовкопляс С. Р. Модель інтелектуального асистента з використанням llm та rag для оптимізації взаємодії викладач-здобувач / Сергій Ростиславович Шовкопляс, Борис Олегович Кузіков // Інформаційні технології і автоматизація – 2024 : XVII МІЖНАР. НАУКОВО-ПРАКТ. КОНФ., Одеса, 31 жовт. 2024 р. – Одеса, 2024. – С. 10–12.

2. Advanced RAG techniques part 1: Data processing - Search Labs [Electronic resource] // Search Labs. – Mode of access: https://www.elastic.co/search-labs/blog/advanced-rag-techniques-part-1 (date of access: 29.11.2024). – Title from screen.

3. Data security for LLM + RAG [Electronic resource] // Raito - Access to data. Fast, Secure, and on Time. – Mode of access: https://www.raito.io/post/how-to-secure-llm-rag (date of access: 29.11.2024). – Title from screen

4. Hong. Security controls in rag-based LLM applications [Electronic resource] / Hong // Medium. – Mode of access: https://medium.com/@hong56/security-controls-in-rag-based-llm-applications-94a72c890ba0 (date of access: 29.11.2024). – Title from screen.

5. Neal Swaelens and Oleksandr Yaremchuk. RAG security 101 [Electronic resource] / Neal Swaelens and Oleksandr Yaremchuk // Protect AI | The Platform for AI and ML Security. – Mode of access: https://protectai.com/blog/rag-security-101 (date of access: 29.11.2024). – Title from screen.

Анотація

У роботі представлено вдосконалену модель інтелектуального асистента на основі великих мовних моделей та генерації з використанням пошуку для оптимізації взаємодії викладач-здобувач у персоналізованому навчальному середовищі. Запропоновано новий підхід до зниження кіберзагроз, що включає аутентифікацію на основі JWT-токенів, використання списків контролю доступу на базі векторних баз даних та розробку спеціалізованого API для систем управління навчанням. Модель спрямована на надання контекстуально релевантних та персоналізованих відповідей при забезпеченні безпеки даних та конфіденційності користувачів.

Ключові слова: штучний інтелект в освіті, великі мовні моделі, генерація з використанням пошуку, персоналізоване навчання, кібербезпека, контроль доступу, векторні бази даних.

Abstract

The paper presents an advanced model of an intelligent assistant based on large language models and retrieval-augmented generation to optimize teacher-learner interaction in a personalized learning environment. A novel approach to mitigating cybersecurity threats is proposed, including authentication based on JWT tokens, the use of access control lists built on vector databases, and the development of a specialized API for learning management systems. The model is designed to provide contextually relevant and personalized responses while ensuring data security and user privacy.

Keywords: artificial intelligence in education, large language models, retrieval-augmented generation, personalized learning, cybersecurity, access control, vector database.

ЗАСТОСУВАННЯ АЛГОРИТМІВ МАШИННОГО НАВЧАННЯ В СИСТЕМАХ ВИЯВЛЕННЯ МЕРЕЖЕВИХ ВТОРГНЕНЬ

Соболь Є.А., студент, yevhen.sobol.kita@donntu.edu.ua;
Нікітенко А.О., асис. кафедри ПМІ, andrii.nikitenko@donntu.edu.ua;
ДВНЗ «Донецький національний технічний університет», м. Дрогобич, Україна

У сучасну епоху стрімкого прогресу у сфері програмного забезпечення, апаратної інфраструктури та масового впровадження мережевих технологій, проблема захисту мережевих пристроїв від різноманітних мережевих атак набуває все більшої актуальності. Постійне удосконалення методів і засобів несанкціонованого доступу до закритих систем, які з кожним роком стають дедалі складнішими та витонченішими, ставить перед дослідниками завдання розробки більш ефективних і адаптивних рішень. У цьому контексті системи виявлення мережевих вторгнень (Network Intrusion Detection Systems – NIDS) виступають ключовим інструментом забезпечення кібербезпеки.

NIDS виконують критично важливу функцію аналізу мережевого трафіку для виявлення потенційно небезпечних дій шляхом виявлення аномалій у потоках даних за допомогою моделей, що заздалегідь пройшли навчання [1]. Такі моделі здатні визначати відхилення від нормальної поведінки мережі, вказуючи на можливі вторгнення. Архітектура NIDS передбачає послідовну реалізацію кількох етапів: попередньої обробки даних, вибору ознак та класифікації. Попередня обробка даних охоплює процеси збору, очищення та нормалізації мережевого трафіку, що забезпечує усунення шуму, видалення неповних або некоректних записів та приведення даних до уніфікованого формату, придатного для подальшого аналізу. Цей етап є критичним для забезпечення якості вхідних даних, які впливають на точність і продуктивність системи. На етапі вибору ознак здійснюється аналіз і відбір найрелевантніших параметрів, які мають найбільший вплив на процес ідентифікації вторгнень. Це дозволяє суттєво зменшити розмірність даних, що, своєю чергою, знижує обчислювальні витрати та підвищує швидкодію моделі. Заключний етап передбачає застосування алгоритмів машинного навчання для класифікації мережевого трафіку. Класифікатори, такі як Random Forest, XGBoost або нейронні мережі, використовуються для розподілу трафіку на категорії: нормальний або потенційно зловмисний. Цей етап забезпечує оперативне виявлення загроз і мінімізацію хибних спрацьовувань, що є вирішальним для функціонування NIDS у реальному часі. Такий структурований підхід дозволяє створювати адаптивні та ефективні системи для забезпечення мережевої безпеки.

Однак розробка ефективної моделі для NIDS є доволі складним завданням через високі вимоги до її точності, адаптивності та здатності працювати

в режимі реального часу. Основним викликом при створенні NIDS є необхідність забезпечення оптимального балансу між здатністю системи виявляти загрози і задачею мінімізацією помилкових спрацьовувань. Застосування неякісної моделі може привести до компрометації системи захисту або значно знизити ефективність роботи системи та ускладнити її впровадження у високонавантажених мережах.

В контексті зростаючих викликів у сфері мережевої безпеки та постійного вдосконалення NIDS, актуальним стає питання пошуку оптимальних алгоритмів для аналізу та класифікації аномалій у мережевому трафіку. Використання методів машинного навчання відіграє ключову роль у розробці адаптивних і високоточних рішень. У цьому напрямі дослідження зосереджені на порівнянні ефективності різних підходів, що дає змогу визначити найбільш перспективні стратегії.

У статті [2] проаналізовано продуктивність алгоритмів машинного навчання для виявлення мережевих вторгнень і класифікації атак. Розглянуто нейронні мережі, опорні вектори, Random Forest, лінійний дискримінантний аналіз, метод найближчих сусідів та алгоритми кластеризації K-means, Mean-shift і DBSCAN. Для об'єктивності результатів використовувалися чотири набори даних: KDD99, NSL-KDD, UNSW-NB15 і CIC-IDS-2017. Експерименти показали, що Random Forest забезпечує найвищу точність і швидкість виконання. Водночас комбінація кластеризації та класифікації підвищує точність виявлення атак, хоча й суттєво збільшує час виконання, що що може створювати труднощі при роботі у реальному часі.

У роботі [3] автори розглядають методології оптимізації вибору ознак для NIDS з метою зниження складності моделі та підвищення її ефективності. Використано метод інформаційного прибутку, що дозволив скоротити ознаки у наборі NSL-KDD з 41 до 28 для кожного типу атаки. Така оптимізація дозволила досягти підвищення загальної точності моделі на тестовому наборі даних до 86.66%. Найкращі результати досягнуто за допомогою ансамблевого методу голосування, який поєднував Random Forest і PART.

У статті [4] автори представляють гібридний підхід до виявлення мережевих вторгнень, який інтегрує кластеризацію K-Means і алгоритм Random Forest для підвищення точності класифікації та зниження рівня помилкових спрацьовувань. У запропонованій методології кластеризація K-Means використовується на етапі попередньої обробки даних для їх розподілу на групи, що зменшує варіативність вхідних даних, після чого класифікація здійснюється алгоритмом Random Forest. Результати експериментальних досліджень демонструють високу ефективність запропонованого підходу.

У дослідженні [5] проведено аналіз ефективності алгоритмів машинного навчання для розробки NIDS з використанням наборів даних NSL-KDD та CSE-CIC-IDS2018. Особливу увагу приділено попередній обробці даних, яка продемонструвала суттєвий вплив на точність моделей, підвищуючи

їхню продуктивність навіть у випадку застосування базових алгоритмів. Запропоновано інтегрований підхід, що включає поєднання методів попередньої обробки та балансування класів. Це дозволило підвищити точність моделей на тестових даних на 2,94% для NSL-KDD та на 0,14% для CSE-CIC-IDS2018. Отримані результати підтверджують важливість оптимізації вхідних даних для забезпечення більшої ефективності систем виявлення мережевих атак.

На основі проведеного аналізу сучасних досліджень можна зробити висновк, що ключові виклики у розробці NIDS безпосередньо випливають із необхідності ефективного вибору моделі, її тонкого налаштування та попередньої обробки даних. Для забезпечення оптимальної роботи таких систем доцільно впроваджувати багатокомпонентний підхід, що охоплює масштабування даних, балансування вибірки, відбір релевантних ознак та оптимізацію параметрів моделі. У цьому контексті все частіше використовуються ансамблеві методи та алгоритми глибокого навчання, що дозволяють моделювати складні взаємозв'язки між даними, досягаючи високої точності. Проте впровадження подібних підходів суттєво ускладнює процес налаштування системи через високу складність моделей та значну залежність від великих обсягів даних. Це вимагає не лише наявності значних обчислювальних ресурсів, але й удосконалених методологій для налаштування та тестування. Розробка ефективних NIDS стає складним завданням що вимагає поєднання різних стратегій для досягнення балансу між точністю, швидкістю роботи та адаптивністю в умовах постійно зростаючих вимог до кібербезпеки.

Література

1. Нікітенко А., "Системи виявлення мережевих вторгнень на основі нейронних мереж глибокого навчання," *Наукові праці ДонНТУ Серія "Інформатика, кібернетика та обчислювальна техніка*, №2 (37), 2023, стр. 15-21, https://doi.org/10.31474/1996-1588-2023-2-37-15-21
2. Leon, M., Markovic, T., & Punnekkat, S. (2021). Comparative evaluation of machine learning algorithms for network intrusion detection and attack classification. *Proceedings of the International Conference on Network Security and Applications*, 16-25**.** https://doi.org/10.1109/IJCNN55064.2022.9892293
3. Abdullah, M., Balamash, A., Alshannaq, A., & Almabdy, S. (2018). Enhanced intrusion detection system using feature selection method and ensemble learning algorithms. *International Journal of Computer Science and Information Security*, *16*(2), 48-55. https://sites.google.com/site/ijcsis/
4. Khaddor, M. A., & Al-Khattib, B. (2020). Intrusion detection systems using K-Means and random forest algorithms. *International Journal of Scientific & Engineering Research*, *11*(9), 217-224. https://ijser.org
5. Нікітенко А., Соболь Є., "Ефективна модель виявлення мережевих вторгнень з використанням методів машинного навчання," Наукові праці ДонНТУ Серія "Інформатика, кібернетика та обчислювальна техніка," №2 (39), 2024, стр. 57-65, https://iktv.donntu.edu.ua/wp-content/uploads/2024/11/07_nykytenko.pdf

Анотація

З розвитком програмного забезпечення та мережевих технологій питання захисту мережевих пристроїв від атак стає надзвичайно важливим. Системи виявлення мережевих вторгнень (NIDS) використовують методи машинного навчання для аналізу трафіку та виявлення аномалій. Розробка ефективних NIDS вимагає оптимізації вибору ознак і налаштування моделей для забезпечення високої точності і швидкості в реальному часі. У роботі розглядаються різні підходи до покращення продуктивності NIDS, зокрема використання комбінованих методів машинного навчання для досягнення балансу між точністю, швидкістю та адаптивністю системи.

Ключові слова: мережеві вторгнення, системи виявлення мережевих вторгнень, машинне навчання, класифікація, кластеризація.

Abstract

As software and networking technologies evolve, the issue of protecting network devices from attacks is becoming increasingly important. Network intrusion detection systems (NIDS) use machine learning techniques to analyze traffic and detect anomalies. Developing effective NIDS requires optimizing the selection of features and tuning models to ensure high accuracy and speed in real time. The paper discusses various approaches to improving NIDS performance, including the use of combined machine learning methods to achieve a balance between accuracy, speed, and system adaptability.

Keywords: network intrusions, network intrusion detection systems, machine learning, classification, clustering.

ІНТЕЛЕКТУАЛЬНИЙ МОНІТОРИНГ ДІЙ КОРИСТУВАЧІВ. РОЗРАХУНОК ТА ПЕРЕДБАЧЕННЯ ЕФЕКТИНОВСТІ СПІВРОБІТНИКІВ

Терехов Є.Р. , магістр ІПЗм-23а, yehor.terekhov.kita@donntu.edu.ua;
Донецький національний технічний університет, Дрогобич, Україна

Моніторинг активності користувачів - складна і багатогранна область, що об'єднує технічні, психологічні, правові та етичні аспекти. Його теоретична основа полягає в тому, як люди взаємодіють з інформаційними системами і як цю взаємодію можна виміряти, проаналізувати та використовувати для досягнення певних цілей.

Основна ідея моніторингу активності користувачів полягає в зборі та аналізі даних про діяльність користувачів в системі для підвищення ефективності, забезпечення безпеки та дотримання нормативних вимог. Це включає відстеження різних форм взаємодії з комп'ютером або мережею.

Основними параметрами в системних логах є ідентифікатор події, дата і час, користувач, програма та тривалість. Формат системних логів повинен бути стандартизованим та читабельним як для людини, так і для машинної обробки. Часто використовуються чіткі розділювачі та позначення параметрів, що дозволяє легко парсити та аналізувати логи за допомогою скриптів або спеціалізованих інструментів. Структурований підхід до формату логів забезпечує ефективність в обробці великих обсягів даних та точність у виявленні необхідної інформації. Приклад структуризації логів наведено на рисунку 1.

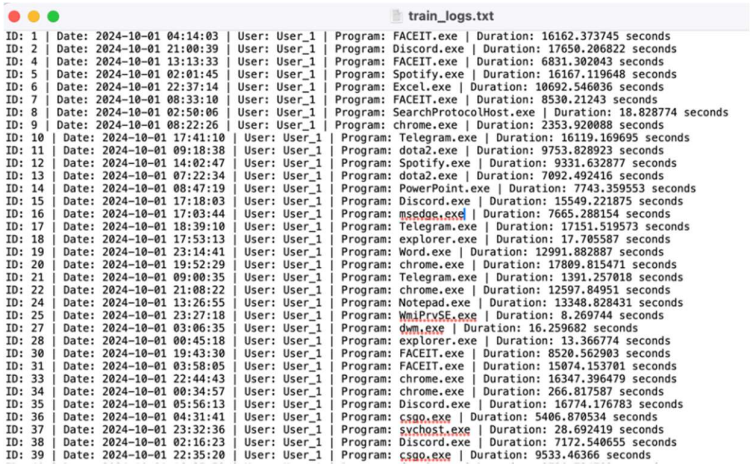


Рисунок 1 – База сгенерованих логів

KPI (Key Performance Indicators) — це ключові показники ефективності, які дозволяють оцінювати досягнення користувача у виконанні завдань

та їх продуктивність. Для кожного запису активності користувача KPI обчислюється як сума базових балів, модифікаторів залежно від умов і контексту наведено у формулі 1.

$$KPI = B + D + F + C + P \quad (1)$$

У цій формулі рахується сума базового балу (B), тривалості активності (D), рівня фокусу, модифікатору контексту (C) і ваги проєкту (P). Для цього потрібно побудувати таблицю міток для кожного логу. Мітки доповнюють логи, класифікуючи їх за рівнями продуктивності, контекстом та іншими параметрами. Поєднання логів і міток дозволяє аналізувати активності користувача з двох точок зору: тривалості та часу використання програм, а також їхньої продуктивності та ефективності. Аналіз тривалості й часу використання допомагає визначити, які програми використовуються найчастіше і скільки часу на них витрачається, тоді як мітки надають змогу зрозуміти, наскільки корисною була конкретна активність для виконання робочих завдань або досягнення цілей.

Архітектура нейронної мережі для передбачення KPI базується на обробці вхідних даних, які містять як числові, так і категоріальні ознаки. Числові дані, такі як "Productive", "Short", та "FocusLevel", проходять нормалізацію, що дозволяє зробити їх більш стабільними для навчання моделі. Ці дані передаються через повнозв'язний шар (Dense) із функцією активації ReLU, що дозволяє виявляти нелінійні залежності. Після цього використовується Dropout для запобігання перенавчанню, відключаючи випадкові нейрони під час навчання.

Категоріальні ознаки, такі як "WorkHours", "Efficient", "ActivityType", "Context", та "Project", обробляються через Embedding Layer, що дозволяє створити числове представлення для кожної категорії. Кожен категоріальний вхід проходить через окремий Embedding Layer, а отримані вектори об'єднуються через Concatenate Layer. Після цього об'єднаний вектор категоріальних ознак передається через шар Dense із функцією активації ReLU для додаткової обробки. У Dense-шарі кожен нейрон має свою вагу, яка використовується для обчислення лінійної комбінації вхідних значень. Потім до цієї комбінації додається зміщення, після чого застосовується функція активації. Математично це реалізовано у формулі 2.

$$y=f(Wx+b) \quad (2)$$

У формулі 2: W — матриця ваг (розміром кількість вихідних нейронів x кількість вхідних нейронів), x — вектор вхідних значень, b — вектор зміщення, f — функція активації, y — вихідний вектор після застосування функції активації.

Після побутови архітектури нейроної мережі було проведено навчання моделі а також проведено тестування, яке зображено на рисунку 2.

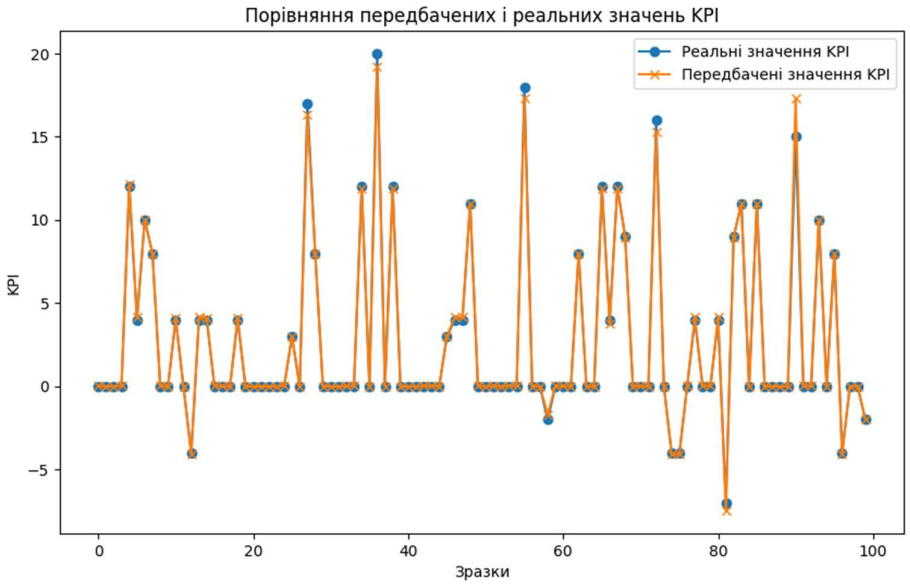


Рисунок 2 – Результати тестування нейронної мережі

Графік показує, що передбачення нейронної мережі дуже близькі до реальних значень KPI, що свідчить про хорошу навчальну здатність моделі.

Література

1. Даньків, Й. Я. Облік і контроль використання робочого часу / Й. Я. Даньків, М. Я. Остап'юк, Л. І. Калинчук / Ужгород : УжНУ, 2013. – Вип. 3(40). – с. 263

2. А. Богосян Нейронні мережі для автоматичного побудови моделі / А. Богосян, Д. Браун, С. Зак, 2022. — 210 с.

Анотація

У роботі представлено дослідження нейронної мережі для передбачення ключових показників ефективності (KPI) на основі вхідних даних. Продемонстровано результати навчання та тестування моделі, які свідчать про високу точність прогнозів. Робота спрямована на підвищення ефективності оцінки продуктивності через аналіз системних логів.

Ключові слова: нейронна мережа, KPI, передбачення, машинне навчання.

Abstract

The study presents research on a neural network for predicting key performance indicators (KPI) based on input data. The results of model training and testing are demonstrated, indicating high prediction accuracy. The work is aimed at improving the efficiency of performance evaluation through the analysis of system logs.

Keywords: neural network, KPI, prediction, machine learning.

РАДІОЛОКАЦІЙНІ СИСТЕМИ КЕРУВАННЯ ПОЛЬОТОМ ВЕРТОЛЬОТА: НОВІ МЕТОДИ ОБРОБКИ СИГНАЛІВ

Сич С.В., e-mail: tslihar6@gmail.com
Кременчуцький льотний коледж Харківського національного університету внутрішніх справ, Кременчук, Україна

Розвиток авіаційних технологій відкриває нові горизонти в автоматизації керування польотом повітряних суден, зокрема вертольотів. Радіолокаційні системи відіграють важливу роль у забезпеченні безпеки та точності виконання польотних завдань. В умовах складної метеорологічної обстановки, обмеженої видимості та високої щільності повітряного руху особливо актуальними стають нові методи обробки радіолокаційних сигналів. У цих тезах розглядаються інноваційні підходи до реалізації таких систем із фокусом на їх застосування в сучасній авіоініці вертольотів.

Загальна характеристика радіолокаційних систем вертольотів

Радіолокаційна система керування польотом вертольота (РЛС) є інтегрованою частиною бортового обладнання, яка забезпечує виявлення перешкод, моніторинг траєкторії та навігаційну підтримку. Типова РЛС включає такі компоненти:

- Радіолокаційний передавач і приймач для випромінювання і прийому сигналів.
- Антени з високою просторовою роздільною здатністю.
- Бортовий обчислювальний комплекс для обробки сигналів і формування інформації для екіпажу.
- Засоби інтерфейсу для передачі даних на дисплеї або у систему автопілота.

Головними функціями сучасних РЛС є:

- Виявлення та класифікація перешкод (гори, дерева, будівлі, інші повітряні судна).
- Допомога в виконанні польотів за складних погодних умов.
- Забезпечення навігації в режимах низької висоти.

Виклики у сучасних РЛС:

Традиційні методи обробки радіолокаційних сигналів, такі як лінійна фільтрація, мають обмеження у випадках значного рівня шуму, багатошляхового розповсюдження сигналів та швидкозмінного рельєфу місцевості. Це вимагає впровадження нових підходів, які дозволять:

- Підвищити точність виявлення малорозмірних перешкод.
- Забезпечити високу швидкість обробки даних.
- Зменшити вплив паразитних сигналів і спотворень.

Нові методи обробки сигналів

Методи машинного навчання (ML):

Інтеграція алгоритмів машинного навчання дозволяє суттєво покращити обробку радіолокаційних даних. Зокрема, глибокі нейронні мережі (DNN) використовуються для: класифікації об'єктів за їх сигнатурами; розпізнавання перешкод на основі аналізу багатоканальних даних; прогнозування траєкторій руху об'єктів.

ML-алгоритми також здатні навчатися на реальних польотних даних, що забезпечує адаптацію до конкретних умов експлуатації.

Методи когнітивного радіолокаційного оброблення:

Когнітивні системи використовують дані з радіолокаційного каналу та інших сенсорів для адаптивного налаштування параметрів роботи РЛС. Це дозволяє: змінювати ширину променя залежно від завдань; оптимізувати частотний спектр для уникнення перешкод; використовувати динамічне управління потужністю випромінювання.

Методи стискання даних без втрат:

Для оптимізації передачі радіолокаційної інформації використовуються алгоритми стискання даних, наприклад, методи адаптивного квантування або хвильового перетворення. Вони дозволяють зменшити обсяг даних, що передаються в реальному часі, без втрати ключової інформації.

Фазові антени з електронним скануванням (ФАР):

Використання ФАР забезпечує швидке перемикання напрямку радіолокаційного випромінювання без рухомих частин. Це суттєво підвищує швидкодію системи та точність визначення координат.

Інтеграція з інерційними навігаційними системами (ІНС):

Поєднання РЛС та ІНС дозволяє отримати додаткові дані про положення і рух вертольота навіть у випадках, коли радіолокаційний сигнал зазнає значних спотворень.

Практичне застосування радіолокаційних систем у вертольотах

Сучасні авіаційні комплекси, такі як Airbus H-145 та Sikorsky UH-60, активно інтегрують удосконалені РЛС із новими методами обробки сигналів. Наприклад, у вертольоті H-145 використовується інтелектуальна система Avoidance Radar, яка здатна автоматично формувати траєкторію обходу перешкод, спираючись на дані з РЛС та GPS.

У вертольотах військового призначення, таких як UH-60 Black Hawk, впровадження адаптивних алгоритмів дозволяє забезпечувати високу точність у складних умовах, таких як нічні польоти в горах.

Перспективи розвитку

Подальший розвиток радіолокаційних систем для вертольотів залежить від: розробки більш ефективних алгоритмів обробки сигналів, зокрема квантових обчислень; розширення інтеграції з іншими бортовими сенсорами

(оптичними, тепловізійними); зменшення енергоспоживання систем завдяки використанню нових матеріалів і технологій.

Нові методи обробки сигналів для радіолокаційних систем керування польотом вертольотів дозволяють значно підвищити ефективність, безпеку та адаптивність авіаційних комплексів. Впровадження таких технологій в авіоніці вертольотів сприяє вдосконаленню автоматизації польотів, зменшенню ризиків зіткнень і забезпеченню точного виконання завдань у складних умовах.

Література

1. Airbus Helicopters: Official technical documentation on H-145 radar systems.
2. Sikorsky Innovations: Adaptive Radar Systems in Black Hawk Series.
3. Mitchell, J. Cognitive Radar Systems: Applications in Aviation. IEEE, 2023.
4. Zhang, T., & Wang, Y. Deep Learning Techniques for Radar Signal Processing. Springer, 2022.

Анотація

У тезах висвітлено сучасні інноваційні підходи до радіолокаційних систем керування польотом вертольотів. Описано основні компоненти систем, їх функції та виклики, що виникають у сучасній авіоніці. Особливу увагу приділено новим методам обробки сигналів, таким як машинне навчання, когнітивне радіолокаційне оброблення та інтеграція з іншими сенсорами. Практичні приклади стосуються вертольотів Airbus H-145 та Sikorsky UH-60. Розглянуто перспективи розвитку технологій для підвищення безпеки та ефективності польотів.

Ключові слова: радіолокаційні системи, вертольоти, управління польотом, машинне навчання, когнітивне радіолокаційне оброблення, обробка сигналів, інерційна навігація, автоматизація, Airbus H-145, Sikorsky UH-60.

Abstract

The theses discuss innovative approaches to helicopter flight control radar systems. Key components, functions, and challenges of modern avionics are described. Special focus is given to advanced signal processing methods, including machine learning, cognitive radar processing, and sensor integration. Practical examples feature Airbus H-145 and Sikorsky UH-60 helicopters. The prospects of technological advancements aimed at improving flight safety and efficiency are outlined.

Keywords: radar systems, helicopters, flight control, machine learning, cognitive radar processing, signal processing, inertial navigation, automation, Airbus H-145, Sikorsky UH-60.

ВИКОРИСТАННЯ CASE-ЗАСОБІВ ДЛЯ КЕРУВАННЯ ВИМОГАМИ ПРИ РОЗРОБЦІ ГОЛОСОВОГО АНАЛІТИКА НА ОСНОВІ ШІ

Жаркіх С.Є., sofiia.zharkikh@nure.ua;
Морозова А.І., кандидат технічних наук, доцент,
anna.morozova@nure.ua
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасна розробка програмного забезпечення, особливо систем на основі Штучного Інтелекту (ШІ), є складним і багатоетапним процесом, що потребує ретельного управління вимогами. Управління вимогами відіграє ключову роль у забезпеченні якості та відповідності кінцевого продукту потребам користувачів. Це особливо актуально для проєктів, які використовують інноваційні технології та розробляються для вирішення специфічних завдань, таких як аналіз мовлення. Раціональним вибором для оптимізації цього процесу є використання CASE-засобів, які автоматизують структурування, аналіз та управління вимогами.

Головною метою даного дослідження є розробка системи голосового аналітика, здатної аналізувати аудіо мовлення користувачів. Основні функції системи включають визначення вимови, граматики, а також підтримку емоційного аналізу. Використовуючи записані аудіофайли, система порівнює їх з еталонними даними та надає персоналізовані рекомендації для покращення якості мовлення. Ефективність і точність аналізу забезпечуються завдяки використанню глибоких нейронних мереж, зокрема архітектури LSTM (Long Short-Term Memory). Це дозволяє системі не лише обробляти поточні дані, а й зберігати контекст та враховувати довготривалі залежності у мовленні користувача.

Успішна реалізація подібного проєкту неможлива без ретельного управління вимогами. На цьому етапі критично важливо правильно формалізувати як функціональні, так і нефункціональні вимоги до системи [1]. Для вирішення цих завдань можуть бути використані CASE-засоби, які забезпечують автоматизацію процесу аналізу вимог, покращуючи якість і скорочуючи час розробки. Зокрема, IBM Rational DOORS обрано для управління вимогами, оскільки цей інструмент дозволяє відстежувати всі зміни на етапах проектування та розробки, а також забезпечує прозорість усього процесу [2].

Для моделювання архітектури системи доцільно використовувати Enterprise Architect, за допомогою якого можуть бути створені UML-діаграми, що чітко відображають основні процеси роботи аналізатора мовлення. Крім того, Jira - це якісний сервіс, що може допомогти впорядкувати

завдання команди розробників та відстежувати прогрес виконання, зокрема ідентифікуючи потенційні ризики ще на етапі формування вимог.

Технічна реалізація системи включає розробку кількох взаємопов'язаних компонентів. Перший компонент займається автоматичним розпізнаванням мовлення (ASR) за допомогою технологій Natural Language Processing (NLP). Другий – синтаксичним і морфологічним аналізом мовлення. Третій компонент включає емоційний аналіз, який допомагає визначити тональність та емоційний стан користувача, що особливо важливо для освітніх платформ або сервісів підтримки.

Технічна реалізація системи включає розробку моделей для автоматичного розпізнавання мовлення (ASR), синтаксичного та морфологічного аналізу, верифікації вимови користувача, а також емоційної зчитки. Важливим компонентом є інтеграція механізму рекомендацій, що базується на результатах аналізу [3]. Наприклад, користувач отримує зворотний зв'язок щодо помилок у вимові, граматиці чи використанні інтонацій, а також пропозиції для покращення цих аспектів.

Додаткову увагу приділено візуалізації результатів аналізу. За допомогою технології WebGL та бібліотеки Three.js розроблено інтерактивний інтерфейс, що надає графічне відображення даних. Користувач може в реальному часі переглядати свої помилки у вигляді зрозумілих 3D-графіків, які демонструють проблемні зони у вимові, граматиці чи інтонації. Це робить процес навчання більш інтерактивним і мотивуючим [4].

Результати тестування прототипу показали, що інтеграція CASE-засобів у процес розробки сприяє зменшенню кількості помилок і покращенню точності аналізу мовлення. Такий підхід дозволяє ефективніше впроваджувати зміни, адаптуючи систему до нових вимог, а також оптимізувати роботу команди. У майбутньому передбачається інтеграція додаткових мов та розширення системи для підтримки різних освітніх платформ.

Напрямки подальших досліджень включають адаптацію системи до багатомовного середовища, зокрема інтеграцію мов із тональними чи граматичними особливостями. Також перспективним є впровадження адаптивного навчання, яке враховуватиме індивідуальні особливості кожного користувача. Окрім освітніх завдань, система може бути застосована у медицині для діагностики мовних порушень чи в бізнесі для оцінювання комунікативних навичок.

Таким чином, розробка голосового аналітика, що базується на ШІ, у поєднанні з сучасними CASE-засобами та інструментами візуалізації відкриває нові можливості для вдосконалення освітніх процесів і підвищення ефективності комунікації.

Література

1. Software Engineering Transparencies. Addison Wesley, 2015. 600 с.

2. Thurimella A. K., Janzen D. Metadoc Feature Modeler: A Plug-in for IBM Rational DOORS. *2011 15th International Software Product Line Conference (SPLC)*, м. Munich, Germany, 22–26 серп. 2011 р. 2011. URL: https://doi.org/10.1109/splc.2011.17 (дата звернення: 02.12.2024).

3. Alla S., Adari S. K. Long Short-Term Memory Models. *Beginning Anomaly Detection Using Python-Based Deep Learning*. Berkeley, CA, 2019. С. 213–256. URL: https://doi.org/10.1007/978-1-4842-5177-5_6 (дата звернення: 02.12.2024).

4. Guha S. WebGL. *Computer Graphics Through OpenGL®*. 4-те вид. Boca Raton, 2022. С. 549–560. URL: https://doi.org/10.1201/9781003287452-26(дата звернення: 02.12.2024).

Анотація

Використання CASE-засобів для управління вимогами при розробці системи голосового аналітика на основі Штучного Інтелекту. Створення ефективної системи, яка аналізує аудіо мовлення користувачів, а також застосування IBM Rational DOORS для управління вимогами, Enterprise Architect для моделювання архітектури системи та Jira для моніторингу прогресу. Опис можливості візуалізації результатів за допомогою WebGL та бібліотеки Three.js.

Ключові слова: CASE-засоби, візуалізація, голосовий аналітик, управління вимогами, штучний інтелект, WebGL, LSTM.

Abstract

The Use of CASE Tools for Requirements Management in the Development of an AI-Based Voice Analytics System. The creation of an efficient system that analyzes users' audio speech and the application of IBM Rational DOORS for requirements management, Enterprise Architect for system architecture modeling, and Jira for progress monitoring. A description of the possibilities for result visualization using WebGL and the Three.js library.

Keywords: CASE-tools, requirements management, voice analytics, artificial intelligence, WebGL, LSTM, visualization.

ВИКОРИСТАННЯ МЕТОДУ OSINT ПРИ ПРОВЕДЕННІ ЖУРНАЛІСТСЬКОГО РОЗСЛІДУВАННЯ

Сенкевич Г.А., кан.наук із соц. ком., доцент кафедри журналістики, gen.senkevich@gmail.com
Вейпан А.О., студентка gen.senkevich@gmail.com
Університету митної справи та фінансів

Журналістське розслідування є одним з найцікавіших жанрів у журналістській діяльності. Воно є кропітким та довготривалим, бо передбачає не тільки пошук інформації, а ще й наполегливу та кропітку роботу з її перевірки, підтвердження попре небажання деяких посадових осіб її оприлюднити. Девід Рендал у своєї книжці «Універсальний журналіст» констатує, що, навіть, первинне розслідування - це «не огляд та не зведення докупи чужих даних та свідчень, а дослідження, яке проводять репортери найчастіше на основі «сирого» матеріалу. Це може бути або проведення великої кількості інтерв'ю, або підбір та співставлення фактів та цифр» [3; с. 54]. Тобто розслідування, на його думку, є тривалою роботою, а не банальним порівнянням фактів та документів. Але точно ніхто доки не визначив, скільки часу треба витратити аби матеріал мав би ознаки журналістського розслідування.

Якщо говорити про якісний матеріал, то його виконанням є не тільки збір даних та підтвердження власної гіпотези, а ще й ретельна перевірка фактури, яка може зайняти набагато більше часу, ніж всі попередні заходи. В деяких випадках треба порівнювати не два, а декілька джерел інформації, визначаючи, котрі з них можуть вважатися достовірними, а яким можна довіряти на рівні чуток. До речі, чутки та плітки теж не можна ігнорувати як джерела інформації, адже в них міститься майже завжди доля правди.

Соціальні мережі відкрили для журналіста-розслідувача безмежний простір даних, котрі допоможуть знаходити і коментарі фахівців, і думки експертів, і архівні дані, і деталі, без яких будь-яке розслідування неможливе. Саме вони дуже часто складають основу доказової бази. Деталізація визначає точність, а точність називають одним з головних стандартів журналістики.

Під час перевірки журналіст повинен ставити запитання до джерел інформації таким чином, щоб інформація ставала щільнішою, зростали її точність і деталізацію. Твердження, що суперечать одне одному, змушують журналіста розширити кількість джерел інформації [2].

Зазвичай журналісти-розслідувачі працюють із різними джерелами, у тому числі з публічними документами, кількість яких може бути вражаючою. Великий обсяг часу займає і робота зі свідками та з конфіденційними джерелами. І не завжди витрачений час може бути ефективним. Саме тоді доречно звернутись по допомогу до OSINT. Використовуючи цифрові бази

даних, блоги, сайти та інші загальнодоступні джерела, журналісти можуть у рази скоротити час пошуку, знайти вірне рішення шляхом застосування комп'ютерної програми. А кваліфікований фахівець з обробки інформації може навіть аналізувати супутникові знімки та топографічні елементи. Останнім часом використання штучного інтелекту надає ще більше можливостей для пошуку і обробки інформації. Google Maps і Google Earth допомагають знаходити візуальні елементи, порівнювати фотознімки та інші зображення, що раніше відносилося до компетенції експертів.

Безперечно, одна з найпотужніших можливостей OSINT — це здатність виявляти приховані зв'язки та закономірності. Відстежуючи зв'язки між особами, установами та подіями, журналісти-розслідувачі можуть краще зрозуміти складні питання. Це цінно в таких сферах, як політика чи економіка, де відносини між різними суб'єктами інколи навмисно приховують. Саме прихована інформація відрізняє журналістське розслідування від пересічного дослідження, тому дуже важливо мати не тільки надійний інструмент пошуку, а ще й доказу, верифікації.

Основна ідея OSINT – цілеспрямований збір інформації (harvesting) щодо об'єкта зацікавленості з метою подальшої обробки та різновекторного контент-аналізу отриманих даних та інтерпретації кінцевих результатів (створення інформаційного «портрету» особи, виявлення неочевидних фактів чи зв'язків, прогноз її ймовірної поведінки тощо) [5; с. 4].

Однією з ключових переваг OSINT-розвідки є її економічна ефективність, більша за традиційні методи журналістських розслідувань. Замість того, щоб наймати команду дослідників або приватних детективів, журналісти можуть використовувати безоплатні або недорогі інструменти для збору та аналізу інформації [1]. Дуже часто розслідуванням займаються команди журналістів, навіть з різних країн. Вони об'єднуються переважно не для того, щоби обробляти великі масиви даних, а зазвичай через те, що існує перешкода пересуванню, інколи людині загрожує небезпека тощо.

OSINT може інколи допомогти журналістам виявити тенденцію, зробити нескладний прогноз. Відомі також приклади, котрі допомагали відстежувати злочинну або екстремістську діяльність, а також контролювати певні організації або угрупування. Подібна здатність може бути особливо цінною у розслідуваннях фактів корупції, порушень прав людини та інших злочинах у будь-якій сфері.

Журналістське розслідування фахівці називають найскладнішим журналістським жанром, котрий об'єднує в собі ознаки інтерв'ю, портрету, репортажу, хроніки, аналізу, синтезу. Завдання розслідування – захопити увагу читача унікальною ситуацією і потім пояснити її сенс, примусити його замислитися над глибокими моральними категоріями, бо саме вони є підґрунтям до дій людини, до його вчинків [4; с. 4].

Дехто з фахівців відносить OSINT до інформаційної розвідки, проте можливості даного інструменту набагато ширші, бо він охоплює пошук,

аналіз, верифікацію і прогноз, значно полегшуючі розслідувальну діяльність та роблячи її ефективною.

Література

1.Вайсберга Нікола. OSINT-розвідка у роботі журналістів. URL: https://youcontrol.com.ua/articles/osint-in-journalists-work/ (Дата звернення 4.12.2024).

2. Квіт С. М. Масові комунікації: підручник для студентів ВНЗ. Київ: Видавничий дім «Києво-Могилянська академія». 206 с. URL: http://politics.ellib.org.ua/pages-8975.html (Дата звернення 4.12.2024).

3. Рендал Девід. Універсальний журналіст. Видавництво Інституту журналістики КНУ ім. Тараса Шевченка. 2006. 362 с.

4. Сенкевич Г. А. Посібник з журналістських розслідувань. Теоретичний та практичний аспекти. Дніпро, 2021. 220 с.

5. Червяков О. І., Зоренко Д. С., Лех Р. В., Кулик Д. О. Використання інструментів та методів OSINT для отримання пошукової інформації: практичний порадник Харків: ІПЮК для СБУ, 2023. 36 с. URL: https://dspace.nlu.edu.ua/bitstream/123456789/19712/1/P_OSINT.pdf (Дата звернення 4.12.2024).

Анотація.

Представлені тези присвячені застосування методу OSINT у журналістському розслідуванні. Розглянуто його основна ідея, переваги та можливості у роботі з інформацією, а також ефективність та напрями використання.

Ключові слова: фактура, база даних, джерела інформації, аналіз.

Abstract.

The theses presented are devoted to the application of the OSINT method in journalistic investigation. Its main idea, advantages and opportunities in working with information, as well as effectiveness and directions of use are considered.

Key words: texture, database, sources of information, analysis.

КЛАСИФІКАЦІЯ ФІШИНГОВИХ АТАК З ВИКОРИСТАННЯМ АЛГОРИТМІВ МАШИННОГО НАВЧАННЯ

Масло А.А., студент, andrii.maslo.kita@donntu.edu.ua;
Нікітенко А.О., асис. кафедри ПМІ, andrii.nikitenko@donntu.edu.ua;
ДВНЗ «Донецький національний технічний університет», м. Дрогобич, Україна

Фішинг є однією з найпоширеніших та небезпечних форм кіберзлочинності, яка спрямована на обман користувачів з метою викрадення особистих даних: паролів, логінів, банківських реквізитів та іншої конфіденційної інформації. Основна мета таких атак – отримання доступу до фінансових ресурсів, облікових записів або приватних даних шляхом імітації довірених джерел або створення фальшивих веб-ресурсів [1].

Типи фішингових атак:

1. Deceptive Phishing – найбільш поширений вид фішингу, коли зловмисники імітують популярні компанії або сервіси з метою крадіжки даних. Така атака зазвичай виглядає як повідомлення від знайомого джерела або відомої організації, наприклад, банку чи інтернет-магазину;
2. Spear Phishing – таргетовані атаки, орієнтовані на конкретних осіб чи організації. Такі атаки зазвичай набагато складніші і використовують персоналізовані елементи, такі як імена, адреси або інші індивідуальні дані, щоб переконати жертву у легітимності повідомлення;
3. Clone Phishing – метод, при якому зловмисники дублюють легітимний електронний лист з підробленими посиланнями або вкладеннями. Цей вид фішингу часто використовує вже відправлені листи, підмінюючи лише частину інформації;
4. Whaling – атаки на важливих осіб або великий бізнес. Мета таких атак — отримання доступу до цінної інформації або фінансових ресурсів через цільові фішингові кампанії проти топ-менеджерів або корпоративних користувачів;
5. Email, SMS, Social Media Phishing – фішинг через різні канали комунікації, такі як електронні листи, текстові повідомлення або соціальні мережі. Це дозволяє зловмисникам охоплювати широку аудиторію та збільшувати шанси на успіх атаки [2].

Фішингові атаки ґрунтуються на використанні фальшивих доменів, шкідливого програмного забезпечення та ботнетів. Зловмисники можуть реєструвати домени, схожі на легітимні, або використовувати існуючі веб-ресурси для маніпуляцій. Крім того, часто застосовуються техніки, які дозволяють приховати справжній характер посилань, таких як редиректи або фальшиві HTTPS-з'єднання.

Традиційні методи боротьби з фішингом, такі як спам-фільтри, підписання електронної пошти та базова перевірка URL-адрес, є важливими, але

не завжди достатніми. Зловмисники постійно вдосконалюють свої методи, тому необхідно застосовувати сучасні підходи для більш ефективного захисту. Основні інноваційні технології включають:

1. Машинне навчання (Machine Learning): Алгоритми машинного навчання використовують дані для виявлення підозрілих ознак у текстах електронних листів або веб-сторінок, таких як структура тексту, URL-адреси чи інші аномалії;
2. Обробка природної мови (Natural Language Processing): Цей підхід дозволяє здійснювати контекстуальний аналіз текстів, виявляючи маніпуляції або непослідовності в змісті повідомлення;
3. Глибоке навчання (Deep Learning): Використання складних моделей глибинного навчання дозволяє підвищити точність виявлення фішингових атак, обробляючи великі обсяги даних і складні патерни.

Класифікація фішингових листів — ключовий напрямок в кібербезпеці, що передбачає використання алгоритмів машинного навчання для автоматизації процесу виявлення фішингових атак. З розвитком технологій ці алгоритми стали набагато точнішими та ефективнішими, дозволяючи значно знизити кількість успішних атак. Серед популярних алгоритмів для класифікації фішингових листів виділяють [6]:

1. Рішення дерев: Це прості і зрозумілі алгоритми, що використовуються для класифікації фішингових листів. Вони поділяють дані на основі критеріїв, що максимізують інформаційний приріст, і часто використовуються для інтерпретації результатів;
2. Випадкові ліси: Це ансамблеві методи, що використовують кілька дерев рішень, щоб покращити точність. Випадкові ліси значно покращують результат в порівнянні з окремими деревами рішень завдяки здатності уникати перенавчання [4];
3. Метод опорних векторів (SVM): Цей метод є одним із найпопулярніших для класифікації текстів, зокрема для фішингових атак. SVM здатний забезпечити високу точність при розмежуванні класів, що робить його ефективним у виявленні фішингових листів;
4. Нейронні мережі: Глибокі нейронні мережі, зокрема рекурентні (Recurrent neural networks) і згорткові (Convolutional neural networks) нейронні мережі, використовуються для автоматичного виділення ознак з тексту та виявлення складних патернів у фішингових листах. Вони демонструють високі результати у розпізнаванні нових типів атак, однак вимагають великих обчислювальних ресурсів [3].

Для ефективного виявлення фішингових атак використовується порівняння різних алгоритмів машинного навчання за такими критеріями, як точність, швидкість навчання та можливість адаптації до нових даних. Основними метриками є точність (accuracy), точність виявлення (precision), повнота (recall) та F1-міра, які дозволяють оцінити ефективність класифікації [5].

У роботі [6] автори розглядають ефективність алгоритмів для виявлення фішингових атак. Зокрема, Decision Tree досяг точності 85%, специфічності 88%, F-міри 0.81, і відгуку 84%. Алгоритм XGBoost показав кращі результати: точність 92%, специфічність 95%, F-міра 0.90, і відгук 91%. SVM забезпечив точність 89%, специфічність 91%, F-міру 0.87, і відгук 88%. У вашому дослідженні гібридна модель, яка поєднувала кілька підходів, перевершила ці результати, продемонструвавши точність 94%, специфічність 96%, F-міру 0.93, і відгук 92%. Це свідчить про високу ефективність гібридних систем у складних сценаріях, де необхідно враховувати різні типи загроз.

Основні перспективи розвитку систем виявлення фішингових атак включають вдосконалення машинного навчання, інтеграцію більш складних алгоритмів і використання нових технологій, таких як блокчейн та квантові обчислення. Однак є й чимало викликів, зокрема необхідність збирання та обробки великих обсягів даних, а також постійна еволюція методів атак.

У підсумку, фішинг залишається однією з найсерйозніших загроз в сучасному цифровому середовищі. Проте інноваційні технології, зокрема використання алгоритмів машинного навчання, відкривають нові можливості для захисту від цієї небезпеки. Розвиток таких систем дозволить підвищити рівень безпеки користувачів і організацій та мінімізувати економічні та репутаційні ризики від фішингових атак [7].

У цьому дослідженні проведено аналіз сучасних методів виявлення та запобігання фішинговим атакам на електронну пошту. Розглянуто основні техніки, що використовують зловмисники, а також сучасні підходи до захисту, включаючи машинне навчання, сигнатурний аналіз та чорні списки.

Методи машинного навчання добре справляються з виявленням нових загроз, але їх застосування має певні труднощі, наприклад, потребу у великій кількості даних для навчання та ризик помилкових спрацьовувань.

У майбутніх дослідженнях планується зосередитись на покращенні точності виявлення фішингових атак за допомогою оптимізованих методів машинного навчання, що потребують менше даних для навчання.

Література

1. Banday, M.T., Qadri, J.A. (2011). "Phishing - A Growing Threat to E-Commerce," The Business Review, ISSN: 0972-8384, 12(2), pp. 76-83, https://doi.org/10.48550/arXiv.1112.5732
2. Bhavsar V., Kadlak A., Sharma S. (2018). “Study on Phishing Attacks”. *International Journal of Computer Applications*. Vol. 182, no. 33,. pp. 27–29, https://doi.org/10.5120/ijca2018918286
3. Sarpong Adu-Manu K., Kwasi Ahiable R., Sarpong K., Essel Mensah E. (2023). “Phishing Attacks in Social Engineering: A Review”. *Journal of Cyber Security*, pp. 1–29, https://doi.org/10.32604/jcs.2023.041095

4. R. R. Patil et al. (2022). “Machine learning approach for phishing website detection : A literature survey”, *Journal of Discrete Mathematical Sciences and Cryptography*, Vol. 25, no. 3, pp. 817–827, https://doi.org/10.1080/09720529.2021.2016224
5. Murti Shri Y., Naveen P. (2023). “Machine Learning Algorithms for Phishing Email Detection”. *Journal of Logistics, Informatics and Service Science*, https://doi.org/10.33168/jliss.2023.0217
6. Do N. Q., Selamat A., Krejcar O., Herrera-Viedma E., Fujita H. (2022). “Deep Learning for Phishing Detection: Taxonomy, Current Challenges and Future Directions”. *IEEE Access*, Vol. 10, pp. 36429–36463, https://doi.org/10.1109/access.2022.3151903.
7. A. Ali et al. (2022). “Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review”. *Applied Sciences*, 2022, Vol. 12, no. 19, pp. 9637, https://doi.org/10.3390/app12199637

Анотація

На сьогодні фішинг є серйозною кіберзагрозою, спрямованою на викрадення конфіденційної інформації через фальшиві веб-сайти, домени та інші методи соціальної інженерії. Сучасні підходи до його виявлення базуються на машинному навчанні, обробці природної мови та глибокому навчанні, що дозволяє автоматизувати аналіз повідомлень і значно підвищити точність класифікації. У роботі досліджуються алгоритми, такі як дерева рішень, випадкові ліси, SVM та нейронні мережі, із метою розробки оптимальних рішень для запобігання фішинговим атакам.

Ключові слова: фішинг, кіберзагрози, машинне навчання, обробка природної мови, класифікація

Abstract

Today, phishing is a serious cyber threat aimed at stealing confidential information through fake websites, domains, and other social engineering methods. Modern approaches to detecting it are based on machine learning, natural language processing, and deep learning, which allows automating message analysis and significantly improving classification accuracy. This paper explores algorithms such as decision trees, random forests, SVMs, and neural networks to develop optimal solutions to prevent phishing attacks.

Keywords: phishing, cyber threats, machine learning, natural language processing, classification

HONEYPOTS ЯК АКТИВНИЙ ЗАХИСТ ВІД КІБЕРЗАГРОЗ ІЗ ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

Кунда М.С., студент, maksym.kunda.kita@donntu.edu.ua;
Нікітенко А.О., асис. кафедри ПМІ, andrii.nikitenko@donntu.edu.ua;
ДВНЗ «Донецький національний технічний університет», м. Дрогобич, Україна

Розвиток комп'ютерів, інтернет-технологій, Інтернету речей (IoT) та штучного інтелекту (ШІ) значно трансформує різні аспекти життя сучасного суспільства. Проте з цим розвитком зростає кількість нових вразливостей в інформаційній та мережевій безпеці, а наслідки використання цих вразливостей зловмисниками стають дедалі серйознішими та руйнівними. Традиційні технології безпеки, такі як криптографія, брандмауери, системи виявлення вторгнень та механізми автентифікації, характеризуються пасивним підходом до захисту, що обмежує їхню здатність забезпечувати високий рівень безпеки в умовах сучасних загроз.

На противагу цьому, технологія honeypot представляє активну стратегію захисту, яка ефективно доповнює обмеження традиційних методів. Використання ШІ у контексті honeypot відкриває можливості для автоматизації та підвищення швидкодії системи, що сприяє оперативному реагуванню на загрози та ефективному їхньому нейтралізуванню.

Honeypot — це унікальний ресурс безпеки, який є частиною механізму безпеки, розгорнутого в організації. Головною ціллю системи honeypots є захист системи і збір інформації про дії зловмисника під час атаки. Працює ж система за принципами симуляції вразливостей для імітування роботи реальних систем, створення контрольованих середовищ для взаємодії із зловмисниками і безпеки реальних систем, фіксація усіх дій і створення журналів для можливості подальшого аналізу цих журналів із ціллю дізнатися методи проведення атак [1].

Загальна класифікація honeypot відбувається у відповідності до рівня взаємодії системи із зловмисником. Тож всі системи honeypot розподіляються на 3 основні групи [2]:

1) Honeypots високого рівня взаємодії – системи які надають високий рівень взаємодії із зловмисником створюючи можливість збору детальної інформації про дії зловмисника. Проте є дорогими у створені і вибагливими в обслуговуванні через надання зловмиснику доступу до реальної системи приховуючи важливі дані системи;
2) Honeypots низького рівня взаємодії – системи з обмеженим рівнем взаємодії, надають доступ до взаємодії із службами ftp, http, ssh, smtp, tcp/ip. Збирає невеликий обсяг даних про дії зловмисників;
3) Honeypot середнього рівня взаємодії (гібридні) – такі системи поєднують два підходи для створення більш стійкої і дієвої системи. Як і

системи низького рівня гібридні не надають доступ до реальної системи, але вони використовують методики систем високого рівня для покращення збору інформації про дії зловмисника під час атаки.

Один із найкращих способів взаємодії штучного інтелекту із honeypot це аналіз журналів створених під час взаємодії із зловмисником для вивчення інформації і прийняття рішень для протидії. Проте більшість розробників штучного інтелекту для взаємодії із honeypot зіткнулися з проблематикою відсутності даних для навчання. Так більшість даних, що надають різноманітність, зібрані системами honeypot які належать великим організаціям, а відповідно всі журнали несуть конфіденційну інформацію. Таким чином для створення дієвої системи необхідно спочатку створити підходящі набори даних. Також великою проблемою є високий рівень абстракції систем, що ускладнює взаємодію штучного інтелекту із системою. Так у honeypot використовують велику кількість методів обфускації, які приховують фактичну команду за різними методами маскування на основі оболонки.

Для навчання штучного інтелекту із даних, що знаходяться в журналі створеному honeypot необхідно вилучити основні ознаки, зазвичай за такі ознаки обирають: ip-адресу, облікові дані, дані протоколу, мітки часу і команди зловмисника.

Таблиця 1 – Журнал даних honeypot SSH [3]

Тип повідомлення	Джерело	Пункт призначення	Корисне навантаження
Підключитися	Клієнт	Сервер	{RemoteAddr: “ 183.81.169.238 ”, Country: “ HK ”} Мітка часу: 1715108300
Автентифікація пароля	Клієнт	Сервер	Ім'я користувача: «root» , пароль: «0» Мітка часу: 1715108300
Автентифікація пароля успішна	Сервер	Клієнт	Ім’я користувача: “root” , автентифіковано: “true” Мітка часу: 1715108302
Виконати програму	Клієнт	Сервер	Програма: apt update && apt install sudo curl -y && sudo useradd -m -p $ (openssl passwd -1 DPdMYqVR) system && sudo usermod -aG sudo system Мітка часу: 1715108302

Через різноманітний характер команд із подібним синтаксисом розглядати команди як рядки є неправильним підходом до аналізу. Тому у статті [3] автори пропонують використовувати LLM для аналізу команд та розуміння основного сенсу команди. Для отримання передбачуваного результату від LLM необхідно використовувати відповідні підказки. Серед мето-

дів для отримання якісних результатів зазвичай рекомендують використання ланцюжка підказок і методу рольової гри. Після цього команди все ще містять зміні такі як ім'я користувача, тому дані потребують постобробки. Для вилучення змінних було запропоновано використання бібліотеки Bashlex для розбору команд bash.

Після систематизації даних журналів створених системами honeypot під час взаємодії із зловмисниками отримуються датасети для навчання ШІ. Головний результат який очікується від ШІ це ідентифікація атаки. Для цього найкраще підходять алгоритми машинного навчання та нейроні мережі класифікатори. Класифікатори є гарним інструментом для пришвидшення визначення типу атаки, що допоможе швидше відслідкувати чи досягли зловмисники своєї мети, спрогнозувати подальші дії і покращити методи захисту для майбутніх інцидентів. Так автори статі [4] пропонують для цього використовувати алгоритми: Naïve Bayes, Decision Tree, KNN, SNN, LSMT. Всі вони є гарними класифікаторами, що мають великий потенціал в аналізі даних honeypot. Підхід LSMT вирізняється серед інших своєю оптимізацією основою його сферою є застосування в мережах IoT за рахунок низької обчислювальної складності. У тому ж дослідженні автори провели тестування всіх наведених підходів на журналах зібраних honeypot з мережі IoT. Для порівняння результатів було використано показники точності (accuracy), правильності (precision), фактичних спостережень, що передбачені правильно (recall) та f1-міри (f1-score).

	Naïve Bayes	Decision Tree	KNN	SNN	LSTM
Accuracy (%)	65	99.92	91.24	81.46	81.15
Precision (%)	94.85	99.92	91.24	67.8	65.85
Recall (%)	65	99.92	90.25	81.46	81.15
F1 Score (%)	75.37	99.92	90.55	73.13	72.7

Рисунок 1 – Продуктивність алгоритмів [4]

Аналіз сучасних досліджень надав розуміння проблематики взаємодії honeypots та ШІ, але можливий результат цієї взаємодії стане великим кроком в покращені активного кіберзахисту. Використання honeypots у поєднанні з інструментами ШІ відкриває нові можливості для ефективного виявлення, аналізу та нейтралізації атак, одночасно забезпечуючи більш глибоке розуміння поведінки зловмисників.

Література

1. A Highly Interactive Honeypot-Based Approach to Network Threat Management / X. Yang et al. *Future Internet*. 2023. Vol. 15, no. 4. P. 127. URL: https://doi.org/10.3390/fi15040127
2. Kambow N., Passi K. L. Honeypots: The Need of Network Security. International Journal of Computer Science and Information Technologies, Vol. 5 (5), 2014, 6098-6101. ISSN:0975-9646.
3. Lanka, P., Gupta, K., Varol, C. (2024). Intelligent Threat Detection—AI-Driven Analysis of Honeypot Data to Counter Cyber Threats. *Electronics*, *13*, 2465. https://doi.org/10.3390/electronics13132465
4. Ahmed Y., Beyioku K., Yousefi M. (2024). Securing smart cities through machine learning: A honeypot-driven approach to attack detection in Internet of Things ecosystems. *IET Smart Cities*. https://doi.org/10.1049/smc2.12084

Анотація

Розглянуто використання honeypots як інструменту активного кіберзахисту у поєднанні зі штучним інтелектом. Honeypots забезпечують запобігання атакам та аналіз їхніх методів, а штучний інтелект автоматизує цей процес, підвищуючи точність виявлення загроз. Увагу приділено розгляданню роботи систем honeypot, їх різновидам та застосуванню алгоритмів машинного навчання, для аналізу атак. Представлені результати, що демонструють рівень ефективності інтеграції honeypots та ШІ у вдосконаленні кіберзахисту.

Ключові слова: honeypots, штучний інтелект, машинне навчання, кіберзахист, аналіз атак, автоматизація.

Abstract

The use of honeypots as a tool for active cybersecurity combined with artificial intelligence is examined. Honeypots provide attack prevention and analysis of their methods, while artificial intelligence automates this process, improving threat detection accuracy. Attention is given to the operation of honeypot systems, their types, and the application of machine learning algorithms for attack analysis. The results demonstrate the effectiveness of integrating Honeypots and AI in enhancing cybersecurity.

Keywords: honeypots, artificial intelligence, machine learning, cybersecurity, attack analysis, automation.

ДОСЛІДЖЕННЯ РЕЖИМІВ ОБ'ЄДНАННЯ КАНАЛУ FRONTHAUL ДЛЯ АРХІТЕКТУРИ CLOUD RADIO ACCESS NETWORK

Токар Л.О.[1], к.т.н., доц., liubov.tokar@nure.ua;
Солоділов В.В.[1], victor.solodilov@nure.ua;
Токар Д.І.[2], dimas1998tr@gmail.com.

[1] Харківський національний університет радіоелектроніки, Харків, Україна
[2] Handicap International - Humanity&Inclusion, Харків, Україна

Актуальність питання.

Архітектуру C-RAN забезпечує канал fronthaul, де блоки Baseband Unit (BBU) розміщуються на відстані від розподілених модулей Remote Radio Module (RRM). Витрати RRM значно нижчі порівняно з традиційними базовими станціями (БС). Використання централізованого пулу BBU значно скорочує кількість необхідних вузлів та дає можливість в об'єднанні ресурсів у великомасштабну мережу, що має перевагу для підтримки зростання безпроводових даних.

Сегмент fronthaul є транспортною мережею з високими вимогами: високою пропускною здатністю, меншою затримкою та точною синхронізацію. Основними факторами, що виникають при розгортанні архітектури C-RAN слід назвати: необхідність у розробці методів взаємодії, взаємопідключення та кластеризації BBU, необхідність вибору методів віртуалізації для пулу BBU та скоординованій обробці трафіку.

Особливістю архітектури C-RAN є те, що об'єднання між BBU і RRM змінюються динамічно, дозволяючи одному BBU підключатися до одного або декількох RRM. За рахунок розподілу BBU по RRM відповідно до навантаження трафіку досягається зниження витрат шляхом скорочення кількості BBU та ефективного використання ресурсів основної смуги частот. Ці питання й визначають актуальність роботи.

Відомі дослідження та публікації.

В роботі проведено огляд підходів для побудови та дослідження в мережі C-RAN. Основну увагу приділено забезпеченню об'єднання BBU та RRM з надійними та гнучкими з’єднаннями й високою пропускною здатністю. У роботі [1] проведено оцінку обсягу ресурсів, необхідних для обробки даних BaseBand в мобільній мережі C-RAN, де отримано виграш від статистичного мультиплексування в BBU. У роботі [2] показана необхідність дослідженні динамічної структури fronthaul/backhaul в мережі мобільного зв'язку 5G на основі системи зв'язку Free Space Optical (FSO). У роботі [3] проведено дослідження, спрямоване на зменшення затримок в архітектурі C-RAN з віртуалізованим пулом BBU з оптимізацією кількості активних Remote Radio Head (RRH)/BBU-блоків в пулі BBU. Поряд з тим, у роботі [4]

зазначено, що правильне агрегування RRH і призначення їх одному пулу BBU надасть можливість полегшити Coordinated Multipoint (CoMP). У роботі [5] запропоновано архітектуру Colony-RAN, яка може динамічно змінювати з'єднання BBU і RRH відповідно до вимог трафіку. У роботі [6] показано, що мультиплексний виграш C-RAN при централізації обробки основної смуги частот у віртуальному пулі БС покращує продуктивність системи.

Постановка задачі.

У системах зв'язку технології 4G для обробки трафіку працюють БС, в результаті чого потрібна велика кількість БС або ресурсів основної смуги частот. Це призводить до додаткового збільшення витрат. Навпаки, в системах зв'язку технології 5G з централізованою архітектурою C-RAN значно скорочується кількість БС на об'єктах, необхідних покриття тих самих територій, що у свою чергу призводить до значного зниження потужності.

Таким чином, завдання об'єднання BBU і RRM, що динамічно змінюються, є необхідним в контексті розподілу BBU по RRM з урахуванням навантаження, слідством якого буде зниження витрат при скороченні кількості BBU та ефективного використання ресурсів основної смуги частот.

Основний матеріал та результати досліджень.

Архітектура C-RAN має функцію об'єднання BBU, яка може змінювати комбінації BBU та RRM. Загальна тенденція до використання ресурсів BBU у зонах покриття модулів RRM не перевищує одиниці. Отже, декілька RRM можуть оброблятися одним BBU. Основна мета дослідження полягає у зменшенні кількості призначень BBU.

Для реалізації функцій об'єднання BBU введено такі умови: скорочення BBU — BBU призначаються RRM так, щоб було якнайменше призначених BBU; агрегація RRM — сусідні RRM призначаються тому самому BBU, коли це можливо. Це дасть можливість полегшення деяких елементів керування між сусідніми RRM. В роботі проведено дослідження з використанням режимів об'єднання BBU-RRM, що архітектурно відповідає каналу fronthaul: динамічних режимів R_A та R_B. Режими R_A та R_B працюють для коротких часових інтервалів. При цьому об'єднання між BBU і RRM перевіряються через певні проміжки часу в залежності від використання ресурсів BBU. Ресурс BBU є необхідним для обробки трафіку даних RRM в одиницю часу. Коли використання ресурсів BBU перевищує верхню межу, деякі RRM, призначені BBU, можуть бути переключені на інші призначені BBU. Такі режими мають високу складність для перемикання BBU-RRM, що пов’язано з коротким часовим інтервалом для перемикання, однак їх можна застосовувати до транспортного навантаження, яке значно коливається. Робота виконується, коли використання ресурсу BBU нижче за верхню межу (режим R_A) або вище за нижню межу (режим R_B). На рис. 1 показано схему алгоритму використання ресурсів BBU-RRM для режимів R_A та R_B.

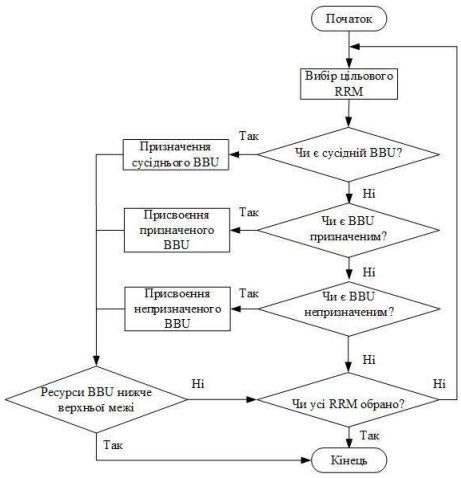


Рисунок 1. Схема алгоритму використання ресурсів BBU-RRM

Цільовий RRM вибирається відповідно до двох пріоритетів: 1) найбільша кількість сусідніх RRM; 2) найменше навантаження трафіку (крок 1). BBU призначається цільовому RRM відповідно до встановлених пріоритетів (крок 2). Після кроку 2 підтверджується використання ресурсів BBU нижче верхньої межі (крок 3). Якщо так, то процедуру перемикання BBU-RRM завершено, в іншому випадку відбувається перевірка, доки не будуть обрані всі RRM у BBU.

Результати використання ресурсів BBU для режиму R_A показано на рис. 2.

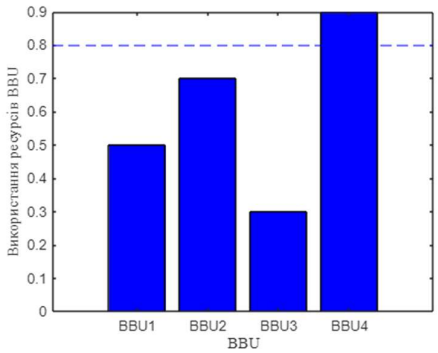


Рисунок 2. Використання ресурсів BBU для режиму R_A

Відмічається, що ресурси BBU4 не використовуються. Перевірка здійснюється для всіх BBU: призначених сусіднім RRM, призначених сусіднім RRM і всіх BBU, використання ресурсів яких нижче за верхню межу. У режимі R_B RRM в BBU переключаються інші сусідні BBU, використання ресурсів яких вище нижньої межі. Результати використання ресурсів BBU для режиму R_B показано на рис. 3.

Відмічається, що ресурси BBU3 не використовується.

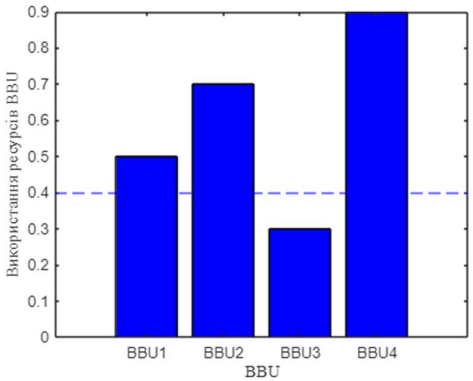


Рисунок 3. Використання ресурсів BBU для режиму R_B

У цьому режимі також перевірка здійснюється для всіх BBU з умовою є використання ресурсів вище за нижню межу.

Висновки.

Проведено дослідження зниження витрат на мережу та ефективного розподілу ресурсів BBU в залежності від навантаження трафіку в каналі fronthaul архітектури C-RAN. Показано, що кількість перемикань у BBU-RRM режимах R_A та R_B може значно збільшитися через короткий інтервал перемикання, але з іншого

боку, ефект від зниження BBU для роботи в режимах R_A та R_B суттєво збільшується.

Література

1. Checko A., Christiansen H., Berger M. Evaluation of energy and cost savings in mobile Cloud RAN / A. Checko, H. Christiansen, M. Berger // Opnetwork. — 2013. — P. 1—8.

2. Song S., Liu Y., Guo L., Song, Q. Optimized relaying and scheduling in cooperative Free Space Optical fronthaul/backhaul of 5G / S. Song, Y. Liu, L. Guo, Q. Song // Optical Switching and Networking.— 2018. — №30. — P. 62—70.

3. Checko A., Christiansen H., Yan Y., Scolari L., Kardaras G., Berger M., Dittmann L. Cloud RAN for Mobile Networks — A Technology Overview / A. Checko, H. Christiansen, Y. Yan, L. Scolari, G. Kardaras, M. Berger // IEEE Communications Surveys & Tutorials.— 2015.— №7(1) .— P. 405—426.

4. Irmer R., Droste H., Marsch P., Grieger M., Fettweis G., Brueck S., Mayer H. P., Thiele L., Jungnickel V. Coordinated multipoint: Concepts, performance, and field trial results / R. Irmer, H. Droste, P. Marsch, M. Grieger, G. Fettweis, S. Brueck, H. P. Mayer, L. Thiele, V. Jungnickel // Communications Magazine.— 2011.— №2.— P. 102—111.

5. Namba S., Matsunaka T., Warabino T., Kaneko S., Kishi Y. Colony-RAN architecture for future cellular network / S. Namba, T. Matsunaka, T. Warabino, S. Kaneko, Y. Kishi // Future Network Mobile Summit (FutureNetw) .— 2012.— P. 1—8.

6. Wu J., D. Ghosal Cost-constrained delay minimization of C-RAN and its multiplexing gain / J. Wu, Ghosal D. // IEEE International Conference on Communications (ICC.— 2016.— P. 1-6.

Анотація

Показано, що архітектуру C-RAN забезпечує канал fronthaul з об’єднанням BBU-RRM, де використання пулу BBU скорочує кількість необхідних вузлів та об'єднання ресурсів у безпроводовій мережі C-RAN. Проведено дослідження зниження витрат на мережу та ефективного розподілу ресурсів BBU в залежності від навантаження трафіку в каналі fronthaul архітектури C-RAN.

Ключові слова: C-RAN, BBU, RRM, об’єднання ресурсів.

Abstract

It is shown that the C-RAN architecture is provided by a fronthaul channel with BBU-RRM aggregation, where the use of a BBU pool reduces the number of required nodes and resource aggregation in the C-RAN wireless network. A study was conducted on reducing network costs and effectively distributing BBU resources depending on the traffic load in the fronthaul channel in the C-RAN architecture.

Keywords: C-RAN, BBU, RRM, resource aggregation..

БЕЗПЕКА ІНФОРМАЦІЙНО-ПОШУКОВОЇ СИСТЕМИ РОДОВОДУ: СУЧАСНІ МЕХАНІЗМИ УПРАВЛІННЯ ДОСТУПОМ

Кузьменко Д.С., студент, dmytro.kuzmenko@nure.ua;
Іванов В.Г., к.т.н, проф., valeriy.ivanov@nure.ua
Харківський національний університет радіоелектроніки, Харків, Україна

Сервіс-орієнтована архітектура (SOA) та її сучасна форма — мікросервісна архітектура — є основою багатьох сучасних систем. Вони дозволяють створювати модульні, масштабовані рішення, які ефективно працюють навіть у розподіленому середовищі. Прикладом такої архітектури є інформаційно-пошукова система родоводу, орієнтована на дослідження генеалогічних даних. Вона забезпечує користувачів інструментами для аналізу архівних документів, побудови родинних дерев, обробки медіафайлів та аналізу генетичних даних. Робота з такими даними потребує високого рівня захисту, оскільки вони містять персональну інформацію та результати біометричних досліджень.

Із впровадженням розподілених архітектур виникають нові виклики в області кібербезпеки. У таких системах питання автентифікації та управління доступом до ресурсів є одним із найбільш критичних. JSON Web Token (JWT) зарекомендував себе як стандарт передачі даних для автентифікації, адже він є компактним, самодостатнім і добре інтегрується в SOA та мікросервісну архітектуру. Проте його використання також супроводжується новими загрозами, які потребують ретельного аналізу й впровадження додаткових механізмів захисту.

JWT складається з трьох основних частин: заголовка (header), корисного навантаження (payload) і підпису (signature). Заголовок містить тип токена та алгоритм підпису, корисне навантаження — інформацію про користувача, таку як його ідентифікатор, роль і права доступу. Підпис гарантує, що дані у токені не було змінено. Основна перевага JWT полягає в його самодостатності: для перевірки токена не потрібен постійний доступ до центрального сервера [1]. Це значно знижує навантаження на систему, особливо в розподілених середовищах.

Проте ця самодостатність є і ключовою вразливістю. У разі компрометації токена зловмисник може використовувати його для доступу до системи без повторної автентифікації. Крім того, у багатьох реалізаціях відсутній механізм відкликання токенів, що ускладнює захист у разі компрометації. Проблемним аспектом є й зберігання токенів: наприклад, використання небезпечних сховищ, таких як localStorage, підвищує ризик XSS-атак.

Для підпису JWT існують два основні підходи: симетричний і асиметричний. Симетричний підхід використовує один секретний ключ для підпису й перевірки токенів. Це забезпечує високу продуктивність і простоту реалізації, адже всі компоненти системи мають доступ до єдиного ключа.

Проте такий підхід має значний недолік: у разі компрометації ключа зловмисник отримує можливість як створювати, так і перевіряти токени, що повністю зруйнує безпеку системи [2]. Крім того, у великих розподілених системах складно безпечно синхронізувати ключ між усіма сервісами.

Асиметричний підхід вирішує цю проблему шляхом використання двох ключів: приватного для підпису й публічного для перевірки токенів. У цьому випадку навіть у разі компрометації публічного ключа зловмисник не може створити валідний токен, адже для цього потрібен приватний ключ, який залишається захищеним на сервері користувачів. Але асиметричні алгоритми, такі як RS256, є більш ресурсоємними, що може впливати на продуктивність системи [3].

Для забезпечення безпеки інформаційно-пошукової системи родоводу необхідно було розробити механізм автентифікації, який враховує сучасні вимоги до захисту даних. Одним із ключових завдань стало забезпечення надійного захисту навіть у разі компрометації одного з компонентів системи. Це потребувало впровадження такого підходу, який би запобігав несанкціонованому використанню викрадених токенів або ключів.

Також важливим аспектом було зниження навантаження на сервер користувачів шляхом мінімізації кількості запитів, що зберігає високу продуктивність системи в умовах розподіленої архітектури [4]. Оскільки система складається з багатьох незалежних компонентів, необхідно було створити механізм, який би забезпечував простоту управління доступом, спрощував взаємодію між сервісами та не вимагав складної синхронізації ключів.

Крім того, потрібно було впровадити сучасні заходи захисту даних, такі як ротація ключів, що дозволяє регулярно змінювати приватний ключ без порушення роботи системи, та використання надійних методів зберігання токенів, щоб уникнути їхнього компрометування через атаки типу XSS або CSRF.

Для виконання цих вимог у системі було обрано асиметричний підхід до підпису JWT із використанням алгоритму RS256. Приватний ключ зберігається на сервері авторизації й використовується для підпису токенів. Публічний ключ поширюється між сервісами системи, що дозволяє виконувати перевірку токенів без додаткових запитів до центрального сервера [5].

Після успішної автентифікації користувач отримує два токени: access token та refresh token. Access token має короткий термін дії — від 5 до 15 хвилин. Це зменшує ризик його використання у разі компрометації. Refresh token діє значно довше — від 7 до 14 днів, але його функціональність обмежена: він використовується виключно для отримання нового access token.

У системі реалізовано механізм перевірки токенів, де кожен запит до кожного з сервісів, де використовується інформація про користувача, супроводжується токеном доступу. Сервіс перевіряє підпис токена за допомогою публічного ключа, розшифровує його та аналізує корисне навантаження.

Якщо токен дійсний і користувач має необхідні права доступу, запит виконується, інакше — повертається помилка відмови в виконанні запиту з вказанням причини.

Для мінімізації ризиків компрометації токенів впроваджено кілька механізмів. По-перше, токени зберігаються у cookies із встановленими атрибутами HttpOnly та Secure [1]. Це забезпечує захист від XSS-атак і унеможливлює доступ до токенів через JavaScript. По-друге, у системі впроваджено ротацію ключів: приватний ключ змінюється раз на 30 днів, але старі ключі залишаються доступними для перевірки токенів, виданих до ротації. Це гарантує безперебійну роботу системи навіть під час оновлення ключів.

Крім того, реалізовано механізм чорних списків (blacklists), який дозволяє відкликати токени у разі підозри на компрометацію. Цей механізм працює таким чином: при відкликанні токена його ідентифікатор (або сам токен) додається до чорного списку, що зберігається на сервері. Під час кожної перевірки access token сервер порівнює його з чорним списком. Якщо токен знайдено у списку, запит блокується, навіть якщо термін дії токена ще не сплив [3].

Для обмеження часу активності access token вони мають короткий термін дії, що унеможливлює їх тривале використання після викрадення. Таким чином, навіть якщо токен був скомпрометований, його шкідливе використання значно обмежується у часі.

Розроблений механізм автентифікації на основі JWT із використанням асиметричного підходу забезпечує високий рівень безпеки та продуктивності. Короткострокові токени доступу в поєднанні з довгостроковими токенами оновлення дозволяють мінімізувати ризики компрометації, а додаткові заходи, такі як ротація ключів і чорні списки, гарантують надійний захист даних. Подальші дослідження можуть бути спрямовані на впровадження адаптивних механізмів захисту, які враховують аномалії у використанні токенів, і автоматизацію управління ключами для підвищення зручності адміністрування системи.

Література

1. Siriwardena P. Microservices security in action / Prabath Siriwardena, Nuwan Dias. — [Б. м.] : Manning Publications Company, 2020. — 616 с.

2. Ivanov V. Development of pre-release software modeling and testing environment / V. Ivanov, A. Nytsik // Information processing systems. — 2010. — Т. 90, № 9. — С. 40–43.

3. Reimer M.-L. Building RESTful Web Services with Java EE 8: Create modern RESTful web services with the Java EE 8 API / Mario-Leander Reimer. — [Б. м.] : Packt Publishing, 2018. — 116 с.

4. The concept of a regional information-analytical system for emergency situations [Електронний ресурс] / Igor Grebennik [та ін.] // IFIP advances in information and communication technology. — Cham, 2019. — С. 55–66. — Режим доступу: https://doi.org/10.1007/978-3-030-18293-9_6 (дата звернення: 04.12.2024). — Назва з екрана.

5. Gough J. Mastering API architecture: design, operate, and evolve api-based systems / James Gough, Daniel Bryant, Matthew Auburn. — [Б. м.] : O'Reilly Media, 2022. — 286 с.

Анотація

У роботі розглянуто особливості застосування JSON Web Token (JWT) для автентифікації та управління доступом у сервіс-орієнтованих (SOA) і мікросервісних архітектурах. Основну увагу приділено питанням кібербезпеки, зокрема ризикам самодостатності токенів, проблемам відкликання та неправильного зберігання. Проаналізовано переваги та недоліки симетричного і асиметричного методів підпису токенів. Запропоновано ефективні заходи захисту: короткострокові access токени, довгострокові refresh токени, ротацію ключів, використання cookies із параметрами HttpOnly і Secure, а також механізми відкликання токенів за допомогою чорних списків. Розроблено рекомендації для інтеграції JWT у системи з розподіленою архітектурою та мінімізацією впливу ризиків.

Ключові слова: JSON Web Token, кібербезпека, SOA, мікросервісна архітектура, симетричний підпис, асиметричний підпис, ротація ключів, короткострокові токени, механізм відкликання.

Abstract

The report discusses the peculiarities of using JSON Web Token (JWT) for authentication and access control in service-oriented (SOA) and microservice architectures. The main attention is paid to cybersecurity issues, in particular, the risks of token self-sufficiency, revocation and improper storage. The advantages and disadvantages of symmetric and asymmetric token signing methods are analyzed. Effective security measures are proposed: short-term access tokens, long-term refresh tokens, key rotation, the use of cookies with HttpOnly and Secure parameters, as well as mechanisms for revoking tokens using blacklists. Recommendations for integrating JWT into systems with a distributed architecture and minimizing the impact of risks have been developed.

Keywords: JSON Web Token, cybersecurity, SOA, microservice architecture, symmetric signature, asymmetric signature, key rotation, short-term tokens, revocation mechanism.

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В BRUTEFORCE-АТАКАХ

Гарбарук І.А., студент, illia.harbaruk.kita@donntu.edu.ua;
Нікітенко А.О., асис. кафедри ПМІ, andrii.nikitenko@donntu.edu.ua
ДВНЗ «Донецький національний технічний університет», м. Дрогобич, Україна

Brute-force атака є одним із найстаріших методів злому, який досі залишається актуальним завдяки своїй ефективності. Основна ідея полягає у систематичному переборі всіх можливих комбінацій паролів для отримання несанкціонованого доступу до системи чи облікового запису. Цей метод став особливо небезпечним у сучасних умовах завдяки технологічним досягненням. Впровадження штучного інтелекту (ШІ) значно підвищує швидкість і точність таких атак, що робить їх невід'ємною частиною кіберзагроз нового покоління.

За даними дослідження 2021 року, 89% атак на вебдодатки здійснювалися із використанням brute-force або викрадених облікових даних, а зростання частоти атак у певні періоди досягало 671% [2], [3]. Такі показники демонструють високу активність зловмисників у використанні цієї техніки. Зокрема, злом у вигляді brute-force може мати різні цілі: викрадення даних, розповсюдження шкідливого програмного забезпечення, шифрування систем із подальшим вимаганням викупу або перенаправлення вебтрафіку на шкідливі ресурси.

Ефективність brute-force атак значно підвищилася завдяки впровадженню інструментів на основі ШІ, таких як PassGAN. PassGAN є революційним алгоритмом, що використовує нейронні мережі для прогнозування найімовірніших паролів на основі даних зі злитих баз. Він здатен здійснювати до 100 мільярдів спроб за секунду, що дозволяє зламувати понад 50% поширених паролів менш ніж за хвилину [1], [4].

Окрім PassGAN, зловмисники активно використовують моделі на основі ймовірності. Такі моделі, зокрема Large Language Models (LLM), використовують попереднє знання про структуру вебдодатків для динамічної генерації URL-адрес під час атаки. LLM базується на розпізнаванні шаблонів у даних та адаптивному прийнятті рішень, що значно підвищує ефективність атак у порівнянні з традиційними словниковими методами.

Інноваційні методи включають побудову "дерева навчання з вагами" (Weighted Training Tree), які аналізують шляхи до каталогів на основі частоти їх використання в подібних веб-додатках. На рисунку 1 зображено структуру процесу, що включає аналіз вхідного шляху, нейронну мережу LSTM та прогнозування нових директорій. Це дозволяє оптимізувати атаки, уникаючи зайвих запитів.

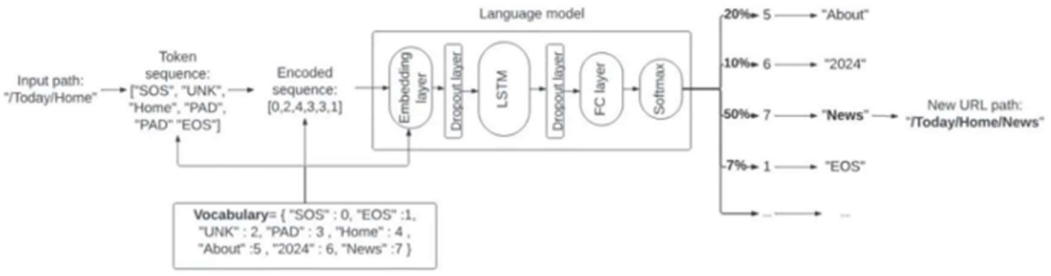


Рисунок 1. Структура процесу аналізу вхідного шляху, нейронну мережу та прогнозування нових директорій [2]

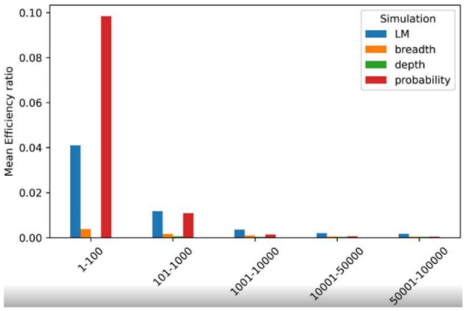


Рисунок 2. Порівняння ефективності атак на основі мовних моделей (LM) та інших підходів, включаючи ймовірнісні та традиційні методи [2]

Інше важливе доповнення полягає у використанні ймовірнісних моделей. Як зображено на рисунку 2, атаки на основі LM показали ефективність, яка перевищує традиційні brute-force підходи на 969%. Ймовірнісні моделі також демонструють високу ефективність у стелс-атаках, коли бюджет запитів обмежений.

Brute-force атаки мають руйнівний вплив на організації. Злам одного облікового запису може призвести до серйозних фінансових втрат, витоків конфіденційної інформації та пошкодження інфраструктури. Наприклад, атака на Alibaba у 2016 році поставила під загрозу 21 мільйон облікових записів [2]. У випадку T-Mobile у 2021 році зловмисники змогли викрасти дані понад 40 мільйонів користувачів, використовуючи комбінацію brute-force та технічних методів [5]. Репутаційна шкода, викликана такими атаками, часто має довготривалий вплив, особливо у випадках витоку особистих даних клієнтів.

Однак, це не гра в одні ворота, існують різні способи протидії brute-force атакам. Серед таких можна виокремити багатофакторну автентифікацію (MFA), яка є ефективним захистом, оскільки додає додатковий рівень перевірки, навіть якщо пароль було зламано [6]. Не менш цікавим є елемент залучення технологій штучного інтелекту. Наприклад, Vade for M365 дозволяє виявляти загрози, пов’язані з електронною поштою, та запобігати внутрішнім атакам. Інше інноваційне рішення, AI EdgeLabs, аналізує мережеві заголовки для ідентифікації аномалій, які можуть вказувати на атаку, що дозволяє виявляти її на ранніх етапах [3].

Серед інших методів виділяється використання унікальних паролів для кожного облікового запису. Це значно ускладнює credential stuffing атаки,

оскільки зловмисникам доводиться працювати з кожною платформою окремо [5]. Важливим аспектом залишається навчання користувачів: вони повинні вміти виявляти фішингові повідомлення та уникати повторного використання слабких паролів [6].

Ці атаки можуть завдати серйозної шкоди організаціям, але їм можна ефективно протистояти, поєднуючи передові технології, такі як Vade for M365 і EdgeLabs AI, з відповідними заходами кібергігієни. Подальше впровадження інновацій у сфері захисту є ключем до збереження безпеки у швидко змінюваному кіберсередовищі. Аналіз наукових джерел та практичних прикладів показує, що використання штучного інтелекту в атаках грубої сили значно підвищує його ефективність, особливо для адаптивних алгоритмів, мовних моделей (LM) та стохастичних підходів. Ці методи дозволяють автоматизувати процес злому і стати дуже небезпечними перед лицем зростаючої складності кіберзагроз. Подальші дослідження повинні бути спрямовані на оцінку плюсів і мінусів існуючих інструментів безпеки, особливо систем на основі штучного інтелекту, таких як Vade для M365 і AI EdgeLabs.

В майбутньому варто розробити нові алгоритми, що враховують еволюцію атак з використанням ШІ, і навчальні моделі, які можуть ефективно виявляти аномалії на ранній стадії. Особливу увагу слід приділяти створенню інструментів, які можуть виявляти складні атаки, такі як заповнення облікових даних і персоналізований фішинг, а також оптимізувати обробку великих обсягів даних для запобігання прихованих атак. Таким чином, подальший розвиток технологій виявлення та протидії атакам методом перебору стане важливою областю кібербезпеки.

Література

1. Keeper Security, “How AI Can Crack Your Passwords,” 17 серпня 2023. [Електронний ресурс]. URL: https://www.keepersecurity.com/blog/2023/08/17/how-ai-can-crack-your-passwords/.
2. Simeon Emanuilov, “AI Brute Force vs. Probabilistic Model,” Medium, 2023. [Електронний ресурс]. URL: https://cybersecuritynews.com/ai-brute-force-vs-probabilistic-model/.
3. EdgeLabs, “How to Address Brute Force Attacks with AI,” 2023. [Електронний ресурс]. URL: https://edgelabs.ai/blog/how-to-address-brute-force-attacks-with-ai/.
4. WhatIsMyIPAddress, “AI-Powered Hackers: How Criminals Are Cracking Passwords,” 2023. [Електронний ресурс]. URL: https://whatismyipaddress.com/ai-password-cracking-hackers.
5. Simeon Emanuilov, “Preventing Brute Force Attacks with Django Middleware,” Medium, 2023. [Електронний ресурс]. URL: https://medium.com/@simeon.emanuilov/ai-security-preventing-brute-force-attacks-with-django-middleware-a15af6114797.
6. VadeSecure, “Brute Force Attacks,” 2023. [Електронний ресурс]. URL: https://www.vadesecure.com/en/brute-force-attacks.
7. Li J.-H. Cyber security meets artificial intelligence: a survey // Frontiers of Information Technology & Electronic Engineering. — 2018. — Vol. 19, No. 12. — P. 1462–1474.

8. Amouei M.H., Rezvani M., Fateh M. RAT: Reinforcement-Learning-Driven and Adaptive Testing for Vulnerability Discovery in Web Application Firewalls // IEEE Transactions on Dependable and Secure Computing. — 2021. — DOI: 10.1109/TDSC.2021.3055417.

Анотація

Brute-force атаки, посилені штучним інтелектом, стають однією з найбільш серйозних загроз для кібербезпеки. У роботі розглядаються механізми використання ШІ для автоматизації злому паролів, включаючи такі методи, як PassGAN, credential stuffing і словникові атаки. Надаються приклади атак у різних галузях, включаючи автомобільну промисловість, роздрібну торгівлю та телекомунікації. Основну увагу приділено стратегіям захисту, зокрема використанню багатофакторної автентифікації, навчання користувачів і впровадженню рішень на основі ШІ, таких як Vade for M365 та AI EdgeLabs.

Ключові слова: brute-force атака, штучний інтелект, кібербезпека, паролі, credential stuffing, PassGAN.

Abstract

Brute-force attacks, enhanced by artificial intelligence, are becoming one of the most significant threats to cybersecurity. The article examines the mechanisms of AI-powered password cracking automation, including methods such as PassGAN, credential stuffing, and dictionary attacks. Examples of attacks in various industries, such as automotive, retail, and telecommunications, are provided. Special attention is given to defense strategies, including multi-factor authentication, user training, and the implementation of AI-based solutions like Vade for M365 and AI EdgeLabs.

Keywords: brute-force attack, artificial intelligence, cybersecurity, passwords, credential stuffing, PassGAN.

TENSOR MODEL FOR DESCRIBING CRITICAL INFRASTRUCTURE

Iaroslav Dorohyi[1], Doctor of Technical Sciences, Associate Professor, yaroslav.dorohyi@donntu.edu.ua;
Vasyl Tsurkan[2], Candidate of Technical Sciences, Associate Professor, v.v.tsurkan@gmail.com;
Vlasyslav Kravchuk[1], Postgraduate Student, vladkrava15@ukr.net

[1] Donetsk National Technical University, Drohobych, Ukraine
[2] Institute of Special Communications and Information Protection of Igor Sikorsky Kyiv Polytechnic Institute, Kyiv, Ukraine

Introduction

The tensor approach to modeling critical infrastructure CI) offers an effective tool for multidimensional analysis of complex systems. Critical infrastructure [1] encompasses diverse subsystems, including the energy sector, transportation networks, information and communication technologies, healthcare systems, and financial services, all characterized by intricate interconnections among themselves and with the external environment. By employing a tensor-based model, it becomes feasible to account for the numerous interdependencies among system elements $C = \{C_1, C_2, \dots, C_n\}$,, their attributes $A = \{A_1, A_2, \dots, A_m\}$, and external influences $P = \{P_1, P_2, \dots, P_p\}$, enabling more precise analysis and forecasting.

The use of tensors provides a structured representation of CI attributes, interactions, and risks, modeled as multidimensional arrays $T \in R^{n \times m \times p}$, where each dimension corresponds to a specific system aspect. For example, the element $T(i, j, k)$ encapsulates the state of the *j*-th attribute of the *i*-th component at a given time or spatial context. Additional tensors such as the interaction tensor $R \in R^{n \times n \times q}$ and the risk tensor $\Theta \in R^{n \times m \times l}$ enrich the model, capturing system interdependencies and vulnerabilities. This multidimensional framework facilitates the identification and mitigation of threats such as cyberattacks, natural disasters, or technological failures.

Foundations of Tensor Representation in CI

The tensor representation of CI enables a compact and flexible analysis framework. Tensor decompositions, including Tucker [2] and CP (CANDECOMP/PARAFAC) [3] decompositions, play a pivotal role in simplifying the analysis by identifying core interactions and latent patterns. For instance, the Tucker decomposition approximates the tensor TT as (1):

$$T \approx G \times_1 U^{(1)} \times_2 U^{(2)} \times_3 U^{(3)}, \quad (1)$$

where G is the core tensor, and $U^{(1)}, U^{(2)}, U^{(3)}$are factor matrices along different dimensions. Such decompositions help isolate critical subsystems, uncover hidden dependencies, and determine clusters of interdependent components.

The model further integrates risk assessment through operations such as the Hadamard product of the characteristic tensor T and the risk tensor Θ, yielding a modified tensor T′ reflecting the impact of risks (2):

$$T' = T \odot \Theta, \quad (2)$$

where T′(i,j,k) represents the risk-adjusted state of the j-th attribute of the i-th component under the k-th risk type.

Practical Applications and Optimizations

The tensor model serves as a versatile tool for assessing system vulnerabilities, optimizing resource allocation, and predicting the effects of various threats. For example, maximum risks can be identified as (3):

$$R_{\max} = \max_{i,j,k} \Theta\,(i,j,k), \quad (3)$$

enabling targeted mitigation efforts. Moreover, optimization strategies can minimize overall risks by redistributing resources, modeled as (4):

$$\text{Min} \sum_{i=1}^{n} \sum_{j=1}^{m} \sum_{k=1}^{l} \Theta(i,j,k). \quad (4)$$

Such methodologies ensure the sustainable and resilient operation of CI under diverse scenarios, from minor disruptions to large-scale crises.

Conclusion

Tensor modeling provides a comprehensive and systematic approach to analyzing and optimizing critical infrastructure. Its multidimensional framework accounts for interconnections, vulnerabilities, and risks, offering valuable insights for proactive risk management and resilience enhancement. This methodology holds significant potential for addressing the challenges faced by CI in an increasingly interconnected and threat-prone world.

References

1. Дорогий Я. Ю., Мохор В. В., Козлюк І. О., Цуркан В. В. Критична інфраструктура: вразливості, загрози, ризики / Я. Ю. Дорогий, В. В. Мохор, І. О. Козлюк, В. В. Цуркан // Тези доповідей ІІ міжнародної науково-практичної конференції «Інформаційні технології та взаємодії», Київ, 2015. С. 46–47.

2. Stolf F., Canale A. Bayesian Adaptive Tucker Decompositions for Tensor Factorization. 2024. URL: https://doi.org/10.48550/arXiv.2411.10218.

3. Kolda T. G., Bader B. W. Tensor Decompositions and Applications / T. G. Kolda, B. W. Bader // SIAM Review. – 2009. – Vol. 51, No. 3. – P. 455–500. URL: https://doi.org/10.1137/07070111X.

Анотація

У цій роботі розглянуто тензорну модель для опису критичної інфраструктури (КІ), яка дозволяє здійснювати багатовимірний аналіз компонентів системи, їх атрибутів, взаємодій та пов'язаних ризиків. Запропонована модель використовує тензори для представлення атрибутів компонентів, функціональних взаємодій і загроз, забезпечуючи системний підхід до аналізу та прогнозування поведінки інфраструктури. Особливу увагу приділено математичним методам, таким як розклади тензорів і оптимізація ризиків, які дозволяють виявляти вразливості системи та розробляти стратегії її захисту. Математичні вирази деталізують запропоновану модель і її застосування для підвищення стійкості та ефективності функціонування КІ.

Ключові слова: тензорна модель, критична інфраструктура, багатовимірний аналіз, оптимізація ризиків, розклад тензорів, система захисту, оцінка вразливості.

Abstract

This paper examines a tensor-based model for describing critical infrastructure (CI), enabling multidimensional analysis of system components, their attributes, interactions, and associated risks. The proposed model employs tensors to represent component attributes, functional interactions, and threats, providing a systematic approach to analyze and predict infrastructure behavior. Special emphasis is placed on mathematical methods such as tensor decompositions and risk optimization to identify system vulnerabilities and develop protection strategies. Mathematical expressions are provided to detail the proposed model and its application in enhancing the resilience and operational efficiency of CI.

Keywords: tensor model, critical infrastructure, multidimensional analysis, risk optimization, tensor decomposition, protection system, vulnerability assessment.

ПЕРСОНАЛІЗАЦІЯ ЦИФРОВОГО МАРКЕТИНГУ ЗА ДОПОМОГОЮ ТЕХНОЛОГІЙ МАШИННОГО ЗОРУ ТА МАШИННОГО НАВЧАННЯ

Шевченко М.О., студент, *mykola.shevchenko.kita@donntu.edu.ua* ***;***
Інякін М.В., студент, *maksym.iniakin.kita@donntu.edu.ua****;***
Любименко О.М., к.ф.-м.н,доц., *olena.liubymenko@donntu.edu.ua* ***;***
Штепа О.А., к.т.н., доц., *oleksandr.shtepa@donntu.edu.ua*
ДВНЗ «Донецький національний технічний університет», м. Дрогобич, Україна

У сучасному світі цифрові технології розвиваються з небаченою швидкістю, впливаючи на всі аспекти бізнесу та суспільства. Зокрема, в галузі маркетингу та реклами відбуваються значні зміни, зумовлені потребою в більш ефективних та інноваційних підходах до взаємодії зі споживачами. Традиційні методи реклами, такі як телебачення, радіо та друковані ЗМІ, поступово втрачають свою ефективність, оскільки не можуть забезпечити персоналізований підхід до клієнта. Споживачі очікують індивідуального підходу, врахування їхніх специфічних потреб та інтересів. Розробка системи, яка б використовувала технології машинного зору для аналізу демографічних характеристик клієнтів і відображення релевантного рекламного контенту в режимі реального часу, є актуальною та значущою задачею.

Технологія машинного зору має великий потенціал для персоналізації банерної реклами. Вона дозволяє отримати дані про персональні характеристики відвідувачів, такі як вік, стать та емоції, що дає змогу показувати більш релевантний контент, який враховує індивідуальні особливості та контекст кожного споживача. Завдяки використанню алгоритмів машинного навчання і великих обсягів даних, система може автоматично адаптувати рекламні матеріали, генеруючи персоналізований контент, аналізуючи інтереси та вподобання людини і створюючи банери з продуктами, які їй можуть сподобатися [1]. Такий підхід дозволяє не лише збільшити ефективність рекламних кампаній, але й покращити користувацький досвід, мінімізуючи нав’язливість контенту.

Водночас впровадження таких рішень вимагає детального технічного підходу та врахування численних викликів. Технологія машинного зору потребує високої точності обробки даних, щоб уникнути помилок у визначенні демографічних характеристик чи емоцій споживачів. Дані, які збираються під час аналізу, повинні бути захищені відповідно до стандартів конфіденційності, таких як GDPR, оскільки це є критично важливим для підтримки довіри споживачів. Крім того, інтеграція системи у роздрібну торгівлю вимагає врахування архітектури існуючої інфраструктури та налаштування її для роботи у режимі реального часу. Слід також враховувати етичні аспекти

використання машинного зору, забезпечуючи прозорість процесів і уникнення потенційної дискримінації.

Наукові дослідження в цій галузі зосереджені на вдосконаленні алгоритмів розпізнавання образів, підвищенні точності аналізу емоцій та побудові ефективних моделей персоналізації контенту. Зокрема, у [2] автори аналізують використання технологій машинного навчання для персоналізації цифрового маркетингу. У роботі підкреслюється, що алгоритми машинного навчання здатні створювати математичні моделі на основі навчальних даних, що дозволяє формувати індивідуалізовані рекламні стратегії для електронної комерції. Особливу увагу приділено таким підходам, як класифікація, регресія та алгоритми кластеризації, що сприяють сегментації споживачів і адаптації контенту до їхніх уподобань. Автори також зазначають, що впровадження таких технологій покращує показники ефективності рекламних кампаній, підвищуючи клікабельність і задоволеність користувачів, що, своєю чергою, збільшує обсяг продажів. Дослідження підтверджує, що персоналізація є ключовою умовою успіху в сучасній електронній комерції та сприяє побудові довготривалих стосунків із клієнтами.

Дослідження [3] розглядає вплив технологій штучного інтелекту, машинного навчання та обробки природної мови на формування лояльності клієнтів. Автори аналізують, як предиктивне моделювання, персоналізація на основі машинного навчання та інтеграція чат-ботів покращують взаємодію з клієнтами, дозволяючи компаніям пропонувати більш індивідуалізовані продукти й послуги. Використовуючи набір даних із 910 компаній, дослідники оцінювали ефективність шести алгоритмів машинного навчання (Logistic Regression, KNN, SVM, Decision Tree, Random Forest, AdaBoost). Найкращі результати досягли алгоритми AdaBoost і Logistic Regression з точністю 64% і 63% відповідно.

У дослідженні [4] розглядається проблема холодного старту в персоналізованих системах мобільної реклами, особливо випадок коли дані про користувача взагалі відсутні. Автори пропонують підхід, який використовує незалежні від користувача атрибути (час, тип пристрою, категорія застосунку тощо) для прогнозування рівня клікабельності оголошень. Експерименти, проведені на реальних наборах даних, підтвердили ефективність запропонованої моделі, навіть за умов обмеженої доступності даних. Дослідження підкреслює важливість використання передових алгоритмів глибокого навчання та ансамблю моделей для подолання проблеми нестачі інформації, що часто зустрічається у сучасних рекламних системах.

Дослідження [6] зосереджене на прогнозуванні клікабельності реклами у масштабних промислових системах, зокрема в контексті рекомендаційних систем Google. Автори застосували методи машинного навчання, такі як глибокі нейронні мережі та оптимізатор Distributed Shampoo, для підвищення точності моделі та забезпечення її ефективності. Використовуючи

дані з мільярдів запитів, було впроваджено факторизацію моделі, що дозволяє розділяти якість реклами та її UI-оформлення, оптимізуючи витрати на обчислення. За рахунок цього вдалося підвищити точність моделі на 0.44% без суттєвого збільшення витрат на навчання. Серед інших досягнень дослідження – використання методів дистиляції, які покращили точність на 0.46%, і автоархітектурного пошуку, що зменшив витрати на тренування на 16%. Також застосування стратегії семплінгу дозволило скоротити обсяг навчальних даних до 25% без втрати точності. Такий підхід сприяє підвищенню продуктивності систем рекомендацій, знижуючи їх витрати та забезпечуючи стабільність у виробничих умовах.

В процесі дослідження встановлено що персоналізація є ключовим елементом ефективності сучасних рекламних систем. Застосування технологій машинного навчання, таких як глибокі нейронні мережі та алгоритми ансамблю, дозволяє створювати релевантний контент, що враховує індивідуальні особливості споживачів. Використання передових підходів та передобробки даних сприяє оптимізації витрат на навчання моделі та забезпечує стабільність роботи систем реальним умовах роботи. Розробка алгоритмів для подолання проблеми холодного старту та інтеграція персоналізованих рішень у реальному часі доводить свою ефективність у підвищенні конверсії реклами та формуванні довготривалих стосунків із клієнтами. Однак реалізація таких систем вимагає подолання значних викликів, серед яких – забезпечення точності аналізу даних, дотримання стандартів конфіденційності та інтеграція в існуючі інфраструктури. Персоналізація що базується на алгоритмах машинного навчання значно трансформує галузь цифрового маркетингу, дозволяючи компаніям ефективніше взаємодіяти з клієнтами та підвищувати загальний рівень задоволеності користувачів.

Література

1.Haleem, A., Javaid, M., Qadri, M. A., Singh, R. P., & Suman, R. (2022). Artificial intelligence (AI) applications for marketing: A literature-based study. International Journal of Intelligent Networks, 3, 119–132. https://doi.org/10.1016/j.ijin.2022.08.005

2. Nikolajeva, A., & Teilans, A. (2021). Machine Learning Technology Overview in Terms of Digital Marketing and Personalization. Proceedings of the International Conference on Modern Systems and Applications, 125-132. https://doi.org/10.7148/2021-0125

3. Patel, Nikhil & Trivedi, Sandeep. (2020). Leveraging Predictive Modeling, Machine Learning Personalization, NLP Customer Support, and AI Chatbots to Increase Customer Loyalty. 3. 1-24.

4. Viktoratos, I., & Tsadiras, A. (2022). A Machine Learning Approach for Solving the Frozen User Cold-Start Problem in Personalized Mobile Advertising Systems. Algorithms, 15(3), 72. https://doi.org/10.3390/a15030072

5. On the factory floor: ML engineering for industrial-scale ads recommendation models. Anil, R., Gadanho, S., Huang, D., Jacob, N., Li, Z., Lin, D., Phillips, T., Pop, C., Regan, K., Shamir, G. I., Shivanna, R., & Yan, Q. 2022. 22 citations (Semantic Scholar/arXiv) [2023-10-16] https://doi.org/10.48550/arXiv.2209.05310.

Анотація

В галузі маркетингу та реклами відбуваються значні зміни, зумовлені потребою в більш ефективних та інноваційних підходах до взаємодії зі споживачами. Споживачі очікують індивідуального підходу, врахування їхніх специфічних потреб та інтересів. Розробка системи, яка використовує технології машинного зору для аналізу демографічних характеристик клієнтів і відображення релевантного рекламного контенту в режимі реального часу має великий потенціал для персоналізації банерної реклами, дозволяючи отримувати дані про персональні характеристики відвідувачів, такі як вік, стать та емоції. Це дає змогу показувати більш релевантний контент, що враховує індивідуальні особливості та контекст кожного споживача. Використання алгоритмів машинного навчання і великих обсягів даних дозволяє системі автоматично адаптувати рекламні матеріали, генеруючи персоналізований контент. Такий підхід підвищує ефективність рекламних кампаній та покращує користувацький досвід, мінімізуючи нав'язливість контенту. Впровадження таких рішень вимагає детального технічного підходу та врахування численних викликів, таких як висока точність обробки даних, захист конфіденційності, інтеграція в існуючу інфраструктуру та етичні аспекти використання машинного зору.

Ключові слова: цифрові технології, машинне навчання, персоналізація, конфіденційність, машинний зір

Abstract

The marketing and advertising industry is undergoing significant changes driven by the need for more effective and innovative approaches to interacting with consumers. Consumers expect an individual approach, taking into account their specific needs and interests. The development of a system that uses machine vision technologies to analyze customer demographics and display relevant advertising content in real time has great potential for personalizing banner advertising, allowing for data on visitors' personal characteristics, such as age, gender, and emotions. This allows for more relevant content to be displayed that takes into account the individual characteristics and context of each consumer. The use of machine learning algorithms and big data allows the system to automatically adapt advertising materials, generating personalized content. This approach increases the effectiveness of advertising campaigns and improves the user experience, minimizing the intrusiveness of content. Implementing such solutions requires a detailed technical approach and consideration of numerous challenges, such as high accuracy of data processing, privacy protection, integration into existing infrastructure and ethical aspects of using machine vision.

Keywords: digital technologies, machine learning, personalization, privacy, machine vision

МОДЕЛЮВАННЯ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ВИЯВЛЕННЯ ЗАГРОЗ

Квітковський І.О., магістр гр. ІПЗм-23,
ivan.kvitkovsky@donntu.edu.ua;
Алтухова Т.В., канд. техн. наук, tetiana.altukhova@donntu.edu.ua
Державний вищий навчальний заклад «Донецький національний технічний університет», Дрогобич, Україна

На сьогоднішній день стан питання забезпечення інформаційної безпеки (ІБ) в Україні та у всьому світі є першочерговим з огляду на те, що з кожним роком спостерігається підвищення проявів порушення безпеки їх критичної інфраструктури та наявності загроз в інформаційному середовищі, тим самим відображаючи всі можливі вразливості для здійснення кібератак [1].

Зараз практично всі підприємства, будь-які установи та організації країн мають свою певну інформаційну систему (ІС), в якій передбачено взаємозв'язок різноманітних методів, засобів та співробітників, формуючи при цьому єдину локальну обчислювальну мережу (ЄЛОМ). В ЄЛОМ забезпечується основний процес отримання, зберігання, обробки і видачі інформації на підприємствах, організаціях та установах. Однак збільшення потоку даних в ній та розширення кола завдань інформаційних систем викликає появу проблеми підвищення частоти здійснення кібератак на ІС та розширення вразливостей інформаційних ресурсів. Причиною виникнення даної проблеми є [2]:

- збільшення кількості завдань, що розв'язуються в інформаційній системі;
- розвиток методів та засобів обробки інформації та порушення інформаційної безпеки;
- збільшення об'єму інформації, яку необхідно обробити;
- розширення функціональних можливостей ЄЛОМ шляхом ускладнення програмно-апаратних компонентів, і, як наслідок, збільшення ймовірності появи вразливостей та помилок в системі [2].

Окрім цього проблема виникає через конкурентність підприємств за отримання доходу, їх стан на ринку за умови ефективного і коректного функціонування інформаційної системи, цілісності інформаційних ресурсів та рівня захисту конфіденційної інформації від несанкціонованого доступу зловмисників як з зовнішнього середовища, так і внутрішнього середовища підприємства. Сучасні процеси забезпечення інформаційної безпеки мають тісний взаємозв'язок із виконанням моніторингу існуючих систем та мереж, в яких відбувається передача інформації і даних [3]. Окрім того, з кожним роком зростають вимоги до систем інформаційної безпеки, що повинні забезпечувати не тільки пасивний захист, наприклад, виконання блокування

несанкціонованого доступу в інформаційній мережі з зовнішнього середовища, а й забезпечувати активний захист, до якого відноситься виявлення кібератак, аналіз причин появи загроз та автоматичне їх усування [4]. Таким чином, проблема забезпечення захисту інформації повинна вивчатися та вирішуватися з точки зору застосування найсучасніших методів і засобів моделювання та новітніх алгоритмів виявлення загроз і автоматизованого прийняття рішень щодо запобігання кібератакам.

Сам процес реалізації загроз порушником ІБ є кібератака на функціональні можливості інформаційної системи задля отримання доступу до конфіденційних даних, тому їх виявлення є першочерговим завданням, яке забезпечить здійснення блокування порушень ІС та знизить можливості витоку інформації і появи інших негативних наслідків вторгнення зловмисника до системи.

Будь-яке порушення інформаційної системи передбачає декілька етапів, що входять в «життєвий цикл кібератаки», які демонструють основну структуру процесу успішної реалізації загроз в ІС зловмисником (рис.1) [5].

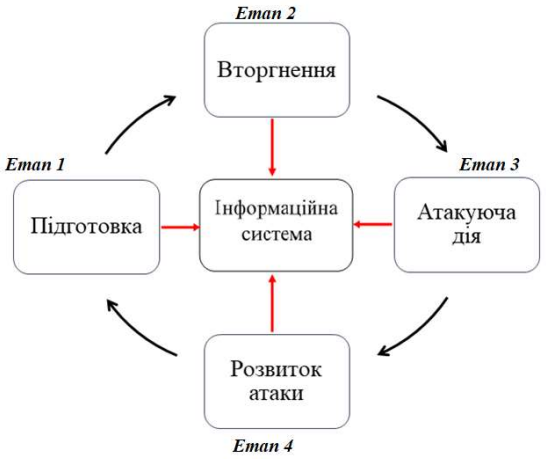


Рисунок 1. Життєвий цикл кібератаки на ІС

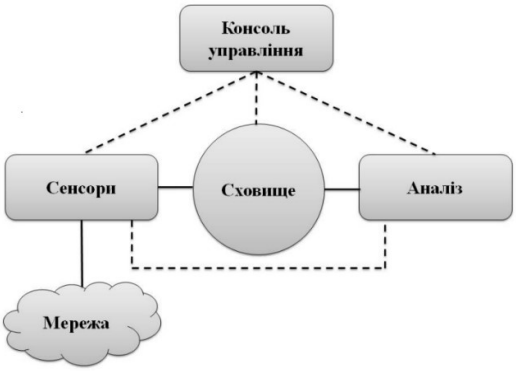


Рисунок 2. Базова структура систем інформаційної безпеки виявлення загроз

З огляду на це, розробка систем інформаційної безпеки виявлення загроз є необхідним засобом захисту інформаційних систем від небезпечної та підозрілої активності в мережі, базова структура якої наведена на рис. 2 [6].

Розробка моделі такої системи здійснювалася із використанням мереж Петрі задля відображення основних процесів виявлення кібератаки на інформаційну систему в залежності від різних факторів впливу та виявлення аномальної поведінки загроз в ній (рис. 3).

Дослідження отриманої моделі здійснювалося у два етапи, а саме моделювання динаміки процесу функціонування моделі мережі Петрі системи інформаційної безпеки виявлення загроз (рис.4) та динаміки її реагування на кібератаки (рис.5). За отриманими результатами дослідження виконана

верифікація та визначена щільність ймовірності часу реагування розробленою системою під час порушення інформаційної системи загрозами (рис. 6).

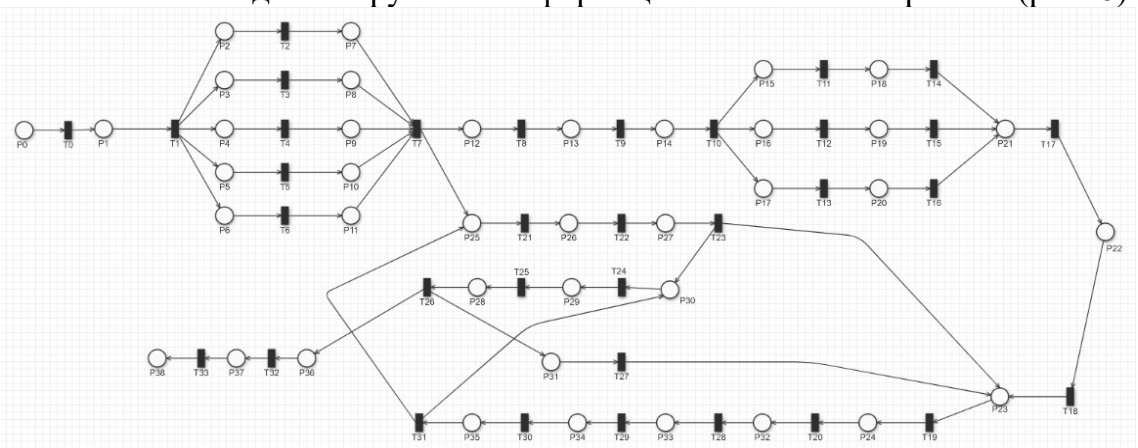


Рисунок 3. Розроблена модель системи інформаційної безпеки виявлення загроз на основі мереж Петрі

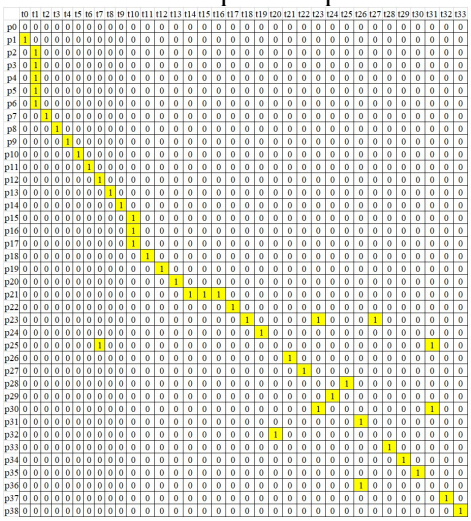


Рисунок 4. Результат дослідження динаміки процесу функціонування побудованої моделі мережі Петрі системи інформаційної безпеки виявлення загроз

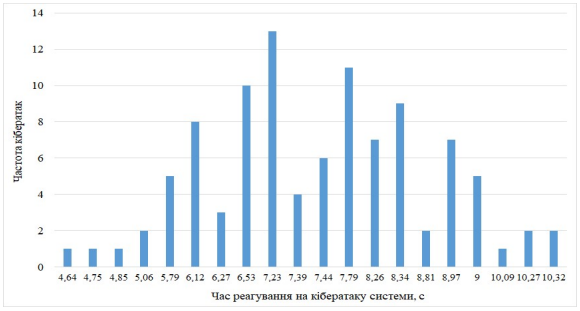


Рисунок 5. Динаміка реагування розробленої системи ІБ виявлення загроз відносно частоти здійснення кібератаки порушниками безпеки

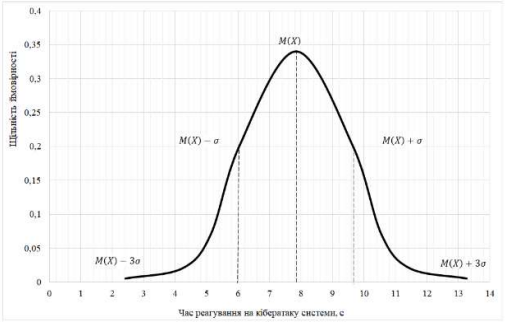


Рисунок 6. Результати визначення щільності ймовірності часу реагування розробленою системою під час порушення інформаційної системи загрозами

Таким чином, отримані результати дослідження показали, по-перше, що отримана модель мережі Петрі володіє такими властивостями, як детермінованість та послідовність, тобто в кожний момент часу мережа буде знаходитися у відповідному стані із існуючих, причому для них можна визначити наявність чи відсутність кіберзагрози з певною ймовірністю. По-друге, виявлено, що середній час реагування розробленою системою під час порушення інформаційної безпеки загрозами знаходиться в межах від 5 до 11 с, що показує ефективність реагування на порушення безпеки загрозами в інформаційній системі.

Література

1. Комаров М. Ю., Гончар С. Ф., Дмітрієва Д. О. Дослідження проблеми кіберживучості об'єктів критичної інформаційної інфраструктури. Ядерна та радіаційна безпека, 1(89), 2021. С. 59-66.

2. Дзьобань О.П., Соснін О.В. Інформаційна безпека: нові виміри загроз, пов'язаних з інформаційно-комунікаційною сферою. Гуманітарний вісник ЗДІА, №60, 2015. – С. 24-34.

3. NVD – Home [електронний ресурс]. Режим доступу: https://nvd.nist.gov/ (дата звернення 04.09.2024).

4. CVE – CVE [електронний ресурс]. Режим доступу: https://cve.mitre.org/ (дата звернення 04.09.2024).

5. Запорожченко М. М. Місце OSINT в життєвому циклі кібератаки /М. М. Запорожченко// Телекомунікаційні та інформаційні технології, №1(78), 2023. – С. 53-60. - DOI: 10.31673/2412-4338.2023.015360

6. Мєшков В. І., Віролайнен В. О. Аналіз сучасних систем виявлення та запобігання вторгнень в інформаційно-телекомунікаційних системах [електронний ресурс]. Режим доступу: https://ela.kpi.ua/server/api/core/bitstreams/2fc5d863-fb1a-4334-a33d-ceee718222ff/content (дата звернення 20.10.2024).

Анотація

В статті проаналізовано причини виникнення проблеми інформаційної безпеки та запропоновано модель системи виявлення загроз із застосуванням мереж Петрі. Проведено дослідження динаміки процесу функціонування розробленої моделі та динаміки реагування її на кібератаки.

Ключові слова: інформаційна безпека, модель системи виявлення загроз, мережі Петрі, динаміка процесу функціонування, час реагування.

Abstract

The article analyses the reasons for the emergence of the information security problem and proposes a model of a threat detection system using Petri nets. The dynamics of the functioning of the developed model and the dynamics of its response to cyber attacks are studied.

Keywords: information security, model of a threat detection system, Petri nets, dynamics of the functioning process, time of response.

ОГЛЯД ЕТИЧНИХ І ПРАВОВИХ АСПЕКТІВ ВИКОРИСТАННЯ СТЕГАНОГРАФІЇ

Кузьменко М.А , студент, mykyta.kuzmenko.kita@donntu.edu.ua
Донецький національний технічний університет, Дрогобич, Україна

Стеганографія — це технологія приховування інформації, яка забезпечує конфіденційність даних, дозволяючи передавати важливу інформацію, не викликаючи підозри у сторонніх осіб. Вона знаходить застосування в різних сферах, зокрема для захисту паролів, важливих документів або приватних комунікацій через медіафайли (зображення, аудіо та відео). Стеганографія дозволяє захистити дані від зовнішнього спостереження, пропонуючи рівень безпеки, що важко порушити за допомогою традиційних методів, таких як шифрування. Крім того, вона застосовується для захисту інтелектуальної власності, зокрема в цифровому авторському праві. Наприклад, стеганографія дає змогу вставляти водяні знаки у зображення або аудіофайли, що дозволяє відслідковувати порушення прав та виявляти незаконне використання контенту.

Однак стеганографія має й іншу сторону. Вона може бути використана для приховування шкідливого програмного забезпечення, незаконних фінансових операцій або організації комунікацій між терористичними угрупованнями. Зловживання цією технологією створює серйозні правові та етичні проблеми. Технологія, яка мала б забезпечувати безпеку та конфіденційність, може бути використана для здійснення незаконних або небезпечних дій, що ставить під загрозу суспільну безпеку та правопорядок.

Етичні проблеми стеганографії з’являються у контексті балансу між правом на приватність і потребами національної безпеки. У демократичних суспільствах право на приватність є основним принципом, що гарантує захист особистої інформації від несанкціонованого втручання. З іншого боку, правоохоронні органи можуть вважати необхідним доступ до такої інформації з метою забезпечення національної безпеки, що створює етичну дилему: як захистити право громадян на приватність, не порушуючи при цьому інтереси національної безпеки [1]?

Крім того, етичні проблеми можуть виникати у випадках, коли стеганографія використовується в журналістиці або мистецтві. Приховування інформації у вигляді цифрових підписів або інших сигналів може бути необхідним для захисту джерел або збереження анонімності авторів. У таких випадках стеганографія дозволяє вберегти людей від переслідувань або захистити конфіденційні дані, які можуть зашкодити правам чи життю авторів. У цьому контексті стеганографія є потужним інструментом для збереження свободи слова і прав людини [2].

Правові аспекти використання стеганографії різняться в залежності від країни. У Європейському Союзі, наприклад, є суворі закони щодо захисту

персональних даних (наприклад, GDPR), які обмежують можливість зловживань стеганографією, таких як приховування незаконних файлів або фінансових транзакцій. Однак виявлення та декодування стеганографічних повідомлень є складним завданням для правоохоронних органів, що ускладнює боротьбу з кіберзлочинністю. Більш того, різні країни можуть мати власні обмеження на використання стеганографії з огляду на національну безпеку. Це може включати вимоги до реєстрації програмного забезпечення, яке використовує стеганографічні методи, або заборону на певні типи стеганографічних технологій[3].

Незважаючи на можливі негативні наслідки використання стеганографії, ця технологія має також величезний потенціал для позитивного впливу на суспільство. Вона дозволяє зберігати конфіденційність особистих даних, захищати авторські права, а також сприяти розвитку нових форм цифрового мистецтва та комунікацій. Тому важливо розробляти правові та етичні рамки, які дозволятимуть ефективно використовувати стеганографію, обмежуючи її потенційне зловживання.

Загалом, стеганографія ставить перед нами не тільки технологічні виклики, а й серйозні етичні та правові питання. Основним завданням для суспільства є створення законодавчого та етичного середовища, яке дозволить забезпечити безпеку та конфіденційність без порушення прав і свобод громадян.

Література

1. Vassilis, T., & Petros, K. (2023). Legal and Ethical Aspects of Digital Privacy Protection in Steganography. International Journal of Law and Technology.

2. S, Yashaswini, & Dr. Jasmine K. S. (2024). Social and Ethical Implications of Steganography: A Case Study Approach. International Advanced Research Journal in Science, Engineering, and Technology.

3. Xing, H., & Zhang, J. (2021). Ethical Dilemmas in Digital Information Hiding: A Critical Review. Journal of Digital Ethics and Security.

Анотація

Стеганографія — це технологія приховування інформації в різних цифрових форматах, що забезпечує конфіденційність та захист даних від зовнішнього спостереження. Вона має широке застосування, зокрема для захисту особистої інформації, інтелектуальної власності та в цифровому авторському праві. Однак стеганографія може використовуватися також зловмисниками для приховування шкідливого програмного забезпечення чи незаконних фінансових операцій. У тезі розглянуто етичні та правові аспекти її використання, що стосуються балансу між правом на приватність і потребами національної безпеки. Крім того, аналізуються можливості стеганографії в журналістиці, мистецтві та захисті прав людини.

Ключові слова: стеганографія, конфіденційність, захист даних, інтелектуальна власність, етичні проблеми, національна безпека, правові аспекти, цифрове мистецтво, шкідливе програмне забезпечення, приватність.

Abstract

Steganography is a technology for concealing information in various digital formats, ensuring confidentiality and protection of data from external surveillance. It is widely used for safeguarding personal information, intellectual property, and in digital copyright. However, steganography can also be exploited by malicious actors to hide malicious software or illegal financial transactions. This paper examines the ethical and legal aspects of its use, focusing on the balance between privacy rights and national security needs. Additionally, it explores the potential of steganography in journalism, art, and the protection of human rights.

Keywords: steganography, confidentiality, data protection, intellectual property, ethical issues, national security, legal aspects, digital art, malicious software, privacy.

МАТЕМАТИЧНА ПОСТАНОВКА ЗАДАЧІ СТЕГАНОГРАФІЇ ЗОБРАЖЕНЬ

Кузьменко М.А , студент, mykyta.kuzmenko.kita@donntu.edu.ua
Хома Д.Ю, аспірант, dmytro.khoma.asp@donntu.edu.ua
Донецький національний технічний університет, Дрогобич, Україна

Стеганографія зображень — це технологія приховання даних у цифрових зображеннях таким чином, щоб зміни в їхній структурі були непомітними для людського ока. Одним із основних завдань стеганографії є мінімізація впливу на якість зображення, оскільки навіть незначні зміни пікселів можуть бути помітними при аналізі зображення. Математична постановка цієї задачі передбачає розгляд кожного пікселя як числове значення, яке може бути змінене для вбудовування інформації [1].

Процес вбудовування інформації в пікселі може бути описаний так: кожен піксель зображення має певне значення інтенсивності або кольору, що записується в двійковій формі. Коли в зображення вбудовується інформація, ці значення змінюються. Технології стеганографії зазвичай використовують методи зміни найменших значущих бітів пікселя (LSB — Least Significant Bit) [2]. Це дозволяє зберегти основну структуру зображення, мінімізуючи зміни, які можуть бути помічені.

Математично цей процес можна виразити через функцію зміни значення пікселя I_i, де $I_i^{'}$ — це нове значення пікселя після вбудовування інформації, а I_i — початкове значення пікселя

$$I_i^{'} = I_i + \Delta I_i \ , \tag{1}$$

де ΔI_i — це зміна, що додається до значення пікселя для вбудовування інформації. Оскільки зміни ΔI_i мають бути мінімальними, щоб не вплинути на якість зображення, важливими стають критерії оцінки цих змін [3].

Одними з основних математичних критеріїв є середньоквадратична помилка (MSE) та пік-сигнальний шумовий коефіцієнт (PSNR). MSE дозволяє оцінити середню величину різниці між оригінальним і зміненим зображенням. Вища MSE свідчить про більший вплив на якість зображення, тоді як нижчі значення вказують на менші зміни [1]

$$MSE = \frac{1}{n}\sum_{i=1}^{n}(I_i - I_i^{'})^2 , \tag{2}$$

де n — кількість пікселів у зображенні. PSNR використовують для визначення ступеня спотворення зображення після вбудовування інформації. Вищий PSNR означає менше спотворення, що є бажаним результатом стеганографії

$$PSNR = 10 \cdot \log_{10}\left(\frac{MAX^2}{MSE}\right), \quad (3)$$

де MAX — максимальне значення пікселя. Важливо, щоб зміни були настільки малими, що PSNR залишався високим.

Сучасні методи стеганографії активно використовують машинне навчання, зокрема генеративні змагальні мережі (GAN), для покращення процесу вбудовування інформації [4]. GAN дозволяють створювати моделі, які здатні не лише приховувати інформацію, але й робити цей процес майже непомітним. За допомогою цих мереж можна генерувати такі стеганографічні зображення, що вони є стійкими до виявлення навіть при використанні складних методів стегананалізу.

Використання нейронних мереж для стеганографії має значний потенціал, оскільки такі мережі можуть оптимізувати процес вбудовування інформації, зменшуючи її вплив на зображення та покращуючи стійкість до стегананалізу. Система SteganoGAN, яка базується на GAN, показує високі результати у збереженні якості зображення при вбудовуванні даних і надає нові можливості для стеганографії в умовах, коли важлива як висока якість зображення, так і невидимість перед стегананалітичними методами [5].

Стеганографія зображень дозволяє приховувати дані з мінімальними змінами, які важко помітити. Використання методів зміни найменших значущих бітів (LSB) допомагає зберегти якість зображення, оцінювану через MSE та PSNR. Сучасні технології, зокрема генеративні змагальні мережі (GAN), покращують стійкість до стегананалізу та зберігають високу якість зображень. Моделі, як SteganoGAN, оптимізують процес вбудовування, підвищуючи ефективність та надійність стеганографії.

Література

1. Ткачук А. П. Математичні моделі стеганографії зображень / А. П. Ткачук // Вісник НУТУ «КПІ». Сер. Радіотехніка. — 2019. — № 45. — С. 78—85.

2. Вілкіна К. А., Клебеко Є. Ю. Стеганографія зображень: методи та реалізація / К. А. Вілкіна, Є. Ю. Клебеко // Науковий вісник БГУІР. — 2021. — № 3. — С. 123—130.

3. Лобач С. В., Меркулов Р. І. Стеганографічні методи захисту інформації в графічних зображеннях / С. В. Лобач, Р. І. Меркулов // Вісник Білоруського державного університету. Сер. Інформатика. — 2020. — № 2. — С. 45—52.

4. Григор'єв В. В. Використання нейронних мереж у стеганографії / В. В. Григор'єв // Науковий вісник НТУУ «КПІ». — 2023. — № 5. — С. 99—105.

5. Стеганографія: теорія та практика / О. І. Рибін, А. П. Ткачук // Журнал комп'ютерних наук. — 2022. — Т. 12, № 1. — С. 15—30.

Анотація

У роботі розглянуто математичні основи стеганографії зображень, зокрема постановку задачі вбудовування інформації в цифрові зображення. Визначено математичні критерії оцінки ефективності стеганографії, такі як середньоквадратична помилка (MSE)

та пік-сигнальний шумовий коефіцієнт (PSNR). Розглянуто вплив новітніх методів глибокого навчання, зокрема генеративних змагальних мереж (GAN), на покращення якості вбудовування даних.

Ключові слова: стеганографія, зображення, математична постановка задачі, середньоквадратична помилка, стегананаліз, генеративні змагальні мережі.

Abstract

The paper examines the mathematical foundations of image steganography, in particular the formulation of the problem of embedding information in digital images. The mathematical criteria for assessing the effectiveness of steganography, such as the mean square error (MSE) and the peak signal-to-noise ratio (PSNR), are determined. The impact of the latest deep learning methods, in particular generative adversarial networks (GANs), on improving the quality of data embedding is considered.

Keywords: steganography, image, mathematical formulation of the problem, mean square error, steganananalysis, generative adversarial networks.

РОЗРОБКА ТА ДОСЛІДЖЕННЯ СИСТЕМИ ДЛЯ ВИЯВЛЕННЯ АНОМАЛІЙ У ПОВЕДІНЦІ ВІДВІДУВАЧІВ ВЕБ-САЙТУ

Кузеляк М.В. студент, магістр, mykhailo.kuzeliak.19@pnu.edu.ua
Прикарпатський національний університет імені Василя Стефаника, м. Івано-Франківськ, Україна

Актуальність питання

Останнім часом безпека веб-сайтів набуває все більшого значення через зростання кількості атак, таких як DDoS, SQL-ін'єкції, шахрайські дії, ботнет-атаки та автоматизоване сканування вразливостей. Зловмисники використовують дедалі складніші методи для обходу систем захисту, що створює серйозні ризики як для власників веб-ресурсів, так і для їхніх користувачів.

Відомі дослідження та публікації

Відомі дослідження у галузі виявлення аномалій охоплюють широкий спектр підходів, що використовуються для забезпечення безпеки веб-ресурсів. Наприклад, дослідження [1-2] узагальнює основні методи виявлення аномалій, зокрема сигнатурний аналіз, евристичні підходи та алгоритми машинного навчання. У звіті [3] розглядаються сучасні тренди у використанні штучного інтелекту, включаючи аналіз великих даних, що є ключовим для підвищення ефективності виявлення аномалій. Разом ці роботи формують теоретичну та практичну основу для створення систем автоматизованого виявлення аномалій у веб-середовищі.

Постановка задачі та методи

Основною метою дослідження є створення моделі, здатної аналізувати логи веб-сервера та ідентифікувати аномальні патерни у поведінкових даних. Для практичного застосування система реалізується у вигляді API-сервісу, що дозволяє автоматизувати аналіз трафіку на основі отриманих даних із логів веб-сервера.

Для досягнення мети виконано такі завдання:

- Проаналізовано предметну область та ключові сценарії аномальної активності.
- Розроблено методологію вибору оптимальних ознак для виявлення аномалій.
- Реалізовано модель на основі автокодувальника для аналізу поведінкових даних.
- Реалізовано систему у вигляді API-сервісу для інтеграції з веб-додатками.
- Оцінено ефективність моделі за допомогою стандартних метрик, таких як accuracy, precision, recall та F1-міра.

У роботі були проаналізовані наступні методи для виявлення аномальної активності:

- Автокодувальники для виявлення аномалій через аналіз помилок реконструкції – це нейронні мережі, що складаються з двох частин: кодувальника, який стискає вхідні дані, і декодувальника, що відновлює їх. Під час навчання автокодувальник вчиться відновлювати нормальні патерни поведінки з мінімальними помилками. Якщо система не може точно відновити дані, це вказує на відхилення від нормальної поведінки, що дозволяє виявляти аномальні події.
- Сигнатурні методи – це методи, які ґрунтуються на пошуку заздалегідь визначених шаблонів атак, таких як SQL-ін'єкції, DDoS-атаки чи спроби несанкціонованого доступу. Ці методи ефективні для швидкого виявлення відомих загроз, оскільки вони порівнюють вхідні дані з базою даних відомих атак. Однак, вони мають обмеження у здатності виявляти нові або змінені загрози, для яких не було зафіксовано шаблонів.
- Методи евристичного аналізу – використовують набір правил і статистичних підходів для виявлення аномалій, які не підпадають під відомі шаблони. Ці методи дозволяють аналізувати поведінку користувачів або системи, шукаючи відхилення від нормальних патернів.

Основний матеріал та результати дослідження

У дослідженні було проведено аналіз логів веб-сервера для виділення ключових ознак, таких як bytes, timestamp, status code. З використанням автокодувальників розроблено модель, яка демонструє високу точність виявлення аномалій (accuracy = 97%, precision = 91%, recall = 99%, F1-міра 93%).

Реалізована система у вигляді API-сервісу, яка дозволяє обробляти дані з логів веб-сервера, аналізувати їх та повертати результат щодо наявності аномалій.

Висновки та подальші дослідження

Дослідження підтвердило ефективність розробленої моделі для виявлення аномальної активності в логах веб-сервера. Використання автокодувальників для аналізу поведінкових даних дозволило досягти високої точності (accuracy та recall) виявлення аномалій. Розроблена модель показала хороші результати за метриками точності, повноти та F1-міри, що свідчить про її надійність для застосування в реальних умовах. Оцінка системи через API-сервіс дозволила ефективно інтегрувати її в інфраструктуру веб-додатків для автоматизованого аналізу логів у офлайн-режимі.

Подальші дослідження передбачають оптимізацію системи для роботи з великими обсягами даних, що дозволить масштабувати рішення для вели-

ких веб-ресурсів. Планується інтеграція з хмарними платформами для покращення масштабованості та продуктивності, а також вдосконалення моделі для виявлення нових типів атак. Важливим напрямом є адаптація системи для роботи в реальному часі, що дозволить оперативно реагувати на загрози та поліпшити загальний рівень безпеки веб-сайтів.

Література

1. Chandola, V., et al. Anomaly Detection: A Survey. IEEE Transactions on Knowledge and Data Engineering. [Електронний ресурс] URL: https://ieeexplore.ieee.org/document/5645624 (дата звернення: листопад 2024 р.)
2. García, J., et al. Anomaly Detection in Web Server Logs: A Review of Techniques and Approaches. [Електронний ресурс] URL: https://ieeexplore.ieee.org/document/9753130 (дата звернення: листопад 2024 р.)
3. Reding, D.F., Eaton, J. Science & Technology Trends 2020–2040. [Електронний ресурс] URL: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf (дата звернення: листопад 2024 р.)

Анотація

Дослідження присвячене вдосконаленню технологій для виявлення аномальної активності на веб-сайтах. Розглянуто основні методи виявлення аномалій у веб-логах, зокрема використання автокодувальників для аналізу поведінки користувачів, сигнатурних методів для виявлення відомих атак та евристичних методів для виявлення відхилень. Досліджено вибір ознак, для моделі виявлення аномалій, оцінено її точність за допомогою стандартних метрик, таких як accuracy, recall, precision. Розроблено API-сервіс для інтеграції з веб-додатками, що дозволяє автоматизувати процес аналізу логів у офлайн-режимі.

Ключові слова: виявлення аномалій, аналіз логів, нейронні мережі, автокодувальники, сигнатурні методи, евристичний аналіз, точність, повнота, F1-міра.

Abstract

The study is dedicated to improving technologies for detecting anomalous activity on websites. The main methods for anomaly detection in web logs are discussed, including the use of autoencoders for user behavior analysis, signature-based methods for detecting known attacks, and heuristic methods for detecting deviations. The feature selection for the anomaly detection model is investigated, and its accuracy is evaluated using standard metrics such as accuracy, recall, and F1-score. An API service has been developed for integration with web applications, enabling the automation of log analysis in offline mode.

Keywords: anomaly detection, log analysis, neural networks, autoencoders, signature-based methods, heuristic analysis, accuracy, recall, F1-score.

ПОПЕРЕДНЯ ОБРОБКА КОРИСТУВАЦЬКИХ ВІДГУКІВ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЙ ЗБАГАЧЕННЯ ДАНИХ

Золотухіна О.А., к.т.н., доц. zolotukhina.oks.a@gmail.com
Горбань А.М., магістрант, mag2385574@stud.duikt.edu.ua
Державний університет інформаційно-комунікаційних технологій, Київ, Україна

Кожного дня значно зростає кількість створеного користувачами контенту на ігрових онлайн-платформах, що призвело до накопичення значної кількості цінної інформації, такої як огляди та рейтинги. Ігрова індустрія є дуже прибутковим сектором з ринковою вартістю в мільярди доларів та демонструє своє стійке зростання та успіх. Щоб підтримувати конкурентну перевагу, розробникам ігор, видавцям і маркетологам вкрай необхідно мати всебічне розуміння вподобань і настроїв геймерів. Огляди комп'ютерних ігор можна розглядати як експертні звіти про досвід, які дають гравцям уявлення про те, чого очікувати від гри, працюючи як посібники для купівлі. У той же час такі відгуки часто мають низьку якість, містять такі особливості як сленгові слова та вирази, скорочення та абревіатури, неоднорідну термінологію, нецензурну лексику, орфографічні помилки, суб'єктивність та неструктурованість тексту, що створює значні труднощі для його обробки та аналізу. Користувацькі відгуки на комп'ютерні ігри мають низку специфічних характеристик, які роблять їх обробку, зокрема очищення, нормалізацію та збагачення, унікальною та складною задачею. Гравці у комп'ютерні ігри (геймери) часто використовують сленг, абревіатури, спеціалізовані терміни що пов'язані з технічними аспектами гри, нетекстові елементи відображення емоцій, як то смайли чи емодзі, капіталізацію (використання великих літер) та інші види неформальної мови, які можуть бути незрозумілими для стандартних інструментів обробки тексту. Попередня обробка текстових даних – це процес приведення тексту до формату, який легко зрозумілий, передбачуваний і аналізується машиною за допомогою різних алгоритмів машинного навчання та є ключовим етапом текстової аналітики та передбачає низку операцій для очищення, нормалізації та структуризації даних, а також розширення необробленого тексту шляхом додавання додаткового контексту, структури або метаданих, отриманих із внутрішніх або зовнішніх джерел.

В результаті аналізу 200 користувацьких відгуків з платформи Steam [1] було визначено основні групи даних та їх формати, що уявляють шум та повинні бути видалені або замінені на етапі попередньої обробки. Серед визначених груп даних, що потребують видалення наступні:

1) структурні елементи (URL, IP та Email адреси, хештеги, HTML теги, дати, номери телефонів);

2) спеціальні символи (смайли, емодзі, графічні символи, розміщуються в доповнюваних площинах Unicode з кодами вище U+10000);
3) комбінації символів (текстові смайли, набори текстових символів);
4) числа;
5) редуплікація літер (підсилення дублюванням літер);
6) надлишкове форматування (зайві пробіли, керуючі символи, капсолізація);
7) надлишкова пунктуація;
8) нецензурна лексика та її маскування.

Крім того, на етапі попередньої обробки видаленню повинні підлягати загальні стоп-слова (перелік слів, що не несуть змістовного навантаження) та контекстні стоп-слова, що пов'язані з власними назвами та поняттями у контексті певної гри. Видалення таких «шумних» даних (окрім нецензурної лексики) пропонується виконувати за допомогою регулярних виразів (RegEx) формуванням відповідних шаблоних описів даних [2].

Серед визначених груп даних, що потребують певного опрацювання визначені наступні:

1) жаргон (акроніми, скорочення, сленг, англіцизми, абревіатури);
2) граматичні помилки, фонетичне написання, транслітерація;
3) змішення мов.

Опрацювання цих груп (а також нецензурної лексики) найбільш зручна обробкою по одному слову, тому пропонується перед їх обробкою проведення токенізації – розділення тексту на окремі частини (слова), що дозволить очистити текстові даних від стоп-слів та омонімів, оскільки вони не підлягають морфологічним змінам [3]. Після токенізації пропонується виконати виправлення помилок написання та формування слів, поділяючі їх попередньо на три основні групи: слова українською мовою, англійською мовою та слова, що містять літерні символи обох мов та/або інші символи. Такий поділ дозволить перевірити на помилки слова словниками та моделями для відповідних мов, а також віднести до окремої групи замасковані нецензурні слова та образи. Для визначення таких слів пропонується використовувати схожість Левенштейна для слів різної довжини та схожість Гемінга для слів однакової довжини. Обробка контекстних стоп-слів та подальше визначення частин мови потребує наявності їх базової форми (леми), тому пропонується перед їх обробкою проведення лематизації – зведення слова до його словникової форми.

Узагальнена блок-схема алгоритму пропонованого підходу до попередньої обробки користувацьких відгуків з використанням технологій збагачення даних наведено на рисунку 1.

За результатами моделювання можна зробити висновки, що розроблений алгоритм дозволяє виконувати попередню обробку користувацьких відгуків від специфічного «шуму» та розширювати їх змістовність.

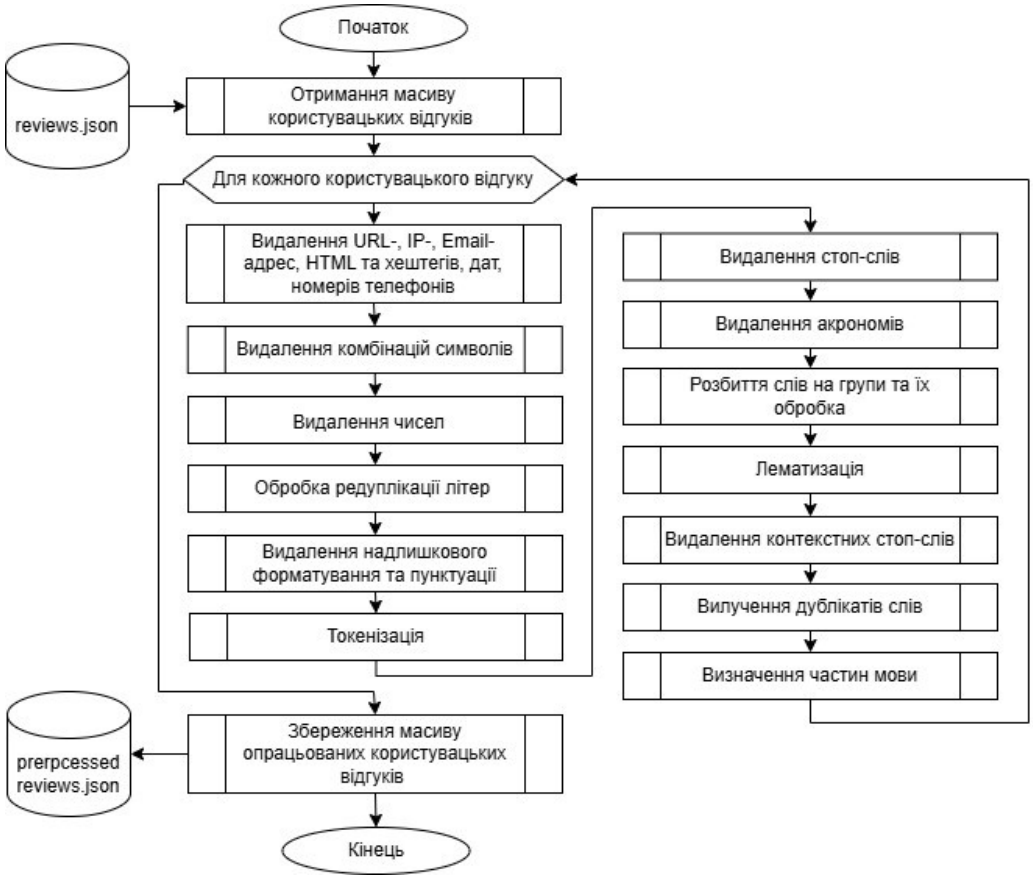


Рисунок 1 – Узагальнена блок-схема алгоритму попередньої обробки користувацьких відгуків

Література

1. Документація Steamworks. Рецензії користувачів — отримання переліку [Електронний ресурс]. – Режим доступу: https://partner.steamgames.com/doc/store/getreviews.

2. Lopez F. Mastering Python. Regular Expressions / F.Lopez, V.Romero : Packt Publishing. – 2014. – 97 p.

3. Bird S. Natural Language Processing with Python / S. Bird, E. Klein, E.Loper: O'Reilly Media. – 2009. – 504 p.

Анотація

Якісна попередня обробка складних текстів забезпечує отримання формату, що є легко зрозумілим, передбачуваним та підлягає машинному аналізу. Пропонується алгоритм попередньої обробки користувацьких відгуків індустрії комп'ютерних ігор, що очищає їх від специфічного «шуму» та розширює їх змістовність.

Ключові слова: користувацький відгук, попередня обробка, збагачення даних.

Abstract

Quality pre-processing of complex texts ensures a format that is easily understandable, predictable and subject to machine analysis. An algorithm for pre-processing user reviews of the computer game industry is proposed, which cleans them of specific "noise" and expands their content.

Keywords: user feedback, pre-processing, data enrichment.

КІБЕРБЕЗПЕКА ФІНАНСОВОГО СЕКТОРУ: ПОДАЛЬШІ ШЛЯХИ ЄВРОІНТЕГРАЦІЇ

Бердиченко І.О.[1] , кандидат юридичних наук, irinaberdychenko@gmail.com;
Дорогий Я.Ю.[2] , доктор технічних наук, доцент, yaroslav.dorohyi@donntu.edu.ua
[1] Чорноморський національний університет ім. Петра Могили, Миколаїв, Україна
[2] Донецький національний технічний університет, Дрогобич, Україна

Вступ

На сьогодні, Національний банк унормував питання організації і забезпечення кіберзахисту в банківській системі України та визначив основні засади функціонування системи кіберзахисту; принципи забезпечення інформаційного обміну між Центром кіберзахисту Національного банку і банками України; вимоги щодо заходів із забезпечення кіберзахисту об'єктів критичної інформаційної інфраструктури; вимоги щодо проведення незалежного аудиту інформаційної безпеки банків [1].

Шляхи імплементації законодавства ЄС

Національний банк України визначає порядок, вимоги та заходи із забезпечення кіберзахисту та інформаційної безпеки банками, іншими особами, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк, операторами платіжних систем та/або учасниками платіжних систем, технологічними операторами платіжних послуг, здійснює контроль за їх виконанням, утворює центр кіберзахисту Національного банку, забезпечує функціонування системи кіберзахисту для банків, інших осіб, які здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк, операторів платіжних систем та/або учасників платіжних систем, технологічних операторів платіжних послуг [2]. Крім того, Національний банк України формує вимоги та забезпечує функціонування системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури у банківській системі України та на ринках небанківських фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк, операторів платіжних систем та/або учасників платіжних систем, технологічних операторів платіжних послуг, і також забезпечує формування та забезпечення функціонування реєстру об'єктів критичної інформаційної інфраструктури у банківській системі України та на ринках небанківських фінансових послуг, регулювання та нагляд

за діяльністю на яких здійснює Національний банк України, операторів платіжних систем та/або учасників платіжних систем, технологічних операторів платіжних послуг [3].

Участь в організації заходів щодо забезпечення кіберзахисту критичної інфраструктури банків здійснює Центр кіберзахисту Національного банку України. Також у банківській системі України функціонує команда реагування на кіберінциденти CSIRT-NBU Центру кіберзахисту Національного банку України, яка приєдналася до міжнародної робочої групи команд реагування на інциденти безпеки TF-CSIRT (Computer Security Incident Response Teams) та отримала статус «ACCREDITED», що є показником відповідності вимогам міжнародних стандартів у цій сфері та показником визнання з боку інших міжнародних команд CERT/CSIRT.

Отже, Національним банком України проведено широкомасштабну роботу для забезпечення цифрової стійкості банківської системи. Разом з тим, враховуючи євроінтеграційні процеси, що активно проводяться в державі, актуальним є питання імплементації положень Регламенту (ЄС) 2022/2554 Європейського парламенту та Ради від 14 грудня 2022 року про цифрову операційну стійкість фінансового сектора та про внесення змін до Регламентів (ЄС) № 1060/2009, (ЄС) № 648/2012, (ЄС) № 600/2014, (ЄС) № 909 /2014 та (ЄС) 2016/1011 [4].

Як зазначено у статті 1 цього Регламенту, з метою досягнення високого загального рівня цифрової операційної стійкості цей Регламент встановлює єдині вимоги щодо безпеки мережевих та інформаційних систем, що підтримують бізнес-процеси фінансових організацій, а саме: вимоги до фінансових організацій щодо управління ризиками у сфері інформаційно-комунікаційних технологій (ІКТ); інформування про значні інциденти, пов'язані з ІКТ, та добровільне повідомлення компетентних органів про суттєві кіберзагрози; надання фінансовими організаціями, зазначеними у статті 2 (1), пунктах (a) – (d), компетентним органам інформації про значні операційні інциденти або інциденти, пов'язані з платежами щодо забезпечення безпеки; тестування сталості цифрових операцій; обмін інформацією та розвідданими щодо кіберзагроз та вразливостей; заходи щодо раціонального управління ризиками третіх осіб у сфері ІКТ; вимоги щодо договірних відносин, укладених між сторонніми постачальниками послуг ІКТ та фінансовими організаціями; правила створення та ведення системи нагляду за критично важливими сторонніми постачальниками послуг ІКТ під час надання послуг фінансовим організаціям; правила співробітництва між компетентними органами, а також правила нагляду та забезпечення дотримання з боку компетентних органів щодо всіх питань, що охоплюються цим Регламентом.

Відповідно до статті 2 цього Регламенту, його дія розповсюджується, серед іншого на такі фінансові установи, як кредитні та платіжні установи. Цей Регламент визначає цифрову операційну стійкість, як здатність фінан-

сової установи створювати, гарантувати та перевіряти свою операційну цілісність та надійність шляхом забезпечення, безпосередньо чи опосередковано, за допомогою використання послуг, що надаються сторонніми постачальниками послуг ІКТ, повного спектра можливостей, пов'язаних з ІКТ, необхідних для забезпечення безпеки мережі та інформаційних систем, які використовує фінансова установа, та які підтримують безперервне надання фінансових послуг та їх якість.

На сьогодні, низка положень цього Регламенту вже знайшла своє втілення в таких Законах нашої держави, як «Про основні засади забезпечення кібербезпеки України» [3], «Про платіжні послуги» [5], «Про критичну інфраструктуру» [6], іншому законодавстві.

Висновки

Враховуючи поточний стан національного законодавства доцільним є здійснення подальших кроків з імплементації положень Регламенту (ЄС) 2022/2554 Європейського парламенту та Ради від 14 грудня 2022 року про цифрову операційну стійкість фінансового сектора та про внесення змін до Регламентів (ЄС) № 1060/2009, (ЄС) № 648/2012, (ЄС) № 600/2014, (ЄС) № 909 /2014 та (ЄС) 2016/1011, стосовно:

- системи управління ризиками ІКТ;
- системи управління інцидентами, пов’язаними з ІКТ, класифікацією інцидентів;
- системи управління ризиками третіх сторін ІКТ;
- заходів впливу за порушення вимог законодавств;
- організації інформаційного обміну щодо таких подій.

Імплементація у національне законодавства вказаних положень Регламенту (ЄС) 2022/2554 дозволить значно підвищити ефективність цифрової операційної стійкості фінансового сектора, а саме банківських та платіжних установ, та створити ефективну вітчизняну систему моніторингу й оцінки, яка відповідає європейським традиціям у зазначеному напрямку функціонування фінансового сектору.

Література

1. Постанова Правління Національного банку України від 12 серпня 2022 року № 178 "Про затвердження Положення про організацію кіберзахисту в банківській системі України та внесення змін до Положення про визначення об’єктів критичної інфраструктури в банківській системі України" [Електронний ресурс]. – Режим доступу: https://bank.gov.ua/ua/legislation/Resolution_12082022_178 (дата звернення: 03.12.2024).
2. Про Національний банк України: Закон України від 20 травня 1999 року № 679-XIV / Верховна Рада України [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/679-14 (дата звернення: 03.12.2024).
3. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII / Верховна Рада України [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 15.11.2024).

4. Регламент (ЄС) 2022/2554 про цифрову операційну стійкість для фінансового сектору (DORA) [Електронний ресурс]. – Режим доступу: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32022R2554 (дата звернення: 16.11.2024).
5. Про платіжні послуги: Закон України від 30 червня 2021 року № 1591-IX / Верховна Рада України [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/1591-20#Text (дата звернення: 03.12.2024).
6. Про критичну інфраструктуру: Закон України від 16 листопада 2021 року № 1882-IX / Верховна Рада України [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 03.12.2024).

Анотація

Діяльність Національного банку України у сфері європейської інтеграції націлена насамперед на імплементацію Угоди про асоціацію між Україною та ЄС, а також інших правових актів ЄС. Реалізація положень європейського законодавства підвищує ефективність ринку фінансових послуг, забезпечує наближення національних норм регулювання і нагляду до правил ЄС та міжнародних стандартів. Це також створює передумови для посилення конкурентоздатності та рівноправної співпраці українських фінансових установ з європейськими, сприяє підвищенню рівня надання фінансових послуг та захисту прав споживачів, і заходи у сфері кібербезпеки та кіберзахисту є невід'ємним елементом такої діяльності.

Ключові слова: кібербезпека, критичні інфраструктура, фінансовий сектор, регулятор, НБУ.

Abstract

The National Bank of Ukraine's activities in the field of European integration are primarily aimed at implementing the Association Agreement between Ukraine and the EU, as well as other EU legal acts. The implementation of European legislation enhances the efficiency of the financial services market, ensures the alignment of national regulatory and supervisory standards with EU rules and international standards. It also creates preconditions for strengthening the competitiveness and equitable cooperation of Ukrainian financial institutions with European counterparts, promotes the improvement of financial service delivery and consumer rights protection. Measures in the field of cybersecurity and cyber defense are an integral part of such activities.

Keywords: cybersecurity, critical infrastructure, financial sector, regulator, National Bank of Ukraine.

ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ МОДЕЛЮВАННЯ ЗАДАЧ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ

Дорогий Я.Ю., доктор технічних наук, доцент, yaroslav.dorohyi@donntu.edu.ua;
Кравчук В.С., аспірант, vladkrava15@gmail.com
[1] Донецький національний технічний університет, Дрогобич, Україна

Вступ

Веб-застосунки є ключовим елементом цифрової інфраструктури, що забезпечують функціонування бізнесу, урядових структур і критичних галузей, включаючи енергетику, транспорт, фінанси та охорону здоров'я. Їхня зростаюча складність, а також інтеграція із системами третьої сторони значно розширюють поверхню потенційних атак. Зловмисники активно використовують вразливості веб-застосунків для компрометації даних, отримання несанкціонованого доступу чи здійснення деструктивних дій. У контексті критичної інфраструктури (КІ) такі атаки можуть мати катастрофічні наслідки для суспільства, включаючи порушення роботи життєво важливих послуг. Це зумовлює потребу у вдосконаленні процесів виявлення та усунення вразливостей.

Аналіз традиційних підходів

Тестування на проникнення (пентестінг) є основним методом оцінки безпеки веб-застосунків, який передбачає імітацію дій зловмисників для ідентифікації слабких місць у системі. Сучасні підходи до пентестінгу комбінують ручний аналіз із використанням автоматизованих інструментів, таких як Burp Suite. Хоча ці методи демонструють високу ефективність, вони є трудомісткими, залежать від кваліфікації фахівців, виділеного на тестування часу, і часто не забезпечують достатнього покриття складних сценаріїв атак. Особливо це актуально для КІ, де оперативність і точність виявлення вразливостей є критичними для уникнення значних ризиків.

Перспективи застосування штучного інтелекту

Штучний інтелект (ШІ) активно інтегрується в кібербезпекові процеси, відкриваючи нові можливості для автоматизації складних завдань. Його застосування у пентестінгу веб-застосунків дозволяє суттєво знизити часові витрати, покращити точність аналізу та забезпечити адаптацію до динамічних умов. У контексті КІ це може підвищити рівень захисту критичних систем від кіберзагроз. Проте наразі відсутні широко відомі ШІ-рішення, які б забезпечували ефективний пентестінг веб-застосунків. Розробка таких моделей є перспективним напрямом, що має значний науковий і практичний потенціал.

В якості напрямків дослідження можуть бути:

– аналіз традиційних методів тестування на проникнення веб-застосунків із врахуванням потреб КІ;

– огляд і оцінку існуючих ШІ-алгоритмів для виявлення вразливостей;

– розробку архітектури ШІ-моделі для інтеграції у процеси пентестінгу;

– проведення експериментального порівняння ефективності автоматизованих ШІ-методів із ручними підходами;

– оцінку ризиків і викликів, пов’язаних із використанням ШІ для пентестінгу КІ;

– інтеграцію прототипу моделі в сучасні інструменти, такі як Burp Suite.

Верхньорівневий опис ШІ-моделі для Burp Suite

Пропонована модель використовуватиме методи машинного навчання та обробки великих даних для ідентифікації вразливостей у веб-застосунках. Основою моделі є використання сучасних підходів до аналізу даних, включаючи тензорний аналіз, який дозволяє обробляти багатовимірні дані та будувати складні залежності між параметрами системи. Це особливо важливо для обробки великих обсягів логів, HTTP-запитів, конфігурацій та інших даних, які характеризують поведінку веб-застосунків. Модель складатиметься з кількох модулів:

1. *Модуль збору даних* – автоматизований збір і попередня обробка інформації про цільову веб-інфраструктуру, включаючи структуру, вхідні точки та API.

2. *Модуль аналізу вразливостей* – застосування тензорного аналізу для виявлення багатовимірних залежностей між характеристиками трафіку, поведінковими моделями користувачів і параметрами системи для ідентифікації аномалій, що можуть вказувати на вразливості.

3. *Модуль симуляції атак* – генерація сценаріїв атак з урахуванням результатів тензорного аналізу, що дозволяє виявляти навіть складні та приховані уразливості.

4. *Модуль оцінки ризиків* – автоматична класифікація виявлених вразливостей за рівнем ризику з використанням машинного навчання, оптимізованого для аналізу тензорних даних, а також надання рекомендацій щодо їх усунення.

5. *Інтерфейс інтеграції* – API для інтеграції з Burp Suite, що дозволить використовувати модель як частину інструментарію пентестера, забезпечуючи безперервний обмін даними та аналіз результатів.

На рисунку 1 представлено верхньорівневу архітектуру моделі та її взаємодію з Burp Suite.

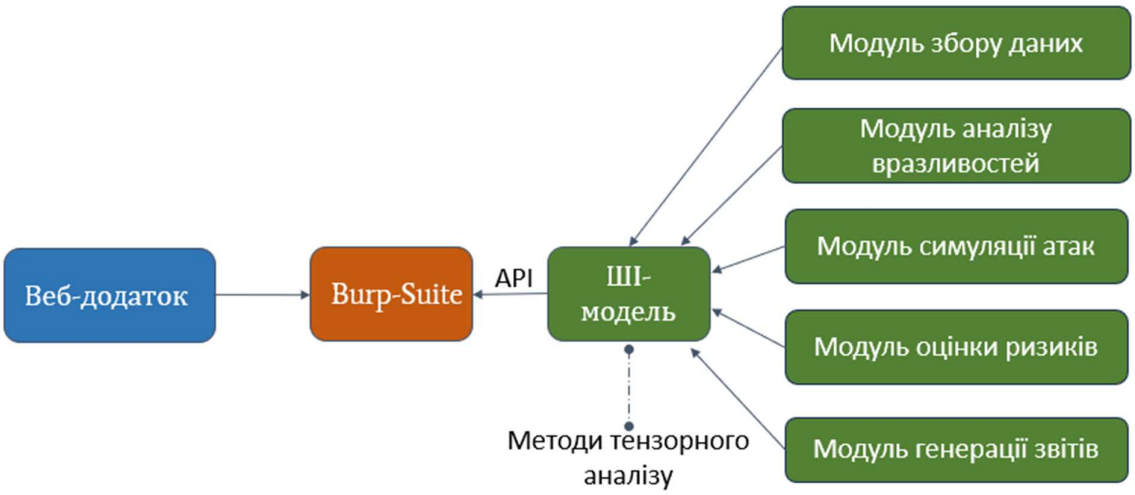


Рисунок 1. Архітектура моделі

Тензорний аналіз забезпечує ефективне виявлення прихованих закономірностей, які можуть залишитися непоміченими при застосуванні традиційних підходів. Він також дозволяє динамічно оновлювати моделі на основі нових даних, підвищуючи точність і адаптивність системи.

Використання тензорного аналізу як складової моделі значно розширює її функціональні можливості, дозволяючи враховувати складні взаємозв'язки у веб-інфраструктурі. Це забезпечить більш точне та оперативне виявлення вразливостей, що особливо важливо для захисту критичної інфраструктури. Інтеграція моделі в Burp Suite сприятиме вдосконаленню існуючих інструментів, роблячи їх доступними для ширшого кола фахівців.

Висновки

Розробка та застосування штучного інтелекту в процесі тестування на проникнення веб-застосунків відкривають нові перспективи для кібербезпеки, особливо в контексті захисту критичної інфраструктури. Використання тензорного аналізу в моделі дозволяє виявляти багатовимірні залежності між параметрами системи, підвищуючи точність і ефективність ідентифікації вразливостей. Інтеграція моделі у Burp Suite забезпечує автоматизацію тестування, скорочення часу на аналіз і мінімізацію залежності від людського фактора.

Отримані результати можуть бути використані для вдосконалення підходів до тестування безпеки, розробки комерційних рішень і зміцнення захисту критичних цифрових інфраструктур. Крім того, модель стане основою для подальших наукових досліджень у сфері кібербезпеки, сприяючи адаптації до нових викликів, пов'язаних із зростанням кіберзагроз.

Література

1. Бренд Л. Векторний і тензорний аналіз / Л. Бренд // Нью-Йорк: John Wiley & Sons. — 1947. — 276 с.

2. Дафти Д. Веб-додатки: Принципы безпеки та пентестування / Д. Дафти // Нью-Йорк. — 2020. — 320 с.

3. Гудфеллоу И., Бенджіо Й., Курвилл А. Глибоке навчання / І. Гудфеллоу, Й. Бенджио, А. Курвілл // Кембридж: MIT Press. — 2016. — 775 с.

Анотація

У статті розглянуто перспективи застосування штучного інтелекту для автоматизованого тестування на проникнення веб-застосунків із використанням тензорного аналізу. Запропоновано архітектуру ШІ-моделі, інтегрованої у Burp Suite, яка дозволяє ідентифікувати вразливості із врахуванням багатовимірних залежностей у даних. Основну увагу приділено ефективності таких методів для захисту критичної інфраструктури. Виконано аналіз традиційних підходів, оцінено потенціал сучасних алгоритмів ШІ та проведено порівняння автоматизованих і ручних методів тестування. Результати дослідження демонструють перспективність використання моделі для підвищення точності, оперативності та масштабованості процесів забезпечення кібербезпеки.

Ключові слова: кібербезпека, критична інфраструктура, штучний інтелект, тестування на проникнення, тензорний аналіз, веб-застосунки, Burp Suite.

Abstract

The article explores the prospects of applying artificial intelligence for automated penetration testing of web applications using tensor analysis. The architecture of an AI model integrated into Burp Suite is proposed, enabling the identification of vulnerabilities considering multidimensional data dependencies. The focus is placed on the effectiveness of these methods for protecting critical infrastructure. An analysis of traditional approaches has been conducted, the potential of modern AI algorithms evaluated, and a comparison of automated and manual testing methods performed. The study results demonstrate the feasibility of utilizing the model to enhance the accuracy, efficiency, and scalability of cybersecurity processes.

Keywords: cybersecurity, critical infrastructure, artificial intelligence, penetration testing, tensor analysis, web applications, Burp Suite.

МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ В УМОВАХ ЗРОСТАННЯ КІБЕРЗАГРОЗ У ХМАРНИХ ТЕХНОЛОГІЯХ

Мариніч В. В., студент, marinicv994@gmail.com
Тернопільський національний технічний університет, Тернопіль, Україна

Хмарні технології стали основою сучасних систем зберігання та обробки даних, адже вони пропонують економічність, масштабовність і гнучкість. Водночас зростання обсягів інформації, що передається і зберігається у хмарі, значно збільшує потенційні ризики.

Незаконний доступ, витік конфіденційної інформації, відсутність належного контролю над правами доступу та труднощі дотримання норм безпеки стають ключовими викликами сучасності. Для організацій, що активно використовують хмарні сервіси, питання безпеки є критично важливим для збереження репутації та довіри клієнтів.

Останні дослідження в сфері кібербезпеки хмарних технологій акцентують увагу на ряді важливих проблем, зокрема вразливостях, що виникають через неправильне управління доступом та автентифікацією. Дослідження показують, що помилки в конфігурації та слабкі методи автентифікації часто призводять до несанкціонованого доступу до хмарних ресурсів. За словами фахівців, такі проблеми можуть бути наслідком неправильного розуміння моделі спільної відповідальності між користувачами та постачальниками хмарних послуг, що веде до виникнення пропусків у забезпеченні безпеки [1].

Останнім часом активно досліджуються новітні методи захисту даних у хмарних технологіях, зокрема в контексті постквантових алгоритмів, які повинні стати відповіддю на потенційну загрозу квантових комп'ютерів для традиційних методів шифрування. В одному з досліджень, проведених у Китаї, звертається увага на те, як постквантові алгоритми можуть забезпечити більшу безпеку в умовах розвитку квантових технологій. Вони особливо важливі для захисту даних у хмарних системах, оскільки здатні забезпечити стійкість до атак з використанням квантових обчислень, що в перспективі можуть зробити традиційні методи шифрування вразливими [2].

З іншого боку, значна увага приділяється інтеграції штучного інтелекту для покращення систем моніторингу безпеки. Дослідження показують, що комбінація аналізу поведінкових моделей користувачів з автоматизованими методами може суттєво підвищити ефективність виявлення аномалій у хмарних мережах, дозволяючи швидше реагувати на потенційні загрози [3].

Метою цього дослідження є аналіз сучасних підходів до захисту інформації у хмарних технологіях, включаючи впровадження надійних алгоритмів шифрування, таких як AES-256 та RSA-2048, які забезпечують високу стійкість до кіберзагроз.

Сучасні криптографічні методи, такі як AES-256 та RSA-2048, є основою для забезпечення безпеки даних, що передаються та зберігаються в хмарних середовищах. AES-256, як симетричний алгоритм шифрування, забезпечує високу швидкість обробки великих обсягів даних і є надійним методом захисту від атак. RSA-2048, з іншого боку, є асиметричним методом шифрування, що використовується переважно для забезпечення безпеки передачі даних через інтернет, зокрема в протоколах SSL/TLS.

Останні дослідження також підтверджують ефективність гомоморфного шифрування, яке дозволяє виконувати обчислення над зашифрованими даними без їх розшифрування, що значно покращує конфіденційність в умовах обробки чутливої інформації [4].

Системи автентифікації, що використовують біометричні технології (відбитки пальців, розпізнавання обличчя), а також одноразові паролі (OTP), забезпечують значний рівень безпеки, оскільки знижують ризик викрадення облікових записів, характерний для традиційних паролів. Більш того, технологія безпарольної автентифікації стає все більш популярною. Вона базується на використанні апаратних токенів або мобільних пристроїв для ідентифікації користувачів, що дозволяє обійти необхідність введення пароля.

За даними Okta та OneLogin, безпарольні методи автентифікації можуть включати біометричні технології або апаратні ключі (наприклад, FIDO2-сумісні пристрої), що дозволяє користувачам здійснювати вхід за допомогою підтвердження через свій пристрій або за допомогою підтвердження через пуш-сповіщення [5]. Це не тільки забезпечує зручність для користувачів, а й підвищує безпеку, оскільки виключає проблеми, пов'язані з традиційними паролями, такі як їх втрата або викрадення.

Моніторинг доступу за допомогою систем SIEM (Security Information and Event Management) є важливим елементом забезпечення безпеки в реальному часі. Ці системи здійснюють збір, аналіз та кореляцію даних про події безпеки, що дозволяє оперативно виявляти та реагувати на підозрілі активності. Сучасні SIEM рішення, зокрема інтегровані з технологіями штучного інтелекту (ШІ) та машинного навчання, значно підвищують ефективність виявлення нових загроз і виявляють аномалії, які можуть залишатися непоміченими в традиційних системах.

Інтеграція ШІ в SIEM системи дозволяє автоматизувати виявлення і реагування на загрози, скорочуючи час на виявлення інцидентів і підвищуючи точність аналізу. Використовуючи алгоритми машинного навчання, ці системи створюють бази нормальної поведінки користувачів і можуть виявляти відхилення від цих норм, що може свідчити про потенційну загрозу. Це дозволяє значно знизити кількість хибних спрацьовувань і покращити якість реагування на реальні загрози, такі як атаки внутрішнього або зовнішнього походження [6].

Для захисту даних, що передаються через мережу, використовуються протоколи SSL/TLS, які підтримують сучасні алгоритми шифрування, зокрема AES-256. Ці протоколи забезпечують безпечне з'єднання для передачі даних через інтернет. AES-256 є одним з найміцніших алгоритмів шифрування, і його надійність забезпечує захист від багатьох сучасних загроз. Однак з розвитком квантових комп'ютерів зростає потреба у нових методах шифрування, що витримають атаки квантових систем. Для цього активно розробляються нові протоколи на основі квантової криптографії, які обіцяють забезпечити абсолютну безпеку в умовах загрози від квантових комп'ютерів [7].

Результати дослідження показують ефективність комплексного підходу до захисту інформації в хмарних технологіях. Впровадження передових методів шифрування, багатофакторної автентифікації та систем моніторингу доступу дозволяє значно знизити ризики кіберзагроз. У майбутньому планується зосередити увагу на розробці нових методів захисту, що враховують виклики квантових технологій, а також на інтеграції блокчейн-рішень для забезпечення прозорості та незмінності даних у хмарних системах. Крім того, важливим напрямком є вивчення впливу автоматизації процесів безпеки на зниження витрат і підвищення ефективності кіберзахисту. Отже, запропоновані підходи можуть стати основою для створення більш безпечного середовища в сфері хмарних технологій, що відповідає сучасним викликам інформаційної безпеки.

Література

1. 17 Security Risks of Cloud Computing in 2024 [Електронний ресурс] // SentinelOne. – Режим доступу: https://www.sentinelone.com/cybersecurity-101/cloud-security/security-risks-of-cloud-computing/ (дата звернення: 05.12.2024). – Назва з екрана.

2. Unpacking the Shared Responsibility Model for Cloud Security: How To Avoid Coverage Gaps and Confusion [Електронний ресурс] // Tenable®. – Режим доступу: https://www.tenable.com/blog/unpacking-the-shared-responsibility-model-for-cloud-security-how-to-avoid-coverage-gaps-and (дата звернення: 05.12.2024). – Назва з екрана.

3. Artificial intelligence and quantum cryptography - Journal of Analytical Science and Technology [Електронний ресурс] // SpringerOpen. – Режим доступу: https://jast-journal.springeropen.com/articles/10.1186/s40543-024-00416-6 (дата звернення: 06.12.2024). – Назва з екрана.

4. Enhanced Security: AES-256 Encryption for SSL and TLS [Електронний ресурс] // LuxSci. – Режим доступу: https://luxsci.com/blog/256-bit-aes-encryption-for-ssl-and-tls-maximal-security.html (дата звернення: 06.12.2024). – Назва з екрана.

5. Witts J. The Top Passwordless Authentication Solutions | Expert Insights [Електронний ресурс] / Joel Witts // Expert Insights. – Режим доступу: https://expertinsights.com/insights/the-top-passwordless-authentication-solutions/ (дата звернення: 06.12.2024). – Назва з екрана.

6. AI SIEM: How SIEM with AI/ML is Revolutionizing the SOC [Електронний ресурс] // Exabeam. – Режим доступу: https://www.exabeam.com/explainers/siem/ai-siem-how-siem-with-ai-ml-is-revolutionizing-the-soc/ (дата звернення: 07.12.2024). – Назва з екрана.

7. Post-Quantum TLS - Microsoft Research [Електронний ресурс] // Microsoft Research. – Режим доступу: https://www.microsoft.com/en-us/research/project/post-quantum-tls/ (дата звернення: 07.12.2024). – Назва з екрана.

Анотація

У статті розглянуто сучасні методи захисту інформації в хмарних технологіях. Проаналізовано криптографічні алгоритми AES-256 та RSA-2048, багатофакторну автентифікацію, інтеграцію штучного інтелекту для моніторингу доступу. Обговорюються перспективи постквантових алгоритмів та гомоморфного шифрування для підвищення безпеки даних.

Ключові слова: хмарні технології, шифрування, автентифікація, постквантові алгоритми, кібербезпека.

Abstract

The article examines modern methods of information protection in cloud technologies. It analyzes cryptographic algorithms AES-256 and RSA-2048, multifactor authentication, and the integration of artificial intelligence for access monitoring. The prospects of post-quantum algorithms and homomorphic encryption for enhancing data security are discussed.

Keywords: cloud technologies, encryption, authentication, post-quantum algorithms, cybersecurity.

ФОРМУВАННЯ ТА ЗАСТОСУВАННЯ СИГНАЛУ З ВИПАДКОВИМИ ХАРАКТЕРИСТИКАМИ

Горбачов О.С., аспірант кафедри автоматизації виробничих процесів, (oleksandr.horbachov@gmail.com)

Установа (Донбаська державна машинобудівна академія), м. Краматорськ, Україна

Сигнали з випадковими характеристиками (СВХ) широко поширені у природі та техніці. Вони описуються як процеси, значення яких у заданий час випадкові і характеризуються певними імовірнісними законами. Приклади СВХ включають шуми в радіотехнічних системах, біомедичні сигнали, а також дані, що передаються каналами зв'язку.

Випадкові сигнали - це сигнали, які не описуються формулою, але мають деякі середні характеристики: середнє значення, дисперсію, функцію щільності ймовірності і т.і.

Рисунок 1. Класифікація випадкових сигналів

Стаціонарні сигнали – це сигнали, середні показники яких не змінюються у часі.

Ергодичними сигналами – називаються випадкові сигнали, середні характеристики яких, отримані усередненням за часом, дорівнюють середнім характеристикам, отриманим усередненням з ансамблю реалізацій.

Випадковий сигнал є конкретною реалізацією у даному інтервалі часу деякого випадкового процесу. Тому функція часу, що описує випадковий сигнал,

називається вибірковою функцією (функцією реалізації) випадкового процесу.

З іншого боку, множина всіх вибіркових функцій (функцій реалізації), які можуть бути отримані при реєстрації деякого процесу, називається випадковим (або стохастичним) процесом.[1].

Методи формування сигналів

Для моделювання СВХ використовують різні підходи:

Генерація за допомогою випадкових чисел – один з методів формування сигналів для моделювання СВХ.

Існує три основні способи отримання випадкових величин:

Таблиці випадкових чисел. Вони формуються один раз зовнішнім джерелом і зберігаються на носії з можливістю подальшого багаторазового використання.

Фізичні датчики випадкових впливів. Вони будуються на основі випадкових фізичних явищ, наприклад, дробових шумів електронних ламп, шуму газового розряду, шумів рекомбінації електронів і дірок в p-n переході, радіоактивного розпаду, фотоефекту та ін..

Генератори псевдовипадкових чисел на ЕОМ. Для генерації рівномірно розподілених випадкових величин зазвичай застосовуються програмні генератори псевдовипадкових послідовностей, в основі яких лежать різні методи генерації: мультиплікативно-конгруентний метод, регістри зсуву, метод Фібоначчі і т. і.

Імітаційне моделювання. Це метод дослідження, при якому система, що вивчається, заміщається моделлю, котра з достатньою точністю описує реальну систему з метою отримати інформацію про неї.

Статистичне моделювання. Дозволяє імітувати на ПК функціонування складних випадкових процесів. При цьому оперують не з характеристиками випадкових процесів, а з конкретними випадковими числовими значеннями параметрів процесів та систем.[2].

Використання методу змінних станів та побудова моделей у формі стохастичних диференціальних рівнянь. Цей підхід передбачає вирішення задачі синтезу таких рівнянь, тобто визначення їх розмірності та коефіцієнтів з необхідною точністю.[1]

Застосування сигналів із випадковими характеристиками телекомунікації:

СВХ моделюють сигнали в каналах з шумами, оцінюють завадостійкість систем зв'язку. До них відносяться:

Канали із випадковими параметрами.

Поділяються на тропосферні, іоносферні і метеорні канали зв'язку. У таких каналах параметри в процесі передачі інформації безперервно і випадковим чином змінюються через дії різних факторів (температури, тиску, щільності середовища і т.і.).

Наземні канали оптичного зв'язку та гідроакустичні канали. У таких каналах сигнал поширюється за умов випадкових змін параметрів середовища, оскільки між передавачем і приймачем існує геометрична видимість.

Для підвищення якості передачі в каналах з випадковими параметрами використовується метод рознесення сигналів. Рішення про прийом повідомлення приймається з урахуванням аналізу кількох різних зразків сигналу, що несуть одне й теж повідомлення.

Радіолокація:

Імітація відображень сигналу радіолокації від складних об'єктів і фонового шуму. Застосування таких сигналів дозволяє:

Реалізувати переваги надширокополосної радіолокації порівняно з традиційною радіолокацією з детермінованими сигналами. Для цього використовуються когерентно-імпульсні зондувальні сигнали з випадковими параметрами (періодом повторення, частотою, фазою квантування і т. д.).

Підвищувати скритність роботи радіолокаційної станції (РЛС), знижуючи рівень помітності об'єкта, що знаходиться під захистом.

Література

1. X. Zhang, B. Wang, M. Yu and X. Fang, "Research on the influence of numerical features of random signal on stochastic modulation," 2018 13th IEEE Conference on Industrial Electronics and Applications (ICIEA), Wuhan, China, 2018, pp. 171-176, doi: 10.1109/ICIEA.2018.8397709.

2. H. Lai and W. Xu, "Statistical Properties of Kendall's Tau Under Contaminated Gaussian Model With Applications in Random Signal Detection," in IEEE Signal Processing Letters, vol. 27, pp. 655-659, 2020, doi: 10.1109/LSP.2020.2987265.

Анотація

У статті розглядаються підходи до формування сигналів з випадковими характеристиками, які знаходять застосування в телекомунікаціях, радіолокації, біомедицині та інших науково-технічних областях. Представлені теоретичні основи випадкових процесів, включаючи класифікацію. Розглянуто методи моделювання таких сигналів, включаючи використання генераторів випадкових чисел, стохастичні диференціальні рівняння, імітаційне моделювання та статистичне моделювання. Описано приклади практичного застосування сигналів з випадковими характеристиками та їх аналіз у різних системах.

Ключові слова: випадкові сигнали, генерація, моделювання.

Annotation

The article discusses approaches to the formation of signals with random characteristics that are used in telecommunications, radar, biomedicine and other scientific and technical fields. The theoretical foundations of random processes, including classification, are presented. Methods of modeling such signals are considered, including the use of random number generators, stochastic differential equations, simulation modeling and statistical modeling. Examples of practical application of signals with random characteristics and their analysis in various systems are described.

Keywords: random signals, generation, modeling.

ВРЕДОНОСНЕ ПЗ: ТИПИ, ПОШИРЕННЯ ТА СПОСОБИ ЗАХИСТУ

Жебрак А.М. , Artem172902@gmail.com
Жебрак А.М. ФОП, Київ, Україна

Актуальність питання

У сучасному цифровому середовищі захист інформаційних систем від шкідливого програмного забезпечення (ПЗ) є однією з головних задач. Шкідливі програми, зокрема комп'ютерні віруси, продовжують бути одними з найбільш серйозних загроз для безпеки користувачів і організацій. Вони здатні викликати значні фінансові збитки, втрату конфіденційних даних, порушення нормальної роботи комп'ютерних систем і навіть загрозу національній безпеці. В умовах постійного розвитку технологій і зростання кількості кіберзлочинів питання захисту від шкідливого ПЗ залишається актуальним.

Відомі дослідження та публікації

Відомо, що шкідливі програми, зокрема віруси, хробаки, трояни та програми-здирники, застосовуються кіберзлочинцями для порушення роботи інформаційних систем, викрадення даних та отримання несанкціонованого доступу до конфіденційної інформації. Як зазначає платформа Proofpoint, такі типи ПЗ можуть поширюватися через заражені файли, електронну пошту, вебсайти, а також за допомогою уразливостей у програмному забезпеченні. Різноманітні методи атак, зокрема соціальна інженерія, роблять шкідливі програми надзвичайно небезпечними та важкими для виявлення і нейтралізації [1].

Постановка задачі

Метою цього дослідження є визначення основних типів шкідливого ПЗ, механізмів його поширення та розробка рекомендацій щодо ефективних методів захисту. У роботі буде проведено огляд існуючих підходів до виявлення і блокування шкідливих програм, а також вивчено способи підвищення рівня кібербезпеки в організаціях.

Основний матеріал та результати досліджень

Шкідливе ПЗ охоплює широкий спектр загроз, серед яких можна виділити такі основні категорії:

1. Комп'ютерні віруси: Вірус — це програма, яка прикріплюється до інших файлів або програм і може поширюватися через їх виконання. Віруси можуть призводити до пошкодження даних, порушення функціонування комп'ютерних систем та крадіжки інформації. Вони часто виявляються у вигляді шкідливих вкладень у електронній пошті або під час скачування програмного забезпечення з неперевірених джерел.
2. Хробаки: Хробаки — це тип шкідливих програм, які можуть самостійно поширюватися через мережі, заражаючи інші пристрої

без участі користувача. Вони використовують уразливості в системах безпеки та можуть поширюватися дуже швидко, що робить їх особливо небезпечними для великих організацій та підприємств.

3. Трояни: Троянські програми маскуються під легітимні додатки, що дозволяє їм проникати в комп'ютерні системи. Трояни можуть бути використані для збору конфіденційної інформації, встановлення додаткового шкідливого ПЗ або надання віддаленого доступу до системи зловмисникам.
4. Програми-здирники (Ransomware): Ці програми блокують доступ до файлів або цілих систем, вимагаючи викуп за відновлення доступу. Вони можуть шифрувати файли або повністю блокувати роботу комп'ютера, і користувачі змушені платити викуп, щоб повернути контроль над своїми даними.

Механізми поширення: Шкідливі програми можуть поширюватися через різні канали, включаючи електронну пошту, вебсайти, заражені файли, програмне забезпечення і навіть USB-накопичувачі. Основними методами поширення є фішинг, соціальна інженерія, а також використання уразливостей у програмному забезпеченні. Наприклад, через уразливості в операційних системах або популярних програмах хакери можуть отримати доступ до систем і встановити шкідливі програми.

Способи захисту

Для захисту від шкідливих програм рекомендується застосовувати комплексні стратегії [1, 2]:

1. Антивірусне програмне забезпечення: Регулярне оновлення антивірусних програм є основним способом захисту від більшості типів шкідливого. Більшість сучасних антивірусів можуть виявляти і нейтралізувати віруси, хробаків, троянів і програми-здирники до того, як вони завдадуть серйозної шкоди.
2. Багатофакторна автентифікація: Впровадження багатофакторної автентифікації дозволяє значно підвищити рівень безпеки облікових записів і запобігти несанкціонованому доступу до інформації.
3. Навчання користувачів: Оскільки людський фактор є одним з основних шляхів проникнення шкідливого ПЗ, важливо проводити тренінги та навчання користувачів щодо безпеки, щоб вони могли виявляти підозрілі повідомлення та уникати шкідливих сайтів.
4. Резервне копіювання даних: Регулярне резервне копіювання важливих даних може допомогти організаціям відновити інформацію після атаки програми-здирника, зменшуючи її наслідки.

Висновки та напрямки подальших досліджень

Захист від шкідливих програм потребує комплексного підходу, що включає як технічні, так і організаційні заходи. Підвищення обізнаності користувачів, впровадження новітніх технологій виявлення загроз та постійне оновлення систем безпеки допоможуть ефективно боротися з цими загрозами. Подальші дослідження мають бути спрямовані на розробку нових методів виявлення шкідливих програм, зокрема, з використанням штучного інтелекту для прогнозування і виявлення невідомих загроз.

Література

1. Proofpoint. What Is a Computer Virus? - Types, Examples & More | Proofpoint US [Electronic resource] / Proofpoint // Proofpoint. – Mode of access: https://www.proofpoint.com/us/threat-reference/computer-virus (date of access: 07.12.2024).

2. BuddyCompany. The 10 Main Types of Computer Virus and How to Avoid Them | BuddyCompany [Electronic resource] / BuddyCompany // Feel Great at Home | BuddyCompany. – Mode of access: https://www.buddycompany.com/post/types-of-computer-virus (date of access: 07.12.2024).

Анотація

У тезах розглянуто актуальність проблеми шкідливого програмного забезпечення (ПЗ) в умовах сучасного цифрового середовища. Детально висвітлено основні типи шкідливого ПЗ, зокрема комп'ютерні віруси, хробаки, трояни та програми-здирники, які становлять найбільшу загрозу для користувачів і організацій. Описано механізми поширення шкідливих програм, включаючи використання фішингу, соціальної інженерії, заражених файлів та уразливостей у програмному забезпеченні. Приділено увагу сучасним методам захисту, таким як використання антивірусних програм, багатофакторної автентифікації, резервного копіювання даних та підвищення обізнаності користувачів. Також окреслено перспективи подальших досліджень у сфері боротьби зі шкідливим ПЗ, включаючи впровадження штучного інтелекту для прогнозування та виявлення невідомих загроз. Матеріали базуються на актуальних дослідженнях та рекомендаціях з кібербезпеки.

Ключові слова: шкідливе програмне забезпечення, кібербезпека, комп'ютерні віруси, програми-здирники, захист даних.

Abstract

The theses address the relevance of malicious software (malware) issues in the context of today's digital environment. They provide a detailed overview of key types of malware, including computer viruses, worms, trojans, and ransomware, which pose significant threats to users and organizations. Distribution mechanisms such as phishing, social engineering, infected files, and software vulnerabilities are examined. Emphasis is placed on modern protection methods, including antivirus software, multifactor authentication, data backup, and user awareness training. Future research directions are outlined, focusing on integrating artificial intelligence for predicting and detecting unknown threats. The materials are based on current studies and cybersecurity recommendations.

Keywords: malware, cybersecurity, computer viruses, ransomware, data protection.

РЕАЛІЗАЦІЯ БАГАТОТОЧКОВИХ МЕТОДІВ РОЗВ'ЯЗАННЯ ЖОРСТКИХ ЗАДАЧ КОШІ ДЛЯ HPE APOLLO 9000 HAWK

Чуб А.О., магістр, anastasiia.chub.kita@donntu.edu.ua;
Назарова І.А., к.т.н., доцент, доцент кафедри прикладної математики та інформатики, iryna.nazarova@donntu.edu.ua
Донецький національний технічний університет, м. Дрогобич, Україна

Одним із найактуальніших напрямів сучасної інформаційної науки є паралельне програмування. Постійне зростання обчислювальних потужностей систем, зміна їх архітектури та технологічної бази відкривають нові можливості для ефективного розв'язання складних задач. Проте, багато обчислювальних проблем вимагають значних ресурсів та обмежені часовими рамками. Тому використання ефективних паралельних алгоритмів та їх оптимальна реалізація на сучасних високопродуктивних комп'ютерних системах є критично важливими.

Об'єкт даного дослідження – застосування архітектурних особливостей паралельних високопродуктивних комп'ютерів для підвищення ефективності інтегрування жорстких систем звичайних диференційних рівнянь великого розміру.

Предмет дослідження – паралельні методи чисельного розв'язання жорстких задач Коші та їх динамічні характеристики.

Мета дослідження полягає у розробці та дослідженні ефективності однокрокових методів з вбудованими способами оцінки локальної похибки (блокових, повністю-неявних) для чисельного розв'язання задач Коші для системи звичайних диференціальних рівнянь. Особлива увага приділяється ефективності реалізації цих методів на паралельній архітектурі системи HPE Apollo 9000 Hawk, що розташована у Надпродуктивному обчислювальному центрі (HLRS) Університету Штутґарта.

Початкова задача Коші зводиться до розв'язання системи звичайних диференціальних рівнянь (СЗДР) першого порядку:

$$\frac{dY(x)}{dx} = F\big(x, y(x)\big), y(x_0) = y_0, x_0 \leq\ x \leq x_{end}. \qquad (1)$$

Для ефективного чисельного інтегрування жорстких СЗДР застосовуються методи з автоматичним вибором кроку. Принцип роботи таких методів полягає у постійному порівнянні фактичної локальної похибки обчислень з допустимою. Залежно від співвідношення цих величин, крок інтегрування динамічно змінюється: збільшується, якщо фактична похибка менша за нижню межу допустимого діапазону, або зменшується, якщо вона перевищує верхню межу. Такий адаптивний підхід дозволяє оптимізувати обчислювальний процес, забезпечуючи високу точність розв'язку при мінімальних обчислювальних витратах [1-2].

В докладі представлено результати розробки та аналізу якості паралелізму для двох класів однокрокових чисельних методів: k-точкових блокових та багатостадійних повністю-неявних методів по типу Рунге-Кути з адаптивним кроком інтегрування на основі розрахунку локальної апостеріорної похибки: дублювання кроку та вкладені схеми.

Блокові методи для СЗДР можуть бути представлені у вигляді системи (2), кожен блок містить k точок:

$$\bar{y}_{n,i} = \bar{y}_{n,0} + ih[\, b_i \bar{f}(x_{n,0}; \bar{y}_{n,0}) + \sum_{j=1}^{k} a_{ij}\, \bar{f}(x_{n,j}; \bar{y}_{n,j})], \quad i = \overline{1,k}, n = \overline{1,N}, \tag{2}$$

де $n -$ номер блоку, $N -$ загальна кількість блоків на інтервалі інтегрування, а $i -$ номер точки в блоці.

Застосування розкладу в ряд Тейлора дозволяє встановити, що максимальний порядок точності такого методу дорівнює $O(h^{k+1})$ [3]. Відповідно, локальна похибка у вузлах блоку має порядок $O(h^{k+2})$.

Реалізація блокових методів передбачає розв’язання системи нелінійних алгебраїчних рівнянь (СНАР) на кожному кроці, що зазвичай здійснюється ітераційними методами. Однак, на відміну від багатостадійних методів, оцінка локальної похибки для блокових методів є більш складною задачею. Відсутність прямих аналогів для блокових методів вимагає розробки спеціальних методик оцінки похибки. Крім того, зміна кроку інтегрування можлива лише після завершення обчислень для всього блоку, що може призвести до додаткових обчислювальних витрат у випадку відхилення розрахунку.

Ідея вкладених формул, яка є ефективною для оцінки локальної похибки в явних методах Рунге-Кутти, може бути успішно застосована до однокрокових багатоточкових/блокових методів. В роботі розглядаються два основні підходи до побудови вкладених блокових методів при розв’язанні нелінійних задач Коші. Перший підхід використовує комбінацію незалежних методів суміжних порядків точності і передбачає використання двох наборів формул, що дозволяють отримати розв’язки різних порядків точності. Різниця між цими розв’язками використовується як оцінка локальної похибки.

Другий підхід – це комбінація формул, побудованих на основі послідовного підвищення порядку точності Крилова. У цьому випадку формули вищого порядку отримуються шляхом додавання нових членів до формул нижчого порядку. Такий підхід дозволяє більш ефективно використовувати обчислювальні ресурси [3-4].

Розв'язання систем звичайних диференціальних рівнянь за допомогою блокових методів передбачає використання трьох рівнів паралелізму:

1) системний (за кількістю рівнянь у системі, m) – розподіл обчислень між p процесорами, кожен з яких обчислює $\lceil m/p \rceil$ компонент вектора розв'язку;

2) блоковий (за кількістю точок у блоці, k) – розподіл обчислень між $p = k$ процесорами, кожен з яких відповідає за обчислення всіх рівнянь в одній точці блоку;

3) комбінація блокового, системного та внутрішнього паралелізму методу (максимально можливий рівень паралелізму, що досягається розподілом обчислень між mk процесорами).

Зауваження: програмні додатки для розроблених чисельних методів, написано на мові Python з використанням бібліотеки «concurrent.futures». Ефективність розроблених алгоритмів для розв'язання СЗДР залежить від кількох ключових параметрів, таких як розмір задачі, властивості чисельного методу та характеристики багатопроцесорної системи. Найкращі показники паралелізму спостерігаються при виконанні таких умов: завдання має багатовимірний характер, складні праві частини СЗДР і швидкі канали передачі даних. Серед розглянутих методів найбільшою ефективністю володіють блокові вкладені методи, що поєднують системний, блоковий паралелізм та внутрішній паралелізм методу.

Паралельна програмна реалізація однокрокових методів чисельного розв’язання задачі Коші виконувалась для високопродуктивній системі HPE Apollo 9000 Hawk за допомогою інтерфейсу «concurrent.futures». Суперкомп’ютер HPE Hawk, побудований на платформі HPE Cray EX і об’єднує найпередовіші обчислювальні технології для забезпечення виняткової продуктивності та масштабованості. Однією з ключових особливостей HPE Hawk є його складна ієрархічна архітектура, яка використовує потужні процесори AMD EPYC. Частковий опис HPE Hawk показано на рис. 1-2. Основним блоком процесора є ядро, що використовується максимум 2 апаратними потоками. Кожні 4 ядра об'єднані в CCX (Core CompleX) разом із загальною кеш-пам'яттю. 2 CCX об'єднані в CCD (Cluster Complex Die), а 8 CCD приєднані до загальної матриці вводу-виводу, щоб сформувати сокет. 2 сокети утворюють вузол (рис. 2).

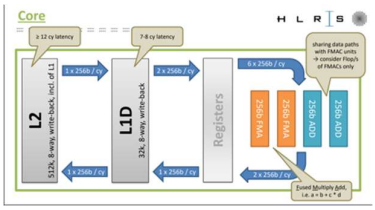


Рисунок 1. Архітектура ядра HPE Apollo 9000 Hawk

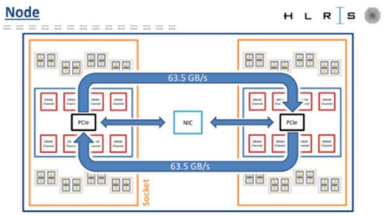


Рисунок 2. Схема вузла архітектури HPE Apollo 9000 Hawk

HPE Apollo 9000 Hawk підтримує стандартні інструменти для паралельного програмування, такі як MPI і OpenMP. Висока продуктивність, універсальність та енергоефективність HPE Hawk роблять його незамінним інструментом для сучасних наукових досліджень та інженерних розробок. Ця платформа дозволяє ефективно вирішувати складні обчислювальні задачі, які виникають у різних галузях знань при моделюванні складних динамічних систем із зосередженими параметрами, що описуються СЗДР.

Майбутні дослідження будуть спрямовані на підвищення ефективності паралельних методів розв'язання задач Коші за рахунок адаптивних стратегій керування кроком та порядком методу, а також використання спектрального аналізу для оцінки стійкості.

Висновки. Таким чином, стаття містить результати досліджень авторів, що стосуються розробки та аналізу ефективності розв'язання жорстких початкових задач Коші на основі однокрокових блокових та багатостадійних повністю-неявних методів. Алгоритмічно-програмна реалізація та експериментальна валідація розроблених алгоритмів на суперкомп'ютері HPE Apollo 9000 Hawk продемонструвала, що досягнення високої ефективності паралельних обчислень вимагає комплексного підходу, який враховує як властивості чисельних методів, так і особливості архітектури обчислювальної системи, включаючи комунікаційну топологію, ієрархію пам'яті та інші фактори.

Література

1. Hairer E., Wanner G. Solving Ordinary Differential Equations II: Stiff and Differential-Algebraic Problems. — Springer Verlag, 2010. — 586 p.
2. Vuik C., Vermolen F.J., Gijzen M.B., Vuik M.J. Numerical Methods for Ordinary Differential Equations. — TUDelft Open, 2023. — 136p.
3. Назарова І.А., Дмитрієва О.А. Паралельні обчислення. — Покровськ: ДВНЗ «ДонНТУ», 2020. — 246 с.
4. Фельдман Л.П., Назарова І.А. Паралельні однокрокові методи чисельного розв'язання задачі Коші: монографія. — Донецьк: «ДВНЗ» ДонНТУ, 2011. — 183 с.

Анотація

Доклад присвячений дослідженню ефективності паралельних однокрокових чисельних методів розв'язання жорстких багатовимірних задач Коші та їх реалізації на суперкомп'ютері HPE Apollo 9000 Hawk. Результати дослідження підтверджують, що ефективність паралельних обчислень залежить як від вибору чисельного методу, так і від особливостей архітектури обчислювальної системи.

Ключові слова: суперкомп'ютер, жорстка початкова задача, однокрокові блокові та повністю-неявні методи.

Abstract

The paper is devoted to the study of the efficiency of parallel one-step numerical methods for solving stiff multidimensional Cauchy problems and their implementation on the HPE Apollo 9000 Hawk supercomputer. The results of the study confirm that the efficiency of parallel computing depends both on the choice of numerical method and on the features of the computing system architecture.

Keywords: supercomputer, stiff initial problem, one-step block and fully implicit methods.

ДОСЛІДЖЕННЯ ОСОБЛИВОСТЕЙ ПОВЕДІНКИ КОРИСТУВАЧІВ ДЛЯ СТВОРЕННЯ ІНФОРМАЦІЙНОГО ВЕБ-РЕСУРСУ

Іванов В.Г., к.т.н, проф., valeriy.ivanov@nure.ua;
Кузнєцов І.С., студент, ivan.kuznietsov@nure.ua
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасні вебресурси стикаються з гострою конкуренцією, що робить UX/UI дизайн вирішальним. Аналіз поведінки користувачів стає все більш важливим для підвищення зручності використання та функціональності інтерфейсів. Інтеграція вебаналітики з методами машинного навчання відкриває нові можливості для автоматизації та оптимізації.

Метою цього дослідження є розробка системи, яка використовує методи штучного інтелекту для аналізу поведінки користувачів, прогнозування проблем UX і надання рекомендацій щодо покращення інтерфейсів [1]. У дослідженні вивчалися вебсайти, орієнтовані на взаємодію з користувачем, щоб оцінити їхню взаємодію з користувачем (UX) та інструменти, які використовуються для оцінки та оптимізації.

З початкового відбору з трьохсот ресурсів було сформовано вибірку зі ста вебсайтів, що представляють різноманітні типи та теми. Критерії відбору включали актуальність дизайну, наявність інструментів вебаналітики та теплових карт, а також можливість вивчати взаємодію користувача з інтерфейсом [2]. Вибрані сайти були розділені на чотири групи:

– інформаційні ресурси, такі як блоги та освітні платформи;
– сайти електронної комерції, включаючи інтернет-магазини;
– корпоративні ресурси, що представляють різні компанії та організації;
– бізнес ресурси, орієнтовані на надання професійних послуг.

Ця структура зразка дозволила нам створити репрезентативну основу для детального аналізу. На основі класифікованої вибірки ми визначили інструменти вебаналітики, які використовуються на різних сайтах, і їхній вплив на взаємодію з користувачем. Основні інструменти включали Google Analytics і Crazy Egg, які полегшували збір даних про кліки, переходи, час, проведений на сторінках, та інші аспекти взаємодії з користувачем. Особливу увагу ми приділили тепловим картам, які візуалізували діяльність користувачів і виділяли як найпопулярніші елементи інтерфейсу, так і потенційні проблемні області. Крім того, для більш глибокого аналізу моделей поведінки використовувалися технології запису сеансу, такі як SessionCam.

На основі зібраних даних ми проаналізували ключові показники взаємодії, включаючи кількість сеансів, середню тривалість сесії, показник відмов, популярні елементи інтерфейсу та частоту повторних відвідувань. Ці показники допомогли нам визначити моделі, які сприяли покращенню взає-

модії з користувачем, а також області, які потребують оптимізації [3]. Візуалізація даних, представлена у вигляді графіків і теплових карт, ефективно ілюструвала виявлені тенденції.

Для збору даних про поведінку користувачів ми пропонуємо використовувати такі інструменти, як Google Analytics і теплові карти, зокрема SessionCam і Crazy Egg. Ці технології дозволяють нам візуалізувати взаємодію користувачів з інтерфейсами, досліджувати їхні кліки, шляхи навігації та час, проведений на сторінках. Очікується, що система використовуватиме дані, зібрані цими інструментами, для подальшого аналізу.

У проекті пропонується використовувати різні методи обробки даних, у тому числі алгоритми машинного навчання, такі як K-середні для кластеризації користувачів на основі подібних поведінкових характеристик, моделі Маркова для аналізу послідовностей дій і випадкові ліси для прогнозування ключових показників взаємодії з користувачем.

Архітектура системи ретельно описана та детально окреслена. Вона включає модулі для збору даних, обробки даних, аналізу та моделювання та візуалізації результатів. План впровадження передбачає запровадження системи на вебсайтах для аналізу користувачів. Спочатку тестування проводитиметься на невеликих вибірках вебсайтів, щоб перевірити точність і ефективність аналізу. На основі результатів система буде доопрацьована та інтегрована в існуючі вебресурси, надаючи розробникам і дизайнерам цінний інструмент для оптимізації взаємодії з користувачем (UX).

Підсумовуючи, ця робота представляє проект, який детально описує, як можна розробити систему для автоматизації аналізу досвіду користувача. Він служить основою для впровадження такого продукту та корисним посібником для розробників, які прагнуть включити подібні системи у свої проекти.

Література

1. Hartson, R., Pyla, P.: Chapter 1 - What Are UX and UX Design? In: Hartson, R., Pyla, P.(eds.) The UX Book 2nd edn., pp. 3–25. Morgan Kaufmann, Boston (2019).

2. Perrin, J.M., Yang, L., Barba, S., Winkler, H.: All that glitters isn’t gold: The complexities of use statistics as an assessment tool for digital libraries. Electron. Libr. 35, 185–197 (2017).

3. Kaur, K., Singh, H.: Click analytics: what clicks on webpage indicates? In: Proceedings on 2016 2nd International Conference on Next Generation Computing Technologies, NGCT2016, pp. 608–614 (2017).

Анотація

Ця робота зосереджена на розробці системи автоматизованого аналізу користувацького досвіду (UX) на вебсайтах з використанням технологій штучного інтелекту та машинного навчання. Мета полягає в тому, щоб покращити зручність використання інтерфейсу шляхом аналізу поведінки користувачів, прогнозування потенційних проблем UX і надання рекомендацій щодо оптимізації дизайну. Система інтегрує вебаналітику з передовими алгоритмами машинного навчання. Розглядаються такі ключові інструме-

нти, як теплові карти, записи сеансів, алгоритми кластеризації та методи візуалізації результатів. Запропонована архітектура дозволяє адаптувати систему до різних типів вебресурсів, оснащуючи розробників необхідними інструментами для покращення UX.

Ключові слова: аналітика вебсайтів, досвід користувача (UX), штучний інтелект, машинне навчання, оптимізація інтерфейсу, теплові карти, візуалізація даних.

Abstract

This work focuses on developing a system for the automated analysis of user experience (UX) on websites using artificial intelligence and machine learning technologies. The goal is to improve interface usability by analyzing user behavior, predicting potential UX issues, and offering recommendations for design optimization. The system integrates web analytics with advanced machine learning algorithms. Key tools such as heat maps, session recordings, clustering algorithms, and methods for visualizing results are examined. The proposed architecture allows for the adaptation of the system to various types of web resources, equipping developers with the necessary tools to enhance UX.

Keywords: website analytics, user experience (UX), artificial intelligence, machine learning, interface optimization, heat maps, data visualization.

АНАЛІЗ ЗАСТОСУВАННЯ АЛГОРИТМІВ МАШИННОГО НАВЧАННЯ ДЛЯ ВИЯВЛЕННЯ ПРИХОВАНИХ КІБЕРЗАГРОЗ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Гільгурт С. Я.[1], д-р техн. наук, ст. наук. співр.
serhii.hilgurt@donntu.edu.ua
Ковилін А.В.[2], аспірант, anton.v.kovylin@gmail.com
1 Донецький національний технічний університет, м. Дрогобич, Україна
2 Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України, м. Київ, Україна

У зв'язку зі зростаючою останнім часом залежністю суспільства від інфраструктурних систем енергетиці, транспорту, водопостачання, зв'язку тощо, кібератаки на подібні системи здатні призвести до катастрофічних наслідків, таких як перебої в електропостачанні, транспортні колапси, витік конфіденційної інформації та ін. В особливо важких випадках можливе навіть виникнення загрози життю людей. Кіберзагрози стають все більш складними та прихованими, що ускладнює їх виявлення традиційними методами. Такі відомі атаки на об'єкти критичної інфраструктури, як Stuxnet, BlackEnergy або Colonial Pipeline, демонструють, наскільки серйозними можуть бути наслідки їх успішної реалізації. З огляду на зростаючу складність і динаміку сучасних кіберзагроз, традиційні підходи, такі як сигнатурний аналіз, часто виявляються недостатньо ефективними. Тому дослідники, спеціалісти з безпеки комп'ютерних систем та дата-аналітики все більш активно використовують методи штучного інтелекту та машинного навчання (англ. Machine Learning – ML) [1].

Мета дослідження полягає в аналізі можливостей і ефективності застосування алгоритмів ML для виявлення прихованих кіберзагроз на об'єктах критичної інфраструктури.

До найбільш поширених методів ML можна віднести: ***Моделі з вчителем*** (Supervised Learning Models) [2], ***Моделі без вчителя*** (Unsupervised Learning Models) [2], ***Напівконтрольовані моделі*** (Semi-Supervised Learning Models) [3], ***Моделі з підкріпленням*** (Reinforcement Learning Models) [4], ***Ансамблеві методи*** (Ensemble Learning Models) [5], ***Глибоке навчання*** (Deep Learning Models) [6]. Підходи до побудови систем кіберзахисту, що базуються на цих методах можуть бути використані для виявлення закономірностей в поведінці інформаційних систем, спираючись на результати аналізу мережевого трафіку або записи в системних журналах.

Для проведення експериментів з метою оцінки кількісних характеристик алгоритмів ML, було створено програмний засіб, використовуючи мову програмування Python та широкий набір бібліотек, в тому числі – спеціалізованих, призначених для аналізу даних, побудови нейронних мереж та за-

стосування технології машинного навчання. В якості джерела вхідної інформації використано відкритий набір даних ***Network Traffic Analysis for Cybersecurity*** (від University of New South Wales, Australia) [7], доступний для вільного використання, який містить детальну інформацію про мережеві з'єднання та аномальні події, що виникають в комп'ютерних мережах. В табл. 1 наведено кількісні значення показників, що були отримані в результати проведення експериментів, а в табл. 2 – їх швидкісні характеристики.

Таблиця 1

Зведення результатів проведених експериментів

Model	Precision	Recall	F1-Score	Specificity	Cohen Kappa	AUC
Isolation Forest	0,70247	0,03096	0,0593	0,972053	0,00195	0,5015
KMeans	0,82258	0,64482	0,7229	0,703625	0,3105	0,6742
DBSCAN	0,96774	0,00251	0,0050	0,999821	0,00149	0,5011
LOF	0,669074	0,02949	0,0564	0,968910	-0,00103	0,4992
MLP Classifier	0,999974	0,99989	0,9999	0,999946	0,9998	0,9999
Label Propagation	0,999848	0,99491	0,99737	0,999678	0,99182	0,9972
Deep Learning Model	0,999941	0,99989	0,9999	0,999875	0,99975	0,9998
Ensemble Model	0,999932	0,99999	0,9999	0,999857	0,99988	0,99992

Аналізуючи результати експериментів, приходимо до наступних висновків. Для випадків, коли потрібна висока швидкодія обробки даних, більш прийнятними є алгоритми K-Means та Isolation Forest (unsupervised), а для менш критичних за часом застосувань доцільно використовувати методи MLP Classifier (supervised) та Label Propagation (semi-supervised), які показують більш точні результати. Найкраще себе показали моделі Deep Learning Model (deep learning на базі sequential) та Ensemble Model, яка використовує в своїй реалізації логістичну регресію (Logistic Regression), метод опорних векторів (SVM) та метод найближчих сусідів (KNN), які об'єднуються в класифікатор з голосуванням (Voting Classifier), що забезпечує хороший баланс між кількістю виявлених аномалій, точністю та швидкістю виконання.

Таблиця 2

Порівняння швидкості аналізу даних за допомогою ML-моделей

Model	Technique Type	Execution Time, sec	Anomalies Detected
Isolation Forest	Unsupervised	1,549	5260
KMeans	Unsupervised	4,722	93551
DBSCAN	Unsupervised	86,408	310
LOF	Unsupervised	44,285	5261
MLP Classifier	Supervised	12,962	119332
Label Propagation	Semi-supervised	30,563	118752
Deep Learning Model	Deep Learning	5,664	119336
Ensemble Model	Ensemble	130,382	119348

Висновки. Результати проведеного дослідження свідчать, що використання алгоритмів машинного навчання розширює можливості дата-аналітиків та спеціалістів з безпеки комп'ютерних систем, та можуть бути ефективно використані для виявлення прихованих кіберзагроз на об’єктах енергетичної інфраструктури.

Проведений теоретичний і практичний порівняльний аналіз майже десятка алгоритмів машинного навчання з використанням публічного набору даних Network Traffic Analysis for Cybersecurity, дозволив виявити з них найбільш перспективні для виявлення аномалій у вхідних даних. Отримані для різних моделей характеристики точності та швидкодії дозволили виокремити алгоритми, найбільш придатні для різних умов використання в системах захисту інформації.

В подальших дослідженнях планується проведення експериментів з більш тонкими налаштуваннями досліджених алгоритмів з метою ще більшого покращення досягнутих показників.

Література

1. State-of-the-art in artificial neural network applications: a survey / O. I. Abiodun et al. Heliyon. 2018. Vol. 4, no. 11. P. e00938. URL: https://doi.org/10.1016/j.heliyon.2018. e00938.

2. A comparison of unsupervised and supervised machine learning algorithms to predict water pollutions / N. Zamri et al. Procedia computer science. 2022. Vol. 204. P. 172–179. URL: https://doi.org/10.1016/j.procs.2022.08.021.

3. Semi-supervised learning for sentiment classification using small number of labeled data / V. L. Shan Lee et al. Procedia computer science. 2019. Vol. 161. P. 577–584. URL: https://doi.org/10.1016/j.procs.2019.11.159.

4. Kumar Shakya A., Pillai G., Chakrabarty S. Reinforcement Learning Algorithms: a brief survey. Expert systems with applications. 2023. P. 120495. URL: https://doi.org/10.1016/j.eswa.2023.120495.

5. Khan A. A., Chaudhari O., Chandra R. A review of ensemble learning and data augmentation models for class imbalanced problems: combination, implementation and evaluation. Expert systems with applications. 2023. P. 122778. URL: https://doi.org/10.1016/j.eswa.2023.122778.

6. Deep learning modelling techniques: current progress, applications, advantages, and challenges / S. F. Ahmed et al. Artificial intelligence review. 2023. URL: https://doi.org/10.1007/s10462-023-10466-8.

7. Cyber Attack Detection with Random Forest. Input Data – UNSW_NB15_training-set.csv. Kaggle. URL: https://www.kaggle.com/ code/akritiupadhyayks/cyber-attack-detection-with-random-forest/input?select=UNSW_NB15_training-set.csv. (дата звернення: 08.12.2024).

Анотація

У дослідженні представлено аналіз застосування алгоритмів машинного навчання для виявлення прихованих кіберзагроз на об'єктах критичної інфраструктури. Досліджено ефективність таких моделей, як Isolation Forest, KMeans, DBSCAN, LOF, MLP Classifier, Label Propagation, Deep Learning Model та Ensemble Model. Розглянуто особливості застосування цих алгоритмів для моніторингу, аналізу аномалій та ідентифікації загроз. Показано, що використання гібридних підходів та ансамблевих моделей підвищує точність виявлення. Результати дослідження підтверджують перспективність інтеграції алгоритмів машинного навчання у системи кіберзахисту критичної інфраструктури. Ключові слова: алгоритми машинного навчання, виявлення кіберзагроз, критична інфраструктура, аномалії, кібербезпека.

Ключові слова: об'єкт критичної інфраструктури, захист інформації, машинне навчання, набір даних.

Abstract

The paper presents an analysis of machine learning algorithms applied to hidden cyber threat detection in critical infrastructure systems. The study evaluates the effectiveness of models such as Isolation Forest, KMeans, DBSCAN, LOF, MLP Classifier, Label Propagation, Deep Learning Model, and Ensemble Model. The features of these algorithms for monitoring, anomaly analysis, and threat identification are explored. It is demonstrated that hybrid and ensemble approaches enhance detection accuracy. The results confirm the potential of integrating machine learning algorithms into critical infrastructure cybersecurity systems. Keywords: machine learning algorithms, cyber threat detection, critical infrastructure, anomalies, cybersecurity.

Keywords: critical infrastructure facility, information security, machine learning, data set.

ДОСЛІДЖЕННЯ ТА РОЗРОБКА МОДЕЛІ ОБРОБКИ ДАНИХ В КОМП'ЮТЕРНИХ СИСТЕМАХ "РОЗУМНИЙ ЦІННИК"

Швайко І.О., студент, ihor.shvaiko.kita@donntu.edu.ua
Любименко О.М., к.ф.-м.н,доц., olena.liubymenko@donntu.edu.ua
Штепа О.А., к.т.н., доц., oleksandr.shtepa@donntu.edu.ua
ДВНЗ «Донецький національний технічний університет», м. Дрогобич, Україна

Сучасний ринок роздрібної торгівлі потребує інноваційних рішень для підвищення ефективності процесів ціноутворення. Одним із перспективних напрямів є впровадження систем типу «Розумний цінник», які дозволяють автоматизувати та динамічно оновлювати цінники за допомогою інтегрованих IoT-пристроїв, машинного навчання та хмарних технологій. Такий підхід дає змогу знизити витрати, мінімізувати кількість помилок, підвищити точність і швидкість оновлення цін, а також покращити загальний досвід клієнтів і конкурентоспроможність бізнесу.

Метою даного дослідження є розробка та тестування моделі обробки даних у системі «Розумний цінник», яка інтегрує IoT та динамічні моделі ціноутворення, щоб підвищити економічну ефективність роздрібних підприємств. Система «Розумний цінник» включає електронні цінники, датчики, шлюзи Bluetooth та програмне забезпечення для обробки даних. Електронні цінники динамічно оновлюють ціни, а дані з датчиків та інших джерел через шлюзи надходять до центрального серверу, де відбувається їх аналіз.Основними елементами системи є: електронні цінники, що забезпечують автоматичне оновлення цін у реальному часі; шлюзи Bluetooth, які передають дані від цінників та сенсорів до серверу і назад; програмне забезпечення, що виконує аналіз попиту, рівня запасів, конкурентних цін та приймає рішення щодо коригування вартості товарів.

Проектування системи передбачає створення математичної моделі ціноутворення, яка враховує рівень попиту, конкурентні ціни та запаси, а також розробку програмного модуля, що реалізує алгоритми оптимізації цін. Для розробки прототипу програмного забезпечення було використано інструменти Python, Excel та бібліотеки для аналізу великих даних. Тестування здійснювалося у три етапи: моделювання точності прогнозування попиту, перевірка системи на згенерованих даних роздрібної торгівлі та оцінка швидкості оновлення даних разом із точністю прогнозів. Результати тестування показали, що система здатна скоротити час оновлення цінників на 80%, підвищити точність даних про запаси на 95% та знизити операційні витрати на робочу силу.

Дослідження охоплювало аналіз предметної галузі, розробку математичної моделі для оптимізації цін та створення прототипу програмної системи, яка пропонує рекомендації та динамічно оновлює ціни залежно від попиту,

конкурентного середовища та наявності товарів. У системі застосовуються технології електронного паперу, RFID/NFC міток, датчики для відстеження покупців і товарів, а також машинне навчання та аналіз великих масивів даних для реагування у реальному часі. Завдяки цьому забезпечується точність і оперативність ціноутворення, оптимізація запасів, індивідуалізація пропозицій для клієнтів та екологічна відповідальність бізнесу.

Світовий досвід засвідчує, що такі системи вже впроваджуються провідними роздрібними мережами. Компанії на кшталт Ahold Delhaize, Walmart та Amazon Go активно експериментують із динамічними цінами, електронними цінниками й технологіями «Just Walk Out», щоб оперативно реагувати на зміни ринку та попиту, підвищувати точність ціноутворення та покращувати досвід покупців.

Етапи реалізації проєкту включали розробку математичної моделі, проектування інфраструктури системи, створення та впровадження прототипу програмного забезпечення, а також комплексне тестування. Розроблена математична модель допомагає формалізувати взаємозв'язок між ціною товару, попитом, запасами та прибутковістю. Вона забезпечує автоматизацію процесів аналізу даних, прийняття рішень та адаптації до мінливих ринкових умов. Зокрема, модель враховує прибуток як різницю між доходом та витратами, попит як функцію від минулих продажів і цін, а також рекомендації щодо коригування вартості товарів.Для перевірки ефективності було створено програмний прототип, що обробляє Excel-файли, аналізує дані про ціни та продажі, генерує рекомендації щодо зміни цін залежно від попиту та залишків товарів. Тестування підтвердило високу ефективність системи: електронні цінники автоматизують до 80% процесів оновлення, оптимізація цін підвищує прибуток, а точність даних дозволяє підтримувати довіру клієнтів. Рішення також сприяє сталому розвитку, мінімізуючи використання паперу та позитивно впливаючи на довкілля.

Наукова цінність розробленої системи полягає у створенні моделі, здатної ефективно обробляти дані з новітніх сенсорів та перетворювати їх на корисну інформацію для динамічного оновлення цін. Практичне значення полягає у можливості впровадження проєкту в повсякденну роботу роздрібних магазинів, що дасть змогу автоматизувати зміну цін, заощадити ресурси, знизити ризики помилок і підвищити якість обслуговування клієнтів.

Таким чином, система «Розумний цінник» має великий потенціал для впровадження у роздрібну торгівлю. Вона автоматизує процеси ціноутворення, швидко реагує на зміни попиту й конкуренції, підвищує ефективність управління запасами та забезпечує кращий користувацький досвід, покращуючи конкурентоспроможність підприємств на сучасному динамічному ринку.

Література

1. Дослідження ринку Майбутнє. Smart Labels Market Size, Share & Growth Report 2032 [Електронний ресурс] // Market Research Future. – Режим доступу: https://www.marketresearchfuture.com/reports/smart-labels-market-10929 (дата звернення: 08.11.2024).

2.Fortune Business Insights. Smart Label Market Size, Share & Industry Growth Report 2030 [Електронний ресурс]. – Режим доступу: https://www.fortunebusinessinsights.com/smart-label-market-103139 (дата звернення: 08.11.2024).

3.Сміт Е. Розумні полиці: що роздрібні торговці повинні знати про новий тренд [Електронний ресурс] // Журнал BizTech. – 2022. – Режим доступу: https://biztechmagazine.com/article/2022/01/smart-shelves-what-retailers-should-know-about-emerging-trend-perfcon (дата звернення: 08.12.2024).

4.Phillips R.L. Pricing and Revenue Optimization. – Stanford: Stanford Business Books, 2005. – 38 с.

Анотація

Наукова новизна дослідження полягає в розробці нових підходів до моделювання та автоматизації процесів обробки даних у системі «Розумний цінник». Практичне значення роботи з можливістю впровадження розробленої системи у практику автоматизації процесів ціноутворення, що сприятиме оптимізації операцій у сфері роздрібної торгівлі.

Ключові слова: розумний цінник, IoT, машинне навчання, динамічне ціноутворення, RFID-мітки.

Abstract

The scientific novelty of the research lies in the development of new approaches to modeling and automation of data processing processes in the "Smart Price Tag" system. The practical significance of the work lies in the possibility of implementing the developed system in the practice of automating pricing processes, which will contribute to the optimization of operations in the retail sector.

Keywords: smart price tag, IoT, machine learning, dynamic pricing, RFID tags.

ОПТИМІЗАЦІЯ МЕХАНІЗМІВ ГОЛОСУВАННЯ В БЛОКЧЕЙН СИСТЕМАХ ЗА ДОПОМОГОЮ КВАДРАТИЧНОГО ГОЛОСУВАННЯ

Попова А.О., магістрант, anna.popova.kita@donntu.edu.ua
Любименко О.М., доцент, e.n.lyubimenko@gmail.com
«Донецький Національний Технічний Університет», Дрогобич, Україна

У сучасному світі блокчейн-технології стрімко еволюціонують, набуваючи популярності у різних сферах завдяки своїм перевагам у безпеці, прозорості та децентралізації. Однією з ключових сфер застосування блокчейну є організація електронного голосування, де критично важливими аспектами є захист від маніпуляцій, гарантія достовірності та стійкість до зовнішніх атак. Використання блокчейну у системах голосування дозволяє забезпечити надійність збереження даних, унеможливлює підробку результатів і гарантує прозорість процедур завдяки децентралізованому підходу.

Попри значні переваги, існуючі системи блокчейн-голосування все ще стикаються з викликами, серед яких ризики маніпуляцій та зосередження впливу в руках окремих суб'єктів. Це демонструє необхідність удосконалення технологій, спрямованих на підвищення справедливості та надійності процесу голосування.

Одним із перспективних рішень є впровадження квадратичного голосування — інноваційного математичного підходу, який спрямований на врахування не лише вибору учасників, але й інтенсивності їхніх переваг. Завдяки квадратичній моделі виборці можуть виражати свої пріоритети через багаторазове голосування, що водночас пропорційно збільшує його вартість. Це забезпечує баланс між впливом учасників і запобігає домінуванню окремих груп, створюючи більш демократичний і безпечний механізм прийняття рішень.

Квадратичне голосування дозволяє виборцям розподіляти свої голоси відповідно до інтенсивності їхніх уподобань, при цьому вартість кожного голосу за альтернативу зростає квадратично. Наприклад, якщо виборець хоче віддати 2 голоси за альтернативу, це коштуватиме йому 4 кредити, а 3 голоси – вже 9 кредитів. Це допомагає врівноважити інтенсивність і широту переваг виборців. Цей метод забезпечує більшу точність у відображенні індивідуальних уподобань виборців, але також ускладнює підрахунок голосів і стратегічне планування під час голосування.

Квадратична функція вартості голосів дозволяє ефективно відобразити інтенсивність переваг виборців, оскільки кожен додатковий голос стає все дорожчим. Це сприяє тому, що виборці обирають пріоритетні альтернативи з більшою обачністю, уникаючи надмірної концентрації голосів на одній альтернативі без вагомої причини.

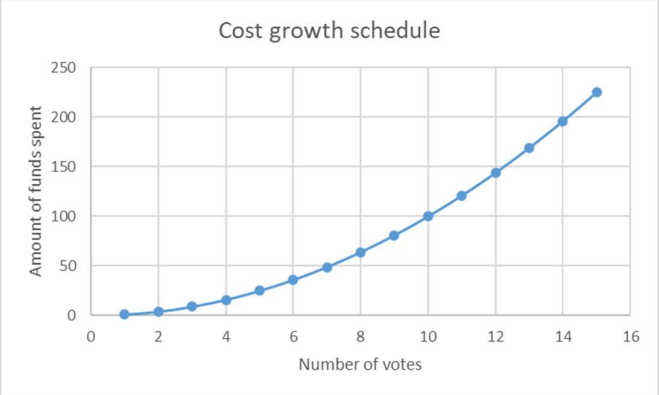


Рисунок 1 – Графік зростання витрат при квадратичному голосуванні

На рисунку 1 представлено графік, який ілюструє збільшення витрат на кожен наступний голос, що наочно демонструє, як змінюються витрати залежно від кількості відданих голосів.

Квадратичне голосування є оптимальним вибором для покращення безпеки та надійності блокчейн-систем, сприяючи створенню справедливого та стійкого процесу прийняття рішень.

Квадратичне голосування – це метод, що базується на квадратичному врахуванні голосів виборців. У цьому методі кожен учасник голосування має надати якусь певну кількість голосів, які потім підносяться до квадрату, щоб виразити їхню вартість. Тоді суму вкладу спонсорів за певний проект можна представити математично наступним чином, як приведено у формулі нижче [1].

$$s(p_m) = \sum_{i=1}^{n} c_i^2 , \quad (1)$$

де p_m – проект, виставлений на голосування;
m – загальна кількість проектів на голосуванні;
s – сума вкладу спонсорів за голоси;
n – загальна кількість спонсорів;
c_i – кількість голосів спонсора.

В такому випадку бюджет конкурсу буде динамічним та мати залежність від вартості голосів. Його можна представити у вигляді формули, приведеної нижче.

$$b = \sum_{i=1}^{m} s(p_i) , \quad (2)$$

де b – бюджет конкурсу;
p_i – проект, висунутий на голосування;
s – сума вкладу спонсорів за голоси;
m – загальна кількість проектів на голосуванні.
Виразимо інакше розрахунок бюджету конкурсу у формулі нижче.

$$b = \sum_{i=1}^{n} d_i , \quad (3)$$

де b – бюджет конкурсу;
n – загальна кількість спонсорів;
d_i – сума вкладу спонсора в бюджет конкурсу.

Далі кожен спонсор може проголосувати за проекти, розподіливши суму свого вкладу в бюджет конкурсу між проектами. Кількість голосів, яку спонсор може надати проекту визначається як корінь квадратний від суми внесених їм коштів за проект.

$$c_i = \sqrt{s_i}\,, \tag{4}$$

де c_i – кількість голосів спонсора;
s_i – сума вкладу спонсора за проект.

Таким чином, виведемо формулу розрахунку кількості голосів для певного проекту. Її приведено нижче.

$$\mathrm{c}(p_m) = \sum_{i=1}^{n} \sqrt{s_i}\,, \tag{5}$$

де c – кількість голосів;
p_m – проект, висунутий на голосування;
n – загальна кількість спонсорів;
s_i – сума вкладу спонсора за проект

Таким чином, модель квадратичного голосування може стати основою для розробки нових інноваційних підходів до проведення безпечних, надійних та справедливих електронних голосувань, що є критично важливим для розвитку сучасного суспільства.

Література

1. Benhaim A., Falk B. H., Tsoukalas G. Balancing Power in Decentralized Governance: Quadratic Voting under Imperfect Information. – 2023. – С. 1-4.

Анотація

У тезах досліджується інтеграція методу квадратичного голосування в децентралізовані блокчейн-системи з метою підвищення рівня безпеки та надійності криптовалютних транзакцій. Основна мета роботи полягає у вдосконаленні процесу прийняття рішень у блокчейні через впровадження механізмів квадратичного голосування, які сприяють справедливості та прозорості. Наукова новизна полягає в адаптації методу до специфіки децентралізованих систем та аналізі його ефективності для оптимізації управління ресурсами.

Ключові слова: блокчейн, криптовалюта, квадратичне голосування, децентралізація.

Abstract

The thesis explores the integration of the quadratic voting method into decentralized blockchain systems to enhance the security and reliability of cryptocurrency transactions. The primary goal is to improve the decision-making processes in blockchain networks by implementing quadratic voting mechanisms, promoting fairness and transparency. The scientific novelty lies in adapting this method to the specifics of decentralized systems and evaluating its efficiency in optimizing resource management.

Keywords**:** blockchain, cryptocurrency, quadratic voting, decentralization.

ДОСЛІДЖЕННЯ ПРИНЦИПІВ 3D-ВІЗУАЛІЗАЦІЇ ТА СТВОРЕННЯ ДОДАТКУ ДЛЯ ПРОЄКЦІЇ СПРАЙТІВ У ТРИВИМІРНОМУ ПРОСТОРІ НА ДВОВИМІРНЕ ЗОБРАЖЕННЯ

Добродомов Д.О., студент, dmytro.dobrodomov.kita@donntu.edu.ua;
Любименко О.М., к.ф.-м.н,доц., olena.liubymenko@donntu.edu.ua ;
Штепа О.А., к.т.н., доц., oleksandr.shtepa@donntu.edu.ua
ДВНЗ «Донецький національний технічний університет», м. Дрогобич, Україна

Дана розробка, візуалізація двовимірних спрайтів у тривимірному просторі, може стати основою для різноманітних проєктів, такі як рушії ігрових додатків, тривимірні графіки, симуляції або візуалізатори.

Ціллю даної розробки є створення простої та не ресурсоємної програми, що симулює відображення спрайтів у тривимірному просторі з урахуванням перспективи, зменшенням розміру спрайтів з відстанню, можливістю управління камерою (переміщення, обертання). Яке саме зображення матиме спрайт, не є принциповим, головною задачею є створення алгоритму проєкції сцени у двовимірне зображення, що надається користувачеві у вікні.

При виборі інструменту необхідно дотримуватись балансу між швидкістю написання коду та продуктивністю. Оптимальною мовою програмування, що поєднує зручність і швидкодійність, є C++. Ідеальним рішенням є використання бібліотеки SFML, яка надає зручний інтерфейс до багатьох компонентів комп'ютера, щоб спростити розробку додатків: система, вікна, графіка, аудіо та мережа [1]. Екран у SFML має певні особливості. Верхній лівий кут має координати (0,0). Правий нижній кут має координати розмінів вікна. Функціоналу є достатнім, щоб створювати візуалізатор.

У загальному випадку, є три основних умовних компоненти, що задіяні у алгоритмі візуалізації.

Перший компонент — камера. З боку камери відбувається проекція сцени на екран. Камера включає точку у просторі, з якої ведеться спостереження за сценою. Якщо є можливість оберту, також вказуються кути повороту за однією або більше осями. Важливим компонентом є фокусна відстань, що визначає, який кут огляду буде доступний при виведенні зображення на екран.

Другий компонент — безпосередньо об'єкт. У даному випадку, об'єкт буде представлено лише двома значеннями — розмір спрайту та довільне положення у просторі. Подальші модифікації залежать від специфіки розробки.

Третій компонент — екран. У даному випадку, екраном буде вважатись вікно обмеженого розміру. Важливою задачею є коректне перенесення спрайтів на екран, з урахуванням принципу роботи бібліотеки з вікном. Важливим способом передачі тривимірного простору є глибина зображення.

Якщо не враховувати поворот камери, то глибиною можна вважати відстань до об’єкта за однією з осей (найчастіше представлена віссю ox).

Для демонстрації принципу представлення глибини, можна скористатись двовимірною схемою, з проєкцією уявної двовимірної сцени у одновимірне зображення.

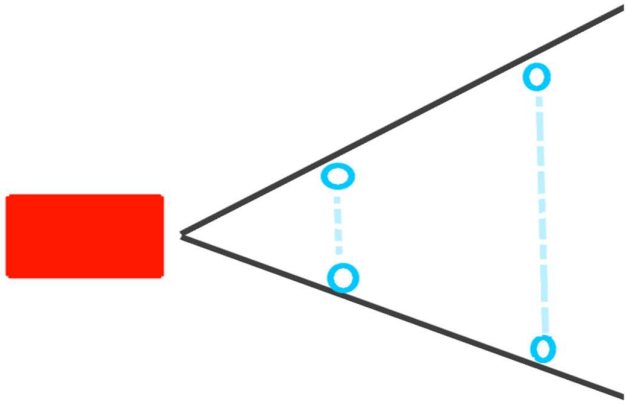


Рисунок 1. Залежність відстані між точками при збільшенні глибини

Зі збільшенням глибини, більші відстані здаються меншими. На рис.1, на проекції відстань між парами точок здаватиметься однаковою, хоча у реальності відстань значно відрізняється.

Отже, якщо представити будь-який об’єкт набором нескінченої кількості точок, то зі збільшенням глибини точки на проекції знаходитимуться щільніше, що викликатиме відчуття зменшення об’єкту. Якщо ж представляти камеру, як нескінчений набір променів у випадкових напрямках, менший відсоток променів потраплятиме на об’єкт, що також викликатиме відчуття зменшення. При будь-якому уявленні результат є однаковим.

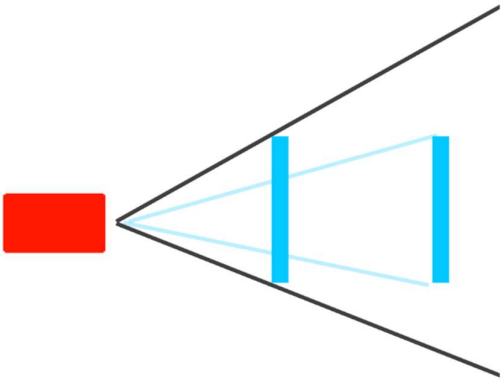


Рисунок 2. Залежність розміру об’єкту від глибини

Об’єкт, що позначено синім кольором, може знаходитись на різній відстані від камери по горизонталі. Сірими променями позначено границі вікна з певним кутом огляду. Об’єкт не змінює свого розміру у дійсності. Але при наближенні до камери по горизонталі, він займатиме більше простору на екрані, що викликатиме відчуття збільшення розміру. Якщо додати залежність від вертикальної відстані, що не є глибиною, можна досягти ефекту викривлення “риб’ячого ока”. Глибиною зображення, при нерухомій камері без обертання буде прийнята вісь ox.

Спершу, якщо відомі координати об’єкту o та камери cam, можна розрахувати зміщенні координати об’єкту, для урахування положення камери:

$$offpos = o.pos - cam.pos$$

Після цього необхідно здійснити обертання об’єкту. У даному випадку, достатньо двох типів обертань — вгору-вниз та управо-уліво. Важливо, що обертати спершу необхідно за віссю oz, а потім — за oy. Так як обертання здійснюється відносно камери, то кути обертання будуть дорівнювати від’ємним кутам нахилу камери:

$$offpos = rotateY(rotateX(offpos, -cam.zrot), -cam.yrot)$$

Знайдено положення об’єкта стосовно камери. Тепер можна прийняти ox за глибину.

Кут огляду fov виражено у радіанах. Відсоток зменшення об’єкту з глибиною розраховується наступним чином:

$$aspect = \frac{1}{offpos.x \cdot \tan(fov \cdot 0.5)}$$

Координати за віссю ox не впливають на положення об’єкту на екрані. За висоту визначено вісь oz. Можна визначити положення об’єкту на уявному екрані, що є двовимірним вектором:

$$screenpos = (offpos.y \cdot aspect; offpos.z \cdot aspect)$$

Розмір спрайту також залежить від значення aspect.

При переведенні зображення у вікно SFML, важливим є те, що y-координата зростає, чим нижче знаходиться точка, а не навпаки. Отже, положення screenpos треба зробити від’ємним. Також потрібно перенести зображення у центр вікна. screensize — двовимірний вектор, розмір вікна:

$$screenpos = (0.5 screensize.x + screenpos.x; screensize.y - screenpos.y)$$

Можна перевіряти відстань об’єкту до камери та не відображати ті об’єкти, що знаходяться далі певної відстані:

$$dist = \sqrt{(o.pos.x - cam.pos.x)^2 + (o.pos.y - cam.pos.y)^2 + (o.pos.z - cam.pos.z)^2}$$

Також необхідно ігнорувати об’єкти, які мають від’ємну глибину, тобто знаходяться позаду камери.

При роботі зі сценами великого розміру, така оптимізація може значно підвищити продуктивність роботи додатку.

Ще однією оптимізацією є ігнорування усіх об’єктів що опинилися поза межами вікна. Отже, якщо камера буде не направлена на об’єкти, незалежно від їх кількості, продуктивність роботи залишатиметься максимальною. Ця функція є важливою, якщо об’єкти оточують камеру з усіх сторін.

Більш специфічною для інструмента оптимізацією є використання RenderImage. Замість того, щоб відправляти запити на відображення кожного об’єкту окремо, усі видимі об’єкти формують повне зображення, і тільки після цього відправляється загальний запит зобразити їх у вікні.

У такий спосіб, можна випадково розміщувати на сцені до 40000 об’єктів без помітних втрат продуктивності.

Було проведено тестування, для зручної демонстрації передачі тривимірного простору, надано можливість переміщуватись сценою. Користувач може керувати гравцем та здійснювати стрибки за висотою. На гравця діє гравітація. Усі точки розміщуються на площині (рис.3).

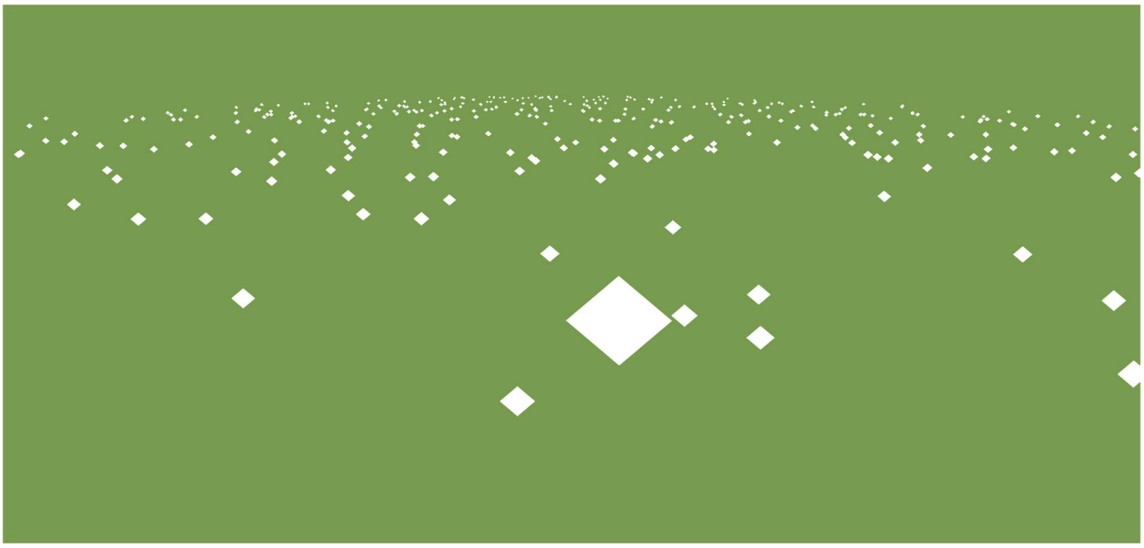


Рисунок 3. Гравець у момент стрибку

На прикладі можна побачити, що створюється відчуття “площини”, над якою піднявся гравець. Також помітні ефекти оптимізації — видно лише частину з 20000 об’єктів.

Література

1. SFML [Електронне джерело]. URL https://www.sfml-dev.org/
2. Christer Ericson, Real-Time Collision Detection. 633с. 2004 рік.

Анотація

Об’єктом дослідження є алгоритм проєкції спрайтів у тривимірному просторі на двовимірне зображення. Метою розробки є створення додатку, що використовує основні принципи проєкції, для відображення глибини, яка може слугувати основою для різноманітних програм, що потребують 3D візуалізації. Основними завданнями є вибір інструментів, побудова математичної моделі, розробка додатку та оптимізація. Практична значимість дослідження полягає у активному використанні технологій 3D візуалізації у різних сферах діяльності.

Ключові слова: SFML, 3D, візуалізація, проєкція, оптимізація, C++, глибина зображення.

Abstract

The object of the research is the algorithm for projecting sprites in three-dimensional space onto a two-dimensional image. The goal of the development is to create an application that uses the basic principles of projection to display depth, which can serve as the basis for various programs that require 3D visualization. The main tasks are the selection of tools, building a mathematical model, developing an application and optimization. The practical significance of the research lies in the active use of 3D visualization technologies in various fields of activity.

Keywords: SFML, 3D, visualization, projection, optimization, C++, depth of image.

ВИКОРИСТАННЯ КОМП'ЮТЕРНОГО ЗОРУ ТА ВІДКРИТИХ БАЗ ДАНИХ ДЛЯ ПОКРАЩЕННЯ НАВИЧОК ВОЛОДІННЯ ЖЕСТОВИМИ МОВАМИ

Ступак Г. В.[1] , ст. викл. каф. АТ, glib.stupak@donntu.edu.ua;
Теличко Г. О.[1], к.т.н., доц. каф. АТ, hanna.telychko@donntu.edu.ua;
Литвин Д. В.[2] , вчитель, dashalitvin24@gmail.com;
Теличко М. С.[2] , учень, n.s.telichko@gmail.com
[1] Донецький Національний Технічний Університет, Дрогобич, Україна
[2] Загальноосвітня школа І-ІІІ ступенів № 9 Покровської міської ради Донецької області, Покровськ, Україна

За даними Всесвітньої організації охорони здоров'я, понад 5% світового населення (приблизно 430 мільйонів людей) страждають від глухонімоти різного ступеня тяжкості [1]. Основним бар'єром в створенні інклюзивного середовища спілкування є малий відсоток людей, що володіють жестовими мовами. Це призводить до порушення психо-емоційного стану як у людей з глухонімотою так і здорових людей через невірну інтерпретацію жестів в процесі спілкування.

Метою дослідження є покращення навичок володіння жестовою мовою як серед глухонімих так і здорових людей. Об'єктом дослідження є процес вивчення жестових мов за допомогою навчальних платформ. Предметом дослідження є технології розпізнавання жестів за допомогою комп'ютерного зору та штучного інтелекту, їх застосування для створення інтерактивного інструмента з покращення володіння жестовими мовами з використанням відкритих баз даних жестових мов.

На початку дослідження була поставлена наступна гіпотеза: використання комп'ютерного зору та відкритих баз даних здатне полегшити процес самостійного навчання жестовій мові, підвищить ефективність та швидкість вивчення, покращить навички володіння, що сприятиме кращій комунікації з глухонімими людьми та створить передумови сталого розвитку інклюзивного суспільства і покращення психо-емоційного стану співрозмовників.

Для досягнення поставленої мети і перевірки гіпотези були поставлені на ступні завдання роботи:

- провести аналіз методик вивчення жестових мов;
- дослідити відкриті бази даних WLASL з наявними навчальними відео матеріалами;
- реалізувати алгоритм розпізнавання жестів за допомогою комп'ютерного зору;
- створити інтерфейс інтерактивного словника жестових мов;
- інтегрувати відкриту бази даних відео-навчальних матеріалів;
- розробити механізм порівняння жестів користувача з еталонними зразками;

– створити алгоритм оцінювання правильності виконання жестів для користувачів.

В досліджені використовувались наступні методи: аналіз літератури, наявних практик вивчення та існуючих рішень у сфері вивчення жестових мов; програмування та розробка алгоритмів комп'ютерного зору; експериментальне тестування розробленої системи.

Дослідження у сфері розпізнавання та перекладу жестової мови активно розвиваються, сприяючи створенню інструментів для подолання комунікаційних бар'єрів між нечуючими та чуючими людьми. Приклади таких проєктів, як FineHand і розробки для розпізнавання пальцевої абетки в реальному часі [2, 3], демонструють успіхи завдяки використанню глибокого навчання та згорткових нейронних мереж. Крім того, ресурси, такі як WLASL Dataset [4], Mediapipe [5] і OpenCV [6], суттєво допомагають у створенні надійних систем розпізнавання жестів.

Попри досягнення, дослідження жестової мови не повністю задовольняють потреби користувачів. Наша система поєднує переклад із навчанням, дозволяючи практикувати жести, отримувати миттєву оцінку й вдосконалювати навички завдяки зворотному зв’язку. Архітектура інтерактивного застосунка з вивчення жестових мов, розробленого на основі використання комп’ютерного зору та відкритих баз даних для покращення навичок володіння жестами представлена на рис.1.

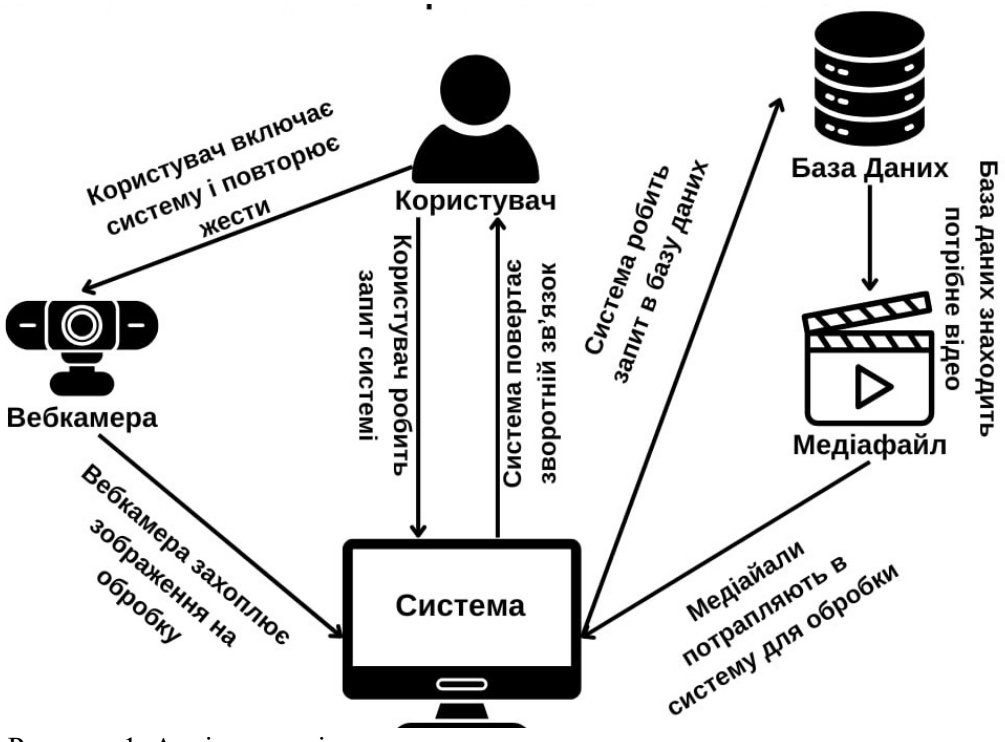


Рисунок 1. Архітектура інтерактивного застосунка з вивчення жестових мов

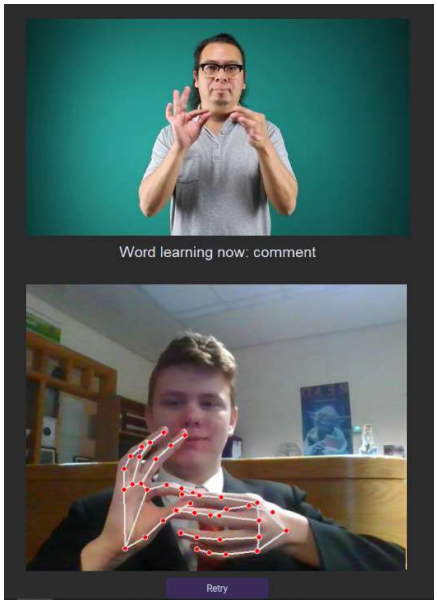


Рисунок 2. Інтерактивний застосунок з вивчення жестових мов

Система забезпечує взаємодію користувача із базою даних через вебкамеру та механізм зворотного зв’язку. Користувач активує застосунок і повторює запропоновані жести, які фіксуються вебкамерою та передаються до системи для обробки (рис. 2). Отримані дані аналізуються, після чого система звертається до бази даних, яка містить навчальні матеріали, такі як відео, і надає користувачеві зворотний зв’язок. Це дозволяє користувачу вдосконалювати свої навички жестової мови в інтерактивному середовищі, отримуючи персоналізовані рекомендації та оцінки. Процес визначення коректності повторення жестів заснований на порівнянні еталонних зразків з відеоряду та рухів реального користувача, що отримані з вебкамери. Це дає можливість отримувати зворотній зв’язок і покращувати навички.

Висновок. Проведене дослідження є важливим кроком у напрямку створення доступних та ефективних інструментів для вивчення жестових мов, що значно покращить комунікацію між глухонімими та здоровими людьми. Особливо важливим є те, що система дає можливість вивчати жестові мови самостійно, без залучення викладачів у будь який зручний для користувачів час. Реалізоване рішення демонструє можливість забезпечення точного розпізнавання жестів та надання візуального зворотного зв'язку. Проведено апробацію у групі з 30 користувачів цільових груп, які відзначили зручність використання застосунку для покращення володіння та вивчення нових жестів. На даний час система розпізнає жести з точністю на рівні 85%, і це значення може бути покращено за рахунок оптимізації програмного забезпечення та навчання штучного інтелекту. Подальший розвиток проєкту передбачає розширення бази даних жестів та адаптацію системи для різних жестових мов світу, а також покращення системи оцінювання, порівняння жестів та зворотного зв’язку.

Література

1. World Health Organization, 2021, Deafness and hearing loss. [Електронний ресурс]. Доступно: https://www.who.int/news-room/fact-sheets/detail/deafness-and-hearing-loss, Дата звернення: 2024/12/02

2. Hosain, A.A., Santhalingam, P.S., Pathak, P., Rangwala, H., Kosecka, J.: FineHand: Learning Hand Shapes for American Sign Language Recognition. arXiv preprint arXiv:2003.08753, 2020, https://arxiv.org/abs/2003.08753, last accessed 2024/12/02.

3. Kang, S., Tripathi, S., Nguyen, T.Q.: Real-time Sign Language Fingerspelling Recogni-tion using Convolutional Neural Networks from Depth map. arXiv preprint arXiv:1509.03001, 2020, https://arxiv.org/abs/1509.03001, last accessed 2024/12/02.
4. Li, Y., Martinez, J., Solou, R., et al.: Word-Level American Sign Language Dataset (WLASL). International Journal of Computer Vision. – 2021, 128(5), p. 1–12.
5. Mediapipe Homepage, https://mediapipe.dev, last accessed 2024/12/02.
6. Bradski, G.: The OpenCV Library. Dr. Dobb's Journal of Software Tools. – 2000, 25(3), p. 122–125.

Анотація

У роботі розглянуто використання комп'ютерного зору та відкритих баз даних для покращення навичок володіння жестовими мовами. Метою дослідження є створення інструменту для ефективного самостійного навчання жестовій мові, що базується на технологіях розпізнавання жестів та інтерактивних методах навчання. Проведено аналіз доступних методик та баз даних, реалізовано алгоритм розпізнавання жестів і створено прототип інтерфейсу інтерактивного словника. Система дозволяє користувачам отримувати зворотний зв'язок та вдосконалювати навички володіння жестовими мовами. Результати дослідження демонструють можливість підвищення точності навчання та створення передумов для інклюзивного суспільства.

Ключові слова: комп'ютерний зір, жестова мова, навчання, штучний інтелект, інклюзія.

Abstract

The study investigates the application of computer vision and open databases to enhance sign language proficiency. Its primary goal is to create a tool that enables effective self-learning of sign language using gesture recognition technologies and interactive teaching methods. The research includes an analysis of existing methodologies and databases, implementation of a gesture recognition algorithm, and development of a prototype interactive dictionary interface. The proposed system provides users with real-time feedback to refine their sign language skills. The findings highlight the potential for improving learning accuracy and contributing to the development of an inclusive society.

Keywords: computer vision, sign language, learning, artificial intelligence, inclusion.

СЕКЦІЯ 2

«Електроніка, радіоелектронні пристрої»

РОЗРОБКА СТРУКТУРНОЇ СХЕМИ ЕЛЕКТРОННОЇ СИСТЕМИ СКАНУВАННЯ ЗЕМНОЇ ПОВЕРХНІ ДЛЯ НАЗЕМНОГО БЕЗПІЛОТНОГО АПАРАТУ

Харламов Є. Р., магістр, yehor.kharlamov@donntu.edu.ua;
Шеїна. Г. О., к.т.н, доцент, ganna.sheina@donntu.edu.ua
ДВНЗ Донецький національний технічний університет, м. Дрогобич, Україна

Безпілотна робототехніка в наш час широко застосовується як для мирних потреб, так і для військових. Зазвичай, такі апарати обладнані системою датчиків для стеження за місцевістю. Апарати або самостійно приймають рішення стосовно руху, або передають інформацію в інше місце, де приймаються рішення для їх керування.

Система датчиків апарату включає:

– LIDAR (light detection and ranging), дистанційне зондування, коли лазер використовується для вимірювання відстаней, також він дозволяє створювати 2-D, 3-D карту навколишнього середовища;
– систему машинного зору на основі відеокамер дозволяє більш детально визначати навколишньою обстановку: зчитувати інформацію з дорожніх знаків чи світлофорів.;
– систему GPS (global positioning system), яка дозволяє точно визначити координати;
– систему інерційної навігації.

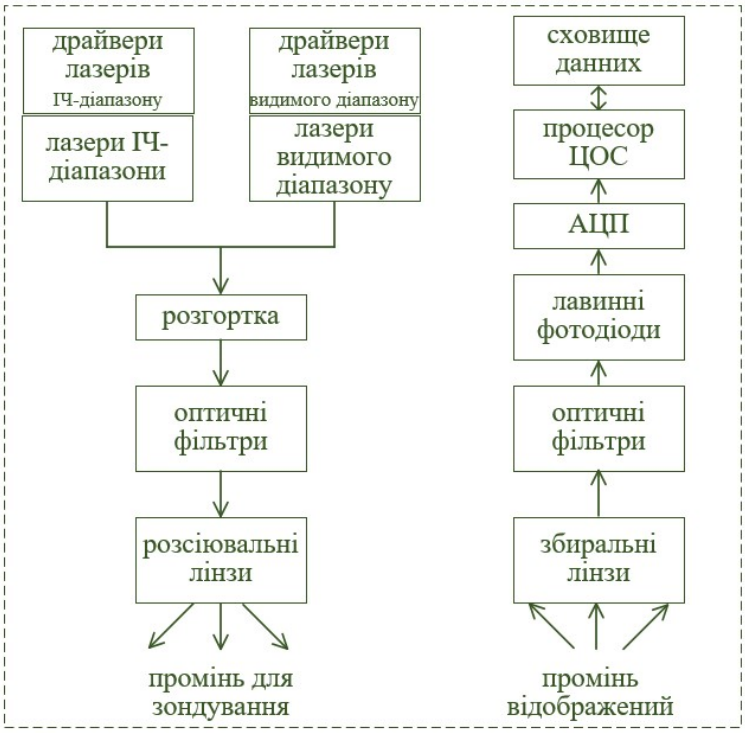


Рисунок 1. Структурна схема електронної системи

Структурна схема електронної системи сканування земної поверхні наведена на рис. 1.

Лазерні випромінювачі системи працюють в інфрачервоному та видимому діапазоні спектра, сканують поверхню. Зауважимо, обов'язково необхідно підтримувати стабільність їх роботи. Розгортка системи передба-

чена для забезпечення вертикальної кутової роздільної здатності і відтворення об'єктів сканування. Оптичні фільтри у променях інфрачервоного та видимому діапазону виділяють тільки необхідний спектр випромінювання. Наступним кроком роботи системи є застосування розсіювальних лінз, які перетворюють паралельні промені в розсіювальні, що дозволяє збільшити вертикальну роздільну здатність системи. Друга частина системи призначена для збору інформації за допомогою промінів, що відображенні від об'єкта сканування. Збиральні лінзи перетворюють розсіяні промені в паралельні. Оптичні фільтри, так само, як і в першій частині системи, пропускають промені визначеного спектру. Отримані промені потрапляють до лавинних фотодіодів, які працюють у тому ж діапазоні хвиль, що і лазерні випромінювачі. Оптичний сигнал за допомогою фотодіодів перетворюється в аналоговий електричний сигнал. Сигнал, наступним кроком, перетворюється в цифровий сигнал. Процесор цифрової обробки сигналів DSP (digital signal processor) працює в подальшому зі сховищем даних.

Відповідно до наведеної структурної схеми для електронної системи сканування поверхні обґрунтовується вибір конструктивних елементів. Спочатку обираємо лазери. З можливих типів твердотільних, газових, волоконних чи напівпровідникових лазерів зупиняємо вибір на останньому типі (рис. 2).

Рисунок 2. Лазерний діод

Напівпровідникові лазери [1] розрізняють інжекторного типу і лазери з оптичним накачуванням. В лазерах інжекторного типу, як в світловипромінювальних діодах, створюється когерентне випромінювання в оптичному діапазоні довжин хвиль. Відмінність полягає в наступному: в світловипромінювальних діодах випромінювання спричинено спонтанною рекомбінацією, а в лазерах інжекторного типу – вимушеною рекомбінацією носіїв заряду. В напівпровідникових лазерах з оптичним накачуванням випромінювання є стимульованим. Їх вибір обґрунтований додатковими перевагами: безперервний режим роботи, компактність, потужність, широкий діапазон робочих температур, стійкість до вібрацій та ударів. Для інфрачервоного діапазону також використовуються напівпровідникові лазери. Для забезпечення стабільності роботи лазера застосовують схеми драйверів [1].

Оптичні фільтри (світлофільтри) для першої частини системи змінюють спектральний склад променів лазера, залишаючи не змінною форму фронту світлових хвиль. Світлофільтри для другої частини системи (між збиральними лінзами і фотодіодами) виконують додаткову функцію поліпшення видимості (контрастності) сигналів за несприйнятливих умов.

З можливих типів фотодіодів: фотодіод Шотткі, фотодіод з гетеропереходом чи лавинний фотодіод зупиняємо вибір на останньому типі (рис. 3).

Рисунок 3. Лавинний фотодіод

Фотодіоди мають (додатково до шарів p-, n- провідності) і-ділянку провідністю близькою до власної. Випромінювання поглинається цією ділянкою. Сильне електричне поле утворюється в і-ділянці при наявності зворотного зміщення. Під дією випромінювання фотоносії розподіляються між p-, n- шарами. Лавинні фотодіоди від звичайних фотодіодів відрізняє наявність внутрішнього посилення сигналу – лавинне електронне посилення. З цією метою до звичайної структури фотодіода додається додатковий шар, який забезпечує лавинне підсилення (множення первинного струму).

З лавинних фотодіодів сигнали надходять до АЦП (аналогово-цифровий перетворювач). Сигнал, який надходить до АЦП, описує різноманітні поверхні (як за висотою, так і за матеріалами), що сканує. Швидкість сканування є високою. Тому АЦП працює з широкосмуговими неперіодичними сигналами. Ці фактори необхідно враховувати при виборі АЦП. Вимоги вибору: швидкодія; висока точність (мінімальна похибка особлива важлива при різких змінах сигналу); мінімальні похибки квантування; висока роздільна здатність. Процесор цифрової обробки сигналів аналізує і перетворює інформацію в сигнал, який використовується в зручному форматі, наприклад графічному.

В роботі досліджувалася структурна схема електронної системи сканування земної поверхні. Виконано огляд основних елементів схеми, їх конструктивне виконання і критерії вибору.

Література

1. Weber, Marvin J. Handbook of Lasers / Marvin J. Weber // Lawence Berkeley National Laboratory University of California Berkeley, California. – 2001. – P. 1186.

Анотація

В роботі виконано дослідження структурної схеми електронної системи сканування земної поверхні. Обґрунтовано вибір основних елементів схеми: напівпровідникові лазери, лавинні фотодіоди, оптичні фільтри.

Ключові слова: електронна система, напівпровідникові лазери, лавинні фотодіоди, оптичні фільтри.

Abstract

The paper studies the structural diagram of an electronic system for scanning the Earth's surface. The choice of the main elements of the scheme is justified: semiconductor lasers, avalanche photodiodes, optical filters.

Keywords: electronic system, semiconductor lasers, avalanche photodiodes, optical filters.

ДОСЛІДЖЕННЯ ЕЛЕКТРОННИХ СИСТЕМ НАВІГАЦІЇ ДЛЯ СІЛЬСЬКОГОСПОДАРСЬКОЇ ТЕХНІКИ

Циплаков-Яблонський С.О., магістр, tsyplakov@ukr.net;
Шеїна. Г. О., к.т.н, доцент, ganna.sheina@donntu.edu.ua
ДВНЗ Донецький національний технічний університет, м. Дрогобич, Україна

Навігація має декілька напрямків завдань, які вирішуються:

- визначення точного місця розташування об'єкта спостереження;
- вибір оптимального напрямку руху об'єкта спостереження.

Для першої задачі, визначення точного місця розташування, розроблені радіонавігаційні системи. Системи визначають місцезнаходження об'єкта на основі випромінювання, прийому та обробки радіосигналів. За місцем розташування системи ділять на бортові (на рухомих об'єктах) і наземні (супутникові). Супутникова радіонавігація зараз найбільш поширена.

Навігація необхідна не тільки для авіаційного, морського чи автомобільного транспорту. Роздивимося іншу галузь, використання супутникової радіонавігації для сільськогосподарської техніки. По-перше, територія, яка використовується для вирощування, значна, але обмежена. Розширювати її немає можливості через ряд факторів. Тому майбутньою стратегією для підвищення ефективного використання сільськогосподарських територій визнано оснащення техніки електронними засобами й автоматизацію виробництва. По-друге, процес вирощування є залежним від вчасного проведення певних технологічних дій. Швидкість і точність є запорукою якісної продукції. Відкласти процес у часі через відсутність технічного оснащення не можна. Актуальним є питання оснащення сільськогосподарської техніки новими електронними засобами навігації та автоматизації процесами.

Отже у чому полягає суть питання? В поєднані досвіду різних галузей. Досвід у сільському господарстві, інновації та інженерний досвід поєднуються для удосконалення виробництва й підвищення його продуктивності.

Відомий Бренд Massey Ferguson (корпорації AGCO) в рекламі сільськогосподарської техніки стверджує, що «використання новітніх технологій забезпечує чудове керування» [1]. Наприклад, вони наводять панель керування сучасним трактором (рис. 1). Навігаційна система трактора використовує відому концепцію hands-free (вільні руки), коли оператор трактора не зосереджений на водінні, а приділяю увагу технологічності процесу. Переміщення трактора вздовж паралельних прямих здійснюється автоматично за допомогою навігаційної системи. Вимоги до системи навігації для сільського господарства відомі: висока точність (в межах сантиметрів), урахування нерівності поверхні землі, урахування індивідуальності кожного окремого поля. До сих пір використовували Global Positioning System (GPS), яка визначала положення об'єкта у World Geodetic System (WGS).

Рисунок 1. Приклад панелі керування трактором

Наявність пристроїв супутникової навігації, бортових комп'ютерів, технічних пристроїв в сільськогосподарській техніці – один із елементів точного землеробства.

Досвід їх експлуатації показав необхідність підвищення точності навігації.

На даний час широкого застосування набуває нова система Real Time Kinematic (RTK).

З досвіду використання сигналів найбільші похибки виникають через наступні завади: неоднорідність атмосфери передачі сигналу, шуми від інших об'єктів, або переривання сигналу. Для корекції похибки використовується пара приймачів, яка сприймає завади однаково. Опорний приймач на основі відомих і виміряних координат розраховує поправки до координат. Для створення такої системи створюють постійні станції і мережі RTK.

Один із лідерів, компанія John Deere, обґрунтовує вибір навігаційних точних систем, керування технікою без втручання з боку оператора, наступними факторами [2]:

- менше навантаження на оператора;
- швидша робота;
- зменшення перекриття й пропусків при роботі;
- зниження виробничих витрат;
- збільшення продуктивності;
- більша тривалість робочих днів в умовах поганої видимості;
- зменшене ущільнення ґрунту;
- покращення ефективності збирання врожаю навіть за складних умов;
- збільшення якості збору врожаю.

Впровадження нових систем навігації, більш точних, у сільське господарство – це довгострокова перспектива, яка підтримає розширення можливостей фермерів і забезпечить розвиток їх господарств.

Література

1. Технології для сільського господарства: [електронний ресурс]. – Режим доступу: https://www.masseyferguson.com/en.html – Загл. з екрану

2. Рішення з навігації [електронний ресурс]. – Режим доступу: https://www.deere.ua/uk/розумні-рішення-для-сільського-господарства/рішення-з-навігації/ – Загл. з екрану

Анотація

У роботі зроблено огляд сучасних методів поєднання навігаційних точних систем для удосконалення сільського господарства й підвищення його продуктивності. Для підвищення точності навігації обґрунтовано застосування RTK-систем навігації.

Ключові слова: навігаційні системи, сільське господарство, RTK-система.

Abstract

The paper reviews modern methods of combining precise navigation systems to improve agriculture and increase its productivity. To increase navigation accuracy, the use of RTK navigation systems is justified.

Keywords: navigation systems, agriculture, RTK system.

СЕКЦІЯ 3

«Автоматизація, комп'ютерно-інтегровані технології»

КОМП'ЮТЕРНО-ІНТЕГРОВАНІ ТЕХНОЛОГІЇ: ПОГЛЯД НА МАЙБУТНЄ АВТОМАТИЗАЦІЇ ВИРОБНИЦТВА ТА УПРАВЛІНСЬКИХ ПРОЦЕСІВ

Пуштарик Б.П., студент
Корнєва В.Р., викладач viktoriia.kornieva@ptfc.ukr.education
Прилуцький технічний фаховий коледж, Прилуки, Україна

Комп'ютерно-інтегровані технології (КІТ) є невід'ємною частиною сучасного виробництва, забезпечуючи інтеграцію комп'ютерних систем з технічними засобами, процесами та операціями для досягнення максимальної ефективності і точності. Вони охоплюють широкий спектр інноваційних рішень, таких як автоматизація, роботизація, використання інтелектуальних систем і застосування цифрових двійників для управління виробничими та бізнес-процесами.

Метою цієї статті є огляд основних напрямків розвитку комп'ютерно-інтегрованих технологій, їх впливу на автоматизацію та управління, а також аналіз перспектив застосування в різних галузях. У статті також буде представлено аналіз основних технологій, які лежать в основі КІТ, а також розглянуто сучасні виклики та тенденції, пов'язані з їх використанням.

Розвиток комп'ютерно-інтегрованих технологій

Історично, перші комп'ютерно-інтегровані технології з'явились на основі інтеграції обчислювальних машин з виробничими процесами, що дозволило значно підвищити продуктивність та знизити ймовірність помилок. Однак лише з початку 2000-х років почався справжній бум застосування новітніх комп'ютерних технологій в промисловості. Поява таких концепцій, як Інтернет речей (IoT), штучний інтелект (ШІ), великі дані (Big Data) і блокчейн, змінила саму природу КІТ.

Використання цих технологій в межах комп'ютерно-інтегрованих систем дало змогу забезпечити безперервний моніторинг та контроль процесів, а також застосування автоматичних рішень для адаптації до змінюваних умов.

Сучасні КІТ стали важливим інструментом у таких сферах, як:

- автоматизація виробничих ліній;
- управління підприємствами та логістичними процесами;
- розробка нових матеріалів та виробничих технологій;
- розвиток робоіндустрії;
- забезпечення інтелектуальних систем управління.

Комп'ютерно-інтегровані технології включають в себе широкий спектр технологічних рішень, які надають підприємствам можливість автоматизувати процеси, оптимізувати управління і знижувати витрати.

Ось деякі основні складові, які входять до складу КІТ:

Автоматизовані системи управління (АСУТП).

Вони дозволяють автоматизувати управління виробничими процесами в реальному часі. АСУТП інтегрують інформацію з різних датчиків, машин та пристроїв, дозволяючи оперативно коригувати параметри і забезпечувати безперебійну роботу систем.

Інтернет речей (IoT).

Завдяки IoT, пристрої в межах комп'ютерно-інтегрованих технологій стають "розумними", здатними збирати та передавати дані про процеси в режимі реального часу. IoT значно підвищує ефективність систем, дозволяючи моніторити та управляти різними аспектами виробництва без необхідності людського втручання.

Штучний інтелект і машинне навчання.

Штучний інтелект дозволяє обробляти великі обсяги даних, прогнозувати майбутні тенденції та приймати рішення, що базуються на аналізі інформації, а також адаптуватися до змінюваних умов. Машинне навчання забезпечує безперервне вдосконалення алгоритмів на основі накопичуваного досвіду.

Цифрові двійники.

Це віртуальні моделі фізичних об'єктів або процесів, що дозволяють прогнозувати їх поведінку, тестувати різні сценарії без ризику для реальних систем, а також забезпечувати точне відображення стану об'єкта або процесу в реальному часі.

Блокчейн.

Технологія, що гарантує безпеку та прозорість даних, дозволяючи вести точний облік всіх операцій, що відбуваються в системі. Використання блокчейн у комп'ютерно-інтегрованих технологіях допомагає забезпечити надійність та безпеку інформації, що передається між різними частинами системи.

Перспективи застосування КІТ в різних галузях

Сфера застосування комп'ютерно-інтегрованих технологій охоплює широкий спектр галузей, від промисловості до медицини та роздрібної торгівлі. Розглянемо деякі перспективи використання КІТ у різних секторах:

Промисловість та виробництво.

Виробничі процеси є одними з головних областей, де комп'ютерно-інтегровані технології досягають найвищого рівня розвитку. Сучасні виробничі лінії стають повністю автоматизованими, де роботи і автоматизовані системи виконують всі операції — від складання деталей до їх тестування та пакування. Використання інтелектуальних систем в управлінні виробничими лініями дозволяє знизити витрати, підвищити точність і швидкість процесів, а також передбачати та запобігати можливим збої.

Логістика та управління ланцюгами постачань.

КІТ дозволяють значно покращити ефективність логістичних процесів завдяки використанню IoT для моніторингу вантажів, а також завдяки про-

гнозуванню з використанням великих даних для оптимізації маршрутів. Системи, засновані на КІТ, можуть автоматично коригувати логістичні операції, враховуючи зміни в умовах попиту та наявності товарів, що дозволяє значно скоротити час доставки та витрати на зберігання товарів.

Охорона здоров'я.

У медицині комп'ютерно-інтегровані технології використовуються для моніторингу стану пацієнтів, автоматизації процесів діагностики та лікування. Інтелектуальні системи допомагають лікарям приймати обґрунтовані рішення на основі аналізу медичних даних, а також передбачати розвиток хвороб на основі історії пацієнта та результатів тестів. Цифрові двійники можуть бути використані для моделювання і планування хірургічних операцій, що значно підвищує їх успішність.

Енергетика та екологія.

Використання КІТ у сфері енергетики дозволяє здійснювати автоматизоване управління енергоспоживанням, оптимізуючи розподіл електричної енергії та знижуючи втрати. Такі технології також дозволяють ефективно контролювати процеси генерації, зберігання та розподілу відновлювальних джерел енергії, таких як сонячні панелі та вітрові турбіни.

Виклики та перешкоди на шляху розвитку КІТ

Попри всі переваги, використання комп'ютерно-інтегрованих технологій стикається з низкою викликів. Серед них:

- Висока вартість впровадження. Інтеграція комп'ютерно-інтегрованих систем вимагає значних інвестицій, що може бути перепоною для малих та середніх підприємств.
- Кібербезпека. Оскільки КІТ включають в себе передачу даних і взаємодію з іншими пристроями, це створює ризики для безпеки даних і може стати мішенню для кібератак.
- Необхідність кваліфікованого персоналу. Впровадження та управління КІТ вимагає висококваліфікованих кадрів, що є викликом для багатьох організацій.

Література

1. Ковальов В.М. Комп’ютерно-інтегровані технології: основи та перспективи / В.М. Ковальов, Ю.А. Смирнов // Науковий вісник Миколаївського національного університету імені В. О. Сухомлинського. – 2018. №3. – С. 45-53.
2. Лещенко В.В. Сучасні комп’ютерні технології в автоматизації виробничих процесів / В.В. Лещенко, І.М. Гриньків // Автоматизація та інформаційні технології в промисловості. – 2021. – Вип. 12. – С. 112-120.
3. Щербань В.П. Інтелектуальні системи в комп’ютерно-інтегрованих технологіях / В.П. Щербань, О.О. Карпенко // Комп’ютерні науки та інформаційні технології. – 2020. – Т. 13, №1. – С. 34-40

Анотація

Комп'ютерно-інтегровані технології є потужним інструментом, що здатен кардинально змінити не лише виробничі процеси, а й управлінські та бізнес-процеси в цілому. Вони забезпечують інтеграцію різних компонентів системи, автоматизацію операцій та оптимізацію ресурсів, що дозволяє досягти високої продуктивності і конкурентоспроможності. Однак для їх успішного впровадження необхідно долати численні виклики, серед яких високі витрати, питання безпеки та підготовка кадрів.

Проте в довгостроковій перспективі, з урахуванням розвитку технологій та зниження вартості, можна очікувати подальшого росту популярності КІТ в різних сферах.

Ключові слова: комп'ютерно-інтегровані технології, автоматизація виробництва, інтелектуальні системи.

Abstract

Computer-integrated technologies are a powerful tool that can radically change not only production processes, but also management and business processes as a whole. They provide integration of various system components, automation of operations and optimization of resources, which allows achieving high productivity and competitiveness. However, for their successful implementation, it is necessary to overcome numerous challenges, including high costs, security issues and personnel training.

However, in the long term, taking into account the development of technologies and cost reduction, we can expect further growth in the popularity of CIT in various areas.

Keywords: computer-integrated technologies, production automation, intelligent systems.

ДОСЛІДЖЕННЯ ТА РОЗРОБКИ АВТОМАТИЗОВАНОЇ СИСТЕМИ КЕРУВАННЯ ТА УДОСКОНАЛЕННЯ В СИСТЕМАХ ОБЛІКУ СПОЖИВАННЯ ЕЛЕКТРОЕНЕРГІЇ СИСТЕМОЮ КЛІМАТ-КОНТРОЛЮ ТОРГОВОГО ЦЕНТРУ

Ільїнський М.І., аспірант кафедри АВП,
fomenkomihail00@gmail.com;
Руденко В.М., кандидат технічний наук, доцент кафедри АВП,
vl_rudenko@ukr.net

Донбаська державна машинобудівна академія, Краматорськ, Україна

Клімат контроль торгівельного центру – завдання важливе і складне. Будь-який об’єкт потребує підтримки температурного режиму, осушення та кондиціонування повітря, щоб знизити випаровування води, потрібно підняти температуру повітря: якщо температура на 2-3 градуси вища за температуру води, можна домогтися підтримки вологості на рівні 40-50%. Це важливо для збереження матеріалів і будівлі. Але підвищення температури не повинно вийти за межі показників, що забезпечують комфорт відвідувачів. Відчуття задухи в приміщенні складається зі співвідношення температури і вологості повітря, і тут потрібно досягти оптимальних показників.

Тільки після проведення всіх розрахунків можна буде визначити обсяг вентильованого повітря та регулювати правильний повітрообмін. Надлишки гарячого повітря можна направити для обігріву інших зон комплексу, що дає суттєву економію електроенергії.

Усі ці завдання вирішують сучасні автоматизовані енергетичні установки. Вони суттєво економлять витрату електроенергії, оскільки їхня робота регулюється датчиками системи WSN, і підтримують задані параметри у всіх зонах одночасно. За допомогою віддаленого доступу керувати такою кліматичною установкою стає простіше та швидше.

У зв’язку з цим розробка механізмів зниження енерговитрат шляхом регулювання кліматичних параметрів в приміщенні торгівельного центру , а також алгоритмів управління є актуальною науково-технічною задачею.

Метою роботи є дослідження методів для зниження енерговитрат на регулювання кліматичних параметрів в приміщеннях торгівельного центру шляхом розробки автоматизованої системи регулювання з використанням математичних методів, інформаційного та програмного забезпечення.

Основними параметрами, що впливають на підтримку необхідних кліматичних умов в торгівельному комплексі є два взаємопов'язаних параметра: температура і вологість внутрішнього середовища, якими можна керувати на відстані, завдяки системі WSN.

Виходячи з особливостей технологічного процесу та поставлених завдань на проектування системи управління мікрокліматом можна виділити наступні контури управління:

- температурою по зонам з контурами протока гарячого повітря через калорифери і холодного повітря при кондиціонуванні;

- вологості.

З метою забезпечення даних вимог проведено математичне моделювання САР температури в приміщеннях торгівельного центру. Побудована математична модель містить теплову модель змішення повітря різних температур та підлеглий контур модель САР регулювання витрати повітря на кондиціонування. [1, 2]:

Для реалізації автоматичного регулювання витрати повітря, що подається в приміщення торгівельного центру прийнята система частотного перетворювача – асинхронний електродвигун (ПЧ-АД) з вентилятором повітродувки.

Порушення теплового балансу приміщення відбувається за рахунок внутрішніх і зовнішніх збурень. До зовнішніх збурень відносяться збурення, пов'язані з кількістю подачі холодного повітря зовні та охолодження приміщень через стіни [4]. В цьому випадку продуктивність системи опалення не буде відповідати кількості підігрітого повітря що подається. Показником такої невідповідності є зміна тиску підігрітого повітря в будь-якій точці приміщення. Таким чином, система автоматичного регулювання (САР) температурного режиму кліматичного контролю повинна виконувати дві функції: компенсувати внутрішні і зовнішні збурення з допомогою одного керуючого впливу - витрати теплого повітря. Для цього використовуються температурні реле (датчики), вмонтовані по периметру приміщень, в яких відбувається температурне регулювання завдяки системі WSN.

САР повинна забезпечити [3]:

– стійку роботу системи (відсутність автоколивань) і обмежену частоту включення регулюючого органу, яка при постійному навантаженні не повинна перевищувати п’яти включень в хвилину;

- підтримання в базовому режимі роботи системи підігріву або охолодження повинна мати температурний режим з відхиленням не більше ±3% від заданого.

В результаті математичного моделювання встановлено, що час перехідного процесу нагріву до заданої температури становить 0,2 години, як і відпрацювання збурюючого впливу з боку тепломережі. Виходячи з цього можна зробити висновок, що всі параметри перехідного процесу знаходяться в заданих межах, вибір і розрахунок параметрів регулятора, вимірювальних перетворювачів і виконавчих механізмів проведені правильно.

Література

1. Дьяконов В.П. MATLAB. Анализ, идентификация и моделирование систем. Специальный справочник./ В.П Дьяконов, В.В. Круглов. – Спб: Питер, 2001. – 480 с.

2. Анхимюк В.Л. Теория автоматического управления / В.Л.Анхимюк, О.Ф.Опейко, Н.Н.Михеев. – Мн.: Дизайн ПРО, 2000. – 352 с.

3. Кокорева И. Системы "Интеллектуальное здание" и "Умный дом": эффективные решения и новейшие разработки. – Электроника: НТБ, 2008, № 7, с. 22–27.

4. Teuber A., Eissfeller B. WLAN indoor positioning based on Euclidean distances and fuzzy logic// Proceedings of the 3rd Workshop on Positioning, Navigation and Communication (WPNC'06), Hannover, Germany, 2006. 168 p.

Анотація

В статті вирішено актуальне науково-технічне завдання зниження енерговитрат на регулювання кліматичних параметрів в приміщеннях торгівельного центру шляхом розробки автоматизованої системи регулювання з використанням алгоритмів, інформаційного та програмного забезпечення. Проведено дослідження особливостей технологічного процесу регулювання температурного режиму в приміщеннях торгівельного центру, встановлення параметрів процесу керування. Удосконалено алгоритм об'ємного регулювання витратою повітря на кондиціонування шляхом частотного регулювання електроприводів повітродувок. Створення автоматизованої системи керування об'ємним регулюванням витрати повітря підігрітого в залежності від температурного режиму приміщень торгівельного центру.

Ключові слова: дослідження, автоматизація, мікроклімат, баланс, енергетична установка

Abstract

The article solves the current scientific and technical task of reducing energy costs for regulating climatic parameters in the premises of the shopping mall by developing an automated control system using algorithms, information and software. The study of the peculiarities of the technological process of regulating the temperature regime in the premises of the shopping mall, setting the parameters of the control process was carried out. An improved algorithm of volumetric regulation of air flow for air conditioning by frequency regulation of electric drives of blowers. Creation of an automated control system for volumetric regulation of the flow of heated air depending on the temperature regime of the premises of the shopping mall.

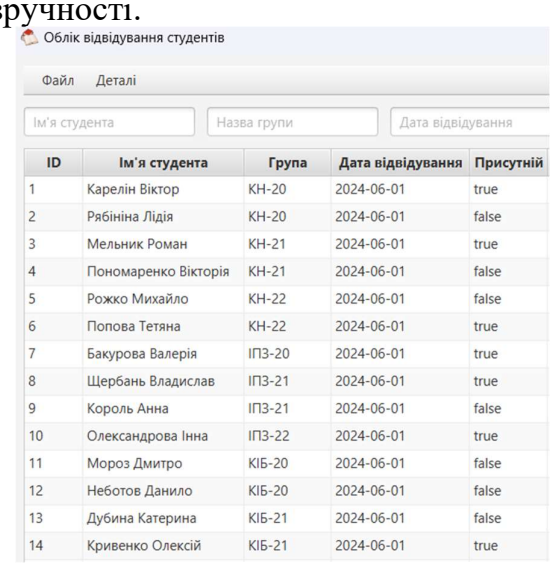
Keywords: research, automation, microclimate, balance, power plant

АВТОМАТИЗОВАНА СИСТЕМА ОБЛІКУ ПРИСУТНОСТІ СТУДЕНТІВ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЙ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ

Рожко А. М., студентка гр. СУАм-24, alina.rozhko.kita@donntu.edu.ua;
Теличко Г. О., к.т.н., доц. каф. АТ, hanna.telychko@donntu.edu.ua;
Ступак Г. В., ст. викл. каф. АТ, glib.stupak@donntu.edu.ua
Донецький Національний Технічний Університет, Дрогобич, Україна

Освіта постійно еволюціонує, впроваджуючи новітні технології для покращення навчального процесу. Одним із важливих аспектів є облік присутності студентів, який традиційно здійснюється вручну, що може призводити до помилок і затримок. У зв'язку з цим, автоматизовані системи обліку присутності стають все більш актуальними. В роботі [1] розглянуто розробку інформаційної системи обліку відвідуваності студентів (рис. 1), яка забезпечує автоматизацію процесів збирання та обробки даних про присутність студентів на заняттях.

Однією з інноваційних технологій, яка дозволить більш ефективно організувати процес обліку відвідуваності студентів, є біометрична ідентифікація, зокрема, використання датчиків відбитків пальців, розміщених на партах. Це дозволить забезпечити високий рівень автоматизації, точності та зручності.



ID	Ім'я студента	Група	Дата відвідування	Присутній
1	Карелін Віктор	КН-20	2024-06-01	true
2	Рябініна Лідія	КН-20	2024-06-01	false
3	Мельник Роман	КН-21	2024-06-01	true
4	Пономаренко Вікторія	КН-21	2024-06-01	false
5	Рожко Михайло	КН-22	2024-06-01	false
6	Попова Тетяна	КН-22	2024-06-01	true
7	Бакурова Валерія	ІПЗ-20	2024-06-01	true
8	Щербань Владислав	ІПЗ-21	2024-06-01	true
9	Король Анна	ІПЗ-21	2024-06-01	false
10	Олександрова Інна	ІПЗ-22	2024-06-01	true
11	Мороз Дмитро	КІБ-20	2024-06-01	false
12	Неботов Данило	КІБ-20	2024-06-01	false
13	Дубина Катерина	КІБ-21	2024-06-01	false
14	Кривенко Олексій	КІБ-21	2024-06-01	true

Рисунок 1. Інформаційна система обліку відвідуваності студентів

Біометрична ідентифікація є сучасним підходом, що використовує унікальні фізичні характеристики особи для її ідентифікації [2]. У нашому випадку розглядаємо використання датчиків відбитків пальців, які будуть встановлені на кожній парті. Це дозволить студентам швидко і безпечно ідентифікувати себе, просто приклавши палець до сенсора.

Розглянемо переваги біометричної ідентифікації:

– Точність, біометричні дані є унікальними для кожної особи, що знижує ймовірність помилок при обліку присутності студентів.
– Швидкість, процес ідентифікації займає всього кілька секунд, що дозволяє зекономити час під час занять.

- Безпека, використання біометричних даних ускладнює можливість фальсифікації присутності, оскільки важко підробити відбиток пальця.
- Автоматизація, система може автоматично генерувати звіти про відвідуваність, що спрощує адміністрування.

Метою дослідження є модернізація автоматизованої системи обліку присутності студентів з використанням біометричного пристрою для реєстрації студентів у базі даних, це дозволить студентам швидко вносити свої біометричні дані.

Проєктування автоматизованої системи обліку присутності з використанням біометричної ідентифікації передбачає кілька ключових етапів:

1. Аналіз вимог – на цьому етапі визначаються потреби навчального закладу, функціональні вимоги до системи, а також технічні характеристики датчиків.
2. Вибір обладнання – необхідно обрати якісні датчики відбитків пальців, які будуть надійними та швидкими у роботі.
3. Розробка програмного забезпечення – створити програмне забезпечення для обробки даних, яке включає в себе базу даних для зберігання інформації про студентів та їх відвідуваність.
4. Тестування системи – після розробки система повинна пройти тестування для виявлення можливих помилок і недоліків.
5. Впровадження – після успішного тестування система впроваджується в навчальний процес.

Незважаючи на численні переваги, впровадження біометричної системи обліку присутності може стикатися з певними викликами. Одним із них є питання конфіденційності даних. Важливо забезпечити надійний захист біометричної інформації, щоб уникнути можливих зловживань.

Крім того, необхідно провести навчання для викладачів та студентів, щоб вони могли ефективно користуватися новою системою. Важливо також врахувати можливі технічні проблеми, які можуть виникнути під час експлуатації системи, і мати план дій на випадок їх виникнення.

Автоматизована система обліку присутності студентів з використанням технологій біометричної ідентифікації має потенціал значно покращити процес обліку відвідуваності в навчальних закладах. Використання датчиків відбитків пальців на партах забезпечить точність, швидкість і безпеку, що, в свою чергу, позитивно вплине на навчальний процес. Однак для успішного впровадження такої системи необхідно врахувати всі виклики та забезпечити належний рівень захисту даних.

Література

1. Rozhko, A., Dorohyi, I. and Telychko, H., “Information system for recording student attendance”. Scientific Papers of Donetsk National Technical University. Series: “Computer Engineering and Automation”. 2, 2(34) (Nov. 2024), pp. 32–38, 2024. doi: 10.31474/2786-9024/v2i2(34).313763

2. Shrilakshmi Prasad, Arpitha D., “Student attendance tracking system using biometrics”. International Research Journal of Engineering and Technology (IRJET), vol. 5, issue 3, pp. 433–437, 2018.

3. Nabeel Salih Ali, Ahmed Hazim Alhilali, Hasanein D. Rjeib, Haider Alsharqi, Basheer Al-Sadawi, “Automated attendance management systems: systematic literature review”. Int. J. Technology Enhanced Learning, vol. 14, no. 1, pp. 37–65, 2022. doi: 10.1504/IJTEL.2022.120559

4. В. М. Васильєв, “Система обліку відвідуваності й успішності студентів –як засіб моніторингу рівня знань у студентів”. Ukrainian Journal of Educational Studies and Information Technology, vol. 3, no. 1, pp. 12–16, 2016. doi: 10.32919/uesit.2016.01.12-16

Анотація

У статті розглядається розробка автоматизованої системи обліку присутності студентів з використанням біометричної ідентифікації на основі датчиків відбитків пальців. Запропоноване рішення сприяє підвищенню точності, швидкості та безпеки обліку, водночас вирішуючи проблеми традиційних методів.

Ключові слова: біометрична ідентифікація, облік присутності студентів, освіта, датчик відбитків пальців.

Abstract

The article discusses the development of an automated system for recording student attendance using biometric identification based on fingerprint sensors. The proposed solution helps to improve the accuracy, speed and security of accounting, while solving the problems of traditional methods.

Keywords: biometric identification, student attendance, education, fingerprint sensor.

АВТОМАТИЗОВАНА СИСТЕМА ОХОЛОДЖЕННЯ НА БАЗІ ПЛАТФОРМИ ARDUINO

Сорока Ю. О., студент, ykotov18@gmail.com
Луцький національний технічний університет, Луцьк, Україна

Дане дослідження присвячене розробці автоматизованої системи охолодження на базі мікроконтролерної платформи Arduino з функцією віддаленого керування через веб-інтерфейс. Розробка системи базувалася на платформі Arduino Uno Wi-Fi (рис. 1), яка забезпечує необхідну продуктивність, гнучкість та доступність для реалізації системи з можливістю моніторингу та керування параметрами через Інтернет [1].

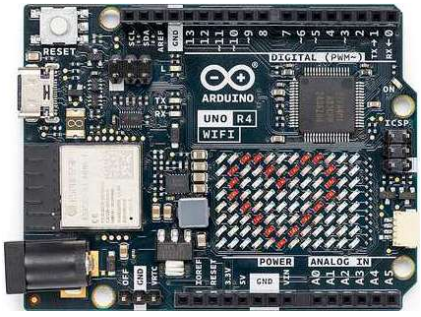


Рисунок 1 – Arduino Uno Wi-Fi

Вибір платформи обґрунтовано її сумісністю із численними сенсорами та виконавчими механізмами, а також доступністю великої кількості бібліотек, які спрощують розробку програмного забезпечення. У роботі реалізовано систему моніторингу температури за допомогою датчика DHT11, який забезпечує зчитування даних про поточну температуру та вологість. На основі отриманих даних здійснюється управління швидкістю обертання вентилятора, що реалізовано через широтно-імпульсну модуляцію (PWM) [2].

Програмне забезпечення системи включає HTTP-сервер, який забезпечує обробку запитів користувача, передачу даних у форматі JSON та надання доступу до веб-інтерфейсу. Особливістю реалізації є інтеграція коду панелі керування у флеш-пам'ять мікроконтролера, що дозволяє ефективно використовувати доступні ресурси.

Панель керування розроблена із застосуванням сучасних веб-технологій, таких як HTML, CSS, JavaScript, що забезпечило адаптивність інтерфейсу для роботи на пристроях із різними розмірами екрана, як на мобільних (рис. 3) так і на десктопних (рис. 4) [3]. Функціонал панелі включає два режими роботи: автоматичний, де система самостійно регулює швидкість вентилятора залежно від температури, та ручний, у якому користувач задає швидкість за допомогою повзунка.

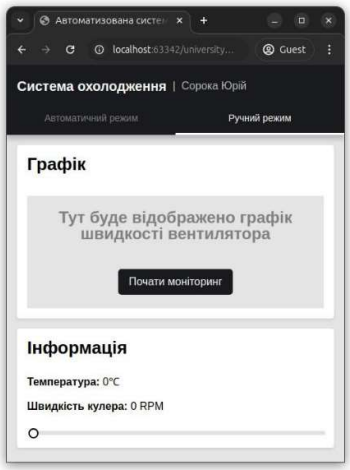


Рисунок 3 – Мобільний інтерфейс панелі керування

Рисунок 4 – Десктопний інтерфейс панелі керування

Для візуалізації даних у реальному часі використано бібліотеку Chart.js, яка дозволяє створювати графіки динамічних змін параметрів, таких як швидкість вентилятора та температура. Запити до сервера здійснюються асинхронно, що забезпечує високу швидкодію та інтерактивність інтерфейсу. Реалізовано механізм передачі даних у форматі JSON для інтеграції системи з іншими додатками або сервісами.

Система пройшла перевірку на коректну взаємодію усіх компонентів системи між собою, стабільність роботи мережевих модулів, точність вимірювань та коректність функціонування автоматичного й ручного режимів (рис. 5).

Здійснено тестування на різних етапах роботи, що включало підключення мікроконтролера до мережі, зчитування даних із сенсорів, обробку запитів сервером та управління вентиляторами. Отримані результати підтвердили стабільну роботу системи та її відповідність заданим функціональним вимогам.

Рисунок 5 – Тестування системи у ручному режимі роботи

Література

1. Кутняк М. М. Аналіз передумов розробки програмно-апаратного комплексу для контролю параметрів мікроклімату на основі платформи ARDUINO. Матеріали LII науково-технічної конференції підрозділів ВНТУ, Вінниця, 21-23 червня 2023 р. : збірник доповідей. 2023. С. 331-332.

2. Основи мікропроцесорної техніки. Лабораторний практикум. Київ : КПІ, 2019. 140 с.

3. Павленко Ю. С. Верстка веб-сторінок з допомогою HTML та CSS: методичні рекомендації до першого модуля нормативної дисципліни «Програмування та підтримка веб-застосувань». Луцьк: ВНУ імені Лесі Українки, 2022. 65 с.

Анотація

Дослідження присвячене розробці автоматизованої системи охолодження на базі платформи Arduino Uno Wi-Fi з віддаленим керуванням через веб-інтерфейс. Система використовує датчик DHT11 для моніторингу температури й вологості та реалізує управління вентилятором через широтно-імпульсну модуляцію. Панель керування, створена за допомогою HTML, CSS та JavaScript, забезпечує адаптивний інтерфейс для мобільних і десктопних пристроїв. Впроваджено функціонал візуалізації даних у реальному часі з використанням бібліотеки Chart.js. Система успішно протестована на відповідність функціональним вимогам і стабільність роботи.

Ключові слова: Arduino Uno Wi-Fi, автоматизована система, охолодження, віддалене керування, веб-інтерфейс, датчик DHT11.

Abstract

The research focuses on the development of an automated cooling system based on the Arduino Uno Wi-Fi platform with remote control via a web interface. The system utilizes the DHT11 sensor for monitoring temperature and humidity and controls the fan speed using Pulse Width Modulation (PWM). The control panel, developed using HTML, CSS, and JavaScript, provides a responsive interface for mobile and desktop devices. Real-time data visualization is implemented using the Chart.js library. The system has been successfully tested for functional compliance and operational stability.

Keywords: Arduino Uno Wi-Fi, automated system cooling, remote control, web interface, DHT11 sensor.

РЕАЛІЗАЦІЯ ТА ВІЗУАЛІЗАЦІЯ ВИБІРКИ ВАЖЛИВОСТІ В ГЛИБОКОМУ НАВЧАННІ AI

Кирилюк В.О. студент, магістр, medoidq@gmail.com
Прикарпатський національний університет імені Василя Стефаника, м. Івано-Франківськ, Україна

Терміни та абревіатури

1) **GRAD-CAM** — Gradient-weighted Class Activation Mapping — метод інтерпретації моделей глибокого навчання для задач класифікації зображень.
2) **SHAP** — SHapley Additive exPlanations — алгоритм оцінки важливості ознак на основі теорії ігор.
3) **LIME** — Local Interpretable Model-agnostic Explanations — метод локальної інтерпретації моделей.
4) **CNN** — Convolutional Neural Networks — згорткові нейронні мережі для аналізу візуальних даних.
5) **RNN** — Recurrent Neural Networks — рекурентні нейронні мережі для послідовних даних.
6) **BERT** — Bidirectional Encoder Representations from Transformers — модель трансформерів для обробки природної мови.
7) **U-Net** — Архітектура нейронної мережі для задач сегментації зображень.
8) **PSNR** — Peak Signal-to-Noise Ratio — метрика оцінки якості зображень.
9) **SSIM** — Structural Similarity Index Measure — метрика для оцінки структурної схожості зображень.
10) **Dropout** — Техніка регуляризації, яка вимикає випадкові нейрони під час навчання моделі.
11) TabNet **—** Модель для роботи з табличними даними, яка інтегрує механізми уваги. Актуальність питання

Актуальність питання

Вибірки важливості ознак у глибокому навчанні полягає у зростаючій складності моделей та обсягу даних, що вимагають ефективних підходів до оптимізації. Вибірка важливих ознак дозволяє знизити обчислювальні витрати, підвищити точність моделей і забезпечити їх інтерпретованість, що є критично важливим для застосувань у медицині, фінансах, безпеці та інших високостakes галузях. Розробка та впровадження сучасних методів, таких як SHAP, GRAD-CAM та LIME, сприяють вирішенню цих задач і відкривають нові можливості для аналізу даних.

Відомі дослідження та публікації

Відомі дослідження та публікації у сфері вибірки важливості зосереджені на розробці та застосуванні методів для інтерпретації моделей глибокого навчання. Серед них виділяються роботи Lundberg S.M. і Lee S.-I. (SHAP), що запропонували уніфікований підхід до оцінки важливості ознак, і дослідження Ribeiro M.T., Singh S., Guestrin C. (LIME), присвячене локальній інтерпретації моделей. Праці Goldstein A. та ін. популяризували візуалізацію індивідуальних впливів ознак, а книга Molnar C. акцентує увагу на зробленні "чорних ящиків" пояснюваними.Постановка задачі та методи

Мета дослідження полягає у розробці методів вибірки важливості для оптимізації процесу навчання моделей глибокого навчання та підвищення їх інтерпретованості. Особливу увагу приділено інтеграції цих методів у програмне забезпечення, здатне завантажувати та обробляти дані з відкритих джерел, що дозволяє покращити ефективність і точність навчання нейронних мереж.

SHAP базується на теорії ігор і використовує значення Шеплі для оцінки внеску кожної ознаки у прогноз моделі. Цей метод забезпечує глобальну й локальну інтерпретованість, показуючи вплив кожної ознаки на результат моделі.

1) Для кожної ознаки і обчислюється внесок у результат моделі:

$$\boldsymbol{\phi i} = \sum_{\substack{S \subseteq N \\ \{i\}}} \frac{|S|!(|N|-|S|-1)!}{|N|!} [f(S \cup \{i\}) - f(S)] ,$$

де: S підмножина ознак без і, $f(S)$ — прогноз моделі для набору ознак S, N — множина всіх ознак.

2) Значення Шеплі Φ_i визначає важливість кожної ознаки.

GRAD-CAM використовується для задач комп'ютерного зору. Метод генерує теплові карти, які показують області зображення, що найбільше вплинули на прогноз моделі.

1) Визначити градієнти функції втрат щодо активацій обраного шару:

$$\alpha_k^c = \frac{1}{Z} \sum_i \sum_j \frac{\partial \text{Lossc}}{\partial A_k^{ij}} ,$$

Де A_{ij}^k— активації на i,j-й позиції k-го каналу, Z — нормалізаційний коефіцієнт.

2) Зважити активації відповідно до ваг α_k^c:

$$L_{Grad-CAM}^c = ReLU(\sum_k \alpha_k^c A_k) ,$$

LIME – це метод інтерпретації моделей машинного навчання, який пояснює передбачення моделі на локальному рівні. Алгоритм будує спрощену лінійну модель для окремої вибірки, що імітує поведінку складної моделі в цьому локальному контексті.

1. Формула LIME для пояснення інтерпретації окремого прогнозу виглядає так:

$$\frac{argmin}{g \in G} L(f, g, \pi x) + \Omega(g)$$

Основний матеріал та результати дослідження

Основний матеріал дослідження зосереджується на розробці та аналізі алгоритмів вибірки важливості даних для задач глибокого навчання. Використано сучасні методи, такі як SHAP, GRAD-CAM і LIME, для різних типів даних: зображень, тексту та табличних наборів. Розроблено програмне забезпечення на Python, що автоматизує вибірку важливих ознак та інтегрує дані з публічних джерел.

Висновки та подальші дослідження

У роботі розроблено та проаналізовано ефективні методи вибірки важливості ознак, що підвищують точність, інтерпретованість і продуктивність моделей глибокого навчання. Алгоритми SHAP, GRAD-CAM і LIME довели свою ефективність у задачах із різними типами даних. Реалізоване програмне забезпечення забезпечує автоматизацію процесів та інтеграцію з відкритими джерелами даних. Подальші дослідження спрямовані на адаптацію методів до мультидоменних даних, оптимізацію обчислювальних ресурсів і застосування у практичних галузях, таких як медицина та фінанси.

Література

1. Тарнавський Ю.А. Технології захисту інформації: підручник. – Київ: КПІ ім. Ігоря Сікорського, 2018. – 162 с. URL: https://ela.kpi.ua (дата звернення: 05.2024 р.).
2. Klima R.E., Sigmon N.P. Cryptology: Classical and Modern with Maplets. – CRC Press, 2013. – 859 p. URL: https://www.crcpress.com (дата звернення: 05.2024 р.).
3. Uçar S., Tas N., Özgür N.Y. A new application to coding theory via Fibonacci and Lucas numbers**.** URL: https://www.matjournals.com (дата звернення: 06.2024 р.).

Анотація

Досліджено методи вибірки важливості ознак у глибокому навчанні, реалізовано алгоритми SHAP, GRAD-CAM, LIME. Розроблено програмне забезпечення для автоматизації вибірки та аналізу результатів. Проведено експериментальний аналіз ефективності моделей у задачах класифікації, регресії та аналізу часових рядів.

Ключові слова: вибірка важливості, глибоке навчання, SHAP, GRAD-CAM, LIME, інтерпретованість моделей, оптимізація.

Abstract

The study explores feature importance methods in deep learning and implements SHAP, GRAD-CAM, and LIME algorithms. Software for automating feature selection and analyzing results was developed. An experimental analysis of model efficiency in classification, regression, and time series tasks was conducted.

Keywords: feature importance, deep learning, SHAP, GRAD-CAM, LIME, model interpretability, optimization.

АРХІТЕКТУРА СИСТЕМИ ВИВЛЕННЯ БПЛА

Очеретній І.Р., магістрант, ihor.ocheretnii.kita@donntu.edu.ua
Донецький національний технічний університет, м. Дрогобич, Україна

Територіально розподілена система виявлення та протидії БПЛА (ТРС ВПБ) являє собою комплексну мережу сенсорів, засобів обробки інформації та систем РЕБ, розташованих на певній території з метою забезпечення ефективного захисту від ворожих безпілотних літальних апаратів. ТРС ВПБ є ефективним засобом захисту від сучасних повітряних загроз. Її комплексна структура, використання різних типів сенсорів та сучасних засобів РЕБ забезпечують високу точність виявлення, ідентифікації та протидії БПЛА. Розвиток таких систем є важливим напрямком у забезпеченні національної безпеки. Функціонування такої системи може базуватись на використанні наступних компонентів:

- Радіолокаційні станції (РЛС): Розміщуються на стратегічно важливих точках для забезпечення раннього виявлення БПЛА на великих відстанях. Використовуються РЛС різних діапазонів, оптимізовані для виявлення малорозмірних та низькошвидкісних цілей.
- Станції радіо- та радіотехнічної розвідки (РРТР): Розміщуються для пеленгації та аналізу радіосигналів, що випромінюються БПЛА та станціями управління. Забезпечують ідентифікацію типу БПЛА та напрямок на джерело сигналу.
- Оптико-електронні станції (ОЕР): Включають камери видимого та інфрачервоного діапазону, встановлені на вежах, будівлях або мобільних платформах. Забезпечують візуальне спостереження та ідентифікацію БПЛА.
- Акустичні сенсори: Розміщуються в районах ймовірного прольоту БПЛА для виявлення за звуком двигуна або пропелерів.

Мережа сенсорів виявлення може бути реалізована у вигляді РЛС, але їх використання в межах лінії бойового зіткнення небажана, через те що вони по суті є цілями для ворожої розвідки. Тому від такого варіанту варто відмовитись. В данному випадку і з метою кращого радіомаскування варто використовувати станції (РРТР) які з легкістю можуть забезпечити такі функції:

- Пеленгування: РРТР визначають напрямок на джерело радіосигналу (БПЛА або станцію управління) за допомогою антенних систем. Для підвищення точності пеленгування використовуються методи триангуляції та інтерферометрії.
- Аналіз сигналів: РРТР аналізують частоту, модуляцію, потужність та інші параметри радіосигналів для ідентифікації типу БПЛА та його призначення.

– База даних сигнатур: Для ідентифікації БПЛА використовуються бази даних сигнатур, що містять характеристики радіосигналів різних типів.

Як вже говорилось у попередньому розділі, то ефективність робьоти систем виявлення БПЛА значно підвищується коли починають працювати комплексні рішення, а саме симбіоз ОЕР та АР. Завдяки такому поєднанню, система може дати більше інформації та більше функцій за рахунок додаткових властивостей:

- можуть включати камери видимого діапазону, тепловізори (інфрачервоні камери) та лазерні далекоміри. Тепловізори ефективні для виявлення БПЛА за тепловим випромінюванням двигуна, особливо вночі. Лазерні далекоміри дозволяють точно визначити відстань до цілі;
- для автоматичного виявлення та супроводження БПЛА використовуються алгоритми обробки зображень, такі як виявлення руху, розпізнавання образів та відстеження об'єктів;
- для підвищення чутливості та напрямленості використовуються мікрофонні решітки, що дозволяють визначити напрямок на джерело звуку;
- алгоритми обробки звуку фільтрують шуми навколишнього середовища та виділяють характерні звуки БПЛА.

Ключовим компонентом, який забезпечує в подальшому постановку того чи іншого типу завади на тому чи іншому напрямі з тими ци іншими параметрами виконується з рахунок рішень, що прийняті в центрі оборобки інформації (ЦОІ) які виконують функції зі збору та обробки даних з використанням алгоритмів обробки сигналів, фільтрації шумів, кореляції даних та штучного інтелекту для виявлення, ідентифікації та класифікації БПЛА, на підставі чого формують єдину картину повітряної обстановки.

Конструктивно ЦОІ складаються з серверів – потужних комп'ютерів, що обробляють дані з сенсорів, спеціалізованого програмного забезпечення для обробки сигналів, кореляції даних, формування тривимірної моделі повітряної обстановки та відображення інформації на екранах операторів та бази даних сигнатур БПЛА, карт місцевості та іншої інформації.

Після прийняття того чи іншого рішення в роботу вступають безпосередньо засоби РЕБ та РЕП які працюють за двома напрямками – як станції створення завад і розміщуються для пригнічення каналів управління, передачі даних та навігації БПЛА, та як системи «Spoofing», і застосовуються для підміни сигналів супутникової навігації. Симбіоз даних систем забезпечує ефективну протидію БПЛА на різних етапах польоту. Щодо технологічних особливостей роботи РЕБ то:

– використовуються різні типи завад, включаючи загороджувальні (шумові), прицільні, маскуючі та імітуючі;
– станції РЕБ працюють в діапазонах частот, що використовуються БПЛА для управління, передачі даних та навігації;
– потужність випромінювання станцій РЕБ достатня для ефективного пригнічення сигналів БПЛА на заданій відстані;

- генерація підроблених сигналів системою «Spoofing» для імітації GPS, ГЛОНАСС, Galileo та BeiDou з спотвореними координатами;
- координація з іншими системами, в тому числі і з нашими, щ метою не нашкодити українським бортам які перебувають на завданні.

Для того щоб система могла існувати і коректно функціонувати, то необхідно щоб командний пункт і відповідні підрозділи мали змогу оперативному обміну інормацією, плюс територіально рознесені сенсори мають також оперативно надавати дані щодо обстановки та радіомоніторингу. Одним з ключових компонентів в автоматизованій системі радіоперешкод є підсистема зв’язку, яка забезпечує обмін інформацією між усіма компонентами системи та використовує захищені канали зв'язку для запобігання перехопленню та глушінню з можливістю резервування у разі виходу з ладу основних каналів.

До переваг такої архітектури варто віднести: великий радіус дії, висока точність виявлення та ідентифікації, ефективна протидія, стійкість до перешкод, гнучкість та масштабованість, синхронізація та координація, захист каналів зв'язку, обробка великих обсягів даних в режимі реального часу, інтеграція з іншими системами ППО.

Література

1. А.В. Атаманчук, І.Ю. Дедів. МЕТОД ВИЯВЛЕННЯ ТА ІДЕНТИФІКАЦІЇ БПЛА З ЗАСТОСУВАННЯМ НЕЙРОННОЇ МЕРЕЖІ//Матеріали XI Міжнародної науково-практичної конференції молодих учених та студентів «АКТУАЛЬНІ ЗАДАЧІ СУЧАСНИХ ТЕХНОЛОГІЙ» – Тернопіль, 7-8 грудня 2022 року. С. 160-161

2. Діапазон виявлення БПЛА з різними масо-габаритними параметрами для РЛС. URL: https://sprotyvg7.com.ua/lesson/informacijno-analitichni-materiali-shhodo-mozhlivostej-viyavlennya-malorozmirnix-bezpilotnix-litalnix-aparativ-zasobami-texnichnoi-rozvidki-zs-rf (дата звернення: жовтень 2024)

3. Батаєв О.П., Ковтун І.В., Корольова Н.А. Теорія електричного зв’язку: Навч. посібник. – Харків: УкрДАЗТ, 2010. - 630 с.

Анотація

Цей документ детально описує концепцію та функціонування територіально розподіленої системи виявлення та протидії безпілотним літальним апаратам. Така система є ефективним засобом захисту від сучасних повітряних загроз, об’єднуючи різноманітні сенсори та засоби радіоелектронної боротьби для виявлення, ідентифікації та нейтралізації БПЛА.

Ключові слова: система, виявлення, радіоелектронна боротьба, БПЛА

Abstract

This document describes in detail the concept and operation of a territorially distributed system for detecting and countering unmanned aerial vehicles. Such a system is an effective means of protection against modern air threats, combining various sensors and electronic warfare means for detecting, identifying and neutralizing UAVs.

Keywords: system, detection, electronic warfare, UAV

УДОСКОНАЛЕННЯ АВТОМАТИЗОВАНОГО РОБОЧОГО МІСЦЯ ІНСПЕКТОРА ДЕКАНАТУ З МЕТОЮ ПІДВИЩЕННЯ ПРОДУКТИВНОСТІ ПРАЦІ ЗА ДОПОМОГОЮ ШТУЧНОГО ІНТЕЛЕКТУ

Журавльов М.О., магістрант, n.zhuravlov13@gmail.com
Донбаська держа́вна машинобудівна академія, Тернопіль, Україна

У сучасних умовах цифровізації освітнього процесу, коли обсяг даних щодо успішності студентів постійно зростає, автоматизація адміністративних процесів стає необхідністю. Автоматизоване робоче місце (АРМ) інспектора деканату є важливою складовою підвищення продуктивності праці та зниження впливу людського фактора на обробку даних.

Прогрес у таких сферах, як Big data, алгоритми, машинне навчання сприяв активному розвитку ШІ. Обробка мов та комп'ютерний зір стали одними з ключових сфер застосування даного інструменту. У широкому спектрі галузей спостерігається тенденція впровадження ШІ[1].

Впровадження ШІ у ВНЗ значно покращує працездатність інспекторів деканату, скорочуючи час відповіді та зберігаючи при цьому персоналізований підхід до кожного студента. Було виявлено що більшість з питань студентів можуть ефективно вирішуватися за допомогою чат-ботів, побудованих на основі ШІ[2].

Постановка задачі

Мета роботи полягає у дослідженні та модернізації системи АРМ інспектора деканату для підвищення ефективності обробки інформації. Актуальним є завдання модернізації серверної частини програмного забезпечення, що забезпечить оптимізацію роботи з базами даних, інтеграцію інтелектуальних алгоритмів аналізу із використанням штучного інтелекту (ШІ) та реалізацію механізмів кешування.

Структура задачі

Процес модернізації системи складається з наступних ключових етапів:

- Аналіз предметної області: вивчення процесів обліку успішності студентів у навчальному закладі.
- Аналіз наявного програмного забезпечення: визначення його сильних та слабких сторін, акцентуючи увагу на продуктивності серверної частини.
- Проектування оновленої архітектури: розробка UML-діаграм, що ілюструють нові функціональні можливості та структурні зміни.
- Оптимізація системи керування базою даних: впровадження сучасних технологій для прискорення обробки запитів, використання найкращих практик.

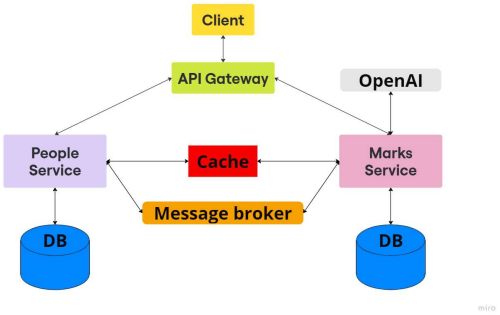


Рисунок 1. Модифікована архітектура системи

– Оптимізація процесів обробки даних щодо успішності студентів: інтеграція інтелектуальних алгоритмів аналізу із використанням штучного інтелекту (ШІ).

– Оптимізація швидкодії системи: зменшення часу відповіді системи шляхом впровадження механізмів кешування.

Основна ідея полягає в розробці підходу до автоматизації процесів обробки даних щодо успішності студентів, що базується на інтеграції інтелектуальних алгоритмів аналізу. Це дозволяє знижувати витрати та забезпечувати надійність зберігання даних.

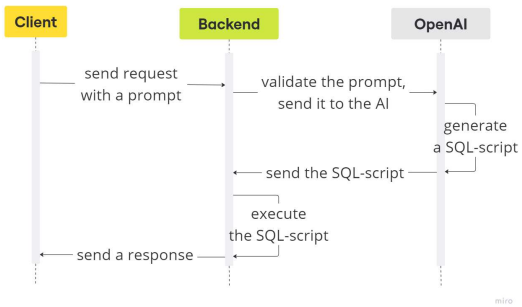


Рисунок 2. Діаграма послідовності обробки запиту

Новизна роботи полягає у впровадженні механізмів, які дозволяють користувачам взаємодіяти з системою через нативні методи, завдяки інтеграції штучного інтелекту для автоматизації складних запитів у системі обліку успішності студентів, яку зображено на рис.1. Для реалізації цього завдання пропонується перехід на мікросервісну архітектуру із поділом на сервіси за доменним принципом[3]. Це дозволяє реалізувати новий рівень функціональності, зокрема інтелектуальне створення SQL-скриптів на основі нативних запитів. Алгоритм виконання наведено на рис.2.

Користувач може через клієнт відправити нативний запит, наприклад, "зроби вибірку із студентів, що не відвідували заняття у певний проміжок часу". Серверна частина веб-додатку отримує цей запит, аналізує та передає його разом зі схемою бази даних до ШІ через API, використовуючи, наприклад, OpenAI. ШІ генерує оптимізований SQL-скрипт, враховуючи усю отриману інформацію, після чого він виконується системою керування базою даних (СКБД) у додатку, реалізуючи запит користувача. Далі бекенд додаток оброблює дані та повертає їх клієнту. За бажанням користувача даний SQL-скрипт може бути збережений для повторного використання.

Висновки та подальші дослідження

Запропоновано систему, що забезпечує підвищення продуктивності праці інспекторів деканату за рахунок оптимізації процесів та інтеграції

штучного інтелекту для взаємодії з користувачами на основі природної мови.

Для подальшого покращення роботи можна приділити більше уваги процесу валідації SQL-скриптів, масштабуванню функціоналу на інші підрозділи закладу освіти, розширення можливостей ШІ та інтеграцію з платформами електронного документообігу.

Література

1. Caiming Zhang. Study on artificial intelligence: The state of the art and future prospects / Caiming Zhang, Yang Lu // Journal of Industrial Information Integration. – 2021. – Т. 23. – С. 100224. — Режим доступу: https://doi.org/10.1016/j.jii.2021.100224. — Заголовок з екрану.

2. Majorana, C. D. B. Enhancing Administrative Efficiency in Higher Education with AI: A Chatbot Solution / Majorana, C. D. B., Gonçalves, R. B., Neto, F. L. A., & Camargo, R. Z. //Review of Artificial Intelligence in Education. – 2022. – Т. 3. – №. 00. – С. e023-e023. — Режим доступу: https://doi.org/10.37497/rev.artif.intell.educ.v3i00.23. — Заголовок з екрану.

3. N. Dragoni. Microservices: yesterday, today, and tomorrow / N. Dragoni, S. Giallorenzo, A. L. Lafuente, M. Mazzara, F. Montesi, R. Mustafin, L. Safina // Present and ulterior software engineering. – 2017. – С. 195-216. — Режим доступу: https://doi.org/10.1007/978-3-319-67425-4_12. — Заголовок з екрану.

Анотація

Представлено результати дослідження комплексу програмного забезпечення автоматизованого робочого місця інспектора деканату та запропоновано процес його модернізації. Особливу увагу приділено інтеграції штучного інтелекту для аналізу нативних запитів користувачів, створення SQL-скриптів та їх виконання. Наведено приклади використання API для взаємодії з ШІ та оптимізації роботи серверної частини програмного забезпечення.

Ключові слова: автоматизація, серверна частина, бекенд, штучний інтелект, SQL-скрипти, OpenAI, кешування.

Abstract

The article presents the results of a study of the software complex of the dean's office inspector's automated workplace and proposes a modernisation process. Particular attention is paid to integrating artificial intelligence to analyse native user requests, create SQL scripts and execute them. Examples of using APIs to interact with AI and optimise the performance of the server side of the software are provided.

Keywords: automation, server-side, backend, artificial intelligence, SQL scripts, OpenAI, caching.

APPROXIMATE METHODS FOR SOLVING OPTIMAL CONTROL PROBLEMS IN MICROCLIMATE MONITORING SYSTEMS OF CIVIL DEFENCE SHELTERS

A. Romaniuk, student, Computerized Control Systems and Automation,
A. Voropaieva, PhD, Associated Professor, Department of Information and Telecommunication Technology and Systems
Ivano-Frankivsk National Technical University of Oil and Gas, Ivano-Frankivsk, Ukraine

Overview of Optimal Control Problems in Microclimate Systems. Optimal control problems in microclimate systems often involve managing parameters such as temperature, humidity, and air quality to achieve desired outcomes, such as energy efficiency. The complexity of these systems is compounded by external factors, including fluctuations in environmental conditions. For instance, Yau and Chew discuss how computer-aided design tools can optimize thermal comfort and energy consumption in buildings, which is directly applicable to microclimate control in shelters [10]. Monitoring systems that can adapt to changes in internal and external conditions are crucial, as they offer the potential for significant energy savings through effective microclimate management.

Approximate Methods for Solving Optimal Control Problems. Several approximate methods have been developed to tackle nonlinear optimal control problems, which are prevalent in microclimate monitoring systems. The direct method is one of the most widely used approaches, as it transforms the optimal control problem into a mathematical programming problem with numerous parameters and constraints [2]. This method allows for the incorporation of real-time data from various sensors, which is essential for maintaining optimal microclimate conditions.

Another notable approach is the method of successive approximations, which has been effectively applied to nonlinear systems. This method iteratively refines the control strategy based on previous estimates, allowing for convergence towards an optimal solution [5]. Moreover, the homotopy perturbation method has been employed to solve both linear and nonlinear optimal control problems, providing a flexible framework for addressing the complexities of microclimate control [1].

Influence of External Factors. The influence of external factors such as temperature and humidity changes is critical in the design of effective microclimate monitoring systems. For instance, Isakov describes an automatic control system that utilizes temperature and humidity sensors to maintain the desired microclimate in vegetable storage, demonstrating the practical application of these concepts [3]. Additionally, studies have shown that sensor fusion techniques can enhance the monitoring and control of greenhouse environments, allowing for more precise adjustments based on real-time data [8, 7].

The integration of cloud-based IoT platforms for precision control of microclimate parameters has also gained traction. These platforms enable continuous monitoring and adjustment of environmental conditions, ensuring that external variations are accounted for in real-time [9]. The ability to collect and analyze data from multiple sources enhances the robustness of control strategies, making them more resilient to fluctuations in external conditions.

Advanced Control Strategies. Model Predictive Control (MPC) is an advanced strategy that has been effectively utilized for optimizing microclimate conditions. MPC allows for the prediction of future states of the system based on current data, enabling proactive adjustments to control inputs. This method is particularly advantageous in environments where rapid changes in microclimate parameters can occur, such as in greenhouses or civil shelters.

Furthermore, the development of automated systems for monitoring microclimate parameters has been demonstrated to significantly improve energy efficiency and maintain optimal conditions [4]. These systems often incorporate machine learning algorithms to predict and adapt to changes in the environment, thereby enhancing the overall performance of microclimate control systems.

Challenges and Future Directions. Despite the advancements in approximate methods for solving optimal control problems, several challenges remain. The need for real-time data processing is paramount, as delays in data acquisition can lead to suboptimal control decisions [8]. Additionally, the integration of various control strategies and technologies poses a challenge in terms of system complexity and reliability.

Future research should focus on enhancing the robustness of control algorithms to better handle the uncertainties associated with external environmental factors. The application of deep learning techniques in controlled environment agriculture has shown promise in addressing these challenges, as they can learn from historical data to improve predictive capabilities [6]. Moreover, the exploration of hybrid control strategies that combine traditional methods with modern computational techniques could lead to more effective solutions for microclimate monitoring systems.

Conclusion. The optimization of microclimate control systems is a multifaceted problem that requires a comprehensive understanding of various approximate methods and their applications. By integrating advanced control strategies, real-time data monitoring, and adaptive algorithms, it is possible to enhance the efficiency and effectiveness of microclimate management in civil defence shelters. Continued research and development in this field will be essential for addressing the challenges posed by external environmental factors and ensuring sustainable practices in building management.

References:

1. Effati, S. and Nik, H. (2011). Solving a class of linear and non-linear optimal control problems by homotopy perturbation method. Ima Journal of Mathematical Control and Information, 28(4), 539-553. https://doi.org/10.1093/imamci/dnr018.

2. Han, Z. and Li, S. (2011). A new approach for solving optimal nonlinear control problems using decriminalization and rationalized haar functions. Advanced Engineering Forum, 1, 387-394. https://doi.org/10.4028/www.scientific.net/aef.1.387.
3. Isakov, A. (2023). Automatic control system for automatic maintenance of microclimate in vegetable storages. E3s Web of Conferences, 458, 01012. https://doi.org/10.1051/e3sconf/202345801012.
4. Kiktev, N., Lendiel, T., Vasilenkov, V., Kapralyuk, O., Hutsol, T., Głowacki, S., … & Kowalczyk, Z. (2021). Automated microclimate regulation in agricultural facilities using the air curtain system. Sensors, 21(24), 8182. https://doi.org/10.3390/s21248182.
5. Nik, H. and Effati, S. (2013). An approximate method for solving a class of nonlinear optimal control problems. Optimal Control Applications and Methods, 35(3), 324-339. https://doi.org/10.1002/oca.2070.
6. Ojo, M. and Zahid, A. (2022). Deep learning in controlled environment agriculture: a review of recent advancements, challenges and prospects. Sensors, 22(20), 7965. https://doi.org/10.3390/s22207965.
7. Reza, M. (2023). Spatial, temporal, and vertical variability of ambient environmental conditions in chinese solar greenhouses during winter. Applied Sciences, 13(17), 9835. https://doi.org/10.3390/app13179835.
8. Rezvani, S., Abyaneh, H., Shamshiri, R., Balasundram, S., Dworak, V., Goodarzi, M., … & Mahns, B. (2020). Iot-based sensor data fusion for determining optimality degrees of microclimate parameters in commercial greenhouse production of tomato. Sensors, 20(22), 6474. https://doi.org/10.3390/s20226474.
9. Sagheer, A., Mohammed, M., Riad, K., & Alhajhoj, M. (2020). A cloud-based iot platform for precision control of soilless greenhouse cultivation. Sensors, 21(1), 223. https://doi.org/10.3390/s21010223.
10. Yau, Y. and Chew, B. (2012). A review on predicted mean vote and adaptive thermal comfort models. Building Services Engineering Research and Technology, 35(1), 23-35. https://doi.org/10.1177/0143624412465200.

Анотація

Оптимізація систем контролю мікроклімату в укриттях цивільного захисту, особливо для екологічних застосувань, є складною проблемою, яка вимагає інтеграції різних факторів, включаючи зміни температури та вологості. Методи наближеного вирішення проблем оптимального керування в цих системах мають вирішальне значення для підвищення ефективності та забезпечення збереження бажаних умов середовища. У цьому огляді синтезовано різні підходи та методології, які були розроблені за останні роки, підкреслюючи їх актуальність для систем моніторингу мікроклімату.

Ключові слова: моніторинг мікроклімату, задачі оптимального керування, наближені методи

Abstract

The optimization of microclimate control systems in civil defence shelters, particularly for environmental applications, is a complex problem that requires the integration of various factors, including temperature and humidity changes. The methods for approximating solutions to optimal control problems in these systems are crucial for enhancing efficiency and ensuring the desired environmental conditions are maintained. This overview synthesizes various approaches and methodologies that have been developed in recent years, highlighting their relevance to microclimate monitoring systems.

Keywords: Microclimate Monitoring, Optimal Control Problems, Approximate Methods.

ПЕРСПЕКТИВНЕ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ IOT ДЛЯ АВТОМАТИЗОВАНОЇ ПЕРЕДАЧІ ДАНИХ

Гаращенко В.С., магістрант гр.СУАм-22,
valerii.harashchenko.kita@donntu.edu.ua
Державний вищий навчальний заклад «Донецький національний технічний університет», Дрогобич, Україна

Технології IoT (інтернет речей) стають невід'ємною частиною сучасного світу завдяки простоті їх реалізації, відносно низькій вартості та гнучкості у застосуванні. Їх успішно використовують у різних сферах, зокрема у забезпеченні безпеки приміщень, автоматизації процесів, моніторингу і контролю. Такі переваги роблять IoT-технології надзвичайно популярними та затребуваними в сучасному світі.

У цій тезі буде розглянуто декілька тем перспективного застосування IoT, зокрема:

- Моніторинг та контроль показників.
- Передача даних з лічильників (тепла, газу, електроенергії).
- Використання автономних систем, які можуть бути повністю енергонезалежними.
- Передача даних через бездротові протоколи на значні відстані (до десятків кілометрів).

Особливу увагу приділено розгляду можливостей бездротової передачі даних за допомогою пристроїв IoT. Представлені технології демонструють значний потенціал у підвищенні якості життя та оптимізації різних процесів.

Автоматизація передачі показів лічильників: технології та архітектура систем

Автоматизація передачі показів лічильників для різних комунальних послуг, таких як електроенергія, вода, газ і тепло, є важливим кроком до підвищення ефективності управління енергоресурсами. Удосконалення методів збору, передачі та аналізу даних дозволяє зменшити втрати енергії, оптимізувати використання ресурсів і знизити експлуатаційні витрати.

Сучасні автоматизовані системи передачі показів лічильників використовують як дротові, так і бездротові технології. Дротові рішення, такі як інтерфейси RS-232, RS-485 та M-Bus, забезпечують надійну передачу даних на короткі відстані та широко застосовуються в багатоквартирних будинках і промислових об'єктах. Зокрема, інтерфейс M-Bus був спеціально розроблений для потреб обліку енергоносіїв і дозволяє об'єднувати в мережу велику кількість лічильників різних типів.

Бездротові технології, такі як GSM/GPRS, WM-Bus, LoRaWAN та NB-IoT, надають можливість передавати дані на значні відстані без необхідності прокладання кабелів. Це особливо актуально для віддалених або важкодо-

ступних об'єктів. Наприклад, технологія LoRaWAN забезпечує передачу даних на відстань до 15 км з низьким енергоспоживанням, що робить її ефективною для міських та сільських територій .

Архітектура автоматизованих систем передачі показів

Архітектура таких систем зазвичай включає кілька рівнів, які працюють у взаємодії для забезпечення точності збору та обробки даних:

1. Рівень пристроїв збору даних (Data Acquisition Layer): На цьому рівні працюють лічильники, оснащені сенсорами для вимірювання параметрів, таких як споживання електроенергії, об’єм використаної води або витрати газу. Сучасні лічильники оснащені інтерфейсами для збирання даних, такими як M-Bus або RS-485/RS-232, що забезпечують надійну комунікацію навіть у складних умовах.
2. Рівень передачі даних (Data Communication Layer): Відповідає за передачу інформації від лічильників до серверів обробки. Залежно від застосування використовуються такі технології:
   - Дротові протоколи: M-Bus та RS-485/RS-232 застосовуються у багатоквартирних будинках та на промислових об’єктах для створення локальних мереж збору даних.
   - Бездротові технології: LoRaWAN, NB-IoT, GSM/GPRS дозволяють передавати дані на значні відстані, мінімізуючи енергоспоживання. Технологія LoRaWAN забезпечує передачу даних на відстань до 15 км, що є ідеальним рішенням для віддалених об’єктів. Також використання протоколу LoRaWAN дає змогу використовувати повністю енергонезалежні системи, модем LoRaWAN під’єднаний до лічильника через шину M-Bus, це дає змогу отримувати дані з місць де навіть може і не бути електроенергії.
3. Рівень обробки та зберігання даних (Data Processing Layer): На цьому рівні дані, отримані від лічильників, обробляються і зберігаються. Часто використовуються хмарні платформи, які забезпечують масштабованість та доступність даних для користувачів і операторів. Алгоритми аналізу дозволяють ідентифікувати аномалії у споживанні ресурсів, прогнозувати навантаження та виявляти можливі технічні проблеми.
4. Рівень управління та застосувань (Management and Application Layer): Комунальні служби та користувачі отримують доступ до даних через веб-додатки або мобільні інтерфейси. Наприклад, у системах "розумного будинку" користувач може відстежувати споживання води чи електроенергії в реальному часі та автоматично налаштовувати режими роботи пристроїв. Комунальні служби отримуючи дані, можуть швидко та точно розраховувати енергоспоживання будинку або квартири та не завищувати сплату за тариф, система стає прозорою, для всіх.

Практичні приклади впровадження автоматизованих систем обліку

1. Системи обліку електроенергії

В енергетиці автоматизовані системи комерційного обліку електроенергії (АСКОЕ) давно використовуються для підвищення точності та прозорості розрахунків між постачальниками та споживачами. Наприклад, у великих містах України, таких як Київ, ПАТ "Київенерго" впровадило АСКОЕ, що дозволило знизити втрати енергії на 15%. Система автоматично збирає дані про споживання електроенергії з лічильників, передає їх через GSM-мережу до центрального серверу, де виконується обробка та формування звітів.

2. Облік води та теплової енергії

Автоматизовані системи обліку води та теплової енергії стали актуальними в умовах урбанізації та зростання вартості ресурсів. Наприклад, у багатоквартирних будинках застосовуються лічильники з M-Bus інтерфейсом, які збирають дані про споживання води та тепла. Ці дані передаються на центральний сервер за допомогою локальної мережі. Такий підхід дозволяє управляючим компаніям аналізувати споживання та оперативно реагувати на аномалії, наприклад, витоки води.

3. Інтеграція в "розумні міста"

Технології IoT стають основою концепції "розумного міста". У Барселоні було впроваджено автоматизовану систему збору даних з лічильників електроенергії, газу та води, яка інтегрована з муніципальною платформою управління. Ця система дозволяє виявляти надмірне споживання ресурсів та прогнозувати потреби різних районів міста. В результаті муніципалітет скоротив витрати на енергоресурси на 20% протягом п’яти років.

Виклики та перспективи впровадження:

Незважаючи на очевидні переваги, впровадження автоматизованих систем обліку стикається з певними викликами. Серед них – необхідність стандартизації протоколів передачі даних, забезпечення кібербезпеки та інтеграція з існуючими інфраструктурами. Проте розвиток технологій та зростаючий попит на ефективне управління ресурсами сприяють активному впровадженню таких систем у різних галузях.

Література

1. Pysarets A., Pysarets Y. Автоматизовані системи передачі показань від приладів обліку енергоносіїв. Частина 1 // Вісник Київського політехнічного інституту. Серія Приладобудування. – 2020. – №59 (1). – С. 95–101. https://visnykpb.kpi.ua/article/view/210037
2. Pysarets A., Pysarets Y. Автоматизовані системи передачі показань від приладів обліку енергоносіїв. Частина 2 // Вісник Київського політехнічного інституту. Серія Приладобудування. – 2020. – №60 (2). – С. 102–108. https://visnykpb.kpi.ua/article/view/221452

3. Григор'єв В.І., Ковальчук О.В. Автоматизована система комерційного обліку електроенергії ПАТ «Київенерго» // Енергетика: економіка, технології, екологія. – 2016. – №2. – С. 45–50. https://energy.kpi.ua/article/download/133101/129549
4. Сучасні способи автоматичної передачі даних з лічильників // Матеріали конференції Житомирського державного технологічного університету. – 2023. – С. 267. https://conf.ztu.edu.ua/wp-content/uploads/2023/02/267.pdf
5. Автоматизовані системи передачі показань від приладів обліку енергоносіїв // Вісник Київського політехнічного інституту. Серія Приладобудування. – 2020. – №60 (2). – С. 95–101. http://visnykpb.kpi.ua/article/view/221452/221238
6. Впровадження автоматизованих систем обліку та контролю електричної енергії / Вісник Вінницького політехнічного інституту. – 2016. – №2. – С. 45–50. URL: https://pdfs.semanticscholar.org/5487/efa3ff7251555ab9d21149bface3be5ea1a5.pdf

Анотація

Технології Інтернету речей (IoT) дедалі частіше використовуються для автоматизації та оптимізації обліку енергоносіїв. У статті розглядаються ключові аспекти впровадження автоматизованих систем передачі показів лічильників для різних послуг (електроенергії, води, газу, тепла). Проаналізовано архітектуру таких систем, включаючи рівні збору, передачі, обробки даних та управління. Представлено практичні приклади впровадження автоматизованих рішень у міській інфраструктурі, промисловості та багатоквартирних будинках. Зазначено виклики, зокрема стандартизацію протоколів і забезпечення кібербезпеки, а також окреслено перспективи розвитку, пов’язані з інтеграцією IoT у "розумні міста".

Ключові слова: електроніка, бездротові технології, пристрої IoT.

Abstract

Internet of Things (IoT) technologies are increasingly utilized for automating and optimizing resource metering. This paper examines the key aspects of implementing automated systems for meter data transmission across various services (electricity, water, gas, and heat). The architecture of these systems is analyzed, including the levels of data acquisition, communication, processing, and management. Practical examples of implementing automated solutions in urban infrastructure, industry, and residential buildings are presented. The challenges, such as protocol standardization and ensuring cybersecurity, are highlighted, along with future prospects related to IoT integration into "smart cities"

Keywords: electronics, wireless technologies, IoT devices.

РОЗРОБКА АВТОМАТИЗОВАНОЇ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ СИСТЕМИ КЕРУВАННЯ КЛІМАТИЧНИМИ ПАРАМЕТРАМИ ЖИТЛОВОГО БУДИНКУ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЙ ІОТ

Дубиняк Є. Р., магістр, yevhen.dubyniak-aksm231@nung.edu.ua;
Воропаєва А.О., к.т.н., доцент, anna.voropaieva@nung.edu.ua
Івано-Франківський національний технічний університет нафти і газу, м. Івано-Франківськ, Україна

У сучасному світі дедалі більше зростає потреба у створенні комфортного житлового середовища, що відповідає сучасним стандартам якості життя, при цьому мінімізуючи енерговитрати та негативний вплив на навколишнє середовище. Зростаюча урбанізація, підвищення житлових стандартів і необхідність оптимального використання ресурсів ставлять перед нами завдання впровадження інноваційних рішень у сфері клімат-контролю [1]. Використання технологій Internet of Things (IoT) для управління мікрокліматом у житлових будинках відкриває нові можливості для автоматизації процесів регулювання температури, вологості, якості повітря та інших параметрів. Такі технології дозволяють забезпечити високий рівень комфорту для мешканців, при цьому значно знизити енергоспоживання завдяки адаптивним механізмам управління, які враховують реальні потреби користувачів і умови навколишнього середовища.

Метою дослідження є розробка автоматизованих систем управління кліматичними параметрами житлових будинків, що інтегрують IoT-рішення для забезпечення не лише комфорту та енергоефективності, але й адаптивності до індивідуальних потреб кожного користувача. Фокусуючись на оптимізації роботи систем клімат-контролю, дослідження спрямоване на створення технологій, що забезпечують баланс між комфортом, енергозбереженням та екологічністю.

Дослідження базуються на аналізі існуючих систем клімат-контролю та їх удосконалення за допомогою IoT, використовуючи сучасні дані з галузі інженерії та аналітики енергоспоживання [2]. Температура, вологість, CO_2, освітленість і швидкість руху повітря є ключовими факторами комфорту. Інтеграція IoT-систем дозволяє проводити безперервний моніторинг і корекцію параметрів у реальному часі.

Системи на базі IoT, такі як датчики та контролери (рис. 1), забезпечують оптимальну взаємодію з іншими елементами розумного будинку. Автоматизація дозволяє впроваджувати такі технології, як рекуперація тепла, зменшуючи енергоспоживання [3]. Зважаючи на чутливість даних, що передаються в системах розумного будинку, необхідно вживати заходів для забезпечення їх цілісності та конфіденційності в станах збере ження, обробки

та передачі на серверну частину інформаційно-комунікаційної автоматизованої системи, а також приділяти увагу її доступності з рівнем не менш ніж три дев'ятки (99,9% часу).

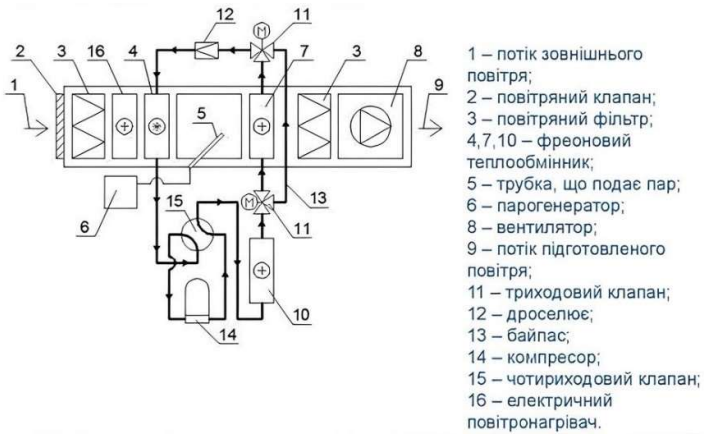


Рисунок 1 - Принцип роботи системи вентиляції з контролем CO_2

Згадані заходи можуть включати в себе: шифрування, двофакторну аутентифікацію, регулярне оновлення програмного забезпечення. Системи IoT не лише забезпечують комфорт, але й підвищують зручність через дистанційне управління та аналіз даних.

Інтеграція IoT в системи клімат-контролю в житлових приміщеннях є ключовим напрямком для підвищення якості життя та енергоефективності. Подальші дослідження спрямовані на вдосконалення протоколів інтеграції та методів кібербезпеки.

Література

1. Д. О. Сапожник і Д. Д. Плечистий, «ВИКОРИСТАННЯ ІНТЕРНЕТУ РЕЧЕЙ ДЛЯ ЕКОНОМІЇ ЕНЕРГЕТИЧНИХ РЕСУРСІВ», Вісник ВПІ, вип. 4, с. 39–45, Серп. 2023.

2. Лановський М. О. ВПРОВАДЖЕННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ ІНТЕРНЕТУ РЕЧЕЙ ДЛЯ ПОЛІПШЕННЯ ЕНЕРГООЩАДНИХ ТЕХНОЛОГІЙ У БУДІВЛЯХ. Наукові записки Міжнародного гуманітарного університету. 2022. № 37. С. 151–153.

3. AUTOMATION OF MICROCLIMATE CONTROL PROCESSES IN RESIDENTIAL PREMISES / Z. Mykytyuk та ін. Information and communication technologies, electronic engineering. 2024. Т. 4, № 1. С. 155–162.

Анотація

У роботі розглянуто можливості автоматизованих систем управління кліматичними параметрами житлових будинків з використанням технологій IoT. Досліджено ключові кліматичні параметри, їхній вплив на комфорт, а також переваги інтеграції IoT для досягнення енергоефективності. Зроблено висновок, що такі системи не лише підвищують комфорт мешканців, але й сприяють зменшенню енергоспоживання.

Ключові слова: автоматизація, IoT, клімат-контроль, енергоефективність, житловий будинок.

Abstract

The paper explores the possibilities of automated systems for managing climate parameters in residential buildings using IoT technologies. Key climate parameters, their impact on comfort, and the benefits of IoT integration for energy efficiency were analyzed. It was concluded that such systems not only enhance residents' comfort but also contribute to reducing energy consumption.

Keywords: automation, IoT, climate control, energy efficiency, residential building.

РОЗРОБКА ТА МОДЕЛЮВАННЯ АВТОМАТИЗОВАНОЇ СИСТЕМИ ЕНЕРГЕТИЧНОГО МЕНЕДЖМЕНТУ ДЛЯ ГРОМАДСЬКИХ БУДІВЕЛЬ

Гусєв Д. М., магістрант каф. АТ, danylo.husiev.kita@donntu.edu.ua;
Теличко Г. О., к.т.н., доц. каф. АТ, hanna.telychko@donntu.edu.ua;
Ступак Г. В., ст. викл. каф. АТ, glib.stupak@donntu.edu.ua
Донецький Національний Технічний Університет, Дрогобич, Україна

Громадські будівлі, такі як офісні приміщення, школи, лікарні, споживають значні обсяги енергії для забезпечення комфортних умов. У сучасних умовах високої вартості енергоресурсів та екологічних викликів енергетичний менеджмент стає пріоритетним завданням. Традиційні підходи, що базуються на ручному моніторингу енергоспоживання, є застарілими, оскільки не забезпечують точності, своєчасності та оптимізації процесів [1][2].

Автоматизовані системи енергетичного менеджменту (АСЕМ) дозволяють вирішувати ці завдання за допомогою сучасних технологій, таких як Інтернет речей (IoT), інтелектуальні алгоритми аналізу даних та автоматизація управління. Це сприяє економії енергії, зниженню експлуатаційних витрат та підвищенню екологічної безпеки.

Метою роботи є розробка та обґрунтування автоматизованої системи енергетичного менеджменту для громадських будівель, яка дозволить оптимізувати енергоспоживання, знизити витрати на обслуговування та забезпечити сталість у використанні ресурсів [3].

Розробка автоматизованої системи енергетичного менеджменту для громадських будівель базується на комплексному аналізі сучасних підходів і технологій, які сприяють зменшенню споживання енергії. У сучасному світі громадські будівлі є великими споживачами енергоресурсів, і їх ефективне управління потребує впровадження сучасних рішень. Запропонована система покликана забезпечити оптимізацію використання ресурсів шляхом інтеграції інноваційних технологій моніторингу, автоматичного аналізу даних та автоматизованого управління основними системами будівлі [4].

Архітектура системи включає датчики, які забезпечують збирання інформації про поточні показники енергоспоживання в режимі реального часу, програмне забезпечення для обробки даних, а також керуючі механізми, що адаптують режими роботи інженерних систем відповідно до поточних потреб будівлі. Датчики розташовуються у ключових зонах, таких як системи HVAC, освітлення та енергопостачання, що дозволяє точно оцінювати споживання та виявляти потенційні аномалії або перевитрати.

Система також інтегрує прогнозні алгоритми, які, базуючись на аналізі зібраних даних, дозволяють оцінювати майбутнє енергоспоживання, враховуючи історичні дані, погодні умови та очікувані зміни в експлуатації будівлі. Це дозволяє оптимізувати режими роботи систем, знижуючи споживання енергії в години пікових навантажень і забезпечуючи комфортні умови для користувачів.

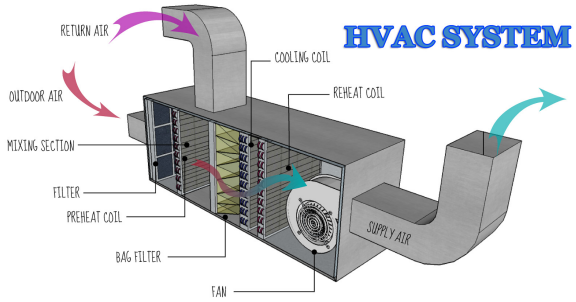


Рисунок 1 – Система HVAC

Поточний етап дослідження включає моделювання роботи системи у віртуальному середовищі для оцінки її потенційної ефективності. За допомогою програмного забезпечення SCADA було змодельовано сценарії функціонування системи в різних умовах, таких як зміни навантаження, погодні фактори та зміни у використанні будівлі. Результати показали, що система здатна забезпечити зниження енергоспоживання завдяки інтелектуальним методам управління.

Наступним етапом є тестування прототипу системи в реальних умовах, що дозволить перевірити її ефективність у практичному застосуванні. Очікується, що впровадження системи надасть змогу знизити витрати на енергоресурси, забезпечити стабільність роботи інженерних систем та покращити комфортні умови для користувачів будівель [1][5].

Таким чином, існуючи сьогодні рішення дозволяють запропонована система автоматизованого енергетичного менеджменту представляє перспективне рішення, здатне значно підвищити енергоефективність громадських будівель, забезпечуючи одночасно економію ресурсів і зниження вуглецевого сліду.

Метою подальшого дослідження є створення та впровадження автоматизованої системи енергетичного менеджменту для громадських будівель, яка забезпечить економію енергоресурсів завдяки точному моніторингу, прогнозуванню та оптимізації енергоспоживання у режимі реального часу. Передбачається підвищення комфорту користувачів будівель через інтеграцію інтелектуальних рішень, таких як автоматичне регулювання освітлення, опалення та вентиляції залежно від зовнішніх умов та завантаженості приміщень. Також планується мінімізація негативного впливу на довкілля шляхом інтеграції відновлюваних джерел енергії та зниження викидів парникових газів. Подальші дослідження спрямовані на розробку фізичного прототипу системи, її тестування в реальних умовах експлуатації та адаптацію для використання у будівлях різного призначення. Така система дозволить забезпечити сталість, економію ресурсів та екологічну ефективність, сприяючи досягненню цілей сталого розвитку у сфері будівельного енергетичного менеджменту [4][6].

Література

1. Smith J., Energy Management in Smart Buildings. — Cambridge: Green Tech, 2020. — 256 p.
2. Коваленко А.І., Автоматизовані системи управління енергоспоживання3м. — Київ: Техніка, 2018. — 144 с.
3. Grus M. Smart Building Energy Efficiency Solutions. New York: Springer, 2019.
4. International Energy Agency. Energy Efficiency 2023: Report and Recommendations. Paris: IEA, 2023.
5. European Commission. Energy Performance of Buildings Directive: Guidelines and Updates. Brussels: EU Publications, 2022.
6. Wang Y., Li H. IoT-Based Energy Management Systems in Smart Buildings. Beijing: Academic Press, 2021.

Анотація

У дослідженні розглянуто концепцію автоматизованої системи енергетичного менеджменту для громадських будівель, яка спрямована на оптимізацію енергоспоживання, підвищення ефективності управління ресурсами та мінімізацію екологічного впливу. Моделювання показало потенціал зниження енергоспоживання. Подальші дослідження будуть спрямовані на тестування системи у реальних умовах.

Ключові слова: енергетичний менеджмент, громадські будівлі, автоматизація, енергоефективність, IoT.

Abstract

The research examines the concept of an automated energy management system for public buildings, which is aimed at optimizing energy consumption, increasing the efficiency of resource management, and minimizing environmental impact. Modeling showed the potential to reduce energy consumption. Further research will be directed not for testing the system in real conditions.

Keywords: energy management, public buildings, automation, energy efficiency, IoT.

АВТОМАТИЗАЦІЯ КЕРУВАННЯ РЕЖИМАМИ ОСВІТЛЮВАЛЬНИХ УСТАНОВОК

Говоров П.П., д.т.н., професор, pilip.govorov@kname.edu.ua;
Кіндінова А.К., аспірантка, anastasiya.kindinova@kname.edu.ua;
Базалєй Д.В., студент, danylo.bazaliei@kname.edu.ua;
Журавель В.В., студент, vladyslav.zhuravel@kname.edu.ua
Харківський Національний університет міського господарства ім. О.М. Бекетова, Харків, Україна

Проблема енергоефективності та якості освітлення набуває все більшої актуальності через зростаючі вимоги до комфорту, безпеки та екологічності. Автоматизовані системи керування освітленням (АСКО) є ефективним інструментом для вирішення цих завдань, оскільки забезпечують оптимізацію енергоспоживання, динамічне регулювання параметрів світлового потоку та підвищення загальної ефективності роботи освітлювальних установок.

Сучасна наукова література акцентує увагу на використанні інтелектуальних технологій у системах освітлення, які дозволяють інтегрувати їх у міську інфраструктуру та промислові об’єкти. Основний акцент робиться на автоматизації управління, адаптації до зовнішніх умов, застосуванні функції димування та створенні динамічних сценаріїв освітлення. Разом із тим, проблематика індивідуального контролю параметрів світлового потоку та впливу цього контролю на загальну ефективність систем залишається недостатньо дослідженою.

Метою цієї роботи є розробка структурної схеми автоматизованої системи керування освітлювальними установками, яка дозволяє індивідуально контролювати параметри кожного світильника, забезпечувати їхню оптимальну роботу та відповідність сучасним вимогам енергоефективності й якості.

У межах дослідження розроблено структурну схему автоматизованої системи, що включає індивідуальні лічильники світлової енергії, датчики освітленості та перетворювачі параметрів світлового потоку. Усі елементи системи інтегровані з централізованим лічильником енергії, що дозволяє здійснювати моніторинг ефективності роботи кожного світильника та системи в цілому[1–3]. Як відомо, кінцевою продукцією освітлювальних систем є світлова енергія, яка споживається населенням у формі світлового потоку необхідної економічності та якості рівня освітленості. Розрахунок світлового потоку (Ф) здійснюється за формулою:

$$\Phi = \frac{P}{K} \qquad (1)$$

де: К — постійний коефіцієнт;. Р — електрична потужність установки.

Розроблена схема (рис. 1) забезпечує контроль параметрів освітлення за такими показниками, як освітленість (E), яскравість (L) та спектр випромінювання (λ).

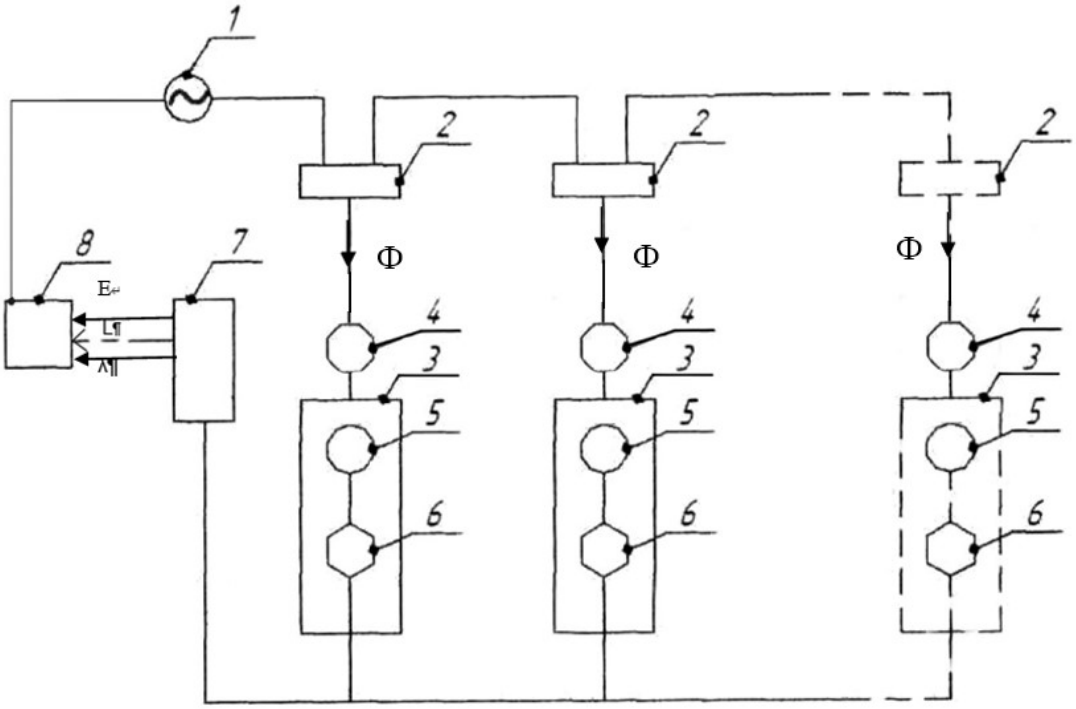


Рисунок 1. Структура схеми освітлювальної установки

На рисунку показано взаємодію ключових елементів системи: джерела живлення, централізованого лічильника електричної енергії, світильників, індивідуальних лічильників світлової енергії та датчиків освітленості. Відображено процес перетворення світлового потоку у цифровий сигнал і його подальший аналіз на диспетчерському пункті [4, 5].

Результати показують, що запропонована система дозволяє створювати динамічні сценарії освітлення, адаптовані до умов експлуатації, знижувати енерговитрати, подовжувати термін служби світильників та покращувати якість освітлення.

Впровадження таких систем є перспективним напрямом розвитку освітлювальних установок. Подальші дослідження зосередяться на вдосконаленні алгоритмів адаптивного управління, інтеграції з іншими елементами «розумного міста» та розширенні функціоналу систем.

Література

1. Говоров П. П. Автоматизація керування режимами міських електричних мереж : монографія / П. П. Говоров, В. Ф. Харченко, В. П. Говоров. — Харків : ХНУМГ ім. О. М. Бекетова, 2017. — 229 с.

2. Akagi H. Analysis and design of an active power filter using quad-series voltage source PMW converters / H. Akagi, Y. Tsukamoto, A. Nabae // IEEE Trans. Ind. Applicat. — 1990. — Vol. 26. — P. 93–98.

3. Babaev V. Sustainable development of territories under martial law / V. Babaev, P. Hovorov, A. Kindinova, V. Hovorov // Sustainable development: Year XII. — Bulgary, 2022. — Vol. 2. — P. 16–24.

4. Hanus O. Mode control of lighting system based on the Smart-Light concept / O. Hanus, P. Hovorov, A. Kindinova // Scientific research of the XXI century : collective monograph. — Sherman Oaks. Los Angeles (USA), 2021. — Vol. 1. — P. 113–120.

5. Говоров П. П. Ефективність та якість освітлення: проблеми і шляхи вирішення / П. П. Говоров, В. П. Говоров, А. К. Кіндінова // VII Міжнародна науково-технічна конференція «Актуальні проблеми світлотехніки» : матеріали конференції. — Харків, 2019. — С. 16.

Анотація

У статті розглядається автоматизація керування режимами освітлювальних установок для підвищення їх енергоефективності та якості роботи. Запропоновано структурну схему автоматизованої системи керування освітленням, яка базується на використанні індивідуальних лічильників світлової енергії, датчиків освітленості та перетворювачів параметрів світлового потоку. Наведено формулу для розрахунку світлового потоку та описано взаємодію елементів системи. Результати досліджень свідчать про ефективність впровадження таких систем у міську інфраструктуру для зниження енергоспоживання, підвищення довговічності світильників та створення комфортних умов освітлення.

Ключові слова: автоматизація, освітлювальні установки, енергоефективність, інтелектуальне освітлення.

Abstract

The article explores the automation of lighting systems' operation modes to enhance their energy efficiency and performance quality. A structural scheme of an automated lighting control system is proposed, based on the use of individual luminous energy meters, illuminance sensors, and light flux parameter converters. A formula for calculating luminous flux is provided, along with a description of the system elements' interaction. The research results demonstrate the effectiveness of implementing such systems in urban infrastructure to reduce energy consumption, extend the service life of luminaires, and create comfortable lighting conditions.

Keywords: automation, lighting systems, energy efficiency, intelligent lighting.

ПЕРСПЕКТИВИ ВИКОРИСТАННЯ АВТОМАТИЗОВАНИХ СИСТЕМ РОЗРОБКИ І РОЗГОРТАННЯ В IoT-ІНФРАСТРУКТУРИ НА ОСНОВІ DevOps ПРАКТИКИ

Садовніченко М.В.,аспірант , maksym.sadovnichenko@donntu.edu.ua
Теличко Г.О., к.т.н, hanna.telychko@donntu.edu.ua
ДВНЗ «Донецький національний технічний університет»,
м. Дрогобич, Україна

Технологія інтернету речей (IoT) є сучасною концепцією, яка охоплює мережу взаємопов'язаних фізичних пристроїв, здатних взаємодіяти між собою та обмінюватися даними через мережу Інтернет без втручання людини. Наразі ця технологія активно впроваджується у різних галузях, таких як: розумні міста[1], Industry 4.0[2], лікуванні, землеробстві і розумних будинках тощо.

В перелічених прикладах, можна побачити що всі ці сфери в яких використовується IoT є великими і масштабними. Що собою представляє складну інфраструктуру, в якій поєднується апаратні пристрої, хмарні сервіси та мобільні технології. У таких умовах стає критично важливим забезпечення ефективного управління, масштабованості та швидкості розробки.

Методологія DevOps може вирішити проблему управління велико масштабованих систем і також автоматизувати розробку програмного забезпечення і його безперебійного постачання. Головні принципи методу є наступні: спільне середовище розробки; автоматизація процесу розробки, тестування та розгортання; постійна інтеграція та постійна доставка(CI/CD); моніторинг та зворотній зв'язок. Всі ці принципи дозволяють автоматизувати і покращити контроль над великими системами, як у випадку з IoT.

Використання DevOps практик у розумних містах дозволяє ефективно інтегрувати та управляти різноманітними IoT-системами, що забезпечують моніторинг і управління інфраструктурою, транспортом, енергетикою тощо. DevOps сприяє швидшій адаптації до змін у вимогах користувачів і технологічному середовищі, що є критично важливим для забезпечення стійкості та ефективності міських систем. [1]

В рамках Industry 4.0, DevOps практики також можуть запропонувати покращення багатьох виробничих процесів для покращення співпраці між розробниками програмного забезпечення та операторами виробництв. Це дозволяє забезпечити безперервний процес адаптації та вдосконалення, де системи моніторяться та аналізуються в реальному часі а нові вимоги швидко реалізуються через автоматизовані тести та оновлення.[2]

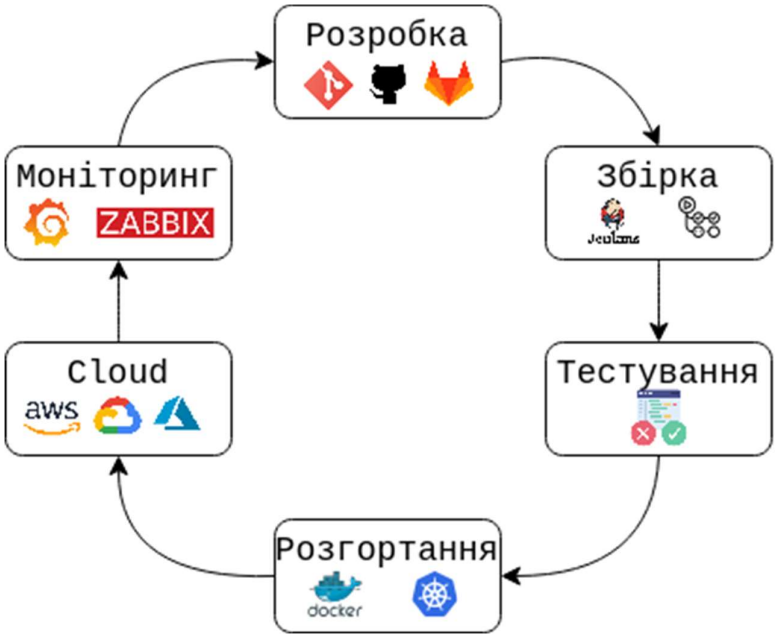


Рисунок 1. Приклад DevOps циклу

Наведений приклад відображає безперервний цикл DevOps, який охоплює всі ключові етапи: від розробки та автоматизації процесів до тестування, розгортання, інтеграції з хмарними сервісами та моніторингу. Кожен етап взаємопов'язаний, забезпечуючи швидке впровадження змін, стабільність системи та ефективне управління інфраструктурою IoT.

Застосування DevOps у IoT-інфраструктурі дозволить ефективно інтегрувати різнорідні компоненти системи, спрощуючи їх узгоджене функціонування. Завдяки контейнеризації та оркестрації можна забезпечити високу масштабованість системи, адаптуючи їх до зростаючих обсягів даних та кількості пристроїв. Крім того, автоматизовані процеси розробки та розгортання значно скорочують час впроваження нових функції, забезпечуючи гнучкість у відповідь на швидкі зміни потреб користувачів.

Впровадження DevOps практики до інтернету речей мають великий потенціал які можуть покращити, що може покращити ефективність управління розподіленими системами, забезпечити їхню масштабованість та прискорити адаптацію до змінних вимог. Подальші дослідження доцільно спрямувати на аналіз можливостей оптимізації життєвого циклу IoT-систем через інтеграцію DevOps методологій, зокрема в аспектах автоматизації розгортання, моніторингу та обслуговування. Крім того, важливим є розроблення універсальних підходів до адаптації DevOps для різних галузей, таких як розумні міста чи промислові IoT-екосистеми, з урахуванням специфічних вимог кожної сфери.

Література

1. Moore, J., Kortuem, G., Smith, A., Chowdhury, N., Cavero, J., & Gooch, D. (2016). DevOps for the urban IoT. Urb-IoT ’16: Proceedings of the Second International Conference on IoT in Urban Space. https://doi.org/10.1145/2962735.2962747

2. Hasselbring, W., Henning, S., Björn Latte, Armin Möbius, Richter, T., Schalk, S., & Wojcieszak, M. (2019). *Industrial DevOps*. https://doi.org/10.1109/icsa-c.2019.00029

3. Олійник, С. С., & Демківська, Т. І. (2023). Автоматизація процесів розробки та впровадження програмного забезпечення за допомогою DevOps методології. https://er.knutd.edu.ua/handle/123456789/25109

Анотація

У статті досліджується застосування DevOps для оптимізації інфраструктури інтернету речей (IoT). DevOps сприяє автоматизації розробки, тестування та розгортання, що забезпечує масштабованість і стабільність IoT-систем. Окреслено перспективи подальших досліджень для адаптації DevOps у різних галузях.

Ключові слова: IoT, DevOps, автоматизація, масштабованість.

Abstract

This article explores the use of DevOps to optimize the Internet of Things (IoT) infrastructure. DevOps automates development, testing, and deployment, which ensures the scalability and stability of IoT systems. Prospects for further research to adapt DevOps in various industries are outlined.

Keywords: IoT, DevOps, automation, scalability.

ПОРІВНЯННЯ МЕТОДІВ ДИСТАНЦІЙНОГО КЕРУВАННЯ КІБЕРФІЗИЧНИМИ СИСТЕМАМИ ЧЕРЕЗ ІНТЕРНЕТ

Заміховська О.Л., к.т.н., доцент
olena.zamikhovska@nung.edu.ua
Сабецький С.І., студент
Івано-Франківський національний технічний університет нафти і газу, м. Івано-Франківськ, Україна

Прогрес у сфері промислової автоматизації зумовлений потребами бізнесу в гнучкості та новими досягненнями в програмному й апаратному забезпеченні, а також інтеграцією інформаційно-комунікаційних технологій у традиційні системи автоматизації [1].

У межах концепції Industry 4.0 кіберфізичні виробничі системи пропонують інноваційні рішення для виробництва, інтегруючи інтелектуальні, вбудовані та мережеві системи у виробничі середовища [3]. Це дозволяє ефективно поєднувати віртуальний і фізичний світи через взаємодію та контроль фізичних пристроїв, що розширює можливості цифрових виробничих процесів [4].

Кіберфізичні системи (КФС) є інтеграцією обчислювальних, мережевих і фізичних процесів, що включають взаємопов'язані пристрої та програмне забезпечення для моніторингу і керування фізичними об'єктами [2].

Дистанційне керування КФС є важливим для централізованого контролю та управління, зменшуючи потребу в людському втручанні, що дозволяє швидко реагувати на зміни умов, підвищує гнучкість і масштабованість, що забезпечує ефективну і безпечну роботу систем.

Дистанційне керування КФС через Інтернет включає різні методи та технології для забезпечення ефективного, надійного та безпечного управління. Однак цей процес супроводжується кількома основними проблемами, серед яких:

- низька затримка та забезпечення відповіді в реальному часі;
- захист від кібернападів та забезпечення цілісності даних;
- масштабованість для ефективного управління систем;
- надійність, що забезпечує стабільну роботу та запобігає збоям.

Мета дослідження − порівняння різних методів дистанційного керування КФС через Інтернет, оцінка ефективності, безпеки та масштабованості хмарних обчислень, периферійних обчислень (edge computing) і розподілених систем керування.

Хмарне управління в КФС використовує ресурси хмарних обчислень для віддаленого моніторингу та управління компонентами. У виробництві хмарні системи замінюють традиційні програмовані логічні контролери (ПЛК) для некритичних застосувань, пропонуючи масштабовані рішення,

дозволяючи ефективно контролювати виробничі процеси, обробляти дані в хмарі та виконувати аналітику для оптимізації продуктивності.

Переваги хмарного управління:

- легка масштабованість для великих обсягів даних і пристроїв;
- доступ до даних і інтерфейсів з будь-якої точки з Інтернетом;
- інтеграція компонентів КФС і джерел даних в єдиний інтерфейс.

Метод периферійних обчислень (edge computing) полягає в обробці даних ближче до пристроїв, що їх генерують, це дозволяє приймати рішення в реальному часі, що критично важливо для чутливих до часу програм. Периферійні обчислення забезпечують безперервний моніторинг і аналітику на підприємствах, підвищуючи ефективність і зменшуючи затримки.

Переваги методу:

- зменшена затримка та швидший час відповіді;
- підвищена надійність завдяки локальній обробці;
- покращена безпека, конфіденційні дані обробляються локально.

Недоліки:

- обмежена потужність обробки порівняно з хмарними ресурсами;
- складність управління розподіленими пристроями;
- потенційні проблеми масштабованості.

Розподілені системи керування (DCS) децентралізують функції керування кількома взаємопов'язаними пристроями та вузлами. Контролери, що використовуються в DCS, забезпечують управління виробничими та технологічними процесами, об'єднуючи кілька контролерів для спільного виконання завдань. Для підвищення ефективності в DCS є функціональні групи (FG), що працюють разом для виконання контрольних завдань.

ПЛК є прикладом децентралізованих систем, обробляючи сигнали від датчиків і генеруючи керуючі сигнали для приводів на визначених інтервалах. Контролери, як ПЛК, використовують зворотний зв'язок для моніторингу та управління процесами.

Переваги:

- підвищена відмовостійкість і стійкість;
- масштабованість за рахунок додавання нових вузлів;
- підвищена гнучкість і адаптивність.

Недоліки:

- складність координації розподілених вузлів;
- комунікаційні витрати між вузлами;
- проблеми безпеки при забезпеченні безпечного зв'язку.

У дослідженні було проаналізовано методи дистанційного керування КФС, зокрема хмарні обчислення, периферійні обчислення та децентралізовані системи керування (DCS), з акцентом на їх застосування та переваги в промисловості. Кожен метод має унікальні переваги, вирішуючи конкретні завдання, що робить їх підходящими для різних додатків у КФС.

Хмарні обчислення відрізняються масштабованістю та централізованим керуванням, але можуть мати проблеми із затримками та безпекою. Периферійні обчислення забезпечують обробку в реальному часі та підвищену безпеку, але обмежені локальними ресурсами, тоді як DCS пропонує надійність і адаптивність, але потребує складної координації та безпечного зв'язку між вузлами.

При виборі методу керування для КФС слід враховувати специфічні потреби, обмеження, затримку, масштабованість і безпеку. Використовуючи переваги кожного методу, можна оптимізувати КФС для кращої продуктивності, надійності та безпеки, сприяючи інноваціям у різних секторах.

Література

1 Коломбо, А.В., та ін.: Промислові хмарні кіберфізичні системи. Підхід Імс-Езопа, 2014 − Springer

2 Кравець, А.Г., Борзін, Р.Ю., Рогожніков, Є.Д. (2024). Промислові кіберфізичні системи: проблеми управління та шляхи їх вирішення. Підхід до бібліометричного аналізу. В: Большаков А.А. (ред.) Кіберфізичні системи. Дослідження в галузі систем, прийняття рішень і управління, том 554. Шпрінгер, Чам. https://doi.org/10.1007/978-3-031-67685-7_1

3 E. Negri et al. A review of the roles of digital twin in CPS-based production systems, Procedia Manuf, (2017), https://doi.org/10.1016/j.promfg.2017.07.198

4 W. Kritzinger et al. Digital Twin in manufacturing: a categorical literature review and classification IFAC-PapersOnLine (2018), https://doi.org/10.1016/j.ifacol.2018.08.474

5 Stephen J. Bigelow. What is edge computing? Everything you need to know – [Електронний ресурс], URL: https://www.techtarget.com/searchdatacenter/definition/edge-computing. – (Дата звернення: 01.12.2024р.).

6. *Sri Harsha Mekala, … Sherali Zeadally,* Decentralized Control System *in* Computer Communications*, 2023* – – [Електронний ресурс], URL: https://www.sciencedirect.com/topics/engineering/decentralized-control-system– (Дата звернення: 01.12.2024р.).

Анотація

У тезі розглянуто порівняння методів дистанційного керування кіберфізичними системами (КФС) через Інтернет, зокрема хмарні обчислення, периферійні обчислення та розподілені системи керування. Описано їх переваги та виклики, зокрема проблеми безпеки, надійності та затримок передачі даних. Теза підкреслює необхідність подальших досліджень для покращення ефективності та безпеки дистанційного управління КФС.

Ключові слова: кіберфізичні системи, дистанційне керування, хмарні обчислення, периферійні обчислення.

Abstract

This thesis presents a comparison of remote control methods for cyber-physical systems (CPS) over the Internet, specifically cloud computing, edge computing, and decentralized control systems. It describes their advantages and challenges, including security issues, reliability, and data transmission delays. The thesis emphasizes the need for further research to improve the efficiency and security of remote control of CPS.

Keywords: cyber-physical systems, remote control, cloud computing, edge computing.

ДОСЛІДЖЕННЯ ТА РОЗРОБКА АВТОМАТИЗОВАНОЇ СИСТЕМИ ПРИЙОМУ ТА ОБРОБКИ ЗВЕРНЕНЬ ГРОМАДЯН ДО ПОКРОВСЬКОЇ МІСЬКОЇ ВІЙСЬКОВОЇ АДМІНІСТРАЦІЇ

Алдохіна Н. Ю., магістр, nataliia.aldokhina.kita@donntu.edu.ua
Теличко Г. О., к.т.н., доцент кафедри автоматики і телекомунікації ДВНЗ ДонНТУ, hanna.telychko@donntu.edu.ua
Ступак Г. В., старший викладач кафедри автоматики і телекомунікацій ДВНЗ ДонНТУ, glib.stupak@donntu.edu.ua
Донецький Національний Технічний Університет, м. Дрогобич, Україна

Права та свободи людини, а також їхні гарантії визначають основний напрямок діяльності держави, оскільки забезпечення і захист прав людини є головним обов'язком держави, що закріплено в статті 3 Конституції України [1]. Право громадян на звернення є одним із механізмів захисту своїх прав. Це право закріплене в статті 40 Конституції, яка встановлює, що кожен має право подавати індивідуальні чи колективні письмові звернення або звертатися особисто до органів державної влади, місцевого самоврядування та їх посадових осіб. Ці органи зобов'язані розглянути звернення та надати обґрунтовану відповідь у задані терміни [2].

Облік звернень громадян у Покровській адміністрації автоматизовано та відповідає сучасним вимогам. Система "Звернення громадян" забезпечує інформаційно-аналітичну роботу всіх підрозділів МВА, але має недоліки.

В роботі [3] було визначено мету дослідження – модернізувати систему обробки звернень, шляхом створення оптимальної структури, та прискорити обробку отриманих звернень [4].

Для покращення процесу обробки звернень громадян, запропоновано створити програму на мові Python із застосуванням бібліотеки aiogram [5]. Цей комплекс забезпечить автоматичний облік та реєстрацію кореспонденції, пов'язаної зі зверненнями громадян, та створить механізм автоматичної генерації реєстраційних номерів.

Для автоматизації прийому звернень громадян було розроблено Telegram-бот, що забезпечує інтерактивну взаємодію з користувачами для збору запитань та звернень. Основний функціонал включає: обробку вхідних даних, ведення журналу подій у файл logs.txt, автоматичне розпізнавання шаблонів запитів, а також надання відповідей на найпоширеніші питання за допомогою інтегрованої бази знань.

Після аналізу фідбеку від користувачів, отриманого через API адміністрації громади, було визначено 10 ключових категорій, для яких бот надає автоматизовану підтримку: комунальне господарство, соціальний захист, медицина, внутрішньо переміщені особи, доступність, освіта, благоустрій, комітет контролю соціального нагляду, старостати та інші напрями.

Для покращення продуктивності й масштабованості Telegram-бот використовує архітектуру на базі мікросервісів з інтеграцією RESTful API, що

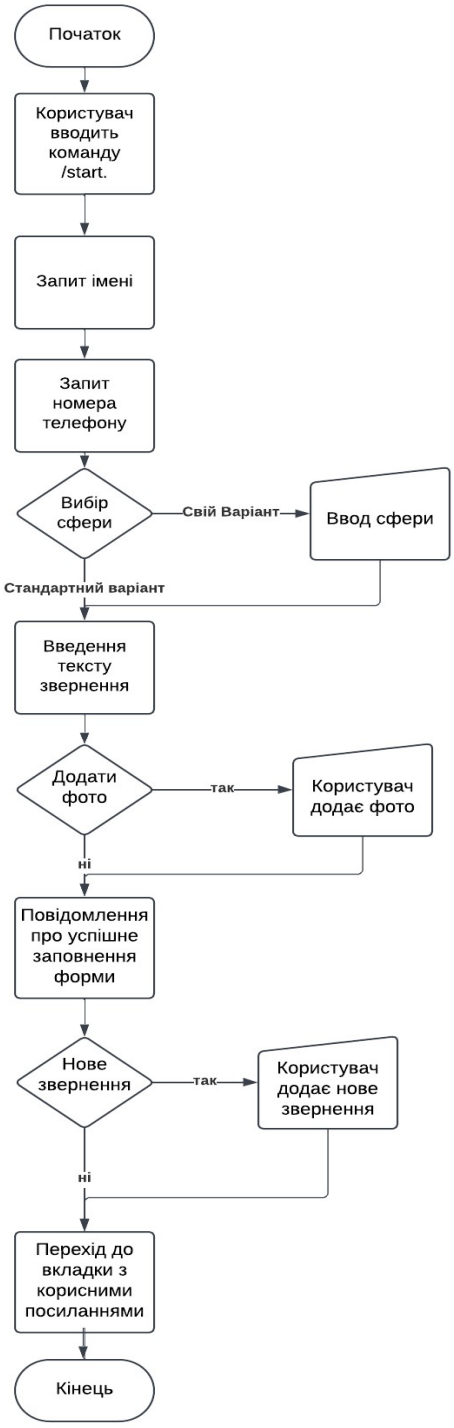


Рисунок 1 – Алгоритм роботи чат-бота

Алгоритм роботи бота представлен наступним чином (рис. 1.) забезпечує високу швидкість обробки запитів та їх класифікацію в реальному часі [5]. Код структурований і використовує стандартні підходи для створення телеграм-ботів з використанням бібліотеки aiogram.

Розробка виконана мовою Python завдяки її простоті та наявності потужних бібліотек, зокрема aiogram, яка забезпечує:

- асинхронність - обробка запитів за допомогою asyncio дозволяє одночасно обробляти до 800 запитів, оптимізуючи ресурси;
- гнучкість - підтримка команд, кнопок, медіафайлів та інтерактивних форм;
- FSM - впровадження багатокрокових сценаріїв для збору даних;
- логування - моніторинг подій через стандартний модуль logging;
- масштабованість - обробка великої кількості запитів без втрати продуктивності.

Інструменти які використовуються для чат-бота це asyncio — асинхронне програмування, та logging — ведення журналів для діагностики [6].

Aiogram забезпечує швидкість, інтеграцію та підтримку актуальних стандартів Telegram API, роблячи її ідеальним вибором для створення навчальних ботів.

Код складається з двох частин - це головна частина (bot.py), та частина з віртуальною клавіатурою (markup.py).

Впровадження чат-ботів стало важливим кроком у процесі цифрової трансформації адміністрації, забезпечивши оптимізацію робочих процесів та суттєво зменшивши навантаження на людські ресурси. Це дозволило перенаправити увагу на стратегічно важливі завдання, підвищивши ефективність і точність обробки запитів. Автоматизація через чат-боти сприяла значному скороченню часу відповіді та покращенню якості обслуговування, що позитивно позначилося на рівні задоволеності користувачів і клієнтів. Окрім того, вдалося значно знизити витрати на операційну діяльність, що підкреслює економічну доцільність впровадженого рішення. Інтеграція чат-ботів стала стимулом для цифрової трансформації, формуючи основу для подальшого розвитку.

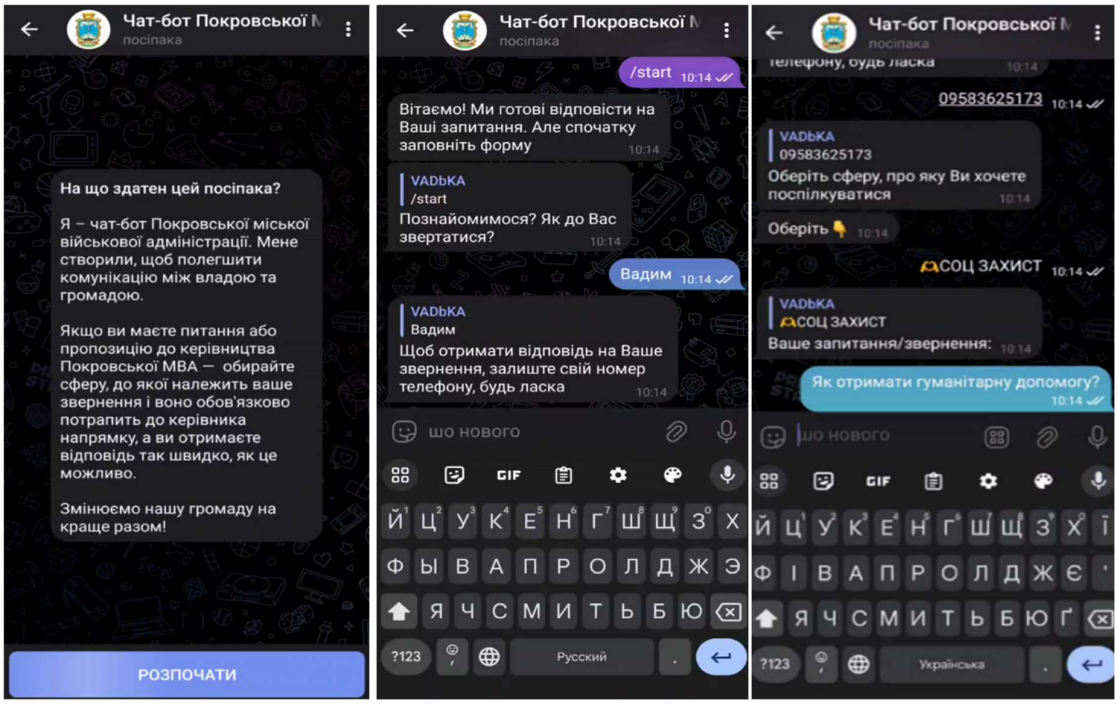


Рисунок 2 – Приклад роботи бота

На перспективу можливе розширення функціоналу чат-ботів, включаючи впровадження інтелектуальних алгоритмів, голосових команд і мультиканальної взаємодії. Персоналізація обслуговування за рахунок аналізу поведінки користувачів та інтеграція системи в складніші адміністративні процеси допоможуть залучити ширшу аудиторію. Використання зібраної аналітики дозволить постійно вдосконалювати роботу чат-ботів, підвищуючи їх адаптивність до змінних умов. Зрештою, розвиток чат-ботів може стати важливим інструментом для залучення громадян до цифрових сервісів, створюючи єдину екосистему взаємодії з владою.

Література

1. Конституція України : офіц. текст. Київ : КМ, 1996. 64 с.
2. Про затвердження Інструкції з діловодства за зверненнями громадян в органах державної влади і місцевого самоврядування, об'єднаннях громадян, на підприємствах, в установах, організаціях незалежно від форм власності, в засобах масової інформації : Постанова Кабінету Міністрів України від 14 квіт. 1997 р. № 348. Офіційний вісник України. 1997. № 16. С. 128–130.
3. Алдохіна Н. Ю., Ступак Г. В. Телеграм-бот «Звернення громадян» // «ТАК»: телекомунікації, автоматика, комп’ютерно-інтегровані технології : зб. доповідей Всеукр. наук.-практ. конф. молодих вчених, 5–6 грудня 2023 р. Луцьк : ДВНЗ «ДонНТУ», 2023. С. 44–46.
4. Соболь В. Розвиток системи опрацювання звернень громадян до органів виконавчої влади: історія, стан та перспективи // Економіка та держава. 2011. № 11. С. 32–35.
5. Мізюк О. Путівник мовою програмування Python. Київ : Видавництво ІТ, 2020. 256 с.
6. Дарк Ф. Л., Кузьменко С. Підручник мови Python / ред. С. Кузьменко. Харків : ІТ-книга, 2005. С. 106–110.

Анотація

Робота присвячена вдосконаленню процесу розгляду звернень громадян в органах державної влади. У роботі розглядаються відносини, які виникають у системі роботи місцевих органів влади зі зверненнями громадян. Для підвищення ефективності цього процесу запропонована розробка програмного комплексу на мові Python із використанням бібліотеки aiogram.

Розроблено Telegram-бот, який виконує функції прийому запитів від громадян, обробки їхніх відповідей і зберігання інформації. Це сприятиме автоматизації взаємодії з громадянами, зниженню навантаження на персонал і підвищенню якості обслуговування. В роботі описано порядок написання коду для чат-бота, представлені структурна та функціональна схема, головна та допоміжна частина коду. Чат-бот Покровської міської військової адміністрації протестовано та надано візуалізацію роботи бота.

Ключові слова: Звернення громадян, обробка звернень, телеграм-бот, Python.

Abstracts.

The article is devoted to improving the process of consideration of citizens' appeals in public authorities. The paper examines the relations that arise in the system of local authorities' work with citizens' appeals. To improve the efficiency of this process, the author proposes to develop a software package in Python using the aiogram library.

A Telegram bot was developed, was created that performs the functions of receiving requests from citizens, processing their responses and storing information. This will help automate interaction with citizens, reduce the workload on staff and improve the quality of service. The paper describes the procedure for writing code for a chatbot, presents a structural and functional diagram, the main and auxiliary parts of the code. The chatbot of the Pokrovska City Military Administration has been tested and a visualization of the bot's work is provided.

Keywords: Citizens' appeals, processing of appeals, telegram bot, Python.

АВТОМАТИЗОВАНА СИСТЕМИ МОНІТОРИНГУ ЯКОСТІ ПОВІТРЯ В МІСТІ ДОБРОПІЛЛЯ

Орос В. О., магістрант, volodymyr.oros.kita@donntu.edu.ua
Теличко Г. О., к.т.н, hanna.telychko@donntu.edu.ua
ДВНЗ Донецький національний університет, м. Дрогобич, Україна

Проблема якості повітря є надзвичайно актуальною для промислових регіонів, таких як Донбас. Добропілля, де вугільна промисловість є основним джерелом забруднення, стикається з суттєвими викликами в охороні довкілля. Забруднення повітря впливає на здоров'я населення, знижуючи тривалість життя та підвищуючи ризик захворювань. У цьому контексті важливою є розробка автоматизованої системи моніторингу, яка забезпечить збір, аналіз і візуалізацію екологічних даних у реальному часі.[1] та [2]

Системи моніторингу повітря розробляються як в Україні, так і за кордоном. Прикладом є програми ЄС (Copernicus), американська система EPA AQI, локальні ініціативи EcoCity. Однак більшість рішень не враховують специфіку локальних промислових районів та особливості інтеграції з локальною інфраструктурою.

Метою роботи є модернізація існуючої системи моніторингу повітря в Добропіллі через впровадження новітніх сенсорних технологій, автоматизацію процесів збору й аналізу даних та інтеграцію з веб-платформами. Основні задачі включають розробку архітектури системи, вибір оптимальних датчиків, створення макросу для аналізу та візуалізації даних.

Аналіз існуючої системи моніторингу якості повітря виявив її обмеження через використання малої кількості стаціонарних станцій, які не охоплювали всю територію міста, що негативно впливало на точність і детальність аналізу. Для вирішення цієї проблеми було розроблено автоматизований комплекс, що включає стаціонарні та мобільні станції з сенсорами для вимірювання PM2.5, PM10, CO2, NO2, SO2 та інших показників. Система інтегрована з веб-додатком для доступу до даних у реальному часі. Результати тестування показали підвищення точності вимірювань на 40% і збільшення швидкості обробки даних на 25%. Виявлено сезонні коливання якості повітря, зокрема високі рівні забруднення взимку. Для підвищення ефективності обробки даних впроваджено алгоритми фільтрації та прогнозування, а також інтегровано систему раннього попередження про критичні рівні забруднення. [3]

Модернізована система моніторингу якості повітря в Добропіллі забезпечує високоточний аналіз стану атмосфери за допомогою шести стаціонарних станцій Air Fresh MAX by EcoCity (модель EOS-M-3.1) та однієї мобільної станції Sapphire-32 by EcoCity, які вимірюють ключові показники забруднення, такі як PM2.5, PM10, CO2, NO2, SO2 тощо. [4]

Дані передаються в реальному часі на інтерактивну Google мапу, де відображаються у вигляді кольорових маркерів доступних громадськості. Крім того, чат-бот @ecocity_smog_alarm_bot забезпечує оперативне інформування населення про перевищення критичних рівнів забруднення.

Архів даних зберігається у сервісі «Кабінет дослідника якості повітря України», який дозволяє доступ до інформації за останні п’ять років для ретроспективного аналізу. Для наукового аналізу використовується спеціальний макрос в Excel, який автоматизує обробку даних, побудову графіків і формування звітів за обрані періоди. Система інтегрує стаціонарні й мобільні модулі, створюючи ефективну платформу для вивчення сезонних і локальних змін якості повітря, підвищення обізнаності населення та прийняття рішень на основі екологічних даних.

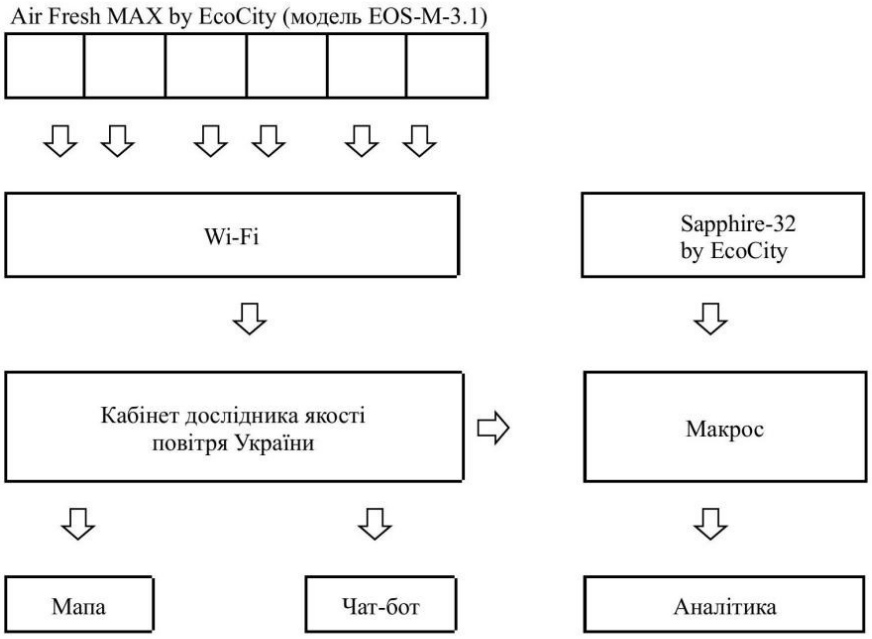


Рисунок 1. Схема автоматизованої системи моніторингу якості повітря у Добропіллі

Розроблена система моніторингу якості повітря в Добропіллі продемонструвала високу ефективність, забезпечуючи точний аналіз і виявлення сезонних коливань забруднення. Подальші дослідження спрямовані на масштабування системи до інших міст регіону, впровадження методів машинного навчання для прогнозування змін якості повітря та інтеграцію з міжнародними екологічними платформами.[5]

Очікується, що ці кроки сприятимуть покращенню екологічної ситуації та підвищенню обізнаності населення щодо стану довкілля.

Література

1. Всесвітня організація охорони здоров'я (ВООЗ). Глобальні керівні принципи якості повітря (2021). [Електронний ресурс]. – Режим доступу: https://www.who.int/publications/i/item/9789240034228.
2. Європейське агентство з охорони навколишнього середовища (ЕЕА). Щорічні звіти про якість повітря. [Електронний ресурс]. – Режим доступу: https://www.eea.europa.eu/en/newsroom/news/eea-trends-and-projections.
3. Грищенко І.М., Паламарчук В.І., Коваленко О.С. Розробка систем моніторингу якості повітря на основі IoT-технологій // Вісник Національного університету "Львівська політехніка". Серія: Комп'ютерні науки та інформаційні технології. – 2021. – №3(129). – С. 45–52.
4. EcoCity. Технічна документація станцій моніторингу повітря Air Fresh MAX та Sapphire-32. [Електронний ресурс]. – Режим доступу: https://ecocity.com.ua.
5. ДСТУ ISO 4226:2020. Якість повітря. Загальні аспекти оцінювання якості атмосферного повітря. – Київ: ДП "УкрНДНЦ", 2020.

Анотація

Робота присвячена розробці та вдосконаленню автоматизованої системи моніторингу якості повітря у промисловому місті Добропіллі. Досліджено недоліки існуючої системи, запропоновано нову архітектуру, яка поєднує стаціонарні та мобільні станції для збору даних. Реалізовано програмно-апаратний комплекс, що забезпечує збір, аналіз, зберігання та візуалізацію даних у реальному часі. У роботі використано алгоритми для фільтрації даних і прогнозування змін якості повітря. Результати роботи можуть бути використані для вдосконалення екологічного моніторингу в інших промислових містах.

Ключові слова: моніторинг якості повітря, автоматизація, сенсори, прогнозування, Добропілля.

Abstract

This thesis is dedicated to the development and enhancement of an automated air quality monitoring system in the industrial city of Dobropillia. The shortcomings of the existing system were analyzed, and a new architecture combining stationary and mobile stations for data collection was proposed. A hardware and software complex was implemented to collect, analyze, store, and visualize data in real time. The study utilized algorithms for data filtering and air quality prediction. The results can be applied to improve environmental monitoring in other industrial cities.

Keywords: air quality monitoring, automation, sensors, forecasting, Dobropillia.

ВИКОРИСТАННЯ АВТОМАТИЗОВАНИХ СИСТЕМ ДЛЯ ПРОГНОЗУВАННЯ ЕФЕКТИВНОСТІ ЛОГІСТИЧНИХ ОПЕРАЦІЙ

Гуржій В.О., студент, магістр, vladyslav.hurzhii.kita@donntu.edu.ua;
Жуковська Д.О., асистент кафедри автоматики та телекомунікацій, daria.zhukovska@donntu.edu.ua
Теличко Г.О., к.т.н., доцент кафедри автоматики та телекомунікацій, hanna.telychko@donntu.edu.ua
Державний вищий навчальний заклад «Донецький національний технічний університет», Дрогобич, Україна

Вступ. Сучасні виклики логістики, зокрема глобалізація ринків, зростання обсягів перевезень, потреба в оперативному прийнятті рішень та зменшенні витрат, обумовлюють необхідність автоматизації логістичних процесів. У цьому контексті роботизовані та автоматизовані системи набувають ключового значення, забезпечуючи підвищення точності, швидкості та ефективності виконання операцій.

Однією з важливих проблем є прогнозування ефективності логістичних операцій, особливо в умовах складних та динамічних систем, що включають різноманітні види транспорту, ланцюги постачання та логістичні вузли. Використання сучасних автоматизованих систем прогнозування дозволяє не лише оптимізувати логістичні процеси, але й покращити адаптивність системи до змінних умов, що є критично важливим у сучасних економічних умовах.

Мета роботи: дослідження можливості використання автоматизованих систем для прогнозування ефективності логістичних операцій з метою виявлення перспективних підходів та формування основ для подальших розробок.

Задачі:

- проаналізувати ключові проблеми, що виникають у складних логістичних системах, та обґрунтувати потребу в автоматизації;
- дослідити сучасні автоматизовані системи прогнозування, їх можливості та обмеження у застосуванні до логістики;
- запропонувати підхід до прогнозування ефективності логістичних операцій з використанням автоматизованих систем.

Сучасні автоматизовані системи у логістиці

Автоматизація в логістиці означає використання технологій і обладнання для оптимізації та оптимізації різних аспектів ланцюга постачання, що допомагає підвищити ефективність, зменшити витрати на робочу силу та підвищити точність логістичних операцій.

Вони також можуть допомогти мінімізувати помилки та затримки, що може мати позитивний вплив на задоволеність клієнтів і загальну ефективність.

Автоматизація в логістиці може включати різні рівні складності, від простих систем сканування штрих-кодів до більш просунутих технологій штучного інтелекту та машинного навчання.

Деякі приклади автоматизованих логістичних систем включають автоматизовані керовані транспортні засоби (AGV) для транспортування матеріалів, автономні дрони для доставки, програмне забезпечення прогнозної аналітики для прогнозування попиту та управління запасами, автоматизовані системи зберігання та пошуку (AS/RS), конвеєрні стрічки, роботизовані руки та інші види обладнання, яке може виконувати такі завдання, як сортування, комплектування, пакування та транспортування [1].

Аналіз підходів до автоматизації. На рис.1 приведено діаграму взаємодії компонентів автоматизації логістики.

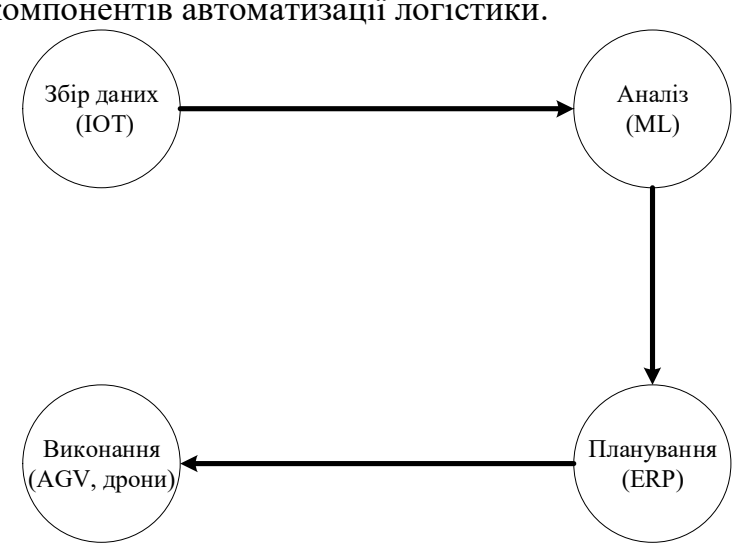


Рисунок 1. Діаграма взаємодії компонентів автоматизації логістики

Для аналізу різних підходів до автоматизації прогнозування ефективності логістичних операцій важливо порівняти існуючі типи автоматизованих систем. Нижче наведена таблиця, яка дозволяє оцінити переваги та недоліки кожного виду систем. Це дає змогу визначити, яка саме технологія є найбільш доцільною для вирішення конкретних завдань у сфері логістики.

Пропозиції для впровадження. На рис.2 представлено графік точності прогнозування різних систем залежно від складності системи.

З огляду на переваги та недоліки, можна зробити висновок, що для високоточного прогнозування в умовах мінливої системи рекомендовано використовувати системи на основі машинного навчання.

Логістика та транспортування є критично важливими компонентами ефективності ланцюга поставок, і автоматизація та штучний інтелект значною мірою сприяють оптимізації цих операцій. Автоматизовані системи, такі як автономні транспортні засоби та дрони, розгортаються для підвищення швидкості та надійності доставки [2]. Наприклад, доставка «останньої милі», традиційно один із найскладніших і найдорожчих аспектів логістики, трансформується за допомогою автономних систем доставки.

Таблиця 1 – Аналізу підходів до автоматизації прогнозування ефективності логістичних операцій

Тип системи	Переваги	Недоліки
ERP-системи (SAP, Oracle, Microsoft Dynamics)	- інтеграція всіх бізнес-процесів у єдину платформу; - автоматизація управління ресурсами та звітності; - можливість адаптації під специфіку компанії	- висока вартість впровадження та обслуговування; - потреба у тривалому навчанні персоналу; - обмежена гнучкість у специфічних задачах прогнозування
Системи на основі машинного навчання (ML)	- висока точність прогнозів у складних динамічних системах; - здатність адаптуватися до змінних даних; - можливість автоматичного вдосконалення моделі	- велика потреба в якісних даних для навчання; - складність розробки та впровадження - залежність від потужних обчислювальних ресурсів
Системи оптимізації на основі математичних моделей	- чіткі алгоритми прогнозування; - висока швидкість розрахунків у простих моделях; - мінімальні витрати на підтримку після впровадження	- низька ефективність у складних багатофакторних системах; - необхідність ручного налаштування для кожного випадку
Хмарні рішення для логістики (TMS, SCM у хмарі)	- доступність даних у будь-якому місці; - швидке оновлення та масштабування. - зниження витрат на інфраструктуру	- залежність від стабільного доступу до Інтернету; - можливі ризики безпеки даних; обмеження у кастомізації
IoT-системи для логістики (розумні датчики, GPS)	- реальний час збору даних; підвищення точності моніторингу транспорту та вантажів; - можливість інтеграції з іншими системами	- висока вартість обладнання та обслуговування; - обмеження в роботі без підключення до мережі; - залежність від якості датчиків та інфраструктури

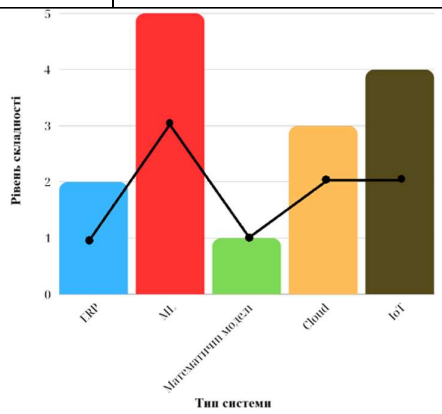


Рисунок 2. Графік точності прогнозування різних систем залежно від складності системи

Ці системи зменшують залежність від людської праці, мінімізують затримки, спричинені трафіком, і працюють цілодобово та без вихідних, забезпечуючи швидшу та ефективнішу доставку. Інструменти оптимізації маршрутів на основі ШІ також відіграють вирішальну роль у логістиці. Аналізуючи дані в режимі реального часу про умови руху, погоду та розклади доста-

вки, алгоритми штучного інтелекту можуть визначати найбільш ефективні маршрути транспортування, зменшуючи споживання палива, час доставки та загальні витрати на логістику. Крім того, штучний інтелект використовується для динамічного планування та оптимізації навантаження, гарантуючи повне використання транспортних засобів і постійну оптимізацію маршрутів доставки відповідно до поточних умов [3].

Висновки. Отже, автоматизація логістичних процесів із використанням сучасних систем набуває особливої актуальності в умовах небезпечних ситуацій і впливу різноманітних зовнішніх чинників. Такі системи забезпечують швидку адаптацію до змінних умов, мінімізують ризики людських помилок і сприяють зменшенню часу реакції на непередбачувані ситуації. Вони дозволяють не лише підтримувати стабільність ланцюгів постачання, але й оптимізувати процеси навіть у складних і динамічних середовищах. Інтеграція штучного інтелекту та автоматизованих рішень підвищує стійкість логістичних систем, забезпечуючи надійність, безперервність роботи та ефективність навіть у ситуаціях підвищеної складності.

Література

1. 5 logistics automation strategies you should be aware of [Електронний ресурс]. – Режим доступу: https://en.codept.de/blog/5-logistics-automation-strategies-you-should-be-aware-of – Назва з екрану.

2. Jagtap, S., Bader, F., Garcia-Garcia, G., Trollman, H., Fadiji, T., & Salonitis, K. (2020). Food logistics 4.0: Opportunities and challenges. Logistics, 5(1), 2.

3. Yu Tao. The Application of Intelligent Logistics Systems in Supply Chain Management and Its Challenges: Case Studies of Automated Warehousing and Unmanned Delivery // Frontiers in Business, Economics and Management. – 2024. – Т. 16, № 2. – С. 2766–824X.

Анотація

У роботі розглянуто актуальність автоматизації логістичних процесів в умовах сучасних викликів, зокрема небезпечних подій та впливу зовнішніх чинників. Проаналізовано переваги та обмеження сучасних автоматизованих систем, таких як платформи на основі машинного навчання, IoT-рішення, хмарні технології та системи оптимізації. Запропоновано підхід до використання автоматизованих систем для підвищення ефективності логістичних операцій, що дозволяє забезпечити адаптивність, зниження витрат і підвищення стійкості логістичних систем у мінливих умовах.

Ключові слова: автоматизація, машинне навчання, IoT, хмарні технології, прогнозування.

Abstract

The paper examines the relevance of logistics process automation under modern challenges, including hazardous events and external factors. The advantages and limitations of modern automated systems, such as machine learning-based platforms, IoT solutions, cloud technologies, and optimization systems, are analyzed. An approach to using automated systems to improve the efficiency of logistics operations is proposed, enabling adaptability, cost reduction, and increased resilience of logistics systems in dynamic conditions.

Keywords: automation, machine learning, IoT, cloud technologies, forecasting.

ВИКОРИСТАННЯ АВТОМАТИЗОВАНОЇ СИСТЕМИ ПРОГНОЗУВАННЯ РОЗВИТКУ СТАРТАПІВ В НАВЧАЛЬНОМУ ПРОЦЕСІ ТА В СТАРТАП-ЕКОСИСТЕМІ

Байтельман Я. Л., МА з англійської мови і літератури та німецької мови; здобувач магістерського освітнього рівня з спеціальності "Автоматизація, комп'ютерно-інтегровані технології та робототехніка", yakiv.baitelman.kita@donntu.edu.ua
Воропаєва В.Я., кандидат технічних наук, доцент, професор кафедри автоматики та телекомунікацій, ДонНТУ, viktoriya.voropayeva@donntu.edu.ua
Донецький національний технічний університет, Дрогобич, Україна

В роботі розглядається автоматизована система прогнозування розвитку стартапу [1]. Дана система базується на авторській системі управління контентом [2] та імплементує алгоритми нечіткої логіки та використовує звернення до великої мовної моделі GPT версії 4. Вона дозволяє будувати фінансові проекції стартапу [3] в залежності від заданих параметрів, а також пропонує перелік визначених ризиків та оцінює ймовірність отримання інвестиції.

Використання даної системи в рамках курсу з інноваційного підприємництва дозволить студентам експериментувати з ключовими аспектами фінансів стартапу, поглиблюючи їхнє розуміння фінансового планування та ухвалення рішень у бізнес-контексті. Зокрема, завдяки такому практичному досвіду вони можуть вивчати:

- Вплив ключових фінансових показників. Експериментуючи з вхідними параметрами, студенти бачитимуть, як кожен фактор впливає на прибутковість та грошові потоки. Вони досліджуватимуть, як різні змінні взаємопов'язані, і отримають розуміння того, як збалансувати витрати з доходами для забезпечення сталого бізнесу.
- Аналіз сценаріїв. Налаштовуючи вхідні параметри, такі як політика залучення клієнтів та тарифікація підписок, студенти зможуть спостерігати, як різні сценарії впливають на фінансові результати. Це допомагатиме їм зрозуміти найкращі та найгірші варіанти розвитку подій, готуючи їх до прогнозування та стратегічного планування в умовах різних бізнес-ситуацій.
- Управління грошовими потоками. Студенти вчитимуться важливості управління грошовими потоками, налаштовуючи прогнози витрат та доходів. Розуміння часових аспектів грошових потоків є критично важливим для життєздатності стартапу, і вони зможуть досліджувати такі концепції, як фінансова «протяжність» (runway) та "спалювання коштів" (burn rate) в реальному часі. Це дозволить студентам отримати

практичний досвід у прийнятті рішень щодо фінансових стратегій і готуватися до реальних викликів, з якими стикаються стартапи.

– Розрахунки беззбитковості та прибутковості. Студенти отримають практичний досвід у розрахунку точки беззбитковості та часових рамок досягнення прибутковості, що є важливим для розуміння того, скільки часу знадобиться стартапу, щоб стати самодостатнім. Це дозволить студентам оцінити, коли стартап може почати генерувати стабільний прибуток і покрити свої витрати, що є критично важливим для ефективного планування та прийняття фінансових рішень.
– Перевірка припущень. Експериментуючи з фінансовими моделями, студенти розумітимуть важливість початку з реалістичних припущень, їхнього тестування та уточнення моделі на основі зібраних даних, що імітує ітераційний процес, через який проходять реальні стартапи. Це допоможе їм зрозуміти, як важливо адаптувати свої припущення та стратегії на основі реальних результатів, а не просто покладатися на початкові спостереження або інтуїцію.

Система прогнозування розвитку стартапів може стати важливим додатком до інструментарію регіональної та національної екосистем стартапів, забезпечуючи виконання наступних ключових функцій:

1. Оцінка життєздатності стартапів. Система дозволяє аналізувати фінансові проекції, оцінювати ризики та прогнозувати ймовірність досягнення точки беззбитковості, що може бути у нагоді як для стартапів, які шукають інвесторів, так і для венчурних фондів, що приймають рішення про інвестування на основі кількісних даних. Для останніх дана система може служити уніфікованим інструментом для створення бізнес-планів та їхнього оцінювання, і таким чином виключити фактори помилки через оформлення та подачу інформації про стартап.
2. Прийняття рішень щодо залучення інвестицій. Інвестори можуть використовувати систему для оцінки ймовірності успіху різних сценаріїв розвитку стартапу. Наприклад, система може визначати вплив темпів росту персоналу або політики залучення користувачів на фінансові результати, що сприяє прийняттю зважених рішень про інвестування.
3. Оптимізація витрат та бізнес-моделювання. Завдяки моделюванню різних сценаріїв система допомагає стартапам зрозуміти, як оптимізувати витрати на залучення користувачів та розробку, зберігаючи баланс між витратами та доходами. Наприклад, моделювання показує, як зміна ціни підписки або вартості залучення користувача впливає на прибутковість.
4. Аналіз конкурентного середовища. Система може визначати конкурентів у певному регіоні або галузі, що дозволяє стартапам адаптувати свою стратегію залежно від ринкових умов.

5. Підтримка стратегічного планування. Засновники стартапів можуть використовувати систему для довгострокового планування, оцінюючи, як зовнішні фактори, такі як вартість хостингу, юридичні послуги або макроекономічні зміни, впливають на бізнес. Це допомагає підготовитись до майбутніх викликів та мінімізувати ризики.
6. Підвищення прозорості для інвесторів. Надання структурованих фінансових проекцій у простому форматі забезпечує прозорість і легкість у сприйнятті інформації. Це сприяє підвищенню довіри між стартапами та інвесторами, що може пришвидшити отримання фінансування.

Таким чином, запропонована автоматизована система прогнозування стає інструментом для підтримки на різних етапах розвитку стартапів – від ранньої стадії до масштабування, забезпечуючи ефективний аналіз і стратегічне планування, а також уніфікацію бізнес-планів, які подаються на розгляд організаторам конкурсів та інвестиційним фондам.

Запропонована система здатна адаптуватися до змін і пропонувати ефективні стратегії розвитку стартапів, зокрема у питаннях оптимізації витрат, зростання команди та залучення клієнтів. Це робить її корисним інструментом для інвесторів та підприємців, які прагнуть покращити планування своїх проектів, оптимізувати витрати, знизити ризики та підвищити шанси на отримання інвестицій та успішний розвиток бізнесу.

Дана система ефективно підтримує навчання підприємництву, надаючи студентам практичний досвід у фінансовому плануванні та бізнес-моделюванні.

Вона також здатна сприяти розвитку стартапів від початкової стадії до масштабування, пропонуючи засновникам інструмент для моделювання, а інвесторам – спосіб автоматизувати відбір та оцінювання стартапів через уніфікацію бізнес-планів і підтримку прийняття рішень. Використання системи прогнозування розвитку стартапів сприяє економічній самоосвіті підприємців.

Література

1. Yakiv Baytelman and Viktoriya Voropayeva “A Start-up for Business Development of Start-ups” ICL2024 – 27th International Conference on Interactive Collaborative Learning 24–27 September 2024, TalTech, Tallinn, Estonia, pp. 1988-1995.

2. Я.Л. Байтельман, В.В. Поцепаєв, “Розробка системи управління контентом та її розгортання на хмарному середовищі”, Наукові праці ДонНТУ, серія “Обчислювальна техніка та автоматизація”, №2(34). С. 14–31. 2024.

3. Yakiv Baytelman, “Business Models in Startup Growth Forecasting”, Research Works of The Donetsk National Technical University, series: "Computing technology and automation”, Vol. 1 No. 1(33). 2023.

Анотація

У роботі розглянуто автоматизовану систему прогнозування розвитку стартапів, яка є інноваційним інструментом, що поєднує нечітку логіку, GPT-4 та систему управління контентом. Функціонал дозволяє будувати детальні фінансові проекції, оцінювати ризики та аналізувати різні сценарії розвитку бізнесу. Система може знайти широке застосування в освітньому процесі, допомагаючи студентам розвивати навички фінансового планування та прийняття рішень в умовах невизначеності. Для стартапів система пропонує інструменти для оцінки життєздатності, залучення інвестицій та оптимізації витрат. Інвестори можуть використовувати систему для швидкої та об'єктивної оцінки потенціалу стартапів. Реалізація автоматизованої системи сприятиме розвитку стартапів та підвищенню ефективності інноваційної екосистеми.

Ключові слова: екосистема, освітній процес, автоматизація, прогнозування розвитку, прийняття рішень, нечітка логіка.

Abstract

The paper considers an automated system for forecasting startup development, which is an innovative tool that combines fuzzy logic, GPT-4 and a content management system. The functionality allows you to build detailed financial projections, assess risks and analyze various business development scenarios. The system can find wide application in the educational process, helping students develop financial planning and decision-making skills under uncertainty. For startups, the system offers tools for assessing viability, attracting investments and optimizing costs. Investors can use the system for a quick and objective assessment of the potential of startups. The implementation of an automated system will contribute to the development of startups and increase the efficiency of the innovation ecosystem.

Keywords: ecosystem, educational process, automation, development forecasting, decision-making, fuzzy logic.

РОЗРОБКА ТА ДОСЛІДЖЕННЯ СИСТЕМИ АВТОМАТИЧНОГО КЕРУВАННЯ ПРИВОДОМ ПІДТЯГУВАННЯ В ВИНЕСЕНІЙ СИСТЕМІ ПОДАЧІ ВИДОБУВНОГО КОМБАЙНА

Моногаров Д.А., аспірант, danulo.monoharov@donntu.edu.ua
Поцепаєв В.В., к.т.н, доцент, valerii.potsepaiev@donntu.edu.ua
Сисенко Є.К., магістрант, yevhenii.sysenko.kita@donntu.edu.ua
Донецький національний технічний університет, Дрогобич, Україна

Значна частка видобувних комбайнів для виїмки тонких пологих пластів оснащена винесеною системою подачі (ВСП), котра дозволяє суттєво скоротити довжину комбайна, що дуже важливо при проходженні порушень у профілі пласта. Функціональна схема системи автоматичного керування (САК) комбайном з ВСП представлена на рис.1.

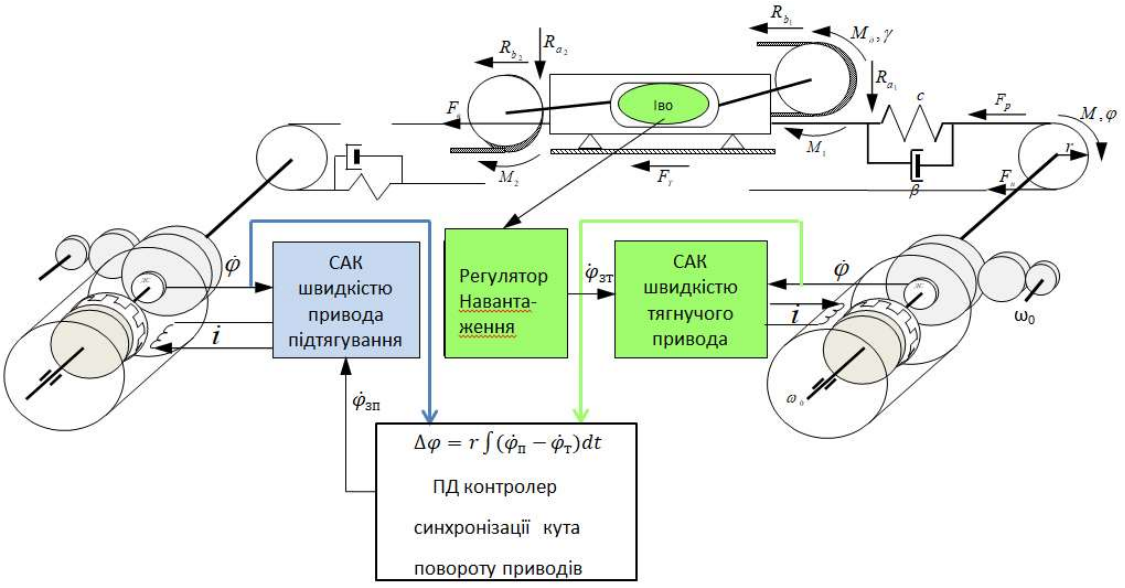


Рис.1. – Функціональна схема САК комбайном з ВСП

Ця система має два винесені на штреки приводи, в яких варіатором швидкості є електромагнітне гальмо ковзання (ЕГК) [3] з м'якими механічними характеристиками. В серійній САК ВСП тягнучий привод, розташований на рис.1 праворуч, керується двоконтурною САК, в якій підлеглим контуром є САК швидкістю, що створює жорсткі механічні характеристики привода. Зовнішнім контуром є регулятор навантаження привода виконавчих органів комбайна, котрий задає його швидкість подачі.

Ліворуч знаходиться привод підтягування, функція якого – підтягувати нижню холосту гілку ланцюгового контуру. Цей привод працює на м'якій механічній характеристиці ЕГК, яка задається вручну виставленням струму в обмотці збудження ЕГК. Ручне налаштування та мінливість сили спротиву

підтягуванню нижньої холостої гілки ланцюга спричиняють нераціональний режим роботи ВСП, при якому виникає необхідність налаштування привода підтягування 7…8 разів за зміну, прослизання ланцюга на зірці тягнучого привода, створення збурень моменту від привода підтягування та виникненню автоколивань кутової швидкості привода підтягування через його м'яку механічну характеристику.

Для усунення всіх вказаних недоліків в роботі розроблено двоконтурну САК приводом підтягування. Підлеглий контур цієї САК ідентичний САК швидкістю тягнучого привода, а зовнішній контур забезпечує синхронізацію кута повороту приводів регулюванням завдання кутової швидкості підлеглому контуру. Зовнішній контур синхронізації кутів повороту приводів є ПД регулятором, вхідним сигналом котрого є різність кутів повороту приводів, а вихідним – завдання за швидкістю підлеглому контуру регулювання швидкості привода підтягування.

Синтез САК синхронізації виконувався на імітаційній Simulink моделі, що наведена на рис. 2.

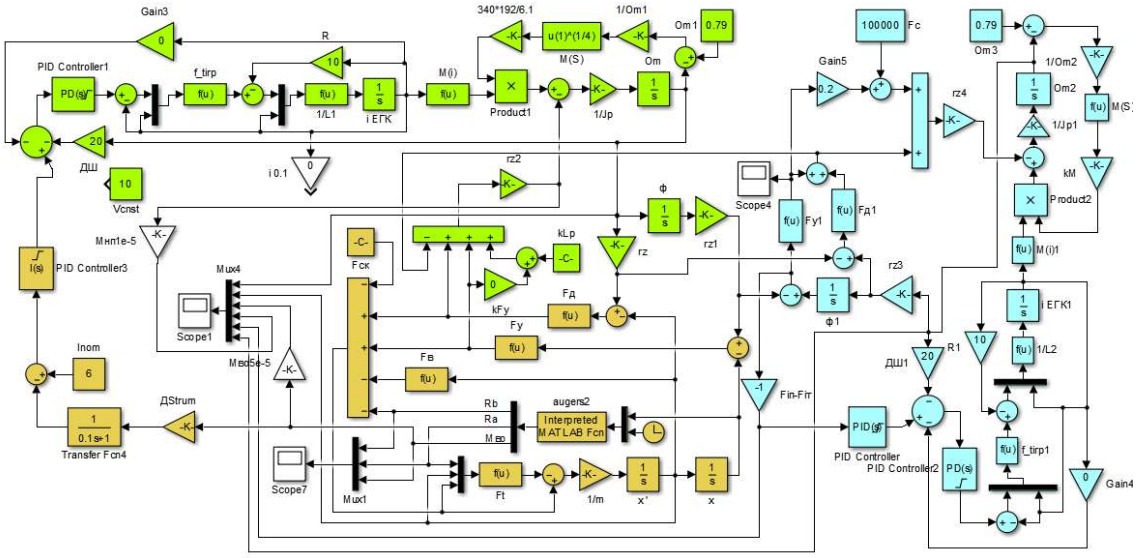


Рис.2. – Simulink модель САК комбайном з ВСП з двома керованими приводами

Наведена Simulink модель побудована на основі математичної моделі [1,2,4]. В блок-діаграмі зелений фон мають блоки, які відносяться до моделі САК швидкістю тягнучого привода. Блакитний фон – блоки, які відносяться до моделі САК швидкістю привода підтягування та контуру синхронізації. Жовтим кольором виділено імітаційну модель комбайна та зовнішній контур системи стабілізації навантаження на виконавчих органах.

На рис.3 наведено результати моделювання роботи комбайна в автоматичному режимі стабілізації при східчастій мінливості опірності вугілля різанню та довжині тягового ланцюга 100 м. На рисунку відображено: чорною лінією – момент навантаження на виконавчих органах у масштабі 1:5e-5, червоною – кутову швидкість тягнучого привода у масштабі 1:1, синьою – кутову швидкість привода підтягування

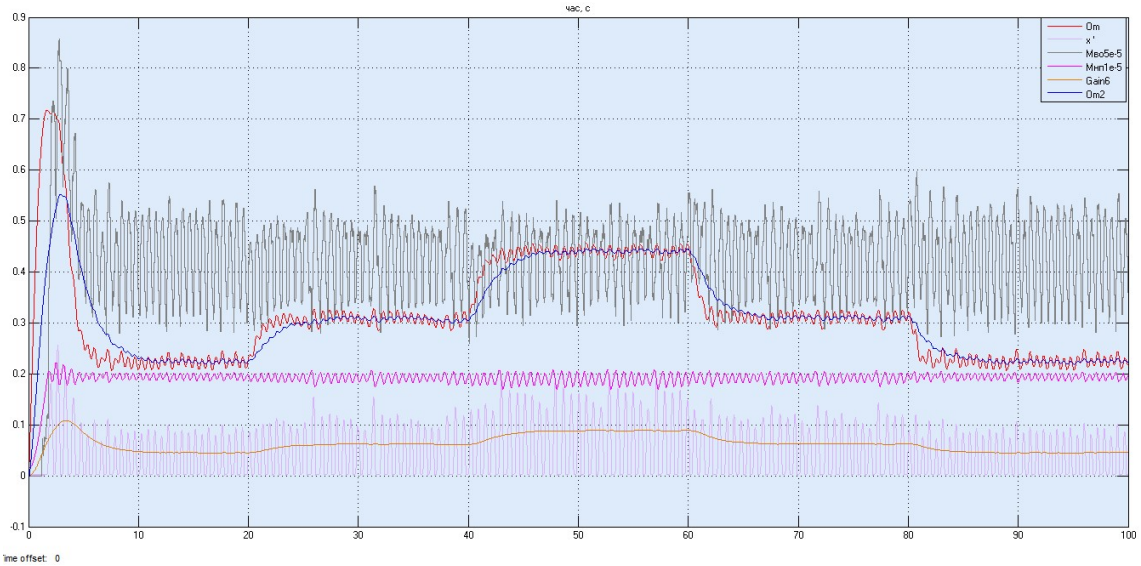


Рис.3 – Автоматичний режим роботи комбайна при мінливій опірності вугілля різанню

подачі у масштабі 1:1, фіолетовою – момент навантаження тягнучого привода, коричневою – різність кутів повороту тягнучого привода та привода підтягування у масштабі 1:1, рожевою – миттєву швидкість комбайна у масштабі 1:1.

Початкова опірність з нульової секунди 300 Н/м, на 20 с зниження до 250 Н/м, на 40 с зниження до 200 Н/м. з 60 с підвищення до 250 Н/м, з 60 с підвищення до 250 Н/м, з 80 с підвищення до 300 Н/м.

Наведені результати свідчать, що незважаючи на мінливість кутової швидкості тягнучого привода по відпрацюванню стрибків опірності, САК синхронізації стабілізує різність кутів повороту приводів з точністю не гірше 0,09 рад. Важливо зауважити, щ це значення є випередженням кута тягнучого привода як і має бути, оскільки привод підтягування не втручається в роботу тягнучого привода. САК синхронізації є стійкою та забезпечує монотонні аперіодичні перехідні процеси регульованої величини та кутової швидкості привода підтягування.

При дослідженнях САК комбайном з ВСП з двома автоматично керованими приводами визначені налаштування ПД регулятора контуру синхронізації: коефіцієнт передачі 100, коефіцієнт при похідній 0,4.

Розроблена САК комбайном з ВСП перевірена моделюванням для всіх реальних довжин тягового ланцюга та навантажень привода підтягування.

Література

1. Поцепаев В.В. Исследование динамики и выбор рациональных параметров вынесенного привода подачи очистных комбайнов: дисс. на соиск. уч. степ. канд. техн. наук. / Поцепаев В.В. – М.: ИГД им. А.А. Скочинского, 1985. – 197 с.

2. Кондрахин В.П., Мельник А.А., Косарев В.В., Стадник Н.И., Мезников А.В. Моделирование рабочих режимов вынесенной системы перемещения очистного комбайна, оснащенной частотно-регулируемым приводом// Наукові праці Донецького національного технічного університету. Серія: «Гірничо-електромеханічна». – 2008. – Вип. №16 (142), с.18 – 27.

3. Дубинин С.В., Бурлака О.М. Исследование переходных процессов автоматизированного электропривода на основе электромагнитного тормоза скольжения // Наукові праці Донецького національного технічного університету. Серія: "Обчислювальна техніка та автоматизація". – Донецьк, 2010 № 19(171) с.54-59.

4. Поцепаєв В.В Математична модель навантажень на виконавчих органах видобувного комбайна / В.В. Поцепаєв // Матеріали сьомої міжнародної науково-технічної конференції "Моделювання і комп'ютерна графіка" 18-24 вересня 2017 року, м. Покровськ, м. Київ . – м. Покровськ: ДонНТУ, 2017. – 285 с. С. 263-266.

Анотація

У статті розроблено та досліджено спосіб усунення нераціональних режимів роботи системи автоматичного керування видобувним комбайном з винесеною системою подачі. Для вирішення проблеми методом імітаційного моделювання синтезовано структуру та параметри двоконтурної системи автоматичної синхронізації кутів повороту тягнучого привода та привода підтягування. Підлеглим контуром в ній є система стабілізації швидкості привода підтягування. Зовнішній контур синхронізації кутів повороту приводів є ПД регулятором, вхідним сигналом котрого є різність кутів повороту приводів, а вихідним – завдання за швидкістю підлеглому контуру регулювання швидкості привода підтягування. Системи автоматичної синхронізації забезпечує різність в кутах повороту приводів не вище 0,09 рад.

Ключові слова: Система автоматичного керування, винесена система подачі, синтез, синхронізація приводів подачі, видобувний комбайн.

Abstract

The article develops and investigates a method for eliminating irrational operating modes of the automatic control system of a mining combine with a remote feed system. To solve the problem, the structure and parameters of a two-circuit system for automatic synchronization of the angles of rotation of the traction drive and the pull-up drive are synthesized using the simulation modeling method. The subordinate circuit in it is the system for stabilizing the speed of the pull-up drive. The external circuit for synchronizing the angles of rotation of the drives is a PD regulator, the input signal of which is the difference in the angles of rotation of the drives, and the output is the speed task for the subordinate circuit for regulating the speed of the pull-up drive. The automatic synchronization system ensures a difference in the angles of rotation of the drives of no more than 0.09 rad.

Keywords: Automatic control system, remote feed system, synthesis, synchronization of feed drives, mining combine.

ВИМОГИ ДО ШВИДКОДІЇ ТА СИНТЕЗ СИСТЕМИ АВТОМАТИЧНОГО КЕРУВАННЯ ВИДОБУВНИМ КОМБАЙНОМ З ВИНЕСЕНОЮ СИСТЕМОЮ ПОДАЧІ

Моногаров Д. А., аспірант, danulo.monoharov@donntu.edu.ua
Поцепаєв В. В., к.т.н, доцент, valerii.potsepaiev@donntu.edu.ua
Соловйов Д. О., магістрант, daniil.soloviov.kita@donntu.edu.ua
Донецький національний технічний університет, Дрогобич, Україна

Аналіз наукових робіт останніх років, присвячених модернізації системи автоматичного керування (САК) видобувним комбайном з винесеною системою подачі (ВСП), свідчить, що швидкодія її приводів суттєво збільшена за рахунок скорочення перехідних процесів струму в обмотці електромагнітного гальма ковзання (ЕГК) [1]. Це дає можливість збільшити швидкодію регулятора навантаження привода виконавчих органів комбайна, який забезпечує основний автоматичний режим його роботи. Це важливо, оскільки більш швидка реакція регулятора на різке збільшення навантаження краще захистить трансмісію привода виконавчих органів від перевантаження, а його електродвигун від перекидання. В зв'язку з викладеним метою роботи є синтез регулятора навантаження привода виконавчих органів комбайна в модернізованій САК комбайном ВСП.

Для виконання завдання використана еквівалентна схема, наведена на рис.1, та відповідна їй математична модель [2].

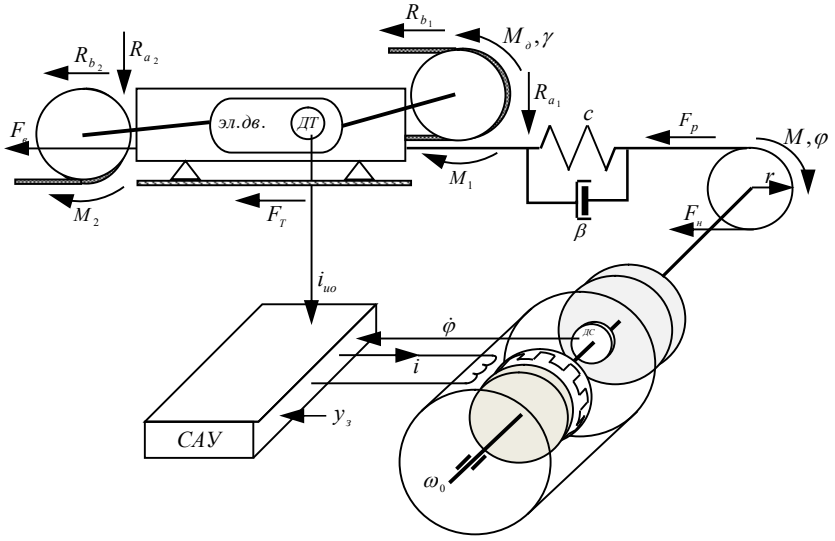


Рис.1. – Функціональна схема САК комбайном з ВСП

За математичною моделлю розроблено імітаційну модель в середовищі Simulink, котра наведена на рис.2.

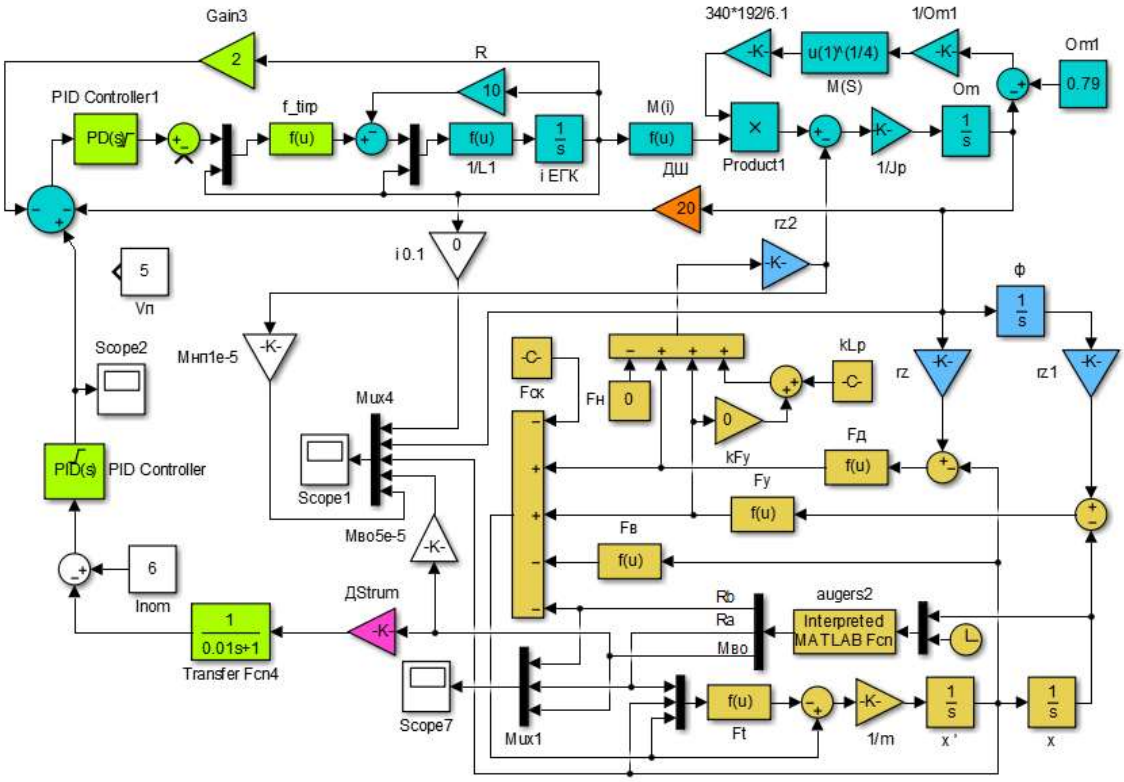


Рис.2. – Simulink модель САК комбайном з винесеною системою подачі

Блоки в моделі мають наступній колір. Синій – модель привода подачі з електромагнітним гальмом ковзання без регулятора швидкості. Жовтий – блоки моделі комбайна. Фіолетовий – датчик струму електродвигуна виконавчих органів. Блакитний – блоки зв'язку між приводом подачі та комбайном: rz, rz1, rz2 – радіуси ділильного кола приводної зірки, вихідний сигнал інтегратора ф - кут повороту приводної зірки. Коричневий – датчик швидкості привода подачі. Зелений – блоки структурного та параметричного синтезу регулятора швидкості привода та навантаження.

Модель комбайна відтворює рух та динаміку комбайна у робочому режимі. Тут обчислюються сили, що діють на комбайн: Fy – пружне зусилля в тяговому ланцюзі, Fд – дисипативна сила в тяговому ланцюзі, Fв – сила спротиву переміщенню верхньої холостої гілки тягового ланцюга, Ft – сила тертя в опорах комбайна, Fск– сила, що скочує. Сили реакції вибію на виконавчих органах – горизонтальні Rb, вертикальні Ra та момент навантаження на виконавчих органах обчислюються функцією MATLAB augers2 за переміщенням комбайна. В ній же задається східчаста мінливість опірності вугілля різанню для оцінки якості стабілізації навантаження.

Як видно з рисунка, САК навантаженням є двоконтурним регулятором. Внутрішній підлеглий контур з ПД регулятором (PID Controller1) забезпечує жорстку форму механічних характеристик привода. Зовнішній контур стабілізації навантаження на виконавчих органах задає завдання за

швидкістю подачі підлеглому контуру в залежності від навантаження на виконавчих органах комбайна.

На рис.3 наведено результати моделювання роботи комбайна в автоматичному режимі при східчастій мінливості опірності вугілля різанню та довжині тягового ланцюга 100 м. На рисунку відображено: червоною лінією – момент навантаження на виконавчих органах у масштабі 1:5e-5, синьою – кутову швидкість привода подачі у масштабі 1:1, сірою – миттєву швидкість комбайна у масштабі 1:1.

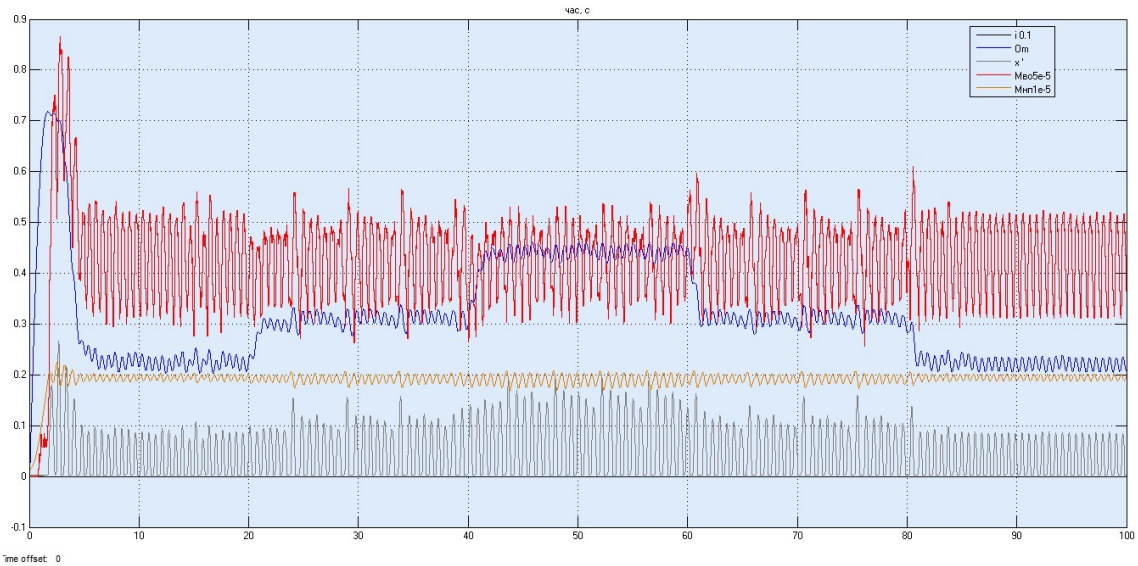


Рис.3 – Автоматичний режим роботи комбайна при мінливій опірності вугілля різанню

Початкова опірність з нульової секунди 350 Н/м, на 20 с зниження до 250 Н/м, на 40 с зниження до 200 Н/м. з 60 с підвищення до 250 Н/м, з 60 с підвищення до 250 Н/м, з 80 с підвищення до 350 Н/м.

Наведені результати свідчать, що САК якісно та стійко стабілізує середній момент навантаження на виконавчих органах з аперіодичними перехідними процесами та усталені режими без коливань при довжині тягового ланцюга до 300 м . Не слід приймати наявність биття у системі, що виникають від синхронізації коливаннями моменту на шнеках пульсацій миттєвої швидкості корпусу комбайна, з нестійкою роботою САК [3,4]. Важливо зазначити, що час зниження швидкості привода подачі вдвоє при східчастому збільшенні опірності складає приблизно 0,5…0,7 с, що менше ніж час перекидання електродвигуна привода виконавчих органів.

В результаті виконаного синтезу визначено: параметри налаштування ПД регулятора в контурі регулювання швидкості привода та коефіцієнт передачі І регулятора в контурі стабілізації навантаження привода виконавчих органів.

Література

1. Моногаров Д.А., Поцепаєв В.В. Вдосконалення динамічних характеристик винесеного привода подачі з електромагнітним гальмом ковзання видобувного комбайна // Науковий вісник ДонНТУ. – 2024. – Вип. №1 (12), с.121 – 128.

2. Поцепаєв В.В Математична модель навантажень на виконавчих органах видобувного комбайна / В.В. Поцепаєв // Матеріали сьомої міжнародної науково-технічної конференції "Моделювання і комп'ютерна графіка" 18-24 вересня 2017 року, м. Покровськ, м. Київ . – м. Покровськ: ДонНТУ, 2017. – 285 с. С. 263-266.

3. Поцепаєв В.В. Дослідження регулятора навантаження виконавчих органів видобувних комбайнів з винесеною системою подачі/ В.В. Поцепаєв // Науковий вісник ДонНТУ. – Покровськ, 2019 № 1-2 2019 с.48-53.

4. Бойко Н.Г. Перемещение очистных комбайнов с гибким тяговым органом/ Бойко Н.Г.// Наукові праці ДонНТУ. Серія: Гірничо-електромеханічна. - 2012. - № 23 (196). - С.11-18.

Анотація

У статті представлено результати синтезу, дослідження та визначення параметрів системи автоматичного керування навантаженням на виконавчих органах видобувного комбайна з винесеною системою подачі. Синтез та дослідження виконані математичним моделюванням на розробленій Simulink моделі системи. Продемонстровано ефективну та стійку з аперіодичними перехідними процесами роботу системи стабілізації навантажень на виконавчих органах при східчастій мінливості опірності вугілля різанню від середнього значення до максимального паспортного. Час зниження швидкості привода подачі вдвоє при східчастому збільшенні опірності складає приблизно 0,5…0,7 с, що менше ніж час перекидання електродвигуна привода виконавчих органів.

Ключові слова: Система автоматичного керування, винесена система подачі, синтез, навантаження, видобувний комбайн.

Abstract

The article presents the results of the synthesis, research and determination of the parameters of the automatic load control system on the executive bodies of a mining combine with a remote feed system. The synthesis and research were performed by mathematical modeling on the developed Simulink model of the system. The effective and stable operation of the load stabilization system on the executive bodies with a stepwise variability of the coal resistance to cutting from the average value to the maximum passport value is demonstrated. The time for reducing the speed of the feed drive by half with a stepwise increase in resistance is approximately 0.5…0.7 s, which is less than the time for the electric motor of the executive body drive to overturn.

Keywords: Automatic control system, remote feed system, synthesis, load, mining combine.

СЕКЦІЯ 4

«Енергетика, електротехніка, електромеханіка та ВДЕ»

ПЕРСПЕКТИВИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В УСТАНОВКАХ ЗБЕРІГАННЯ ЕНЕРГІЇ

Лугін Д.М., студент, luhin.denys@lll.kpi.ua;
Шевчук О.А., д.е.н, професор, shevchuk-oa@ukr.net
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського» , Київ, Україна

Актуальність питання

Роль установок зберігання енергії (УЗЕ) у підвищенні стабільності розподільчих мереж зростає з кожним днем. Така тенденція пов’язана зі збільшенням частки відновлюваних джерел енергії (ВДЕ) у загальному обсязі генерованої потужності, що вимагає підвищеної гнучкості системи [1]. Інтеграція УЗЕ в системи з ВДЕ принесло появу нових викликів споживанню відновлюваної енергії та регулюванню частоти на піку попиту, а робота електромережі ускладнилася. Для можливості використання такої інтеграції необхідна технологія управління, яка враховує як достатність генерації потужності, так і гнучкість виробництва електроенергії. Цю проблему можуть допомогти розв’язати передові алгоритми технології штучного інтелекту (ШІ), що привертають велику увагу в галузі зберігання енергії.

Відомі дослідження та публікації

Проблема ефективного використання УЗЕ з ВДЕ привернула увагу багатьох вчених та дослідників по всьому світу. Серед запропонованих ними рішень вирішення цього питання є застосування ШІ та алгоритмів машинного навчання, які були висвітлені в цій роботі.

Постановка задачі

У секторі зеленої енергетики основними завданнями традиційно вважалися експлуатація та обслуговування: технічне обслуговування, моніторинг вихідної потужності панелей та стану інверторів тощо. З появою УЗЕ з'явилися численні варіанти використання ВДЕ, включаючи можливість оптимізації зберігання енергії для зниження витрат, підвищення стійкості та сталості системи, а також збір даних для проведення прогнозного аналізу. Оскільки людині-оператору стало неможливо обробляти величезні обсяги даних, що постійно надходять, ШІ має на меті зменшити це навантаження і за допомогою методів швидко вирішувати поставлені задачі.

Результати досліджень

Технологія інтелектуального зберігання енергії вимагає високої продуктивності, довговічності, надійності та раціонального управління енергоспоживанням. ШІ може значно прискорити розрахунки, підвищити точність прогнозування, оптимізувати інформацію та підвищити продуктивність си-

стеми. У багатьох дослідженнях розглядаються різні методи ШІ, такі як нечітка логіка (НЛ) на основі роботи людського мозку, штучна нейронна мережа (ШНМ), метод рою частинок (МРЧ), алгоритм оптимізації на основі навчання, бджолиний алгоритм або генетичний алгоритм (ГА), а також алгоритм імітації відпалу (simulated annealing*)* [2]. Результати застосування цих алгоритмів наведені в табл.1.

Таблиця 1 - Системи зберігання енергії на основі методів штучного інтелекту[3]

Алгоритми ШІ	Тип УЗЕ	Фактори	Результати дослідження
МРЧ	Водневі системи та літій-іонні акумуляторні батареї	Витрати, термін служби та ефективність	Мінімізація операційних витрат (29,36%) Максимізація ефективності системи (27,21%) Продовження життєвого циклу пристроїв (43,43%)
	Електрохімічна система зберігання енергії	Вихідна потужність	Зменшення коливання напруги після підключення електрохімічного накопичувача енергії
Багатоцільовий МРЧ	Теплова енергія та акумуляторна система	Результат, що залежить від потужності	Підвищення продуктивності та стабільності системи передачі
Гібридний МРЧ та оптимізація на основі навчання	Літій-іонні акумуляторні батареї	Обсяг, час і витрати	Алгоритм успішно вирішує запропоновані проблеми постачання енергії.
Бджолиний алгоритм + МРЧ	Гібридні енергетичні системи	Втрати потужності, індекс стабільності напруги та енергоспоживання	Достатня послідовність та більша різноманітність порівняно з гібридним МРЧ
Алгоритм агломеративної ієрархічної кластеризації	Літій-іонні акумуляторні батареї	Час	Дані часових рядів (5–135 днів) достатні для покращення продуктивності системи на 5%.
Генетичний алгоритм сортування без домінування	Гідроакумулююча станція, літій-іонні акумуляторні батареї	Витрати та енергоспоживання	Система економічна та екологічна. Покращення продуктивності.
Оптимізація гармонійного пошуку	Літій-іонні акумуляторні батареї	Ціноутворення в залежності від часу використання	Оптимальне планування роботи системи зберігання енергії за тарифами, що не залежать від часу використання.
Гібридний ГА та ШНМ	Літій-іонні акумуляторні батареї	Вартість, вихідна потужність	Мінімізація середніх капітальних витрат Підвищена стабільність системи

УЗЕ мають двостороннє регулювання потужності, наприклад, споживання та відпуск енергії. Методи керування на основі штучного інтелекту можуть використовуватися для підвищення потужності, продуктивності, стабільності та надійності системи. Наприклад, схема керування УЗЕ на основі нечіткої нейронної мережі дозволяє ефективно керувати 100-мегаватною системою зберігання енергії [4], а якщо взяти систему керування на основі ШНМ та динамічного програмування, то можна очікувати мінімізацію втрат потужності, коливань струму акумулятора та збільшення терміну служби батареї [5].

Машинне навчання (МН) також стало популярним і широко використовується в галузі зберігання енергії. Багато дослідників повідомляють про різні застосування МН з УЗЕ. Інтеграція людської неелегантності в машинне навчання може значно підвищити надійність і продуктивність систем. Загалом, системи зберігання енергії на основі МН застосовуються в системах V2G (Vehicle to grid), а саме підвищують продуктивність і надійність, покращують життєвий цикл, а також забезпечують швидкі та надійні обчислення.

Висновки та напрямок подальших досліджень

Оскільки попит на надійні, високопродуктивні технології зберігання є вимогою часу, багато дослідників використовують методи штучного інтелекту, такі як нечітка логіка, штучні нейронні мережі, щоб забезпечити краще рішення і в найкоротші терміни. Також разом зі штучним інтелектом машинне навчання поступово стає популярним в індустрії зберігання енергії. Надійність і стійкість машинного навчання може підняти технологію зберігання енергії на ще вищу сходинку.

Література

1. Terlouw, T.; AlSkaif, T.; Bauer, C.; van Sark, W. Multi-objective optimization of energy arbitrage in community energy storage systems using different battery technologies. Appl. Energy, 2019. – P. 356–372.

2. Ahmed N. Abdalla, Muhammad Shahzad Nazir, Hai Tao, Suqun Cao, Rendong Ji, Mingxin Jiang, et al., Integration of energy storage system and renewable energy sources based on artificial intelligence: an overview, J. Energy Storage 40 (2021) 1-13. Vol.

3. Kumar, N. (Ed.). Emerging Trends in Energy Storage Systems and Industrial Applications, 2022. – 649 p.

4. WU, Yingjun, et al. Study on energy storage system participating in frequency regulation of wind farm based on polyline fuzzy neural network. In: *2018 5th IEEE International Conference on Cloud Computing and Intelligence Systems (CCIS)*. IEEE, 2018. – P. 1086-1090.

5. J. Shen, A. Khaligh, A supervisory energy management control strategy in a battcry/ultraca- pacitor hybrid energy storage system, IEEE Trans. Transp. Electr. 1 (3), 2015. – P. 223—231.

Анотація

У роботі представлено рішення проблеми ефективного використання установок зберігання енергії разом з відновлюваними джерелами енергії. Розглянуто результати дослідження застосування методів та алгоритмів штучного інтелекту, методи керування установками зберігання енергії та область застосування машинного навчання.

Ключові слова: установка зберігання енергії, відновлювані джерела енергії, штучний інтелект, метод, машинне навчання.

Abstract

The paper presents a solution to the problem of efficient use of energy storage facilities together with renewable energy sources. The results of the study of the application of artificial intelligence methods and algorithms, methods of energy storage facility management and the scope of machine learning are considered.

Keywords: energy storage facility, renewable energy sources, artificial intelligence, method, machine learning.

ПІДВИЩЕННЯ ЕНЕРГЕТИЧНОЇ ЕФЕКТИВНОСТІ СИСТЕМ ОСВІТЛЕННЯ

Говоров П.П., д.т.н., професор, pilip.govorov@kname.edu.ua;
Кіндінова А.К., аспірантка, anastasiya.kindinova@kname.edu.ua;
Волошин Д.М., danylo.voloshyn@kname.edu.ua;
Карасьов С.Ю., студент, serhii.karasov@kname.edu.ua;
Рибалка В.О., студент, vladyslav.rybalka@kname.edu.ua
Харківський Національний університет міського господарства імені О.М. Бекетова, Харків, Україна

Актуальність питання підвищення енергетичної ефективності систем освітлення обумовлена зростаючими вимогами до зменшення енергоспоживання та впливу на довкілля. В умовах високих витрат на енергоносії і необхідності скорочення викидів парникових газів, пошук нових рішень для оптимізації освітлення стає надзвичайно важливим.

Відомі дослідження показують, що проблеми енергоефективності в освітленні активно досліджуються вітчизняними та міжнародними науковцями. Зокрема, значну увагу приділено використанню світлодіодних (LED) технологій, що дозволяють знижувати споживання енергії, а також розробці інтелектуальних систем керування освітленням, які враховують різноманітні параметри, такі як освітленість, рух, час доби тощо.

Постановка задачі полягає у визначенні ефективних методів підвищення енергетичної ефективності освітлювальних систем. Це включає як технічні, так і організаційні рішення, що дозволяють мінімізувати витрати на енергію при збереженні належної якості освітлення.

Основний матеріал досліджень показує, що оптимізація технологічних рішень у сфері освітлення може значно покращити енергетичну ефективність. Використання LED-джерел світла дозволяє знизити енергоспоживання завдяки високому коефіцієнту корисної дії та тривалому терміну служби. Крім того, сучасні оптичні системи, які забезпечують рівномірний розподіл світлового потоку, значно знижують енерговитрати. Інтелектуальні системи керування, що застосовують датчики руху, освітленості та часу доби, дозволяють автоматизувати процеси вмикання та вимикання освітлення в залежності від реальних умов. Завдяки використанню IoT-рішень можливо здійснювати моніторинг і коригування енергоспоживання в реальному часі, що дозволяє досягти ще більших заощаджень [1, 2].

Економічний аналіз, проведений у рамках дослідження, підтверджує значні фінансові переваги від впровадження новітніх технологій у системи освітлення. Модернізація освітлювальних мереж дозволяє значно знизити витрати на електроенергію, а також скоротити витрати на обслуговування завдяки меншій частоті заміни ламп і компонентів [3].

Висновки з дослідження свідчать, що для підвищення енергетичної ефективності систем освітлення необхідно інтегрувати новітні технології, такі як LED-освітлення та інтелектуальні системи керування. Напрями подальших досліджень включають розробку математичних моделей для прогнозування енергозбереження в різних умовах, а також вдосконалення алгоритмів управління освітленням з можливістю самонавчання для досягнення максимальної ефективності.

Література

1. Hovorov P., Kindinova A., Hovorov V. Mode control of urban electrical networks based on the smart grid concept / P. Hovorov, A. Kindinova, V. Hovorov // 2021 IEEE 2nd KhPI Week on Advanced Technology, KhPI Week 2021 - Conference Proceedings. — 2021. — С. 88–93.

2. Hovorov P., Kindinova A., Hovorov V., Abdelrhim O. Control of modes of power supply and lighting systems of cities based on the concept of Smart-Grid / P. Hovorov, A. Kindinova, V. Hovorov, O. Abdelrhim // 2022 IEEE 8th International conference on energy smart systems, Kyiv, Ukraine, October 12-14, 2022. — С. 1–7.

3. Трунова І. М. Вдосконалення методики енергетичного аудиту системи освітлення / І. М. Трунова, Л. Ю. Волотка, Т. Л. Насєдкіна // Вісник ХДТУСГ. Проблеми енергозабезпечення та енергозбереження в АПК України. — 2012. — Вип. 130. — С. 33–35.

Анотація

У тезах розглядаються актуальні питання підвищення енергетичної ефективності систем освітлення, зокрема в контексті використання сучасних технологій, таких як світлодіоди (LED) і інтелектуальні системи керування. Аналізуються переваги застосування цих технологій у порівнянні з традиційними джерелами світла, а також наводяться результати досліджень, що підтверджують ефективність впровадження інноваційних рішень. Зокрема, звертається увага на оптимізацію енергоспоживання за допомогою інтеграції автоматизованих систем керування освітленням, що враховують різні фактори впливу, такі як освітленість, рух та час доби. У статті також наводяться приклади економічних переваг від модернізації освітлювальних мереж, що дозволяє знижувати витрати на енергію та обслуговування.

Ключові слова: енергетична ефективність, системи освітлення, інтелектуальні системи керування, автоматизація, енергозбереження.

Abstract

The abstract discusses the current issues of improving the energy efficiency of lighting systems, particularly in the context of using modern technologies such as light-emitting diodes (LED) and intelligent control systems. The advantages of applying these technologies compared to traditional light sources are analyzed, and research results confirming the effectiveness of implementing innovative solutions are presented. Specifically, attention is paid to optimizing energy consumption by integrating automated lighting control systems that take into account various influencing factors such as illuminance, movement, and time of day. The article also provides examples of the economic benefits of modernizing lighting networks, which reduce energy and maintenance costs.

Keywords: TAC, basic requirements, design rules. energy efficiency, lighting systems, intelligent control systems, automation, energy savings.

СТРУКТУРА РОЗПОДІЛУ ГЕНЕРАЦІЇ В ОЕС УКРАЇНИ

Ступак М.В., інж. каф. автоматики та телекомунікацій,
maryna.stupak@donntu.edu.ua
Донецький національний технічний університет, Дрогобич, Україна

Сьогодні сталість і стабільність роботи енергетичної інфраструктури в Україні є одним з найчутливіших викликів, що постали в умовах війни проти нашої держави. ОЕС (об'єднана енергетична система) України є централізованою, з центром управління в Києві, і відокремленим підрозділом – Бурштинським енергоостровом. В ОЕС України паралельно працюють АЕС, ТЕС, ГЕС, ТЕЦ, а також електростанції з ВДЕ. Всі вони об'єднані в єдину інфраструктуру [2] з встановленою потужністю близько 561159 МВт (рис. 1) [1].

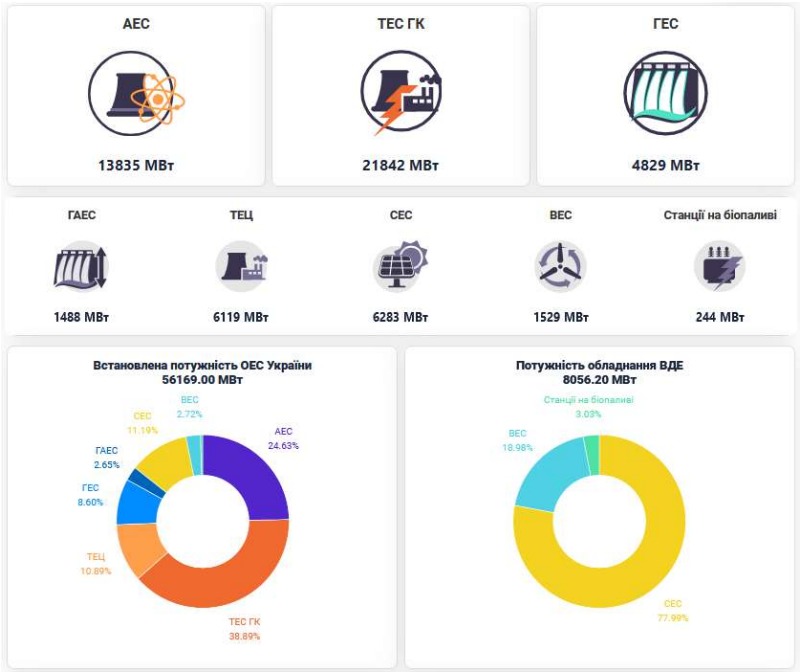


Рисунок 1 - Встановлена потужність ОЕС України

У відповідності з рис. 1, ОЕС України містить такі види генерації:

- атомні електростанції (АЕС) – працюють рівномірним графіком і створюють енергетичну базу протягом всієї доби. Атомні електростанції не можуть змінювати рівень виробництва під час добових коливань споживання;
- теплоелектростанції (ТЕС) – найчастіше це маневрові потужності з швидким реагуванням на зміни споживання, найчастіше такі станції працюють на спалюванні вугілля, газу або мазуту;
- теплоелектроцентралі (ТЕЦ) – станції такого типу виробляють не

тільки електричну енергію, а й теплову. Найчастіше вона використовується у містах для гарячого водопостачання та опалення;

- гідроелектростанції та гідроакумулючі електростанції (ГЕС/ГАЕС) – станції такого типу найчастіше використовуються для покривання пікового споживання в енергосистемі країни.;
- відновлювальні джерела енергії (ВДЕ). Сонячні електростанції (СЕС) – екологічно чиста генерація електроенергії, що здійснюється завдяки сонячному випромінюванню. Вітрові електростанції (ВЕС) – екологічно чиста генерація, яка використовує енергію вітру для генерації електроенергії. Біостанції – для генерації електричної енергії дані станції використовують біологічні відходи з виробництв та біогаз. Особливістю "зеленої" генерації є повна залежність від погодних умов та сезонність її генерування [2].

ОЕС України на сьогодні є одним з найбільших енергооб'єднань Європи. Станом на 23.02.2022 у складі ОЕС України діло 32 оператори систем розподілу та 6 регіональних електроенергетичних систем (Дніпровська, Західна, Південна, Південно-Західна, Північна і Центральна):

1. Дніпровська ЕС (ДнЕС) здійснює електропостачання Дніпропетровської, Запорізької, Кіровоградської областей, а також південно-західної частини Донецької області. Загальна протяжність ПЛ 330-750 кВ по трасі дорівнює 4577,68 км. ДнЕС експлуатує 26 ПС напругою 220-750 кВ.
2. Західна ЕС (ЗЕС) охоплює регіональну енергосистему в межах Волинської, Закарпатської, Івано-Франківської, Львівської та Рівненської областей. ЗЕС обслуговує 3796,36 км ліній електропередачі напругою 220, 330, 400 і 750 кВ. До складу ЗЕС також входить «Острів Бурштинської ТЕС», що працює у складі об'єднання енергетичних систем країн Європи – ENTSO-E з підключенням до енергосистем Угорщини, Словаччини та Румунії.
3. Південна ЕС (ПдЕС) здійснює електрозабезпечення Одеської, Миколаївської та Херсонської областей. ПЕС обслуговує лінії напругою 35-750 кВ, в тому числі 2370,23 км ПЛ 220-750 кВ і 280,91 км міждержавних ПЛ 35-110 кВ. Південна ЕС експлуатує одну ПС 750 кВ, 12 ПС 220-330 кВ і 4 ПС 110 кВ;
4. Південно-Західна ЕС (ПЗЕС) здійснює електрозабезпечення Чернівецької, Тернопільської, Хмельницької і Вінницької областей загальною площею 69 тис. км2. Загальна протяжність ПЛ 330-750кВ по трасі складає 2259,87 км. ПЗЕС експлуатує ПС 750 кВ і 8 ПС 330 кВ.
5. Північна ЕС (ПнЕС) здійснює електрозабезпечення Харківської, Сумської, Полтавської областей і півночі Донецької та Луганської областей. ПнЕС обслуговує ЛЕП напругою 35-800 кВ, загальна протяжність яких по трасі складає 3644,17 км. В експлуатації знаходиться 22 ПС 220-750 кВ;

6. Центральна ЕС (ЦЕС) здійснює електрозабезпечення Житомирської, Київської, Черкаської, Чернігівської областей та м. Київ. Загальна протяжність ПЛ 35-750 кВ складає 2689 км, до складу входить 42 силових трансформаторів на 13 ПС 330-750 кВ [3].

Щодо кількісного представлення виробників електроенергії в Україні до повномасштабного вторгнення [4], то до складу входить 4 АЕС, 15 ТЕС, 43 ТЕЦ, великі ГЕС на Дніпрі, а також Ташлицька ГАЕС на річці Південний Буг (8 ГЕС та 3 ГАЕС), СЕС в Нікопольському районі Дніпровської області, ВЕС в Запорізькій області та західних областях.

Як бачимо, то ОЕС України є самодостаньою з можливістю доволі гнучкого регулювання в широких діапазонах в залежності від рівня споживання а також з забезпеченням перетоків між електромережами партнерів. Бойові дії та обстріли енергетичної інфраструктури показали стійкість системи та одночасно вказали певні її вади, над усуненням яких необхідно працювати.

Література

1. Встановлена потужність енергосистеми України на 12/2021 [Електронний ресурс] – Режим доступу: https://ua.energy/vstanovlena-potuzhnist-energosystemy-ukrayiny/

2. Структура електрогенерації в Україні та її зв'язок із тарифами на електроенергію [Електронний ресурс] – Режим доступу: https://tek.energy/news/struktura-elektrogeneratsii-v-ukraini-ta-ii-zvyazok-iz-tarifami-na-elektroenergiyu

3. План розвитку системи передачі на 2022-2031 роки [Електронний ресурс] – Режим доступу: https://ua.energy/wp-content/uploads/2021/12/Plan-rozvytku-systemy-peredachi-na-2022-2031_-shvalenyj-Postanovoyu-NKREKP-vid-10.12.2021-2477.pdf

4. Звіт з оцінки відповідності (достатності) генеруючих потужностей [Електронний ресурс] – Режим доступу: https://ua.energy/peredacha-i-dyspetcheryzatsiya/zvit-z-otsinky-vidpovidnosti-dostatnosti-generuyuchyh-potuzhnostej/

Анотація

В доповіді описана структуру ОЕС України, включаючи типи електростанцій та їхню роль у енергозабезпеченні країни. Особлива увага приділяється важливості енергетичної безпеки України та адаптації енергосистеми до нових викликів. Зазначається, що атаки на об’єкти енергетики виявили як сильні сторони української енергосистеми, так і її вразливі місця, що потребують негайного усунення.

Ключові слова: енергетика, безпека, електростанція, енергосистема

Abstract

The report describes the structure of the Ukrainian Unified Energy System, including the types of power plants and their role in the country's energy supply. Particular attention is paid to the importance of Ukraine's energy security and the adaptation of the energy system to new challenges. It is noted that attacks on energy facilities have revealed both the strengths of the Ukrainian energy system and its vulnerabilities that require immediate elimination.

Keywords: energy, security, power plant, energy system

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ОСВІТЛЕННЯ З УРАХУВАННЯМ НЕВІЗУАЛЬНОГО ВПЛИВУ СВІТЛА

Євлахов Є.В., студент, yevhen.ievlakhov@kname.edu.ua;
Аксьонов Д.К., студент, daniil.aksonov@kname.edu.ua;
Бокатов М.І., студент, maksym.bokatov@kname.edu.ua;
Афанас'єв О.М., студент, oleksandr.afanasiev@kname.edu.ua
Харківський Національний університет міського господарства імені О.М. Бекетова, Харків, Україна

Актуальність питання підвищення ефективності освітлення з урахуванням невізуального впливу світла є надзвичайно важливою у контексті сучасних вимог до енергозбереження та здоров'я людини. Вивчення впливу різних спектральних розподілів випромінювання джерел світла на людський організм дозволяє розробити освітлювальні системи, що оптимально поєднують візуальні та невізуальні ефекти. Врахування невізуального впливу світла, зокрема його впливу на циркадні ритми, сприяє покращенню загального добробуту людини та підвищенню ефективності енергоспоживання.

Відомі дослідження та публікації, що стосуються спектральних розподілів випромінювання, показують, що вплив будь-якого спектрального розподілу яскравості на мезопічні фотометричні величини можна охарактеризувати за допомогою величини S/P. Це співвідношення визначає, наскільки ефективно джерело світла впливає на фоторецептори нічного зору. Чим вищий S/P-фактор, тим ефективніше джерело світла діє на адаптацію очей в умовах низької освітленості, що, в свою чергу, дозволяє зменшити споживану енергію при досягненні необхідного рівня освітленості.

Постановка задачі полягає в розробці методики розрахунку фактору S/P для різних джерел світла та аналізі впливу цього показника на енергетичну ефективність освітлення. Для цього необхідно враховувати спектральні розподіли випромінювання різних джерел світла та порівнювати їх ефективність за допомогою таблиць функцій світлової ефективності для денного та нічного зорів.

Основний матеріал та результати досліджень включають експериментальні дані щодо урівнювання світлоти для різних типів джерел світла, що підтверджують ефективність джерел з вищим S/P-фактором. Наприклад, результати експериментів щодо відношення середніх освітленостей, наведені в табл. 1, показують, що джерела з різними спектральними характеристиками потребують різної кількості енергії для досягнення однакового рівня освітленості. Зок-

Таблиця 1

Опорна осв., лк	Відношення середніх освітл.	КЛЛ/НЛВД	МГЛ1/НЛВД	МГЛ2/НЛВД
2,0	0,694	0,694	0,729	0,679
7,5	0,718	0,718	0,733	0,724
10,0	0,732	0,732	0,724	0,738

рема, відношення середніх освітленостей для різних типів джерел світла змінюється в межах 0,679–0,738 залежно від рівня освітленості, що демонструє можливість зменшення енергоспоживання при покращенні візуальних характеристик освітлення. Ці результати свідчать про можливість покращення візуальних характеристик та зменшення енергоспоживання.

Висновки та напрямок подальших досліджень полягають у необхідності розробки методики розрахунку S/P-фактора для різних джерел світла з урахуванням їх спектральних характеристик. Врахування цього показника стане важливим критерієм для виробників освітлювальних систем, що дозволить оптимізувати енергоспоживання та забезпечити більш комфортні умови освітлення для користувачів. Подальші дослідження можуть бути спрямовані на удосконалення методів вимірювання S/P-фактора та розробку нових стандартів для джерел світла з урахуванням невізуального впливу.

Література

1. CIE 191:2010. Recommended System for Mesopic Photometry Based on Visual Performance. Vienna: CIE; 2010.

2. Назаренко Л. А. Спектральний розподіл потужності світла та присмеркова фотометрія / Л. А. Назаренко, Т. В. Можаровська, Д. О. Усиченко // Український метрологічний журнал. — 2017. — № 1. — С. 43–52.

3. The effects of lighting spectral on visual performance at mesopic light levels / M. Eloholma [et all.] // Proceedings of the CIE Symposium ―75 Years of CIE Photometry‖: Report theses. — Budapest, Hungary; Vienna, Austria, 1999. — P. 5.1–5.4.

4. Fotios S. A. Lighting for subsidiary streets: investigation of lamps of different SPD. Part 2– Brightness / S. A. Fotios, C. Cheal //Lighting Research and Technology. — 2007. — Т. 39, № 3. — P. 233–249.

Анотація

У доповіді розглядаються аспекти підвищення енергетичної ефективності освітлення з урахуванням невізуального впливу світла. Особливу увагу приділено спектральним розподілам випромінювання різних джерел світла та їх впливу на фоторецептори нічного зору, який оцінюється за допомогою величини S/P. Розглянуто результати експериментальних досліджень, що підтверджують можливість покращення візуальних характеристик освітлення при зменшенні енергоспоживання. Наведено методику розрахунку S/P-фактора для джерел світла, а також значення функцій світлової ефективності для денного та нічного зорів. Підкреслено важливість цього показника для характеристик джерел світла та необхідність його включення до стандартів виробництва освітлювальних систем.

Ключові слова: ефективність, освітлення, невізуальний вплив світла.

Abstract

The report discusses the aspects of increasing the energy efficiency of lighting systems considering the non-visual effects of light. Special attention is paid to the spectral distributions of radiation from different light sources and their impact on the night vision photoreceptors, evaluated using the S/P ratio. The results of experimental studies confirming the possibility of improving visual characteristics of lighting while reducing energy consumption are presented. The methodology for calculating the S/P factor for light sources is provided, as well as the values of the light efficiency functions for both daylight and night vision. The importance of this parameter for the characteristics of light sources is highlighted, and the need to include it in the standards of lighting systems production is emphasized.

Keywords: energy efficiency, lighting, non-visual light effects.

ОПИС ДЕЯКИХ ОСОБЛИВОСТЕЙ ВІДНОВЛЕННЯ ПАЛАДІЄВИХ МЕМБРАН ПІСЛЯ ВОДНЕВОЇ ВЗАЄМОДІЇ

Любименко О.М., к.ф.-м.н,доц., olena.liubymenko@donntu.edu.ua
ДВНЗ «Донецький національний технічний університет», м. Дрогобич, Україна

Водень відіграє важливу роль в атомній енергетиці, оскільки є не лише побічним продуктом певних процесів у ядерних реакторах, а й використовується в системах охолодження та контролю газів. Через це контроль концентрації водню в атомних реакторах має критичне значення. Для очищення газів та утримання водню в безпечних концентраціях застосовують паладієві мембрани, які пропускають водень. Це забезпечує контрольоване використання водню та запобігає небажаним реакціям і аваріям. Однак контакт мембран із воднем призводить до їх деформації, змін фізичних властивостей та зниження ефективності. У зв’язку з цим нами проведено комплексні дослідження, зокрема:

Дифузії водню в мембранах.

Водень проникає в матеріал мембрани, викликаючи концентраційні напруження. Утворений сплав "метал-водень" складається з двох атомних підсистем (металевої та водневої), дифузійна рухливість яких суттєво відрізняється. Ми порівняли напруження для межі пружності сплаву паладій-водень, характерні для металевої підсистеми. Зважаючи на те, що напруження, які виникають у кантилевері під час експериментів, перевищують межу пропорційності, стає очевидним, що в таких сплавах збільшується рухливість дислокацій, а сили міжатомної взаємодії між атомами паладію в системі Pd-H зменшуються.

Відновлення форми мембран

При певних умовах, таких як зниження тиску водню чи зміна температури, мембрани можуть поступово повертатися до початкової форми. Це свідчить про зворотність процесів деформації за умови відсутності фазових перетворень і протікання процесів у сплаві α-PdHn. Однак цей процес може бути повільним і менш ефективним після тривалого використання мембрани.

Експериментально встановлено, що вигин кантилеверу під час дегазації сплавів α-PdHn відбувається у два етапи:

1. Перший етап триває короткий час (9–30 секунд) і характеризується швидким досягненням максимального вигину із формуванням плато тривалістю 3–30 секунд. Наявність плато підтверджує встановлення термо-баро-пружньої рівноваги в сплаві.
2. Другий етап триває довше, характеризується поступовим зменшенням вигину, що супроводжується поверненням кантилеверу до вихідного

положення або досягненням стаціонарного стану з невеликим відхиленням, що вказує на реалізацію когерентного механізму деформації.

Утворення тимчасових градієнтних матеріалів

Вплив водню на паладієві мембрани призводить до утворення тимчасових градієнтних матеріалів, таких як сплави α-PdHn, які мають змінені фізичні властивості порівняно з чистим паладієм. При підвищених температурах (220–260˚C) мембрани змінюють форму через дифузію водню, що потребує їх відновлення. Тимчасові зміни форми можуть бути частково або повністю зворотними, залежно від умов експлуатації.

Градієнт концентрації водню контролюється його дифузійним переміщенням із об'єму металу до поверхні і залежить від параметрів дегазації, таких як температура і тиск. Саме цей градієнт визначає характеристики тимчасового градієнтного матеріалу, включно з градієнтами дилатації кристалічних ґраток, міжатомних сил, механічних властивостей і концентраційних напружень.

Дегазація мембран

Зміна форми мембран під час дегазації сплавів α-PdHn також відбувається у два етапи:

1. Перший етап триває 9–30 секунд і супроводжується досягненням максимального вигину з утворенням плато, що підтверджує встановлення термо-баро-пружньої рівноваги.
2. Другий етап триває довше, характеризується зменшенням вигину та поверненням мембрани до початкової форми або стаціонарного стану з мінімальним відхиленням.

Використання багатошарових мембран

Багатошарові мембрани, що включають тонкий шар паладію, мають підвищену стійкість до деформацій і краще витримують вплив водню при високих температурах. Дослідження показують, що такі мембрани знижують ступінь деформації та подовжують термін їх служби.

Практична значущість досліджень полягає у визначенні специфічних особливостей взаємодії водню з паладієвими мембранами та вивченні процесів дифузії, дегазації та відновлення мембран у сплавах α-PdHn

1. Оптимізація технологій охолодження та контролю газів у ядерних реакторах. Результати досліджень дозволяють покращити контроль концентрації водню, що знижує ризик аварійних ситуацій.
2. Підвищення ефективності паладієвих мембран. Розробка методів зменшення деформацій мембран під впливом водню та їхнього відновлення подовжує термін служби обладнання.
3. Розробка нових матеріалів. Отримані дані сприяють створенню градієнтних матеріалів із заданими властивостями, що можуть бути застосовані у водневій енергетиці та інших галузях.

4. Підвищення безпеки та економічної ефективності атомної енергетики. Застосування багатошарових мембран із високою стійкістю до дії водню дозволяє знизити витрати на обслуговування та ремонт обладнання.
5. Застосування у високотехнологічних системах. Результати досліджень можуть бути корисними для розвитку водневих технологій у транспорті, зберіганні енергії та інших сферах, що потребують використання надійних газопроникних мембран.

Література

1. O.M Lyubimenko, K. V. Gumennyk, E. P. Feldman. Kinetics of permeation and absorption of hydrogen in palladium during bending and unbending of a palladium cantilever. // J. of Applied Physics, 127, № 24: 245104 (2020). DOI: https://doi.org/10.1063/5.0011826

2. E. P. Feldman, O. M. Lyubimenko Dynamics of hydrogen-elastic stresses in palladium cantilever //Journal Acta Mechanica. 2023, DOI10.1007/s00707-022-03471-5.

Анотація

У дослідженні розглянуто використання паладієвих мембран, які селективно пропускають водень, дозволяючи утримувати його концентрацію на безпечному рівні. Проаналізовано процеси дифузії водню в паладієвих мембранах, які спричиняють концентраційні напруження та деформації, а також виявлено механізми відновлення форми мембран за певних умов. Встановлено двоетапний характер дегазації сплавів α-PdHn із формуванням термо-баро-пружньої рівноваги та когерентного механізму вигину. Досліджено утворення тимчасових градієнтних матеріалів, які мають змінені фізичні властивості, та вплив параметрів експлуатації (тиску, температури, часу) на ці процеси. Результати досліджень можуть бути застосовані в атомній енергетиці, водневій енергетиці та інших високотехнологічних сферах, підвищуючи безпеку та ефективність роботи систем.

Ключові слова: водень, паладієві мембрани, дифузія водню, дегазація, концентраційні напруження, градієнтні матеріали.

Abstract

The study considered the use of palladium membranes that selectively pass hydrogen, allowing its concentration to be maintained at a safe level. The processes of hydrogen diffusion in palladium membranes, which cause concentration stresses and deformations, were analyzed, and the mechanisms of membrane shape restoration under certain conditions were identified. The two-stage nature of the degassing of α-PdHn alloys with the formation of thermo-baroelastic equilibrium and a coherent bending mechanism was established. The formation of temporary gradient materials with changed physical properties and the influence of operating parameters (pressure, temperature, time) on these processes were studied. The results of the research can be applied in nuclear power, hydropower and other high-tech areas, increasing the safety and efficiency of systems.

Keywords: hydrogen, palladium membranes, hydrogen diffusion, degassing, concentration stresses, gradient materials.

ЗМІСТ

НАУКОВЕ ВИДАННЯ

«ТАК»:
Телекомунікації, автоматизація, комп’ютерно-інтегровані та інформаційні технології

Збірка доповідей Всеукраїнської науково-практичної
конференції молодих учених
(Луцьк, 12 грудня 2024 р.)

Редагування, коректура та комп’ютерна верстка *Гліб Ступак*

Формат 60х84/16.
Ум. друк. арк. 15,4
Тираж 300 прим.

Видавець та виготовлювач: Державний вищий навчальний заклад «Донецький національний технічний університет», юридична адреса: пл. Шибанкова, 2, м. Покровськ, Донецька обл., 85300, фактична адреса: вул. Самбірська, 76, м. Дрогобич, Львівська обл., 82111, Україна

Свідоцтво про державну реєстрацію суб’єкта видавничої справи: серія ДК №4911 від 09.06.2015