МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЗАПОРІЗЬКА ПОЛІТЕХНІКА»

ТИЖДЕНЬ НАУКИ-2024

Факультет інформаційної безпеки та електронних комунікацій

Збірник тез доповідей щорічної
науково-практичної конференції серед студентів, викладачів, науковців, молодих учених і аспірантів
15–19 квітня 2024 року

Електронне видання на DVD-ROM

Запоріжжя • НУ «Запорізька політехніка» • 2024

УДК 621.3+004+519.6

Т39

Рекомендовано до видання Вченою радою
Національного університету «Запорізька політехніка»
(Протокол № 10 від 04.06.2024 р.)

Т39 **Тиждень науки-2024. Факультет інформаційної безпеки та електронних комунікацій.** Тези доповідей науково-практичної конференції, Запоріжжя, 15–19 квітня 2024 р. [Електронний ресурс] / Редкол. : Вадим ШАЛОМЄЄВ (відпов. ред.) Електрон. дані. – Запоріжжя : НУ «Запорізька політехніка», 2024. – 146 с. – 1 електрон. опт. диск (DVD-ROM); 12 см. – Назва з тит. екрана.

ISBN 978-617-529-456-7

Зібрані тези доповідей, заслуханих на щорічній науково-практичній конференції серед студентів, викладачів, науковців, молодих учених і аспірантів. Збірка відображає широкий спектр тематики наукових досліджень, що проводяться на **факультеті інформаційної безпеки та електронних комунікацій** Національного університету «Запорізька політехніка». Збірка розрахована на широкий загал дослідників та науковців

УДК 621.3+004+519.6

ISBN 978-617-529-456-7

ЗМІСТ

СЕКЦІЯ «РАДІОТЕХНІКА ТА ТЕЛЕКОМУНІКАЦІЇ»

СЕКЦІЯ «ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ЕЛЕКТРОНИХ ЗАСОБІВ»

СЕКЦІЯ «ІНФОРМАЦІЙНА БЕЗПЕКА ТА НАНОЕЛЕКТРОНІКА»

СЕКЦІЯ «РАДІОТЕХНІКА ТА ТЕЛЕКОМУНІКАЦІЇ»

УДК 621.373.826
Логачова Л.М.[1]
[1] старш. викл. НУ «Запорізька політехніка»

ЗАСТОСУВАННЯ АКУСТООПТИЧНИХ ПРИСТРОЇВ У СУЧАСНІЙ ОПТИЦІ

Представлений матеріал буде використовуватися для вдосконалення лекційного курсу з дисципліни КВ РТПС.

Акустооптичні (АО) пристрої - модулятори, дефлектори, фільтри - широко використовують як функціональні елементи сучасної оптики. Це активні елементи, побудовані на технології динамічних дифракційних решіток, створюваних за допомогою ультразвукових хвиль. До їхніх переваг належать відсутність рухомих елементів, компактність, надійність, швидкодія, програмованість і багато інших фізичних, технічних, конструктивних та експлуатаційних властивостей.

На сьогодні не всі ці властивості використовуються повною мірою, а деякі ще до кінця не вивчені. Технологія динамічних дифракційних решіток дає можливості для створення нового покоління АО пристроїв, також вона дає змогу змінювати параметри решіток за мікросекунди та керувати характеристиками пристроїв у реальному часі, і розв'язати проблеми масового випуску АО комірок.

В основі АО-приладів лежить фізичний процес дифракції світла на збуреннях середовища, створюваних акустичною хвилею. У результаті взаємодії виникає ефект подвійного променезаломлення і відбуваються просторово-періодичні зміни поверхні показника заломлення мінералу, що створюють у середовищі розподілену фазову структуру, що являє собою об'ємну дифракційну решітку, яка впливає на поширення світла.

У результаті змінюються характеристики світлових хвиль, напрямок поширення, поляризація, інтенсивність, фаза, швидкість. На цій основі створено низку функціональних пристроїв керування оптичним випромінюванням і його аналізу: модулятори, дефлектори, фільтри.

Класичні схеми побудови цих пристроїв не є єдино можливими. Розглянемо один із можливих нових підходів - мультиплексування, в якому здійснюється численна АО - взаємодія в одному оптичному елементі.

Акустооптичний модулятор змінює в часі інтенсивність вихідного лазерного променя (рис. 1, а). Закон модуляції визначається варіацією потужності збуджуваної звукової хвилі Ps(t):

$$I(t) \sim I0\ M2\ Ps(t)\ L2 / \lambda 2, \quad (1)$$

де I0, I(t) – падаючий і вихідний (модульований) світлові потоки; L – довжина кристала; M2 – коефіцієнт його АО-якості; λ – довжина хвилі світла.

Глибина модуляції дифрагованого пучка становить 100 %. Максимальна частота модуляції може досягати мегагерцових частот для фокусованих світлових пучків. Такий модулятор розташовується всередині резонатора лазера і виконує функцію затвора.

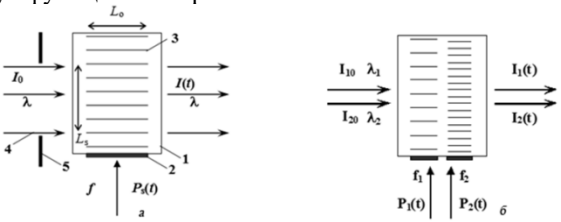


Рисунок 1 - Схеми АО-модулятора: *(а)* – класична; *(б)* - мультиплексована із секціонованим випромінювачем
1 - світлозвукопровід; 2 - електроакустичний випромінювач; 3 - акустичний пучок; 4 - світловий пучок; 5 – діафрагма

У модуляторі під час мультиплексування (рис. 1, *б*) збуджуються кілька акустичних хвиль, які для падаючого світлового випромінювання є комбінацією кількох монохроматичних пучків із різними довжинами хвиль, які можуть модулюватися незалежно.

Багатоспектральні пучки виникають, наприклад, на виході генераторів гармонік, параметричних генераторів і підсилювачів світла. Такі пучки, складені з променів кількох лазерів, також використовуються для створення кольорових зображень на екрані.

АО-дефлектор (рис. 2, а) відхиляє світловий пучок на заданий кут θ. Закон відхилення визначається варіацією частоти f звукової хвилі:

$$\theta(t) \sim \lambda f(t) / v_S. \quad (2)$$

Загальне число розв'язних кутових положень може досягати 1 000. Дефлектори, зокрема, використовують для управління випромінюванням потужних технологічних лазерів у системах різання, зварювання металу, маркування виробів тощо.

Також їх широко застосовують як засоби розгортки для систем створення зображень на екранах. У випадку мультиплексування відхилення лазерного пучка відбувається в декілька положень (рис. 2, *б*). Наприклад, при використанні двох акустичних частот виходять два дифраговані пучки, що призводить до збільшення швидкості роботи пристрою. Це збільшення може

бути доволі суттєвим за великої кількості ультразвукових хвиль (до восьми). На рис. 2, *б* зображено спосіб генерації багаточастотного сигналу шляхом подачі декількох частот на один п'єзоперетворювач.

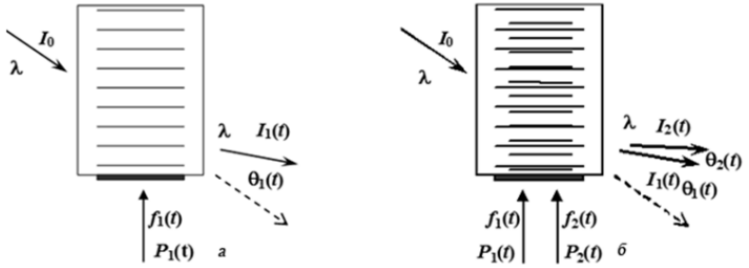


Рисунок 2 - Схеми АО-дефлектора: (а) - класична; (б) - мультиплексована з мультичастотним електроакустичним випромінювачем

Акустооптичний осередок містить два суттєвих елементи: світлозвукопровід і електроакустичний випромінювач. У якості світлозвукопроводу можна в принципі використовувати будь-яку речовину, оскільки фотопружність присутня в будь-якому середовищі. Але на практиці для цього використовують монокристалічні середовища або оптичне скло, що мають значну анізотропію. Наприклад, в ультрафіолетовому (УФ) діапазоні застосовують кристали кварцу (SiO_2), іноді нелінійні оптичні кристали – KDP (Дигідроортофосфат калію KH_2PO_4). Для неколінеарної дифракції у видимому діапазоні використовують парателлурит (TeO_2), також використовують молібдат кальцію (CaMoO4). У цілому в діапазоні 0,4...4,4 мкм застосовують переважно парателлурит, а в УФ-діапазоні - 0,2...0,4 мкм - кварц.

Електроакустичний випромінювач. Формування робочого акустичного пучка відбувається шляхом відбиття ультразвуку від похилої грані кристала, при цьому відбувається перетворення акустичних мод. Розташування вхідної та вихідної оптичної граней зазвичай буває косим для правильної орієнтації світла відносно звуку. І при цьому основні грані мають бути відполіровані, а оптичні - просвітлені. Також необхідно зазначити, що АО-осередки для подвійних монохроматорів вимагають спеціальних технологій виготовлення.

УДК 621.395
Сметанін І.М.[1], Костенко В.О.[2]
[1] старш. викл. НУ «Запорізька політехніка»
[2] канд. техн. наук, доц. НУ «Запорізька політехніка»

АЛГОРИТМ ГІБРИДНОГО МЕТОДУ ФОРМУВАННЯ ГРУП АБОНЕНТІВ

У відомому способі підвищення точності прогнозу локального перевантаження в стільниковій мережі мобільного зв'язку [1] було запропоновано фіксувати кількість абонентів, вимірювати і аналізувати параметри потоків переміщення абонентів в однієї комірці мережі і в сусідніх комірках шляхом формування векторів переміщення з встановленим інтервалом часу для кожного абонента.

Такий спосіб прийнятний, коли до аттрактору в комірці прагнуть абоненти, чисельність яких не перевищує декілька сотень. Інша справа, коли до аттрактору в комірці рухатимуться тисячі абонентів. При такому розвитку подій вимірювати і аналізувати параметри переміщення для кожного абонента стає неможливим, оскільки це приведе до перевантаження сигнального трафіку фрагмента мережі.

Для вирішення такої проблеми пропонується застосування гібридного методу формування груп абонентів. Суть його відображає алгоритм, наведений на рисунку 1.

На початковому етапі загрози перевантаження для кожного *i*-го абонента комірки визначаються координати $(x_i^{(t=0)}, y_i^{(t=0)})$ шляхом запиту місця розташування його мобільної станції (МС). Після повторного зняття координат $(x_i^{(t+\Delta t_j)}, y_i^{(t+\Delta t_j)})$ визначаються параметри переміщення МС, такі як швидкість $v_i^{(t)}$ $[0, V_{\max}]$ і кут напряму $\theta_i^{(t)}$ в діапазоні $[0, 2\pi]$. При цьому із загального числа МС можна виділити статичні (n_s) станції та ті, що рухаються (n_m). В цілому в комірці знаходяться N абонентів:

$$N = n_s + n_m, \tag{1}$$

На підставі результатів вимірювання параметрів переміщення для кожного *i*-го абонента з множини n_m будується вектор напряму руху $\overline{\theta_i^{(t)}}$. Надалі для усіх n_m абонентів комірки визначається сумарний вектор напряму руху $\overline{\theta_g^{(t)}}$ групи

$$\overline{\theta_g^{(t)}} = \sum_{i=1}^{N} \overline{\theta_i^{(t)}}\,, \qquad (2)$$

Рисунок 1 – Алгоритм формування груп при гібридному методі формування

При досягнені щільності абонентів порогового значення $D_{пор}$ пропонується формувати групи, використовуючи відому модель мобільності групи для персональних мереж (PNMM) [2].

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Пат. 81170 Україна, МПК2013 H04W 48/00, H04W 72/00 Спосіб підвищення точності прогнозу локального перевантаження в стільниковій мережі рухомого зв'язку [Текст] / Сметанін І.М., Сметанін Р.І., Піза Д.М., Костенко В.О.; заявник Запорізький національний технічний університет. – № u201214522; Заявл. 18.12.12; Опубл. 25.06.2013; Бюл. №12. – 7 с.

2. Yanying, G., Mobility Modeling for Personal Networks [Text] / Gu Yanying, R. Venkatesha Prasad, Ignas Niemegeers // Wireless Personal Communications. – 2011. – Vol. 58, № 2, – P. 169–196.

УДК 621.395
Сметанін І.М.[1], Мороз Г.В.[2]
[1] старш. викл. НУ «Запорізька політехніка»
[2] старш. викл. НУ «Запорізька політехніка»

ВПЛИВ НАЙКОРОТШОГО ШЛЯХУ НА РЕАЛІСТИЧНІСТЬ СТВОРЕННЯ ПОВЕДІНКОВИХ МОДЕЛЕЙ ПЕРЕМІЩЕННЯ АБОНЕНТІВ

Як відомо [1] для прогнозу перевантаження у фрагменті стільникової мережі мобільного зв'язку, в якості набору даних для побудови реалістичних математичних моделей мобільності абонентів, як правило використовують, вплив цільових аттракторів та параметри руху (швидкість, прискорення і зміна кута напряму), а також залежності між ними, величина часу зупинки абонентів в дорозі і елементи, які відображають зовнішні чинники.

Також в таких моделях треба враховувати схильність людини йти до цільового аттрактору найкоротшим шляхом. Навіть, незважаючи на виникаючу необхідність в подоланні стаціонарних перешкод при географічних обмеженнях, коли рух людини може бути змінений в зв'язку появою на його шляху будівель, споруд і автомобільних доріг, людина у своєму прагненні до аттрактору завжди робить вибір на користь найкоротшого шляху. Виходячи з цього, можна припустити, що абонент z_i вибере маршрут руху по дотичній до контуру в обхід перешкоди O_i, яка знаходиться на його шляху, який буде найкоротшим.

При обході перешкоди для пошуку найкоротшого шляху важливо урахувати його форму.

Якщо розглядати місцезнаходження абонента в двовимірному просторі, то в основному такі перешкоди матимуть форми багатокутників або кола. В принципі перешкоду, яка має округлу форму можна розглядати як апроксимований багатокутник.

Топографічні форми можуть бути у вигляді опуклих або увігнутих багатокутників. Тоді стає очевидним, що маршрут для подолання стаціонарної перешкоди прокладається по набору вершин багатокутника [2]:

$$M = \{M_0 = (x_0,y_0); M_1 = (x_1,y_1); ...; M_i = (x_i,y_i); ...; M_l = (x_l,y_l)\}, \quad (1)$$

де M_0 – найближча до поточного місця розташування абонента вершина багатокутника (перешкоди Oi) з координатами x_0,y_0;

$M_1;...;M_i$ – – проміжні вершини шляху з координатами x_1,y_1 і x_i,y_i, відповідно;

M_l – остання вершина багатокутника (перешкоди Oi) з координатами x_l, y_l, від якої відстань до цільового аттрактору буде мінімальною.

Таким чином, виходить набір вершин M, який відображає дискретну траєкторію обходу стаціонарних перешкод. Для виконання умов обходу перешкод по найкоротшому шляху, абонент z_i повинен послідовно пересуватися уздовж об'єкта O_i від початкової точки M_0 до кінцевої M_l, у напрямі з мінімальною довжиною шляху до мети *a*.

Окрім стаціонарних перешкод на шляху абонента можуть виникнути і рухомі перешкоди.

Зважаючи на те, що людям властиво здійснювати вибір траєкторії свого руху, щоб якомога менше зачіпати сусідів, абонент спробує відхилитися від зіткнення з іншими людьми. Для цього він змінить свій шлях на кут θ_{ik}, утворений своїм новим напрямом і напрямом руху іншої людини. Така зміна маршруту має бути не значною, оскільки орієнтація вектору $\vec{u}_{i\perp}(t)$, перпендикулярного миттєвій швидкості $\vec{v}_i(t)$ абонента z_i, буде вибрана так, щоб звести до мінімуму відхилення від найкоротшого шляху до мети.

Таким чином, вказані чинники і параметри є основою для формування поведінкових моделей руху абонента.

Але для побудови реалістичного прогнозу перевантаження у фрагменті стільникової мережі мобільного зв'язку на основі переміщення абонентів необхідно мати якомога точніші дані про їх фактичне місце розташування. Тому виникає необхідність провести детальніші дослідження ефективності існуючих методів позиціонування по точності визначення місця розташування мобільних станцій стільникового зв'язку.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Сметанін І.М., Захарова М.В. Вплив аттракторів на реалістичність моделей переміщення абонентів мобільного зв’язку [Текст] / І.М. Сметанін, М.В. Захарова// Тиждень науки – 2016 : Щоріч. наук.-практ. конф. серед студентів, викладачів, науковців, молодих учених і аспірантів, 18–12 квітня 2016 р., м. Запоріжжя : зб. тез доп. в 4 т. / відп. ред. Ю. М. Внуков – Запоріжжя : ЗНТУ, 2016. – Т. 1 . – С. 264–265.

2. Beuran, R. Behavioral Mobility Model with Geographic Constraints [Text] / R. Beuran, S. Miwa, Y. Shinoda // Workshops of 27th International Conference on Ad-vanced Information Networking and Applications (WAINA), – 2013. – P. 470–477.

УДК 621.396.62:621.396.96
Чорнобородова Н.П.[1], Чорнобородов М.П.[2], Кабак В.С.[3]
[1] інж. ТОВ НВФ "Сведа, Лтд"
[2] канд. техн. наук, доц. НУ «Запорізька політехніка»
[3] канд. техн. наук, доц. НУ «Запорізька політехніка»

РЕГЕНЕРАЦІЯ СИНХРОІМПУЛЬСІВ ВІДЕОСИГНАЛУ

Параметри аналогових джерел відеосигналу закладались виробниками різноманітної апаратури з розрахунку на його відтворення аналоговими приймачами. За цього виробник завжди формував зображення на екрані, а задача забезпечення якості зображення у недостатніх умовах прийому цілковито лягала на плечі споживача: або мирись з "снігом", зниканням кольорів, появою кольорових рисок тощо, або підсилюй вхідний сигнал.

За переходу на цифрові приймачі, виробник забезпечує формування зображення на екрані лише за рівня сигналу, що перевищує деякий мінімальний рівень. Це призводить до того, що споживач отримує або якісне зображення, або напис "Немає сигналу". І невідомо: сигналу немає в принципі чи він є, але недостатньої потужності.

Проблема посилюється тим, що оновлення програмного забезпечення (прошивки мікроконтролера) цифрового приймача може (у тому числі) нести в собі збільшення порогового рівня без відома споживача. І разом з корисним ефектом від оновлення версії мікропрограми пристрою (наприклад, виправлення виявлених помилок, розширення функціональних можливостей тощо) споживач може отримати напис "Немає сигналу" у тих же самих умовах прийому.

Іншою причиною погіршення рівня сигналу можуть бути дії споживача, який захоче виводити на один монітор зображення від двох різних джерел шляхом їх паралельного з’єднання на один приймальний вхід. За простого накладання двох відеосигналів погіршується не тільки якість зображення, але й у суттєво більшому ступені його синхронізація.

Одним із шляхів подолання цих проблем може бути використання регенераторів синхроімпульсів відеосигналу, що відновлюють усі часові й амплітудні параметри імпульсів відеосигналу. У простих випадках цілком достатньо відновити необхідну амплітуду рядкових і кадрових синхроімпульсів, а у більш складних випадках - ще й їхню тривалість та форму.

Принцип роботи регенераторів полягає у видаленні наявних синхроімпульсів з вхідного сигналу й формуванні нових додатковим генератором. Пристрій (див. рис. 1) складається з каналу підсилювання відеосигналу й генератора синхроімпульсів.

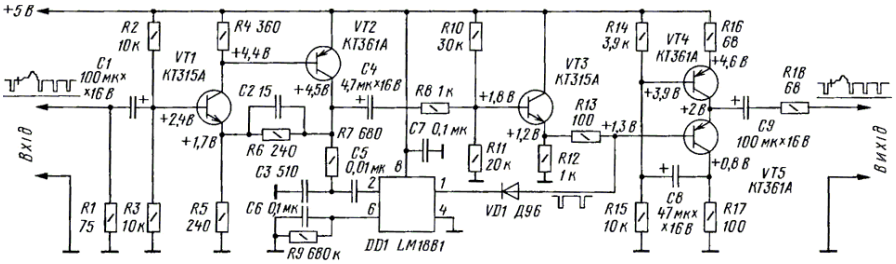


Рисунок 1 - Регенератор синхроімпульсів

Вхідний сигнал підсилюється у каскадах на транзисторах VT1 й VT2 і надходить до генератора DD1 (ланцюгом C5C3R7) й до буферного каскаду на транзисторі VT3 (колом C4R8), що узгоджує опір вхідного й вихідного каскадів.

Вихідний каскад виконано на транзисторах VT4 й VT5. Саме тут й забезпечується заміна старих синхроімпульсів на нові, які надходять діодом VD1 від генератора DD1.

За такої обробки полярність вихідного відеосигналу не змінюється.

Формувачем синхроімпульсів у регенераторі слугує мікросхема LM1881 (DD1). У ній використано вузол виділення синхроімпульсів, побудований за схемою компаратора, вихід якого додатково відіграє роль комутатора вихідного каскаду каналу підсилювання відеосигналу. Зформовані в мікросхемі й відкалібровані за амплітудою синхроімпульси з її виходу (виведення 1) комутувальним діодом VD1 надходять на базу транзистора VT5 вихідного каскаду під час появи синхроімпульсів відеосигналу на вході 2 мікросхеми DD1. Внаслідок цього, базу транзистора за допомоги діоду VD1 буде з'єднано із спільним дротом, чим досягається видалення старих імпульсів синхронізації й одночасна заміна їх на нові.

УДК 621.396.1
Бугрова Т.І.[1], Красов С.О.[2]
[1] канд. техн. наук, доц. НУ «Запорізька політехніка»
[2] асп. НУ «Запорізька політехніка»

ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ТЕЛЕКОМУНІКАЦІЙНІЙ ІНФРАСТРУКТУРІ

Сьогодні термін "штучний інтелект" (ШІ) є предметом інтенсивних дискусій. Він визначає галузь інформатики, що створює системи, здатні

виконувати завдання, аналогічні людським, включаючи розпізнавання мови і тексту, навчання та вирішення різних проблем. ШІ знаходить широке застосування у підвищенні ефективності телекомунікаційної інфраструктури. Технології ШІ мають потенціал для ефективного вирішення неструктурованих та, здавалося б, невирішуваних проблем, пов'язаних з великими обсягами даних в мереж 5G та B5G, зокрема, при впровадженні нових технологій на основі ШІ з гетерогенними нейронними мережами. ШІ може вирішити труднощі, які виникають при взаємодії різних мов завдяки необхідності автоматичного якісного синхронного перекладу мови в мережі зв'язку.

Під час роботи було досліджено використання ШІ в інформаційно-комунікаційній галузі, де вони зараз застосовуються не в повному обсязі. Мережеві операції можуть працювати без прямого втручання людини. В процесі досліджень можливості використання штучного інтелекту для управління технічними системами проаналізовано досвід застосування ШІ в провідних телекомунікаційних компаніях світу. Також було досліджено алгоритми відомих телекомунікаційних моделей з використанням систем ШІ, що підкреслило його ефективність в даній області та дозволило порівняти їх продуктивність.

Для задоволення постійно зростаючих очікувань клієнтів, постачальники послуг повинні підвищити інтелектуальний рівень своїх мережевих операцій, їх планування та оптимізацію.

Телекомунікаційні компанії активно переформовуються за допомогою ШІ, особливо у сфері оптичних мереж та повної оптимізації інфраструктури. Використання ШІ у цьому секторі спрямоване на забезпечення доступу до необхідної інформації, підвищення прозорості, спрощення аналізу та зменшення ризиків. Крім того, воно спрямоване на розробку критеріїв і встановлення вимог до процесу модернізації телекомунікаційних систем.

Досліджувались наявні моделі та на їх основі здійснювались розрахунки і вдосконалювались самі моделі.

Проводився аналіз впливу ШІ на мобільні мережі, здійснювався прогноз та розрахунок впливу ШІ на 5G (рис.1).

Є перспектива розробки стратегії впровадження мережі 6G за допомогою штучного інтелекту.

Однак, поки що в Україні відсутнія ця мережа. Проте, був розроблений алгоритм для бездротової мережі зв'язку з архітектурою для 5G, а також план його реалізації з використанням архітектури, створеної штучним інтелектом, і технологій машинного та глибокого навчання.

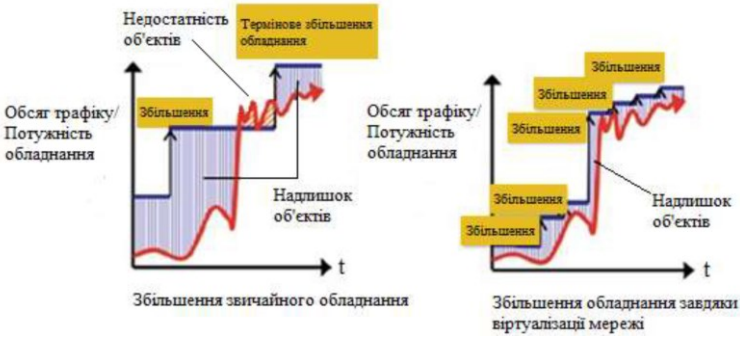


Рисунок 1 – Віртуалізація мережі за рахунок застосування ШІ.

Цей план базується на гетерогенних нейронних мережах, які постійно удосконалюються, оскільки час не стоїть на місці. Хоча системи штучного інтелекту ще не використовуються в повному обсязі у телекомунікаціях, все швидко змінюється. Докладний план дій для впровадження 5G за допомогою штучного інтелекту наведений у роботі, що підтверджує актуальність та доцільність проведених досліджень.

Загалом, в роботі зазначено, що застосування штучного інтелекту в телекомунікаціях має численні переваги. Встановлено, що основна перевага полягає в швидкій адаптації до змінюваних умов.

В галузі послуг та мережевого зв'язку це означає покращення концепції зв'язку без обмежень топології та збільшення швидкості Інтернету.

У сфері навчання штучний інтелект сприяє покращенню надання освітніх послуг в умовах дистанційної освіти.

У сфері бізнесу це призводить до збільшення ефективності застосування масового трафіку в роумінгу, розширення комерційних операцій і збільшення прибутку від торгівлі за рахунок зростання обсягу продажів.

У галузі розваг це забезпечує мобільність, оскільки швидкість дозволяє користувачам миттєво підключатися з будь-якого місця.

УДК 621.396.963
Гладун К.В.[1], Самойлик С.С.[2], Кабак В.С.[3]
[1] асп. НУ «Запорізька політехніка»
[2] канд. фіз.-мат. наук, доц. НУ «Запорізька політехніка»
[3] канд. техн. наук, доц. НУ «Запорізька політехніка»

ВИМІРЮВАННЯ КООРДИНАТИ ВИСОТИ В ДВОКООРДИНАТНИХ РАДІОЛОКАЦІЙНИХ СТАНЦІЯХ МЕТРОВОГО ДІАПАЗОНУ

Вимірювання координати висоти в двокоординатних радіолокаційних станціях метрового діапазону має ряд особливостей, які роблять цю задачу складною. До основних проблем належать: невисока точність, обумовлена тим, шо метровий діапазон хвиль має більшу довжину хвилі, ніж сантиметровий, що призводить до меншої точності вимірювання координат, а так як двокоординатні РЛС вимірюють лише дальність до цілі та кут місця і не дають прямої інформації про висоту, висота розраховується за допомогою тригонометричних співвідношень, що додатково знижує точність. Двокоординатні РЛС мають обмежений динамічний діапазон, що може призводити до втрати інформації про цілі, які мають малий ехо-сигнал.

Для покращення характеристик РЛС, пропонується використовувати пристрій, що відноситься до радіолокації, а саме до способів визначення параметрів положення цілі при прямолінійному рівномірному русі навколо радіолокаційної станції (РЛС) і може бути використаний для отримання додаткових даних про переміщення об'єктів у просторі, включаючи висоту, при використанні двокоординатних РЛС, які здійснюють круговий або секторний огляд простору. Технічний результат полягає в розширенні функціональних можливостей існуючих двокоординатних РЛС.

Цей результат досягається за рахунок введення між блоком вторинної обробки інформації та блоком індикації інформації блоку післяобробки даних траєкторії цілі, що складається з вираховувача, віднімача і компаратора. На вхід блоку післяобробки даних траєкторії цілі з блока вторинної обробки інформації надходять фільтровані виміри положення цілі, з яких вибирають три послідовні виміри, обробляють їх в вираховувачі, вибирають і зберігають відповідне значення припущеної висоти цілі при прямолінійній траєкторії, потім, в разі проведення першої ітерації, переходять до обробки в вираховувачі наступних вимірів положення цілі, а при проведенні другої і наступних ітерацій в віднімачі визначають відхилення новополученої припущеної висоти від раніше обчисленої, в компараторі фіксують відхилення, оцінюють правильність гіпотези прямолінійності і рівномірності, приймають обчислене значення висоти, яке передають у блок індикації інформації, і далі переходять до обробки наступних вимірів, що надійшли в блок післяобробки даних траєкторії цілі.

Висоту цілі за допомогою двокоординатної РЛС визначається наступним чином. Ехо-сигнали від приймача РЛС проходять порогову обробку та виділення цілей на тлі шумів у блоку первинної обробки інформації 1, після чого виміри положень цілей передаються до блоку вторинної обробки інформації 2 для фільтрації та визначення їх траєкторії. Між блоком вторинної обробки інформації 2 та блоком індикації інформації 3 розміщується блок післяобробки даних траєкторії цілі 4.

На вхід блоку після обробки даних траєкторії цілі 4 від блоку вторинної обробки інформації 2 надходять відфільтровані виміри положень цілі. Блок післяобробки даних траєкторії цілі 4 складається з вираховувача 4.1 віднімача 4.2 та компаратора 4.3.

На рисунку 1 зображено схему втілення методу визначення висоти цілі за допомогою двокоординатної РЛС, де 1 - блок первинної обробки інформації, 2 - блок вторинної обробки інформації, 3 - блок індикації інформації, 4 - блок післяобробки даних траєкторії цілі, 4.1 - вираховувач, 4.2 - віднімач, 4.3 - компаратор.

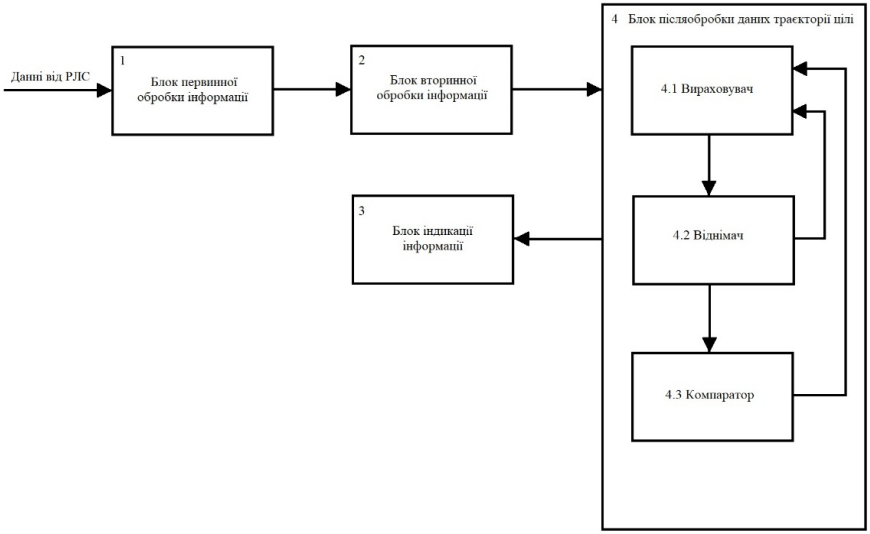


Рисунок 1 – Визначення висоти цілі за допомогою двокоординатної РЛС.

Розроблений метод в радіолокації спрямований на вдосконалення процесу визначення параметрів руху цілі біля радіолокаційної станції. Він може допомогти отримати більше інформації про рух об'єктів у просторі, зокрема їх висоту, за допомогою двокоординатних РЛС, обробка вимірів відбувається послідовно, з урахуванням попередніх результатів, що дозволяє отримати більш точні дані про рух цілі.

УДК 621.396.67
Мороз Г.В.[1], Комінов Є.Є.[2], Піза Д.М.[3]
[1] старш. викл. НУ «Запорізька політехніка»
[2] асп. НУ «Запорізька політехніка»
[3] д-р техн. наук, проф. НУ «Запорізька політехніка»

КОМУТАЦІЙНИЙ ПРИСТРІЙ ІНІЦІАЦІЇ БОЄПРИПАСІВ ДЛЯ ДРОНІВ КАМІКАДЗЕ

Дрони стали символом цієї війни, включаючи тактичні, оперативні, розвідувальні та ударні варіанти. FPV-дрони, здатні замінити артилерію, боєприпасів до якої дефіцитні, виконують особливо важливі завдання. Дешеві дрони-камікадзе з боєприпасами виявили високий потенціал, швидко зайнявши своє місце поряд з іншими видами озброєння. Пристрій ініціації боєприпасів для дронів-камікадзе є необхідним та має кілька цілей та переваг. По перше активація вибухового пристрою на дроні-камікадзе у відповідний момент. Він забезпечує точність та ефективність удару, оскільки забезпечує вчасну і правильну ініціацію вибухового пристрою під час атаки. По друге забезпечення автономності тим самим прискорює процес підготовки до атаки, роблячи дрон-камікадзе більш автономним у виконанні своєї місії. Це зменшує вплив людського фактора і підвищує точність удару. По третє збільшення ефективності: Пристрій ініціації боєприпасів може бути налаштований на виявлення цілей або певних областей для атаки, що підвищує його ефективність. І четверте зниження втрат у противника. Відсутність потреби в операторі або пілоті знижує ризик виявлення та знищення дронів-камікадзе противником. Таким чином, він може наносити удари безперервно та з меншими втратами для власних сил. Згідно із заяв багатьох підрозділів випробувань і сертифікації озброєння військової техніки, ризик передчасної детонації збільшується під час транспортування, під час спорядження, під час перевірок бойової частини, у разі випадкового падіння в пакуванні або під час підготовки до бойового застосування, а також у випадках порушень у роботі елементів безпілотника та інтегрованої бойової частини. Саме тому головним науково технічним завданням стоїть розробити безпечний пристрій ініціалізацію з спрацюванням по радіоканалу та відстрочкою в часі для відльоту FPV від пілота. Конструкція пристрою повинна передбачати наступний порядок використання. Після встановлення джерела живлення в пристрій ініціації інженер переводить пристрій в тестовий режим, приєднує тестер до виходів на контактній колодці і за відповідною світловою індикацією на пристрої та за даними тестера оцінює справність датчиків, ланцюгів живлення. Вимикає тестовий режим, від'єднує тестер з LED індикаторами від контактів, і встановлює перевірену плату на боєприпас, приєднує до контактної колодки плати дроти електродетонатора.

Безпосередньо перед вильотом інженер переводить пристрій в бойовий режим. Через 3 хв після переведення в бойовий режим (або за окремою командою з радіопередавач оператора) датчики активовуються і боєприпас стає на бойове зведення. Пристрій автоматично активує боєприпас при настанні будь-якої з таких подій: при ударі, при появі металевого предмету в радіус до 10 см від дрону, за радіосигналом який подається з окремого передатчика, при зупинці дрону, через 60 секунд після припинення руху. Для дотримання вищевикладеного, була побудована структурна схема пристрою рисунок 1:

Рисунок 1 – Структурна схема пристрою

Алгоритм роботи пристрою полягає в наступному. Після включення пристрою ми одразу попадаємо у тестовий режим. У ньому реалізована перевірка основних елементів, які повинні працювати нормально і злагоджено. Запобіжником буде працювати магніт. До того моменту поки він не буде прибраний від герконового датчику пристрій буде знаходитись у тестовому режимі. Кожні пів секунди блимає жовтий діодний індикатор, який означає що пристрій знаходиться в тестовому режимі. При спрацюванні сигналу з каналу дистанційного підриву жовтий індикатор безперервно буде горіти 10 секунд. Після чого повернеться до блимаючого режиму. Якщо до ультразвукового датчика буде менше 20 сантиметрів, то спрацює жовтий індикатор у безперервному режимі на 10 секунд. Після чого повернеться до блимаючого режиму. При знятті «запобіжника»(магніта) пристрій перейде у режим підготовки до бойового режиму. При цьому світлодіодний індикатор поперемінно буде загорятися жовтим та червоним кольором, а також буде звуковий сигнал. У цьому режимі інформація з датчику відстані і сигнал дистанційного підриву не працюють. Часовий проміжок цього режиму – 180 секунд. Якщо протягом цього часу повернути «запобіжник»(магніт), то пристрій перейде до тестового режиму. При переході в бойовий режим почне працювати таймер на самоліквідацію(15 хвилин).У бойовому режимі кожні пів секунди буде блимати червоний діодний індикатор, який означає що пристрій знаходиться в тестовому режимі. При отриманні сигналу з каналу дистанційного підриву, а також при спрацюванні контактного датчика в

бойовому режимі контролер перемикає реле комутує ток на колодці електродетонатора на 10 секунд. При цьому червоний індикатор безперевно буде горіти ті самі 10 секунд, що замкнено реле, після чого повернеться до блимаючого бойового режиму. На колодці детонатора може працювати навантаження зі спротивом 2 Ома з силою струму до 2 Ампер при напрузі приблизно 4 Вольта. Відповідно цього був побудований пристрій рисунок 1.2

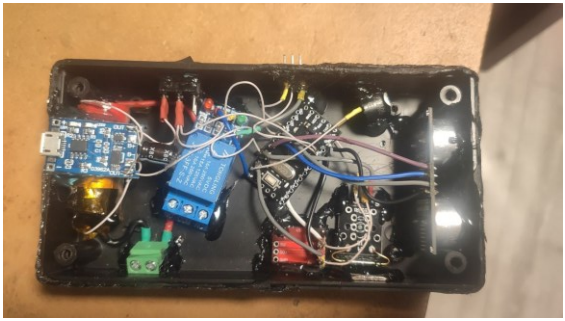


Рисунок 1.2 – Вигляд пристрою-прототипу

УДК 621.3.052.63.4
Бугрова Т.І.[1], Петрочко М.В.[2]
[1] канд. техн. наук, доц. НУ «Запорізька політехніка»
[2] студ. гр. БК-211сп НУ «Запорізька політехніка»

АНТЕНА ВІВАЛЬДІ

Широкосмугові антени та антенні решітки є одним з найважливіших функціональних складових радіотехнічних систем різного призначення, зокрема, в бездротових інформаційних мережах, в радіо- і відеолокації і т.д. У зв'язку з цим значний інтерес представляє конструювання антен, невеликих за розміром, таких, які легко маскуються, і водночас, недорогих. Сучасні антенні системи працюють в різних стандартах передачі інформації (WiMAX, EDGE, WCDMA, UMTS, LTE), для кожного з яких виділяються певні частотні канали зв'язку. Природньо, що дослідники звертаються до антен Вівальді. Даний тип антен має достатньо широку смугу пропускання.

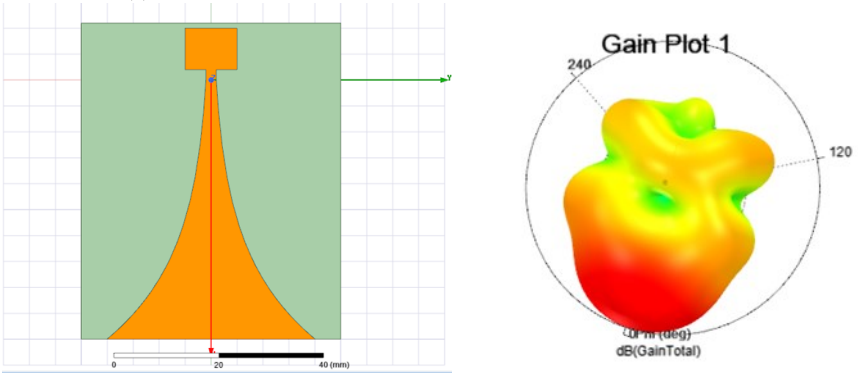
Перевагами антен Вівальді є їх широкосмугові характеристики (необхідні для обробки надширокосмугових сигналів), прості у виготовленні з використанням звичайних методів виробництва друкованих плат і легко узгоджуються з лініями живлення.

Антена Вівальді, або конічна щілинна антена є копланарною широкосмуговою антеою, яка конструктивно виготовляється з з діелектричної пластини, металізованої по обидва боки.

Антени Вівальді можуть бути виготовлені для лінійно поляризованих хвиль або з використанням двох пристроїв, розташованих в ортогональному напрямку - для передачі / прийому поляризації обох орієнтацій. Технологія виготовленя друкованих плат робить цей тип антени технологічно та економічно придатним для частотного мікрохвильового діапазону більше за 1 ГГц.

На рис. 1 зображено топологію антени Вівальді з квадратним збуджуючим резонатором та її 3D діаграму спрямованості, яка розрахована в середовищі електродинамічного симулювання ANSYS HFSS на частоті 2,4 ГГц. На рис. 2 зображено частотні залежності ступеню узгодження антен Вівальді з щілинним, квадратним та круглим резонаторами. Найкращі показники узгодження на частоті 3,35 ГГц має конструкція з квадратним резонатором (фіолетова крива).

Наостанок можна дійти наступних висновків. Внаслідок побудови і дослідження спрямованих властивостей та характеристик узгодження трьох конструкції антен Вівальді з прямокутною, круглою та квадратною формами резонаторів в середовищі ANSYS HFSS в широкому діапазоні частот від 1 до 5 ГГц встановлено, що діаграми спрямованості мають широку головну пелюстку, при цьому форма діаграми та її вторинні параметри слабо залежиать від частоти.



а б

Рисунок 1 – Антена Вівальді (а) та її діаграма спрямованості (б), розрахована в ANSYS HFSS

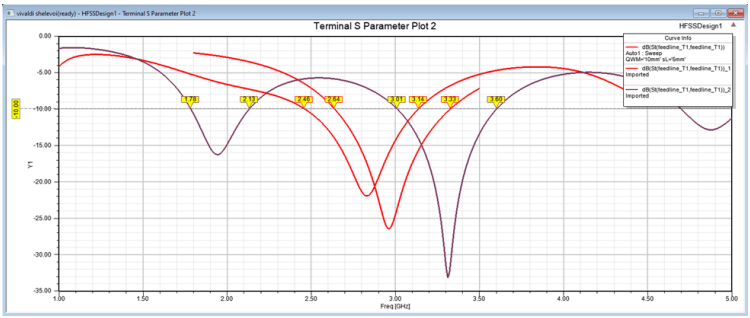


Рисунок 2 – Коефіцієнт відбиття в діаразоні частот 1…5 ГГц

На частоті поблизу 3,3 ГГц отримано найкращі показники КСХ 1.045…1,229 та коефіцієнт відбиття на рівні -23дБ. Коефіцієнти відбиття, КСХ та величина повного імпедансу в першу чергу залежать від лінійних розмірів провідника та діелектрика.

Діаграма спрямованості має велику ширину порядку 120 градусів. Це підтверджує можливість використання антени Вівальді в 4G, 5G мобільних пристроях широкосмугового швидкісного доступу до інтернету, а також в якості елемента антенної решітки в складі репітера WiFi.

УДК 621.791.5
Костенко В.О.[1] , Шведенко В.В.[2]
[1] канд. техн. наук, доц. НУ «Запорізька політехніка»
[2] студ.гр. БК-911сп НУ «Запорізька політехніка»

ОХОРОННА СИГНАЛІЗАЦІЯ НА БАЗІ МІКРОКОНТРОЛЕРА

Впровадження систем охоронної сигналізації є найбільш поширеним засобом, що використовують для охорони приміщень. Основне призначення охоронних систем- виявлення несанкціонованого проникнення у приміщення, і, як наслідок, забезпечення цілісності майна.

На сьогоднішній день технології дозволяють створювати системи, які своєчасно попереджають про проникнення зловмисників в чуже житло.

Різноманітність ситуацій у нашому житті піднімає проблему своєчасного сповіщення. Статистика вказує на те, що навіть наявність простої охоронної системи зменшує ймовірність зазіхань грабіжників на здійснення проникнення на територію, що охороняється.

Для розширення функціональних можливостей і для зниження вартості при розробці охоронної системи варто використовувати мікропроцесори, що

дозволить реалізувати апаратуру з поліпшеними технічними і споживчими характеристиками.

Сьогодні мікроконтролерна техніка є одна з найбільш розвинутих областей сучасної обчислювальної техніки.

Особливістю цього пристрою є простота в обслуговувані та доступність до управління охороною сигналізацією та її контролем.

Мета проекту – створення домашньої охоронної сигналізації на базі мікроконтролера з можливістю самостійної та простої подальшої її модифікації. Бажано також забезпечити високу надійність та низьку вартість даної охоронної сигналізації.

Сучасні охоронні системи скоріше представляють з себе цілий проект з великим набором різноманітних датчиків, з яких можна зібрати велику, надійну та безвідмовну охоронну сигналізацію. Але такі охоронні сигналізації часто не по кишені більшості можливих покупців.

В якості ядра системи обрано мікроконтролер ATTiny 13. Прошивку для МК виконано за допомогою Arduino.

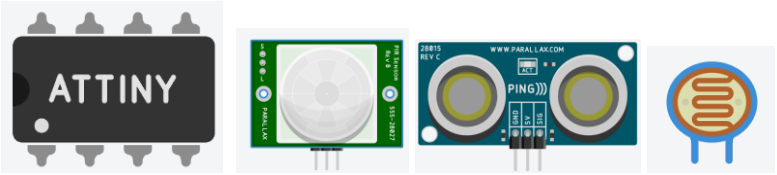


Рисунок 1

Ось необхідні деталі:

1. МК ATtiny 13 - 1 шт.
2. Резистор - 10Ком, 0,125 Вт -1 шт.
3. Резистор - 100-300 Ом, 0,125 Вт - 1 шт.
4. Датчик інфрачервоний
5. Датчик ультразвуковий
6. Фоторезистор
7. Світлодіод
8. Динамік
9. Тримач для елемента живлення типу CR 2024
10. Елемент живлення
11. Монтажна плата

Зав. кафедри Сергій САМОЙЛИК

Відповідальний на факультеті Станіслав ШАПТАЛА

СЕКЦІЯ «ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ЕЛЕКТРОНИХ ЗАСОБІВ»

УДК 519.87
Яковенко В.В.[1],Фурманова Н.І.[2]
[1] д-р техн. наук, проф. НУ «Запорізька політехніка»
[2] канд. техн. наук, доц. НУ «Запорізька політехніка»

ЗАСТОСУВАННЯ МАРКІВСЬКОЇ МОДЕЛІ ДЛЯ ІДЕНТИФІКАЦІЇ СИСТЕМ

Марківська модель – це математична модель, яка описує стохастичний процес, у якому ймовірність переходу системи з одного стану в інший залежить тільки від поточного стану системи, а не від попередніх станів або шляху, яким система досягла поточного стану [1].

Марківські моделі широко використовуються в різних галузях, таких як теорія ймовірностей, математична статистика, економіка, інженерія та біологія, для моделювання випадкових процесів, що мають елемент випадковості та часу.

У марківській моделі визначаються стани системи та ймовірності переходу між ними. Це дозволяє прогнозувати майбутні стани системи на основі поточного та робити рішення, пов'язані з управлінням та оптимізацією.

Марківські моделі також можуть бути використані в системному аналізі для ідентифікації систем [2, 3]. Тут декілька способів їх використання в цьому контексті:

– моделювання структури системи;
– аналіз динаміки системи;
– ідентифікація ключових параметрів;
– прогнозування майбутніх станів системи.

Марківські моделі можуть допомогти визначити структуру системи шляхом аналізу взаємозв'язків між різними станами або компонентами системи. Це може бути корисно для розуміння того, як система працює та які процеси в ній відбуваються.

Марківські моделі можуть допомогти в аналізі динаміки системи, включаючи переходи між станами та ймовірності таких переходів. Це дозволяє отримати уявлення про те, як система реагує на зміни у вхідних даних або умовах.

Марківські моделі можуть допомогти ідентифікувати ключові параметри системи, такі як ймовірності переходів між станами або час перебування в певних станах. Це може бути корисно для подальшого аналізу та управління системою.

На основі марківської моделі можна прогнозувати майбутні стани системи на основі її поточного стану та даних про переходи між станами. Це може бути корисно для планування та управління ресурсами системи.

Загалом, марківські моделі можуть бути потужним інструментом для ідентифікації та аналізу систем, допомагаючи зрозуміти їх структуру, динаміку та ключові параметри.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Gagniuc, Paul A. (2017). Markov Chains: From Theory to Implementation and Experimentation. USA, NJ: John Wiley & Sons. pp. 1–256. ISBN 978-1-119-38755-8.

2. C. Brighenti, B. Wahlberg and C. R. Rojas, "Input design using Markov chains for system identification," Proceedings of the 48h IEEE Conference on Decision and Control (CDC) held jointly with 2009 28th Chinese Control Conference, Shanghai, China, 2009, pp. 1557-1562.

3. Phan, M. Q., Juang, J. N., & Longman, R. E. (1998). Markov parameters in system identification: old and new concepts. In Structronic Systems: Smart Structures, Devices and Systems: Part II: Systems and Control (pp. 263-293).

УДК 528.42:004.9

Костяной П.А.[1],Фарафонов О.Ю.[2]
[1] асп. НУ «Запорізька політехніка»
[2] канд. техн. наук, доц. НУ «Запорізька політехніка»

ЕТАПИ ПОБУДОВИ ТРИВИМІРНОЇ КАРТИ МІСЦЕВОСТІ ЗА ДАНИМИ З БПЛА

Побудова тривимірної карти місцевості з використанням даних, отриманих з безпілотних літальних апаратів (БПЛА) або підводних автономних роботів, є важливою областю досліджень та застосувань у різних сферах, таких як геодезія, картографія, військова справа, екологія та багато іншого [1]. Загальний процес побудови тривимірної карти місцевості можна представити у вигляді послідовності наступних етапів:

– збір даних;
– обробка даних;
– створення хмари точок;
– тріангуляція та побудова моделі;
– візуалізація.

БПЛА або підводні автономні роботи мають різні типи датчиків, такі як камери, лідари (лазерні сканери), радари та інші. Ці датчики

використовуються для збору інформації про поверхню місцевості, рельєф, об'єкти і перешкоди.

Після збору даних необхідно провести їхню обробку для видалення шуму, вирівнювання, фільтрації та об'єднання різних сенсорних потоків. Цей крок включає використання комп'ютерного зору, алгоритмів обробки зображень і обробки сигналів.

Отримані дані зазвичай подаються як хмари точок, де кожна точка має координати (x, y, z) і, можливо, додаткові атрибути, такі як колір або інтенсивність сигналу.

За допомогою алгоритмів тріангуляції та реконструкції поверхні з хмари точок будується тривимірна модель місцевості. Це може бути зроблено шляхом з'єднання точок у трикутники або використання більш складних методів, таких як методи реконструкції сіток. Тріангуляція - це процес поділу простору на набір трикутників, таким чином, щоб усі точки даних знаходилися всередині цих трикутників, і кожна точка даних є вершиною хоча б одного трикутника. Існує кілька методів тріангуляції, включаючи алгоритм Делоне та алгоритми Вороного. Зазвичай у контексті побудови тривимірних моделей місцевості використовується алгоритм Делоне, який будує тріангуляцію таким чином, щоб мінімізувати кути трикутників та забезпечити їх максимальну однорідність. Після виконання тріангуляції кожен трикутник є поверхневою частиною моделі місцевості. Однак для створення повноцінної тривимірної моделі потрібно більше інформації, ніж просто набір трикутників. Зазвичай використовується алгоритм реконструкції поверхні з хмари точок, що апроксимує поверхню місцевості на основі наявних даних. Цей алгоритм може використовувати різні методи, такі як інтерполяція, фільтрація, згладжування та інші, щоб створити більш точну та реалістичну модель місцевості. Під час побудови моделі місцевості враховуються різні особливості, такі як рельєф, об'єкти, перешкоди і т. д. Для цього можуть використовуватися додаткові дані, наприклад, дані з камер або інших сенсорів. Це дозволяє створити більш детальну та корисну модель, яка може бути використана для різних цілей, від навігації до аналізу середовища.

Зшиття двох відсканованих карт, отриманих з різних датчиків, відбувається за допомогою процесу, який називається реєстрацією даних. Цей процес включає кілька етапів. Спочатку відбувається знаходження спільних точок на обох картах, які можуть бути використані для вирівнювання карт. Далі використовуються математичні моделі для трансформації однієї карти так, щоб вона відповідала іншій. Це може включати масштабування, обертання та зсув. На етапі оптимізації відбувається підбір параметрів трансформації для мінімізації розбіжностей між картами. Далі виконується об’єднання даних з обох карт у єдину

інтегровану карту. Для цього процесу часто використовуються спеціалізовані програмні засоби та алгоритми комп'ютерного зору. Важливою частиною є також калібрування обладнання, щоб забезпечити точність даних.

Після побудови моделі місцевості її можна візуалізувати за допомогою спеціалізованих програмних засобів, таких як ГІС (геоінформаційні системи), CAD (комп'ютерне архітектурне проектування) або спеціалізовані програми для роботи з тривимірними даними. Це дозволяє користувачам досліджувати місцевість, виконувати аналіз даних та приймати рішення на основі отриманої інформації. Таким чином, тріангуляція і побудова моделі місцевості є ключовим процесом у створенні тривимірних карт з використанням даних, отриманих з безпілотних літальних апаратів або підводних автономних роботів.

Для кожного з цих етапів існують різні методи та алгоритми, а також різні програмні та апаратні засоби, які можуть бути використані залежно від конкретних вимог проекту та характеристик середовища.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Андрєєв, С. М., Жилін, В. А. (2019). Застосування даних аерофотозйомки з безпілотних літальних апаратів для побудови 3d-моделей місцевості. Системи управління, навігації та зв'язку. Збірник наукових праць. 1. 3-16.

УДК 621.391
Онищенко В.Ф.[1],Магльованний В.А.[2]
[1] канд. фіз.-мат. наук, доц. НУ «Запорізька політехніка»
[2] асп. НУ «Запорізька політехніка»

НАПРЯМКИ ЗАСТОСУВАННЯ НЕЙРОННИХ МЕРЕЖ У СИСТЕМАХ ДОНАВЕДЕННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

Використання нейронних мереж у системах донаведення безпілотних літальних апаратів (БПЛА) може відбуватися на різних рівнях і відігравати різні ролі в залежності від конкретних завдань і умов застосування.

Одним із типів застосування нейронних мереж є використання їх для обробки сигналів, отриманих від різних сенсорів на БПЛА. Наприклад, нейронні мережі можуть бути використані для обробки візуальної інформації з камер або зі супутників для автоматичного визначення об'єктів на місці призначення, виявлення перешкод або різних образів.

Також нейронні мережі можуть використовуватися для управління самим БПЛА. Наприклад, нейронні мережі можуть бути використані для

автопілоту, який визначає оптимальний шлях польоту, уникнення перешкод або реагування на зміни в навколишньому середовищі.

Іншим важливим аспектом є використання нейронних мереж для вдосконалення систем штучного інтелекту, які відповідають за прийняття рішень у реальному часі на основі отриманих даних. Наприклад, це може бути система, яка аналізує ситуацію, засновану на даних з різних джерел, і приймає рішення про подальші кроки або давати рекомендації пілоту або оператору.

Ось декілька напрямки, які можуть бути застосовані при використанні нейронних мереж у системах донаведення БПЛА:

– автономне навігаційне планування;

– виявлення та відстеження об'єктів [1];

– автопілот та донаведення [2];

– уникнення зіткнень;

– оптимізація використання палива.

Нейронні мережі можуть використовуватися для розв'язання складних задач навігації та планування маршрутів у реальному часі. Вони можуть адаптуватися до змінних умов навколишнього середовища та враховувати різноманітні фактори, такі як погодні умови, перешкоди тощо.

Нейронні мережі можуть бути навчені виявляти та відстежувати об'єкти на землі або в повітрі, що може бути корисним для місій розвідки, пошуку та рятування, моніторингу тощо.

Нейронні мережі можуть бути використані для реалізації автопілота та систем донаведення, що дозволяє БПЛА автоматично коригувати свій курс, висоту та швидкість для досягнення поставленої мети.

Нейронні мережі можуть аналізувати оточуюче середовище та передбачати можливі зіткнення з іншими об'єктами або літальними апаратами, допомагаючи уникнути аварій.

Штучні нейронні мережі можуть бути використані для оптимізації маршрутів та управління енергозбереженням, що дозволяє ефективніше використовувати ресурси палива.

Ці техніки можуть допомогти покращити автономність, ефективність та безпеку дії безпілотних літальних апаратів у різних областях застосування, включаючи військове, цивільне та комерційне використання.

Загалом, використання нейронних мереж в системах донаведення БПЛА може покращити їхню продуктивність, точність і надійність у різних умовах і сценаріях застосування.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Фесенко, О. Д., Бєляков, Р. О., Радзівілов, Г. Д., & Гулій, В. С. (2020). Експериментальний аналіз застосування нейронних мереж для керування траєкторією польоту БПЛА. Збірник наукових праць ВІТІ, 1, 97-112.

2. Журавська, І. М. (2018). Генерація субоптимальних маршрутів безпілотного літального апарата з використанням нейронної мережі Хопфілда. Проблеми інформаційних технологій, (1), 181-185.

УДК 004.94

Баранов Є.О.[1], Малий О.Ю.[2]

[1] асп. НУ «Запорізька політехніка»

[2] канд. техн. наук, доц. НУ «Запорізька політехніка»

МЕТОДИ ЗАБЕЗПЕЧЕННЯ АВТОНОМНОГО ВИКОНАННЯ ЗАВДАНЬ БЕЗПІЛОТНИМИ ЛІТАЛЬНИМИ АПАРАТАМИ В УМОВАХ ОБМЕЖЕНОГО АБО ВІДСУТНЬОГО ДОСТУПУ ДО GPS

Забезпечення автономного виконання завдань безпілотними літальними апаратами (БПЛА) в умовах обмеженого або відсутнього доступу до GPS та віддаленого керування є дуже актуальною та викликає великий інтерес в галузі авіаційних технологій та робототехніки (табл. 1). Наведемо перелік рішень, які можуть застосовуватись для цієї теми [1]:

– інерційні навігаційні системи (INS) не залежать від зовнішніх сигналів і можуть використовуватися для визначення положення, орієнтації та швидкості БПЛА на основі даних про прискорення та кутові швидкості, що отримуються від гіроскопів та акселерометрів;

– візуальна навігація (VSLAM – Visual Simultaneous Localization and Mapping) дозволяють БПЛА орієнтуватися у просторі, аналізуючи зображення з камер. Алгоритми VSLAM створюють та оновлюють карту навколишнього середовища в реальному часі, водночас визначаючи місцезнаходження апарату відносно цієї карти;

– лідари та радари – це сенсори можуть використовуватися для отримання інформації про відстані до об'єктів навколо БПЛА, що допомагає в уникненні перешкод і пілотуванні в складних умовах.

– алгоритми машинного навчання та штучного інтелекту може підвищити здатність БПЛА до самонавігації, самостійного вирішення завдань та адаптації до змінних умов середовища.

– резервні системи навігації та зв'язку можуть використовуватись для підвищення надійності та безпеки БПЛА, такі як UHF/VHF радіо, які менш чутливі до загороджень або перешкод.

Таблиця 1 дає змогу краще зрозуміти, які технології та методи можуть бути використані для забезпечення ефективної роботи БПЛА в умовах, коли стандартні системи навігації та керування недоступні або неефективні [2].

Таблиця 1 - Методи навігації та управління БПЛА у відсутності доступу до GPS та віддаленого керування:

Метод	Застосування	Переваги	Технології, що використовуються
Інерційні навігаційні системи (INS)	Орієнтування та позиціонування БПЛА без зовнішніх сигналів.	Незалежність від зовнішніх сигналів, висока точність на короткі відстані.	Гіроскопи, акселерометри.
Візуальна навігація (VSLAM)	Орієнтування в навколишньому середовищі за допомогою візуальної інформації.	Висока точність в добре освітлених умовах, можливість мапування території.	Камери, алгоритми обробки зображень, комп'ютерний зір.
Лідари та радари	Визначення відстаней до об'єктів та уникнення перешкод.	Висока точність у визначенні відстаней, ефективність в умовах поганої видимості.	Лідарні та радарні сенсори.
Машинне навчання та ШІ	Адаптація до змінних умов, самостійне вирішення задач.	Здатність до навчання та адаптації, покращення рішень з досвідом.	Нейронні мережі, алгоритми глибокого навчання.
Резервні системи зв'язку	Забезпечення зв'язку в умовах збоїв стандартних систем.	Надійність, здатність до роботи в умовах перешкод.	UHF/VHF радіо, альтернативні методи передачі даних.

Описані методи та технології дозволяють БПЛА виконувати складні завдання в умовах, коли традиційні методи навігації та керування недоступні або ненадійні. Розробка та впровадження таких систем вимагає глибоких знань у сфері робототехніки, штучного інтелекту та інженерії.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Saeed Faizi F., Khorsheed Alsulaifanie A. Visual-Based Simultaneous Localization and Mapping (VSLAM) Techniques for Robots: A Scientific Review. Academic Journal of Nawroz University. 2023. Vol. 12, no. 3. P. 213–229. URL: https://doi.org/10.25007/ajnu.v12n3a1500

2. Szántó M., Bogár G. R., Vajta L. ATDN vSLAM: An All-Through Deep Learning-Based Solution for Visual Simultaneous Localization and Mapping. Periodica Polytechnica Electrical Engineering and Computer Science. 2022. Vol. 66, no. 3. P. 236–247. URL: https://doi.org/10.3311/ppee.20437

УДК 004.94

Гаврилюк А.О.[1], Малий О.Ю.[2]

[1] асп. НУ «Запорізька політехніка»

[2] канд. техн. наук, доц. НУ «Запорізька політехніка»

МЕТОДИ ОБМІНУ ДАНИМИ З БПЛА ІМПУЛЬСНИМИ ПАКЕТАМИ З ПСЕВДОВИПАДКОВИМ ПЕРЕМИКАННЯМ КАНАЛІВ ЗВ'ЯЗКУ

Обмін даними з безпілотними літальними апаратами (БПЛА) за допомогою імпульсних пакетів з псевдовипадковим перемиканням каналів зв'язку є досить актуальною і цікавою в сучасних дослідженнях у галузі безпеки та ефективності телекомунікацій. Цей метод може бути використаний для підвищення надійності та безпеки передачі даних, зокрема у випадках, коли БПЛА використовуються в складних умовах або у середовищах із високим рівнем електромагнітних завад [1].

Імпульсні пакети (або імпульсно-пакетна модуляція) передбачають передачу інформації за допомогою коротких імпульсів на високій швидкості, що зменшує ймовірність перехоплення і підвищує ефективність використання спектру [2].

Псевдовипадкове перемикання каналів зв'язку дозволяє змінювати частоту передачі даних випадковим образом, що ускладнює завдання потенційних атак на зв'язок, оскільки атакуючій стороні потрібно вгадати правильну частоту для перехоплення сигналу [3].

Разом ці технології можуть формувати потужний засіб для забезпечення безпеки та надійності в системах зв'язку БПЛА, особливо у місіях, де є значні ризики щодо безпеки даних або потреби у високій пропускній здатності. Це важливо як для військових, так і для цивільних застосувань, де БПЛА виконують критичні задачі, такі як моніторинг навколишнього середовища, пошук і рятування, або дистанційне зондування.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Grubesic T. H., Nelson J. R., Wei R. UAV Operating Environments. UAVs for Spatial Modelling and Urban Informatics. Cham, 2024. P. 17–32. URL: https://doi.org/10.1007/978-3-031-54114-8_2 2.

2. UAV-ENeRF: Text-driven UAV Scene Editing with Neural Radiance Fields / Y. Wang et al. IEEE Transactions on Geoscience and Remote Sensing. 2024. P. 1. URL: https://doi.org/10.1109/tgrs.2024.3379649 (

3. Ye J., Si Y., Pan G. UAV-to-UAV Communications. UAV Communications: Modeling and Analyses. Singapore, 2024. P. 87–112. URL: https://doi.org/10.1007/978-981-97-0383-8_3

УДК 004.94

Левченко Д.С.[1], Малий О.Ю.[2]

[1] асп. НУ «Запорізька політехніка»

[2] канд. техн. наук, доц. НУ «Запорізька політехніка»

ОГЛЯД МЕТОДІВ ОБРОБКИ ДАНИХ З БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

Використання безпілотних літальних апаратів (БПЛА) у зйомці території представляє трансформаційний підхід до збору геопросторових даних, пропонуючи значне підвищення точності, ефективності та економічності порівняно з традиційними методами. У роботі досліджуються останні досягнення в технологіях БПЛА, зосереджуючись на їх інтеграції в геодезичну практику, розробці спеціалізованих алгоритмів для обробки даних і потенційних наслідках для майбутніх стратегій землеустрою [1].

Традиційні методи землевпорядкування часто вимагають багато часу, праці та обмежені фізичними обмеженнями місцевості. Поява технології БПЛА запровадила багатообіцяючу альтернативу, здатну збирати дані високої роздільної здатності у важкодоступних або небезпечних районах [2].

Технології моніторингу, що використовуються в аерознімальних системах на борту БПЛА, базуються на кількох ключових властивостях. Перша з них - це сприйняття, яке означає здатність аерознімального комплексу розпізнавати важливу інформацію від власних датчиків. Це допомагає БПЛА розуміти свій стан і стан навколишнього середовища. Дані про місцеположення під час знімання, маршрут польоту та інші допомагають уточнити сприйняття зніманих матеріалів. Як автономний агент, БПЛА має бути свідомим свого стану, свого розташування в просторі, зовнішніх умов і картографії, що в кінцевому підсумку сприяє оптимальному плануванню траєкторій і розробці програм для обробки даних. Планування включає в себе визначення оптимального часу для знімань, вибір обладнання, порядок

проведення зйомок і методики їх обробки з метою задоволення потреб замовника.Керування полягає у вмінні БПЛА виконувати заплановані дії. У контексті аерознімання це також включає завдання по локалізації і відображенню, які тісно пов'язані між собою [3].

У рамках методичних досягнень в галузі застосування БПЛА значний прогрес було досягнуто в автоматизації польотів і збору даних. Удосконалення програмного забезпечення для планування польотів дозволяє тепер програмувати траєкторії польоту дронів, які можуть автоматично покривати визначені зони огляду з мінімальним втручанням людини. Ця автоматизація відіграє ключову роль у зборі послідовних та вичерпних наборів даних. Одночасно, основним напрямком досліджень стала розробка алгоритмів для ефективної обробки цих об'ємних даних. Ці алгоритми фокусуються на покращенні швидкості та точності перетворення необроблених даних датчиків у формати, придатні для подальшого використання, а також на покращенні виявлення різноманітних особливостей та оптимізації процесів зберігання даних.

Перелічимо декілька ключових типів алгоритмів, які часто використовуються в цій галузі:

– фотограмметрія використовує зображення з кількох точок зору для створення 3D-моделей місцевості. Він особливо корисний для точного моделювання і вимірювання великих територій;

– LiDAR обробка даних включає аналіз великої кількості точок, зібраних за допомогою лазерного сканування, для створення детальних 3D карт та моделей;

– класифікація образів за допомогою технік машинного навчання та глибокого навчання аналізує зображення для ідентифікації та класифікації об'єктів на землі, наприклад, рослинності, будівель та водних шляхів;

– алгоритми часових рядів використовуються для аналізу змін, які відбулися на ділянці протягом часу, з допомогою послідовних польотів БПЛА, що дає змогу моніторити зміни у рослинності, ерозію ґрунту та інші екологічні параметри;

– геопросторовий аналіз включає обробку даних GPS та інших локаційних даних для визначення точних координат об'єктів на землі, важливих для картографічних та землевпорядних застосувань;

– аналіз текстур і шаблонів використовується для визначення характеристик поверхонь за зображеннями, отриманими з БПЛА. Це може допомогти в ідентифікації різних типів рослинності, стану ґрунтів, та інших природних чи штучних об'єктів.

Кожен з цих алгоритмів має свої специфікації та краще підходить для певних типів даних та завдань, забезпечуючи широкий спектр інструментів для ефективного аналізу та використання інформації, отриманої з БПЛА.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Регулювання крену бпла із застосуванням прогнозуючої моделі / M. Denysenko та ін. Системи управління, навігації та зв'язку. Збірник наукових праць. 2023. Т. 1, № 71. С. 15–18. URL: https://doi.org/10.26906/sunz.2023.1.015

2. Застосування БПЛА для медичної евакуації пацієнтів / A. Humennyi та ін. Aerospace technic and technology. 2023. № 6. С. 5–13. URL: https://doi.org/10.32620/aktt.2023.6.01

3. Іщенко В. Підвищення ефективності систем візуальної навігації бпла. Наукові перспективи (Naukovì perspektivi). 2021. № 6 (12). URL: https://doi.org/10.52058/2708-7530-2021-6(12)-23-31

УДК 004.93

Малий О.Ю.[1], Мірошніченко В.В.[2]

[1] канд. техн. наук, доц. НУ «Запорізька політехніка»

[2] асп. НУ «Запорізька політехніка»

АВТОМАТИЗОВАНИЙ РЕВЕРС ІНЖИНІРИНГ ДРУКОВАНИХ ПЛАТ З ВИКОРИСТАННЯ КОМП'ЮТЕРНОГО ЗОРУ

У деяких випадках єдиним способом отримати дизайн оригінального продукту є зворотне проектування. Для деяких старих продуктів, які не вироблялися 20 і більше років, оригінальні 2D-креслення більше не доступні. Часто відсутня можливість зв'язатися з оригінальним виробником, оскільки компанія вже не працює.

Зворотне проектування друкованої плати — це процес аналізу існуючої друкованої плати (PCB) і відтворення її конструкції для створення нової, функціонально еквівалентної версії. Цей процес складається з кількох кроків, включаючи вилучення схематичних діаграм, реконструкцію макета друкованої плати та створення списку матеріалів (BOM).

В роботі розглянуто розробку зворотної розробки друкованих плат з використанням комп'ютерного зору для забезпечення можливості ідентифікації електронних компонентів, визначення написів на них, виявлення малюнку доріжок.

Під час розробки задачу було розбито на підзадачі:

– розробка алгоритмів для кадрування RoI та вирівнювання багатошарової друкованої плати;

– реалізація алгоритму глибокого навчання для виявлення та локалізації компонентів.

– розробка класичних алгоритмів обробки зображень для покращення та доповнення виявлення компонентів;

– розробка методу сегментації зображення для виявлення металу внутрішнього шару;

– розробка процесу вилучення інформації про з'єднання елементів схеми;

– оцінка ефективності виявлення компонентів.

У проекті є три основні частини:

– попередня обробка зображення друкованої плати, під час якої кожен шар друкованої плати вирівнюється, а RoI обрізаються для наступного процесу;

– виявлення та локалізація електронних компонентів;

– сегментація металу внутрішнього шару та вилучення інформації про з'єднання.

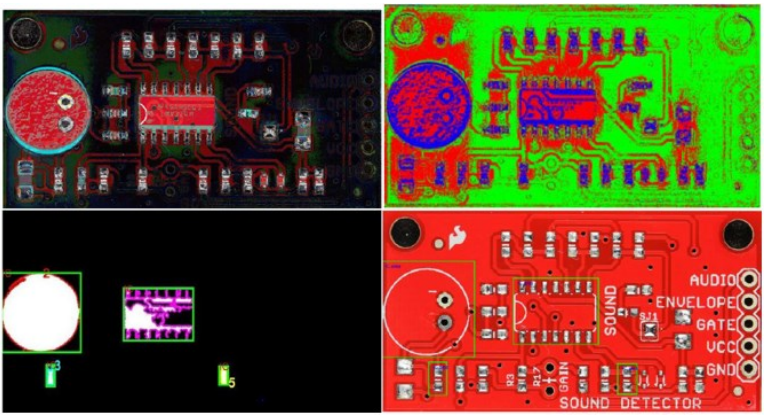


Рисунок 1 – Кластеризація друкованої плати

Реальні зображення друкованих плат можуть бути зібрані не на стандартному рівні горизонту/вертикалі, як наші шаблонні зображення які отримувалися на плоскому чорному пластиковому полі. Це спричинить помилку зіставлення шаблону через значну різницю в кореляційній карті. Ми пропонуємо метод корекції, заснований на техніці зіставлення шаблонів і реєстрації зображень.

Робота спрямована на отримання інформації про схему із зображень друкованої плати. В роботі ми зосередилися на виявленні електронних компонентів і з'єднанні внутрішніх шарів. Була застосовано передові методи виявлення об'єктів і запропонована стійка генеративна система, яка може використовувати результат для покращення навчальної бази даних класифікації зображень електронних компонентів.

Запропонована нами обробка зображень друкованої плати не адаптується автоматично до різної якості зображення, як-от умови освітлення, проблеми фону та тіні компонентів. Хоча в реальних галузевих випадках важко забезпечити, щоб усі вхідні дані були уніфіковані в стандартній вимозі.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Herchenbach, D,, Li, W., and Breier, M. (2013). Segmentation and classification of THCs on PCBAs. In IEEE International Conference on Industrial Informatics, pages 59-64.

2. Lu, H.; Mehta, D.; Paradis, O.P.; Asadizanjani, N.; Tehranipoor, M.; Woodard, D. FICS-PCB: A Multi-Modal Image Dataset for Automated Printed Circuit Board Visual Inspection. IACR Cryptol. ePrint Arch. 2020, 2020, 366.

УДК 621.391

Малий О.Ю.[1], Онуфрієв М.С.[2]
1 канд. техн. наук, доц. НУ «Запорізька політехніка»
2 асп. НУ «Запорізька політехніка»

ВИКОРИСТАННЯ ЗСУВУ ЧАСТОТИ ДЛЯ ЗБІЛЬШЕННЯ КІЛЬКОСТІ КАНАЛІВ БЕЗДРОТОВИХ АНАЛОГОВИХ ВІДЕОПЕРЕДАВАЧІВ

Бездротове передавання відеосигналу є одним з основних функціональних потреб для здійснення керування БПЛА, робототехнічними наземними та неводними системами, пристроями віддаленого візуального контролю виробництва. В поточний момент на ринку представлено велика кількість передавачів аналогового відеосигналу для БПЛА, але всі вони працюють в двох діапазонах (1,3 та 5,8 ГГц) з обмеженою кількістю каналів.

В роботі пропонується розробка мільтичастотного бездротового відеопередавача аналогового сигналу з можливістю переналаштування частоти та на основі доступних на цивільному ринку компонентів.

Для розробки власного відеопередавача було проведено аналіз структури і схемотехнічних рішень побудови існуючих аналогових передавачів відеосигналу.

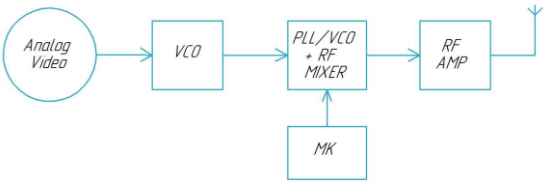


Рисунок 1 – Структурна схема відеопередавача

Аналоговий відеосигнал потрапляє на генератор, керований напругою де отримає несучу частоту порядку сотен МГц (встановлюється при схемотехнічному налаштуванні), цей сигнал подається на мікшер, множник частоти з власним генератором керованим напругою.

Генератор, керований напругою (ГКН; англ. VCO) - електронний генератор, частота коливань якого залежить від керуючої напруги яка подається на нього. Мікшер та вбудований генератор керуються мікроконтролером, що дозволяє змінювати режими роботи і частоту сигналу з яким буде складатися частота на вході і відповідно змінювати несучу частоту кінцевої радіопередачі. Після частотних маніпуляцій сигнал передається на підсилювач потужності та випромінюється.

Не дивлячись на те що звісно у цій структурній схемі всіма налаштуваннями керує мікроконтролер – він не є основним елементом адже навіть при його відсутності якщо сигнал після вхідного генератора, що керується напругою потрапить на підсилювач, він вже буде мати несучу, що відповідає налаштованій частоті генератору. Частина схеми, що містить в собі мікшер та мікроконтролер необхідна для зміни частоти відеопередавача, а також може керувати потужністю випромінювання змінюючи поточну вихідну потужність підсилювача.

З цього випливає, що основним елементом передавача є модулятор та генератор, керований напругою. Модулятор застосовується стандартний, а ось генератор, керований напругою було обраних з числа тих, що не зустрічались у відомих передавачах аналогового відеосигналу.

У якості вхідного генератора, керованого напругою було обрано мікросхему MAX2608. У якості мікшера було обрано мікросхему RF2052. Використання цього мікшера дозволить регулювати частоту відеопередавача в діапазоні 30-2500 МГц.

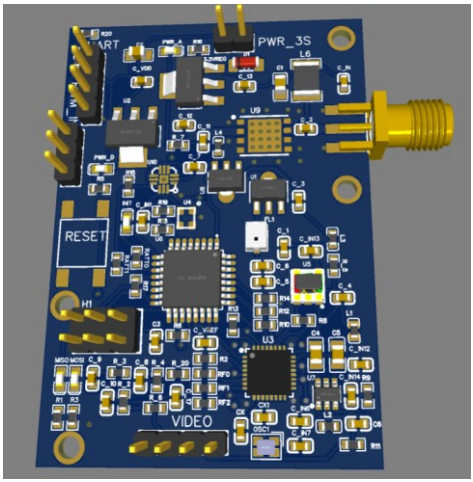


Рисунок 2 – 3Д модель розробленої друкованої плати з встановленими на неї елементами

В роботі проведено аналіз сигналів, що поступають з камер на передавачі аналогового відео, проаналізовано частотні канали стандартних цивільних відеопередавачів аналогового відеосигнала, що використовуються в БПЛА, проведено аналіз структури та схемотехнічних рішень побудови відеопередавачів аналогового відеосигналу, розроблено методику зсуву несучої частоти передавання аналогового відеосигналу.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. T. Nguyen and A. Zakhor, “Multiple sender distributed video streaming,” Multimedia, IEEE Transactions on, vol. 6, pp. 315 – 326, april 2004

УДК 621.396

Malyi O.Y.[1], Chornoborodov M.P.[2], Vychuzhanina S.A.[3]
[1] PhD (Technical Science), assistant professor NU «Zaporizhzhia Polytechnic»
[2] PhD (Technical Science), assistant professor NU «Zaporizhzhia Polytechnic»
[3] PhD student NU «Zaporizhzhia Polytechnic»

POLYPHASE CODE SEQUENCES WITH OPTIMAL AUTOCORRELATION FUNCTION

A phase-shift keyed (PSK) signal is a sequence of N rectangular radio pulses of the same duration and amplitude. The law of change of the initial phase φ of

each partial radio pulse determines the shape of the autocorrelation function (ACF) of the PSK-signal and the structure of its compression filter. Changing the initial phase φ according to the Barker code by 180º determines the optimal ACF with a simple matches filter structure. Though Barker codes are known only for unique phase sequences of 3, 4, 5, 7, 11 and 13 pulses. For the remaining N values, no signal structure consistent with the structure of the Barker filter has been found.

An alternative to finding pseudo-noise sequences with optimal ACF is to switch to other values of the initial phase shift. In this case, the coherent accumulation of the main lobe of the compressed signal will be possible only by complicating the matched filter, in which the weights will be not ± 1, but a complex conjugate harmonic function.

Table 1 shows the new phase sequences φ_i and the levels of the ACF lobes y_i. The known 180º-phase Barker sequences, which can also be compressed by a complex matched filter, are not listed here.

Table 1 – Phase sequences φ_i and the levels of the ACF lobes y_i

Code No	N	φ_1	φ_2	φ_3	φ_4	φ_5	φ_6	φ_7	y_1	y_2	y_3	y_4	y_5	y_6	y_7	y_8	y_9	y_{10}	y_{11}	y_{12}	y_{13}
3-2-1	3	120	0	0					-1	1	3	1	-1								
3-3-1	3	0	60	0					1	1	3	1	1								
3-3-2	3	0	90	0					1	0	3	0	1								
3-3-3	3	0	120	0					1	1	3	1	1								
4-3-1	4	0	120	0	0				1	1	0	4	0	1	1						
4-6-1	4	0	90	90	0				1	0	1	4	1	0	1						
4-6-2	4	0	120	120	0				1	1	0	4	0	1	1						
5-10-1	5	0	120	120	120	0			1	1	0	1	5	1	0	1	1				
7-23	7	0	120	0	120	120	0	0	1	1	0	1	1	0	7	0	1	1	0	1	1

On the basis of research of statistical parameters and characteristics of detection of the synthesized phase sequences the conclusion on possibility of expansion of an ensemble of PSK-signals with optimum ACF from 7 pieces is made (Barker codes) up to 16 pieces (see table).

The expansion of the ensemble of phase-code-manipulated signals has became possible due to the transition to the use of phase change from 0º to an angle of 60º, 90º, 120º or 180º depending on the sequence.

УДК 681.865.8
Єфименко.М.В.[1], Бойко.Е.О.[2]
[1] д-р техн. наук, проф. НУ «Запорізька політехніка»
[2] студ. гр. БК-612м НУ «Запорізька політехніка»

УПРАВЛІННЯ ТРАЄКТОРІЄЮ ПОЛЬОТУ КВАДРОКОПТЕРА

Отримано математичну модель квадрокоптера як об'єкта управління. Модель має наступний вигляд:

$$m\ddot{r}_E = F_E, \qquad F_E = P_E + G_E$$

$$P_E = k_p(\omega_1^2 + \omega_2^2 + \omega_3^2 + \omega_4^2)n_E \qquad n_E = \tilde{\Lambda}_{BE} \circ n_B \circ \Lambda_{BE}$$

$$n_{B=}\begin{pmatrix}0\\1\\0\end{pmatrix} \qquad G_E = mg\begin{pmatrix}0\\-1\\0\end{pmatrix}$$

$$J\dot{\omega}_B^{BE} = -\omega_B^{BE} \times J\omega_B^{BE} + M_u \qquad 2\dot{\Lambda}_{EB} = \Lambda_{EB} \circ \omega_B^{BE},$$

$$M_u = \begin{pmatrix}\omega_{Bz}^{BE}\\0\\-\omega_{Bx}^{BE}\end{pmatrix}(\omega_1 + \omega_3 - \omega_2 - \omega_4) + R\begin{pmatrix}\omega_1^2\\\omega_2^2\\\omega_3^2\\\omega_4^2\end{pmatrix},$$

$$R = \begin{pmatrix}k_p\ell & 0 & -k_p\ell & 0\\-k_m & k_m & -k_m & k_m\\0 & k_p\ell & 0 & -k_p\ell\end{pmatrix}.$$

В моделі E – земна система координат, B – жорстко зв'язана з ЛА система координат, Λ_{EB} - кватерніон переходу від земного базису E до зв'язаного базису B, r_E – вектор r, що задає положення центру мас квадрокоптера проекціями на осі базису E; ω_B^{BE} – вектор кутової швидкості обертання базису B відносно базису E, заданий проекціями на осі базису B; J – тензор інерції рами квадрокоптера; $\circ$ – символ кватерніонного множення; $\sim$ – позначення сполученого кватерніону; m – маса квадрокоптера; ω_i, i=1,2,3,4 – кутові швидкості обертання повітряних гвинтів, l, k_m – задані постійні коефіцієнти, g=9.81 м/с^2 – прискорення сили тяжіння на Землі.

На основі розробленої моделі отримані алгоритми управління просторовим рухом квадрокоптера а саме алгоритм визначення необхідного напрямку сили тяги гвинтів для переведення квадртреокоптера з поточного положення в задане та алгоритми управління кутовим рухом квадрокоптера,

які забезпечують збіг реального напрямку сили тяги гвинтів з розрахунковим та стабілізацію кута нишпорення. Розрахунковий напрям сили тяги гвинтів $\vec{n_B^*}$ за рахунок наявності збурюючих сил може відрізняється від реального напряму $\vec{n_B}$. Для усунення цього явища у відомий аналітичний алгоритм рішення двоточкової крайової задачі [1] додано стабілізуючу складову у вигляді зворотного зв'язку за станом. Це значно покращало точність наведення квадрокоптера у задане положення. На основі динамічного рівняння для кватерніона [2] запропоновано оригінальні алгоритми управління кутовим рухом квадрокоптера, які забезпечують збіг реального напрямку сили тяги гвинтів з розрахунковим і стабілізацію з відносно земної системи координат. Розроблені алгоритми дозволяють реалізувати всі основні режими автономного польоту: режим стабілізації в якому літальний апарат автоматично підтримує нульовий крен, тангаж та стабілізує кут курсу; режим утримання заданого положення в якому апарат автоматично зависає над заданою точкою земної поверхні; режим автоматичного польоту за точками; режим автоматичного зльоту та посадки. Результати моделювання показали працездатність розроблених алгоритму та можливість їх реалізації.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. О.К. Новіков, Синтез оптимальных управлений на основе аналитического решения линейной стационарной двухточечной краевой задачи *Радіоелектроніка Інформатика Управління*. 2006. № 2. С. 133–156.

2. N. Yefymenko , R. Kudermetov , Quaternion models of a rigid body rotation motion and application for spacecraft attitude control , Acta Astronautica , 194 (2022) 76-82.

УДК 629.762
Малий О.Ю.[1], Моїсеєв В.Є.[2]
[1] канд. техн. наук, доц. НУ «Запорізька політехніка»
[2] студ. гр. БК-612м НУ «Запорізька політехніка»

НАВЕДЕННЯ БПЛА КВАДРОКОПТЕРНОГО ТИПУ НА РУХОМІ ОБ'ЄКТИ ПІД ЧАС ПОЛЬОТУ

Суворіший нагляд за використанням приватних дронів мотивується численними інцидентами за участю невеликих дронів, зазвичай керованих дистанційно, в громадських місцях. Потенційним вирішенням може стати захоплення чи виведення з ладу несанкціонованих БПЛА. Сучасні технології боротьби з БПЛА існують здебільшого у військовому секторі у вигляді засобів РЕБ або засобів ураження з поверхні землі. Потрібне рішення, яке

буде досить гнучким, щоб захопити широкий спектр БПЛА в місцевому повітряному просторі.

БПЛА квадрокоптерного типу мають високу маневреність з 4 ступенями свободи і можуть розганятися до високих швидкостей до цілі з невідомим планом польоту чи характеристиками.

Залежно від розміру та форми цілі (наприклад, нерухоме крило, мультиротор, вертоліт, дирижабль), а також відстані до неї не можна припускати, що 3D-датчик, такий як лідар або стереоскопічний зір, може використовуватися для точної локалізації цілі у просторі. Наприклад, через їх рідкісні, а іноді й сітчасті рами, мультикоптери особливо складно локалізувати за допомогою дешевих скануючих лідарів або стереокамер на великій відстані. Таким чином, основна увага в роботі приділяється використанню монокулярного зору та адаптації методів наведення для використання лише приблизних оцінок глибини, коли це необхідно.

На рис. 1 показано плавну траєкторію, створену шляхом відстеження шляхів, згенерованих примітивами руху. Спочатку знаходимо індексований за часом мінімальний шлях прибуття, який може виявитися неможливим для польоту квадрокоптера, а потім формуємо коридор польоту у вільному просторі, в якому генеруємо допустиму траєкторію. Використовується поліноміальний базис Бернштейна і представляємо траєкторію у вигляді шматкової кривої Безьє.

Кольорові лінії становлять окремі примітиви руху. Квадрокоптер відстежує початкову частину кожної згенерованої траєкторії, утворюючи повну зшиту траєкторію, представлену чорною лінією.

Щоб йти по траєкторіях, контролери вибирають бажану траєкторію, що зазвичай складається з колійних точок, кожна з яких має відповідну швидкість, і видають команди приводу квадрокоптеру. Це було продемонстровано на відкритому повітрі з точністю до 50 см.

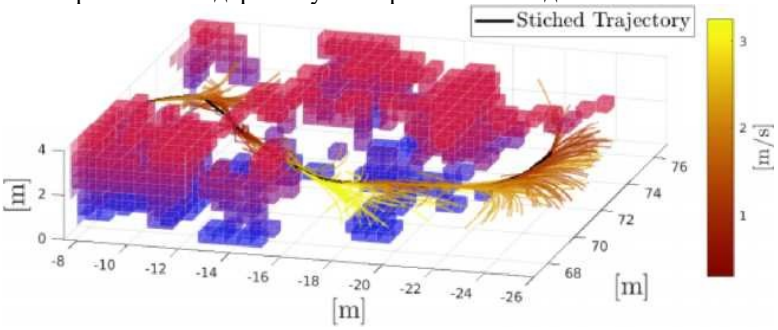


Рисунок 1 – Приклад складених траєкторій у захараченому середовищі

Стосовно квадрокоптера в цій роботі вектор прискорення подається в контролер швидкості шляхом інтеграції команди, яка передає команди крену, тангажу, відхилення від курсу та тяги внутрішнім контролерам автопілоту. Таким чином, замість того, щоб коригувати курс задоволення бічних прискорень, застосування TPN в цій роботі засноване на контролі кута крену.

У своїй найпростішій формі прогнозування руху цілі включає оцінку швидкості цілі в 3D, розрахунок майбутнього розташування мети по прямолінійному шляху і створення траєкторії курсу зіткнення до цієї точки простору зі швидкістю, яка завершує траєкторію. у вказаний час. Цей метод робить три важливі припущення: (i) ціль має нульове прискорення, (ii) ми можемо приблизно оцінити час до зіткнення, розрахувавши час вздовж поточного вектора прямої видимості, і (iii) прогнозоване положення цілі змінюватиметься повільно, тому створення прямих траєкторій достатньо , щоб отримати остаточну, гладку зшиту траєкторію.

У цій роботі було розроблено та реалізовано різноманітні алгоритми наведення в змодельованому та реальному середовищах. Показники, які використовуються для оцінки ефективності кожного методу, включають частоту влучень першого проходу та тривалість переслідування. Методи наведення LOS були отримані з алгоритму справжньої пропорційної навігації, який взято з літератури з наведення ракет.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Markus Ryll, John Ware, John Carter, and Nick Roy. Efficient trajectory planning for high speed flight in unknown environments. In 2019 International Conference on Robotics and Automation (ICRA), pages 732-738. IEEE, 2019

2. Fei Gao, William Wu, Yi Lin, and Shaojie Shen. Online safe trajectory generation for quadrotors using fast marching method and bernstein basis polynomial. In 2018 IEEE International Conference on Robotics and Automation (ICRA), pages 344-351.

УДК 621.396

Малий О.Ю.[1], Цвятков А.А.[2]
[1] канд. техн. наук, доц. НУ «Запорізька політехніка»
[2] студ. гр. БК-612м НУ «Запорізька політехніка»

ДОСЛІДЖЕННЯ СИСТЕМ ВИЯВЛЕННЯ КООРДИНАТ БПЛА

У роботі розглянуто сенсорні методи та алгоритми підвищення точності визначення координат БПЛА на основі модифікованого методу Ньютона. Метод Ньютона вивчався з метою скорочення часу обчислення координат.

Встановлено, що для отримання достатньої точності визначення координат матриця Якобі повинна бути розрахована на перших трьох кроках ітерації.

Виходячи з недоліків існуючих систем моніторингу, а також швидкості, відповідної вирішенню задачі визначення, і спрямованості БПЛА був запропонований шлях інтеграції системи звукового моніторингу і доплерівського содару, в його пасивному прояві (рис.1).

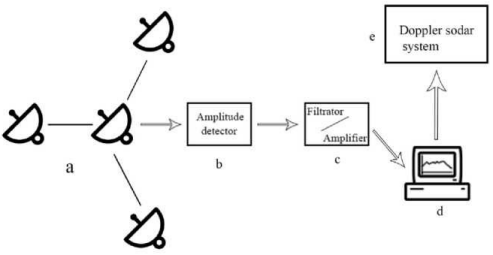


Рисунок 1 – Загальна структура запропонованої системи звукового моніторингу

В основі запропонованого методу лежать особливості принципу роботи доплерівських содарів, а саме їх залучення переважно до систем активного звукового моніторингу. На рис. 1 представлена антенна установка пасивної системи звукового моніторингу, яка в загальному вигляді включає 4 параболічні антени, виходячи з баз визначення координат місцезнаходження БПЛА диференціально-дальномірним методом.

Далі, після спектрального аналізу, в персональних і закладених системах забезпечується фільтрація сигналу, з подальшим його посиленням, для більш точного визначення характеру поведінки шуму, з подальшим визначенням участі шуму в окремих характеристиках БПЛА. звукового моніторингу.

Суть запропонованого методу полягає в тому, що після визначення оператором у навушниках (застосовується на портативних системах), або блоку прийняття рішень (застосовується для стаціонарних систем) участь шуму, який видає БПЛА після позитивного знаку. Додатково підключається доплерівський содар, для точкового визначення швидкості запланованого та виділеного БПЛА. Більш точна структурна схема запропонованого способу звукового моніторингу на основі параболічних антен наведена на рис.2.

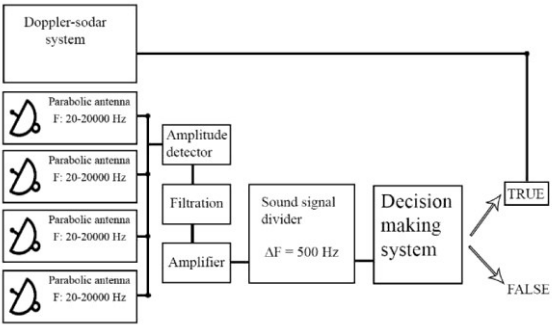


Рисунок 2 – Структурна схема запропонованого методу моніторингу звуку на основі параболічної антени

Для підвищення точності визначення БПЛА пасивними системами звукового моніторингу на основі наявності систем акустичного дослідження на основі параболічних антен і мікрофонів спрямованої дії, метод впровадження, з подальшим ускладненням системи.

Загалом в роботі розроблено метод визначення координат БПЛА, який базується на розв'язуванні системи нелінійних рівнянь, що описують похибки вимірювань за критерієм найменших квадратів. Такий метод дозволяє враховувати похибку вимірювання затримки часу приходу сигналу для кожної зі станцій окремо за рахунок введення вагових коефіцієнтів.

Удосконалений метод визначення координат БПЛА на основі модифікації методу Ньютона дозволяє значно скоротити час обчислення координат БПЛА при незначному погіршенні точності обчислення, що важливо при великій кількості БПЛА.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Panteev R.L. Modification of a method of Newton concerning the decision coordinate-route tasks passive automatic complexes maintenance of air targets / Tkachenko V. M., Korotkov V. V., Panteev R.L. // Soundtekhnika magazine. - 2012. - No 170, Page 157-161.

2. Panteev R.L. Processing of results of measurements by the passive systems of a sodar-location for the solution of coordinate- route task. / Panteev R.L. // Collection of theses of reports of the IV scientific and practical conference of students and graduate students "Instrument making prospection". - Kiev, 2011. - Page 39

УДК 004.94:681.5
Приймак В.І.[1], Шаптала С.В.[2], Миронова Н.О.[3]
[1] студ. гр. БК-611сп НУ «Запорізька політехніка»
[2] асист. НУ «Запорізька політехніка»
[3] канд. техн. наук, доц. НУ «Запорізька політехніка»

РЕАЛІЗАЦІЯ АЛГОРИТМІВ КОМП'ЮТЕРНОГО ЗОРУ РОБОТІВ В СИСТЕМІ СИМУЛЯЦІЇ WEBOTS

У сучасному світі машинний зір використовується практично в усіх технологічних процесах. Найбільш яскравими прикладами добре фінансованих наукових центрів по розвитку машинного зору можуть служити Лабораторія Штучного Інтелекту Массачусетського Технологічного Інституту(MIT Artificial Intelligence Laboratory), UC Berkeley Computer Vision Group, Vision and Autonomous Systems Center Університету Корнеги-Меллона, Stanford Vision Laboratory [1].

Основними глобальними виробниками систем машинного зору є компанії Cognex, Sensopart, Visionics, Eyematic і ін. [1].

За допомогою машинного зору роботи орієнтуються в довкіллі і допомагають здійснювати відеоконференції. У промисловості машинний зір – популярний метод автоматизації виробництва із застосуванням сучасних роботів [1].

Важливу роль машинний зір грає в соціальній і домашній робототехніці. Системами бачення оснащені навіть роботи-пилососи, які дозволяють роботові легко орієнтуватися в приміщенні. Сервісні роботи також є величезним полем діяльності для машинного зору (наприклад, область охоронних систем для ідентифікації особи, розпізнавання і відстежування об'єктів, що рухаються). У багатьох ресторанах, готелях, торгових центрах і офісах вже давно використовуються роботи для обслуговування клієнтів. Істотний попит на комп'ютерний зір спостерігається з боку сільськогосподарських організацій, де потрібна автоматизація діяльності по візуальному контролю і сортуванню продуктів [1].

Машинний зір грає велику роль для військових безпілотників, оскільки розпізнавання об'єктів потрібне для проведення місій спостереження і розвідки. Відзначається зростання інтересу до систем машинного зору і у сфері медицини [1].

Системи машинного зору стають усе більш актуальні, оскільки покликані вирішувати найбільш значимі проблеми людства, такі як безпека, медицина, промислові завдання.

В роботі було виконано реалізацію алгоритмів комп'ютерного зору роботів, а також було реалізовано модифікацію до камери робота Custom Robot для розпізнавання об’єктів для в системі симуляції Webots.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Системи машинного зору роботів. Історія розвитку, сфери застосування, плани на майбутнє. – URL: https://robotics.ua/systemy-mashynnoho-zrenyia.-ystoryia-prymery-plany/ (дата звернення: 15.04.2024)

УДК 004.94

Кобець М.К.[1], Миронова Н.О.[2]

[1] студ. гр. БК-611сп НУ «Запорізька політехніка»

[2] канд. техн. наук, доц. НУ «Запорізька політехніка»

РОЗРОБКА АПАРАТНОГО ТА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ МЕТЕОСТАНЦІЇ

Сучасні технології надають унікальні можливості для розробки інноваційних систем моніторингу довкілля. У цьому контексті розроблено та реалізовано проєкт метеостанції, призначеної для вимірювання різноманітних параметрів атмосфери та забезпечення доступу до цих даних як у режимі реального часу, так і у вигляді аналітичної інформації. Цей проєкт поєднує сучасні технології з метою створення універсальної та надійної системи моніторингу кліматичних умов. В роботі представлені основні аспекти розробки та впровадження метеостанції, а також її практичне значення в сучасному світі.

Мета роботи це створити повно функціональний прототип метеостанції, здатної вимірювати атмосферний тиск, вологість повітря та рівень освітленості, а також передавати та зберігати ці дані для подальшого аналізу.

Технічна реалізація апаратного забезпечення: використання різноманітних датчиків для вимірювання параметрів атмосфери, включаючи атмосферний тиск, вологість повітря та рівень освітленості. Для зручності користувача дані з датчиків виводяться на РК-дисплей.

Метеостанція оснащена можливістю передачі даних через внутрішню мережу за протоколом TCP/IP. Це дозволяє користувачам отримувати віддалений доступ до даних станції.

Дані з метеостанції також зберігаються в хмарній базі даних Firebase. Це забезпечує зручний доступ до даних з будь-якого місця, де є підключення до Інтернету, і забезпечує безпеку даних у разі втрати на пристрої.

Розроблено програмне забезпечення, що дозволяє користувачам підключатися до метеостанції через IP-адресу, переглядати поточні показання датчиків у режимі реального часу та отримувати доступ до даних із хмарної бази даних. Застосунок також забезпечує аналіз даних для створення прогнозів погоди на основі історичних даних датчиків.

Розробка такої метеостанції має велике практичне значення, оскільки її можна використовувати в різних областях, де важливий доступ до актуальних даних про погоду та клімат. Крім того, проект демонструє можливість інтеграції апаратних і програмних компонентів для створення повної системи збору та аналізу даних.

В результаті роботи була розроблена та впроваджена метеостанція з широким функціоналом, що здатний вимірювати атмосферний тиск, вологість повітря та рівень освітленості, а також надавати доступ до цих даних через внутрішню мережу та хмарну базу даних. Розроблене програмне забезпечення дозволяє зручно взаємодіяти з метеостанцією як в режимі реального часу, так і для аналізу та прогнозування погодних умов на основі історичних даних. Таким чином, даний проєкт демонструє ефективне використання сучасних технологій для створення повнофункціональної та універсальної системи моніторингу клімату, яка має широкий потенціал застосування в різних сферах.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. ASP.NET Core Blazor. Microsoft. – URL: https://learn.microsoft.com/en-us/aspnet/core/blazor/?view=aspnetcore-7.0 (дата звернення 12.10.2023).

УДК 004.94:681.5

Білка Д.О.[1], Миронова Н.О.[2], Шаптала С.В.[3]
[1] студ. гр. БК-610 НУ «Запорізька політехніка»
[2] канд. техн. наук, доц. НУ «Запорізька політехніка»
[3] асист. НУ «Запорізька політехніка»

РОЗРОБКА ПРОТОТИПУ ЦИФРОВОГО ДВІЙНИКА РОБОТОТЕХНІЧНОГО ПРИСТРОЮ ДЛЯ ВІДТВОРЕННЯ РУХУ В ПРОСТОРІ

У наш час використання цифрових двійників встигло прижитися у багатьох галузях нашого життя, таких як:

– робототехніка – розробка прототипів пристроїв у 3D середовищі з подальшою імітацією фізики мотора автомобіля;

– медицина – саме просте що можна уявити це – імітацію тіла людини під час операцій, імітація його рухів;

– автомобільна промисловість – імітація рухів автомобіля у потоку, імітація поведінки автопілоту у різних складних ситуаціях на дорозі;

– віртуальна та ігрова індустрія – цифрові двійники можуть виконувати різні складні рухи, котрі не може повторити людина, наприклад політ, тоді береться людина котру саджають у спеціальний пристрій, котрий її піднімає

вгору(у небо наприклад) і там вона вже виконує потрібні рухи, котрі також зчитуються датчиками та передаються у комп'ютер.

Також елементи цифрового двійника використовуються у кінорежисурі – у фільмах, де потрібні складні та небезпечні сцени, таки як експлозії, погоні та бойові сцени, актори можуть бути замінені цифровими двійниками. Наприклад, у фільмах про супергероїв, де герої виконують неймовірні трюки та акробатичні вправи, часто використовуються цифрові двійники для створення ефектів, які були б неможливі для здійснення реальними акторами. Таким чином, цифрові двійники дозволяють режисерам знімати сцени, які були б ризикованими або неможливими для зняття з реальними акторами, і створювати вражаючі візуальні ефекти.

І також у промисловій автоматиці є дуже багато імітацій роботи заводу, знову ж відтворення температурного режиму, відтворення роботи конвеєрних ліній, їх пропускна здатність, впровадження штучного інтелекту у технологічні процеси з питань автоматизації.

Мета роботи: розробити прототип цифрового двійника з передачею даних за допомогою модулів платформи Arduino.

Для досягнення поставленої мети необхідно вирішити наступні задачі:

– розробити фізичний прототип цифрового двійника;

– розробити прототип цифрового двійника в Unity середовищі;

– розробити програмну частину цифрового двійника;

– виконати інтеграцію даних з датчиків(акселерометру та гіроскопу);

– розробити програмну частину для керування робототехнічним пристроєм (наприклад зміна даних на гіроскопі у ручному режимі управління дозволяє змінити положення робота у реальному світі та у програмі з цифровим двійником);

– виконати інтеграцію бази даних(Firebase або MySQL).

Цифровий двійник буде складатися з платформи з колесами, власному джерелу живлення(акумулятори, батарейки), мікроконтролеру esp8266wifi з wifi модулем і також датчиків акселерометру, гіроскопу.

УДК 004.94

Ткачов І.М.[1], Миронова Н.О.[2]
[1] студ. гр. БК-611сп_2 НУ «Запорізька політехніка»
[2] канд. техн. наук, доц. НУ «Запорізька політехніка»

ДОСЛІДЖЕННЯ ТА РЕАЛІЗАЦІЯ ТЕХНОЛОГІЇ РОЗУМНОГО ЗАМКУ З ЛАЗЕРНОЮ СИСТЕМОЮ БЕЗПЕКИ

У сучасному світі технологічних інновацій та повсюдного поширення смарт-технологій необхідність у створенні розумних систем безпеки стає все

більш актуальною. Застосування інтегрованих систем, таких як RFID-технології, датчики вологості та звукові сенсори, дозволяє забезпечувати не тільки надійність, а й зручність використання у повсякденному житті.

Мета роботи – розробити технологію розумного замку для системи безпеки на основі мікроконтролера ESP32[1] та з використанням лазеру. В роботі використовуються такі компоненти, як RFID-сканер RC522 [2] для ідентифікації та авторизації, п'єзодатчик для виявлення акустичних аномалій, датчик вологості HR202 для контролю мікроклімату та інші додаткові елементи, що створюють повноцінну екосистему розумної безпеки.

Ключовою особливістю проєкту є інтеграція із сучасними веб-технологіями. Завдяки API та можливостям веб-комунікації система здатна відправляти повідомлення та дані в реальному часі, що робить її високоефективним інструментом для контролю та моніторингу.

В роботі представлено докладний опис всіх розроблених компонентів системи, розглянуто особливості їхньої взаємодії, а також обґрунтовано вибір програмного та апаратного забезпечення для її реалізації. Сукупність всіх цих елементів дає уявлення про складність і багатогранність сучасних систем безпеки, а також підкреслює їх важливість в умовах технологічного ландшафту, що швидко змінюється.

Результати даної роботи можуть бути використані як у приватних домогосподарствах, так і в комерційних організаціях, які бажають забезпечити максимальний захист своїх ресурсів та даних.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. ESP32. – URL: https://www.espressif.com/en/products/socs/esp32

2. RC522. – URL: https://www.alldatasheet.com/datasheet-pdf/pdf/346109/NXP/RC522.html

УДК 004.94:681.5

Нагурний В.В.[1]

[1] студ. гр. БК-613м НУ «Запорізька політехніка»

РОЗРОБЛЕННЯ ПІДХОДУ ОПТИМІЗАЦІЇ СТРУКТУРИ НЕЙРОННОЇ МЕРЕЖІ ДЛЯ ПЕРЕДАЧІ МЕДІАКОНТЕНТУ

У сучасному світі медіаконтент, такий як аудіо, відео чи зображення, відіграє велику роль у повсякденному житті майже всіх людей. Проте бездротова передача таких файлів в робототехнічних пристроях, особливо з високою якістю, може спричиняти деякі проблеми. Наприклад, великі файли можуть передаватися досить довго, пошкоджуватися під час передачі, або навіть займати занадто багато комп’ютерної пам’яті.

Використання нейронних мереж для зберігання, передачі та відновлення медіаконтенту може бути дуже потужним інструментом, особливо коли заради економії можна поступитися дрібними деталями. Проте для виконання завдань не завжди зрозуміло, яку саме структуру нейронної мережі необхідно використовувати.

Поширена думка, що більша кількість нейронів в нейронній мережі дозволяє отримувати від нейронної мережі кращі результати. Проте, експериментальним шляхом доведено, що в цьому правилі бувають виключення.

Створення програми, яка дозволить проводити досліди різних нейронних мереж та отримувати результати при однакових заданих умовах, дозволить легко обирати найбільш ефективну архітектуру. До того ж, саме спростування міфу про більшу кількість нейронів і кращу ефективність роботи вже змінить вектор роздуму з приводу покращення роботи нейронних мереж. Доведення того факту, що значно менша нейронна мережа може досягати тих же результатів, що й більша – дозволить значно економити не тільки ресурси, але й час.

Для бездротової передачі даних в робототехнічних пристроях може бути використано нейронна мережа типу «автокодувальник» (рис. 1), який дозволяє не тільки відтворювати отриману інформацію, а й обробляти її, знешумлювати, зменшувати розмір, кодувати дані тощо. Особливістю такого виду нейронної мережі є те, що кількість нейронів у вхідному шарі відповідає кількості нейронів у вихідному, що дозволяє отримувати результат тим чи іншим шляхом схожий на оригінал.

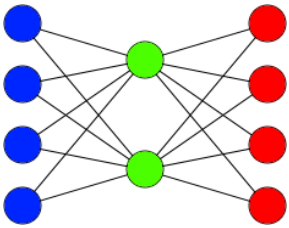


Рисунок 1 – Приклад архітектури автокодувальника

Проте окрім вхідного та вихідного шарів, автокодувальник має ще й приховані і саме їх структура може бути різною. Тож дослідження різних архітектур нейронних мереж може стати не тільки корисним, а ще й дуже вигідним процесом для будь якої зацікавленої компанії.

УДК 004.94
Баранова О.А.[1], Миронова Н.О.[2]
[1] студ. гр. БК-613м НУ «Запорізька політехніка»
[2] канд. техн. наук, доц. НУ «Запорізька політехніка»

СИНХРОНІЗАЦІЯ ДАНИХ З ДАТЧИКІВ ЗА ДОПОМОГОЮ LAB STREAMING LAYER

У сучасному світі датчики є невід'ємною частиною технологічних систем. Вони використовуються в науці, промисловості, медицині та інших сферах діяльності. Однак іноді виникає необхідність у їхній синхронізації.

Синхронізація датчиків – це процес, при якому кілька датчиків працюють одночасно і надають дані в точній відповідності один з одним. Це дозволяє уникнути помилок та отримати більш точні результати вимірювань.

Існує кілька методів синхронізації датчиків. Один із них – використання спеціального пристрою, який забезпечує точну часову синхронізацію між датчиками. Інший спосіб – програмна синхронізація, коли датчики підключені до однієї системи та синхронізуються за допомогою програмного забезпечення. Залежно від конкретного завдання та вимог до точності вимірювань, вибирається оптимальний спосіб синхронізації датчиків.

Апаратна синхронізація часто неможлива або надзвичайно дорога. Lab Streaming Layer (LSL) пропонує програмний підхід до синхронізації потоків даних на основі мітки часу для вибірки та синхронізація часу в загальній локальній мережі. Екосистема LSL підтримує понад 150 пристроїв та забезпечує взаємодію з клієнтським програмним забезпеченням, написаним на кількох мовах програмування, включаючи C/C++, Python, MATLAB, Java, C#, JavaScript, Rust і Julia. Стійкість і універсальність LSL зробили його основною платформою синхронізації мультимодальних даних: даних про динаміку мозку (у першу чергу ЕЕГ), фізіологію (ЕКГ, ЕМГ, серцевий ритм, дихання, провідність шкіри та ін.), поведінкові данні (захоплення руху, відстеження очей, сенсорна взаємодія, вираз обличчя та ін.), стан оточення та комп'ютерних програм (наприклад, мітки подій, мітки з клавіатури та інших пристроїв) [1].

На рисунку 1.1 представлений проєкт в основу якого покладена синхронізація даних з датчиків за допомогою LSL.

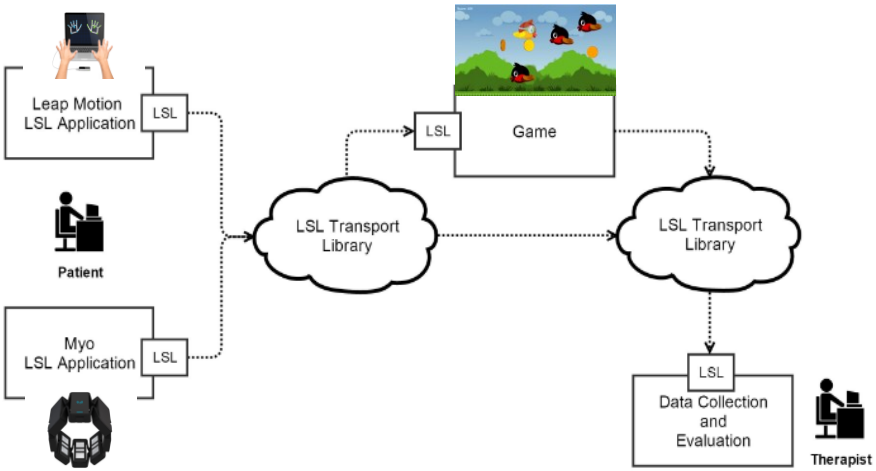


Рисунок 1.1 – Структура запропонованого ігрового реабілітаційного середовища

Ідея, що реалізується у проекті доволі проста. За допомогою LSL отримується і синхронізується інформація з датчиків 2 пристроїв для відстеження руху пальців та руки (Leap Motion, Thalmic Myo). Потоки даних, які були надані програмами LSL, перетворюються у імітацію натискань клавіш. Наприклад, рух певного пальця вгору буде перетворено на подію клавіші зі стрілкою вгору. Так за допомогою руху пальцями і руки здійснюється керування птахом у грі, який повинен збирати монети і ухилятися або стріляти в супротивників (також птахів). Дані з датчиків, а також дані з гри записуються та зберігаються для подальшого аналізу експертом (наприклад, терапевтом пацієнта) [2].

Не дивлячись на велику популярність і широку застосовуваність LSL є не єдиним рішенням для синхронізації даних в бездротових сенсорних мережах. Серед альтернатив можна назвати наприклад бібліотеку OpenSync [3].

У результаті роботи було досліджено можливості інструменту Lab streaming layer та доцільність і зручність його використання для синхронізації даних з датчиків.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Kothe C. The Lab Streaming Layer for Synchronized Multimodal Recording / Kothe C [та ін.]. – 14.02.2024 р. (Препринт). – URL:

https://www.biorxiv.org/content/10.1101/2024.02.13.580071v1 (дата звернення: 07.04.2024).

2. Schlesinge M. An LSL-Based Sensor Platform for Mobile Brain Imaging, Brain-Computer Interfaces and Rehabilitation : магістерська робота. Graz, 2016. 91 p. URL: https://diglib.tugraz.at/download.php?id=5891c78a8aa83&location=browse (дата звернення: 07.04.2024).

3. https://arxiv.org/pdf/2107.14367.pdf. – URL: https://arxiv.org/pdf/2107.14367.pdf (дата звернення: 07.04.2024).

УДК 004.94

Шевченко Т.В.[1], Миронова Н.О.[2]
[1] студ. гр. БК-613м НУ «Запорізька політехніка»
[2] канд. техн. наук, доц. НУ «Запорізька політехніка»

ПІДХОДИ ДО РОЗРОБКИ 3D ПРИНТЕРІВ НА БАЗІ ОДНОПЛАТНИХ КОМП'ЮТЕРІВ

На даний час 3D-принтери стали більш доступнішими, завдяки чому кожен зараз може його придбати. Аналіз оптимальної доступності, вартості та функціоналу 3D-принтерів є актуальним завданням.

Метою роботи є аналіз наукових та оглядових статей та матеріалів стосовно побудови 3D-принтерів та визначення найбільш оптимальної моделі для побудови 3D-принтеру у домашніх умовах.

Стаття «Journal of 3D Printing and Additive Manufacturing» надає найбільш глибокий дослід 3D-принтерів на базі Arduino, наводячи порівняльні дані для заводського принтеру (принтер X) та саморобного (на Arduino) принтеру. Тут описано те, чому варто обирати Arduino Mega 2560 в якості органу керування, які обирати двигуни та драйвери для них; також наведена загальна конструкція 3D-принтеру та схема каркасу. Основна перевага створеного вручну принтеру – ціна; ця перевага не наводиться напряму, але постійно згадується на протязі всієї статті (приблизно 115$ проти 190$ за заводський принтер; ціна наведена приблизно з конвертації індонезійської рупії у долар США). Також серед переваг виділено міцність каркасу (у 5 разів вища ніж у заводського 3D-принтеру), щільність друку (деталі, надруковані на зібраному 3D-принтері, витримують трохи вищі навантаження) та доступність програмного забезпечення (ПЗ), оскільки зараз дуже багато прикладів програм для 3D-принтеру на базі Arduino можна знайти у вільному доступі. Серед недоліків виділено відсутність підігріву стартової платформи (впливає на якість друку) та більша похибка відхилень (похибка незначна, але вища ніж у заводського принтеру) [1].

У статті «Developing low cost 3D printer» наводиться більш детальна схема побудови 3D-принтерів, також наводяться структурні діаграми, таблиці переліку ресурсів та підсумовуючі таблиці (таблиця вартості тощо), також наводяться приклади ПЗ, яке здатне працювати з саморобним 3D-принтером. В якості органу керування також використовували контролер Arduino Mega. Під час ретельного дослідження вдалося встановити принцип друку: слайсер (у даному випадку Cura) створює інструкції для друку, які єдиним кодом передаються на плату методом «Repetier Host», також код можна передавати іншими способами. Але зі статті випливає одне питання: слайсер може працювати безпосередньо з контролерами Arduino, чи на контролер необхідно встановлювати певну прошивку (ПЗ)? [2].

Під час перегляду відеохостингу було знайдено оглядове відео, у якому розповідалося про нанесення металізації на модель за допомогою часткового електролізу відразу під час друку деталі, і випадково було виявлено, що цей 3D-принтер було побудовано на базі Raspberry Pi, яка керувала платою Arduino. Такий спосіб реалізації керування є надто складним і вартісним для домашньої реалізації, але має перевагу у високій функціональності, мобільності, а також наявність можливості вдосконалення для 3D-принтерів [3].

Згідно досліджених статей та матеріалів можна зробити висновок, що для побудови 3D-принтерів на базі одноплатних комп'ютерів найбільш доцільно використовувати платформу Arduino. Оскільки переважна більшість статей, які є у вільному доступі, описують 3D-принтери, які побудовані на базі Arduino; серед переваг Arduino можна відзначити простоту створення керування низькорівневими пристроями (крокові двигуни, датчики тощо) та низьку вартість плати контролеру.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Journal of 3D Printing and Additive Manufacturing [Електронний ресурс]. – Режим доступу: https://www.researchgate.net/profile/Mahros-Darsin/publication/356171717_Design_of_Portable_Cartensia_3D_Printer_Portable_Using_Arduino_Mega_2560/links/618e7d613068c54fa5d8f989/Design-of-Portable-Cartensia-3D-Printer-Portable_-Using-Arduino-Mega-2560.pdf (дата звернення: 10.03.2024). – Назва з екрана.

2. Developing low cost 3D printer [Електронний ресурс]. – Режим доступу: https://www.researchgate.net/profile/Mohd-Javaid/publication/313161193_Developing_low_cost_3_D_printer/links/5891a455aca272f9a558022f/Developing-low-cost-3-D-printer.pdf (дата звернення: 16.03.2024). – Назва з екрана.

3. I made a METAL 3D-Printer at home! [Електронний ресурс]. – Режим доступу: https://www.youtube.com/watch?v=W1d36wbx_yg (дата звернення: 31.03.2024). – Назва з екрана.

УДК 004.94:681.5
Довженко В.М.[1], Миронова Н.О.[2]
[1] студ. гр. БК-612м НУ «Запорізька політехніка»
[2] канд. техн. наук, доц. НУ «Запорізька політехніка»

ДОСЛІДЖЕННЯ ТА РЕАЛІЗАЦІЯ ПІДХОДІВ ЩОДО ПРОЕКТУВАННЯ РОЗУМНОЇ АВТОМИЙКИ

Автомийка – пристрій для миття автомобілів, а також підприємство, що здійснює миття автомобілів і яке надає супутні послуги (чистку салону автомобіля тощо). Найчастіше автомийки розташовуються на автозаправних станціях або поряд з автомагазинами та станціями технічного обслуговування автомобілів. Існують кілька типів автомийок:

– ручні, безконтактні;
– портальні;
– тунельні.

Щодо способів видалення забруднень, мийки поділяються на:

– контактні (з використанням механічного видалення бруду та хімічних мийних засобів);
– безконтактні (де забруднення видаляється за допомогою поверхнево-активних мийних речовин і потужних струменів води під високим тиском).

Завдяки технології Інтернету речей (IoT) можна отримати доступ до безпрецедентної кількості даних, які можуть бути використані для аналізу та прийняття стратегічних рішень. Ось деякі основні переваги використання IoT в автомийках:

– моніторинг та оптимізація робочих процесів;
– підвищення ефективності та зниження витрат;
– покращення безпеки та якості;
– управління ланцюгом праці.

Один з аналогів – це система автомийки самообслуговування на платформі. Завдяки цьому проєкту власник автомийного центру зможе точно відстежувати кількість помитих автомобілів.

Також можна виділити систему дистанційного моніторингу автомийки самообслуговування на основі технології NB-IoT. Ця система була розроблена для вирішення проблеми збільшення витрат на технічне обслуговування операторів самообслуговування мийних машин.

Система керування автомийкою самообслуговування з промисловим програмованим логічним контролером з можливостями IoT є ще одним аналогом автоматизованої системи, яка спрямована на удосконалення моніторингу, контролю та збору даних про роботу автомийки. Ця система використовує сучасні промислові програмовані логічні контролери, які мають можливості IoT. Вона спрямована на досягнення більш ефективної роботи та оптимізації обслуговування клієнтів.

Система гаражної смарт мийки авто на основі технології IoT використовується для оптимізації процесу мийки автомобілів та забезпечення високої ефективності обслуговування. Основною метою є інтеграція всіх датчиків на базі IoT для збору та аналізу даних, що дозволяє здійснювати ефективний моніторинг та контроль за процесом мийки автомобілів.

Основні компоненти системи включають:

– датчики IoT: збирають дані про різні параметри мийки автомобілів, такі як витрата води, тиск, температура тощо;

– шлюз LAN: відправляє дані, зібрані датчиками, до хмарної бази даних для подальшої обробки;

– хмарну база даних: зберігає та обробляє дані, що надходять від датчиків, і генерує звіти про роботу мийки автомобілів;

– блокчейн технологію: забезпечує безпеку та надійність даних шляхом генерації унікальних хеш-значень для кожного блоку даних.

УДК 004.94:681.5
Мєльніков О.В.[1], Миронова Н.О.[2]
[1] студ. гр. БК-612м НУ «Запорізька політехніка»
[2] канд. техн. наук, доц. НУ «Запорізька політехніка»

ДОСЛІДЖЕННЯ ІНСТРУМЕНТІВ МОДЕЛЮВАННЯ ТА РОЗРОБКИ, ЩО ВИКОРИСТОВУЮТЬСЯ В СИСТЕМАХ СИМУЛЯЦІЇ ПРОМИСЛОВИХ РОБОТІВ

Для промислових роботів ключове програмне забезпечення та інструменти моделювання включають Robot Operation Systems (ROS, операційну систему роботів) для керування. Крім того, такі інструменти, як ANSYS, V-Rep (Virtual Robotics Experimentation Platform) і MATLAB/Simulink, широко використовуються для моделювання та аналізу в галузі мехатроніки та робототехніки. ANSYS використовується для числового аналізу та моделювання різних інженерних систем, включаючи механічні, термічні та електричні аспекти. V-Rep використовується для симуляції та віртуального тестування робототехнічних систем. MATLAB/Simulink застосовується для моделювання та симуляції систем

керування та автоматизації. Розглянемо кожен з перелічених інструментів більш докладно: ROS, ANSYS, V-Rep, MATLAB/Simulink та Webots [1].

ROS забезпечує стандартні служби операційної системи, такі як: апаратну абстракцію, контроль пристроїв на низьких рівнях, реалізацію часто використовуваних функцій, передачу повідомлень між процесами, і управління пакетами. ROS заснований на архітектурі графів, де обробка даних відбувається в вузлах, які можуть отримувати і передавати повідомлення між собою. Бібліотека орієнтована на Unix-подібні системи та має дві основні «сторони»: операційну систему ros, як описано вище і ros-pkg, набір підтримуваних користувачами пакетів (організованих в набори, які називаються стеками), які реалізують різні функції робототехніки: SLAM, планування, сприйняття, моделювання та інші [2].

ANSYS надає комплексні рішення для симуляції, включаючи інструменти для систем симуляції промислових робототехнічних систем. Це дозволяє моделювати та аналізувати різні аспекти робототичних систем, такі як рух, структурна цілісність та теплова ефективність [3].

V-Rep має програмне забезпечення, яке надає інтерфейс для написання скриптів за допомогою мови Lua, що дозволяє користувачам розробляти складні поведінки та стратегії управління для симульованих роботів. Крім того, доступні API для інтеграції з зовнішніми мовами програмування, такими як Python чи C++. Також V-Rep має змогу симулювати сенсори, включаючи камери, LiDAR та сенсори наближення, що сприяє тестуванню та валідації алгоритмів в віртуальному просторі. Можна симулювати не лише окремі роботи, а й цілі системи з численними взаємодіючими компонентами, що робить його цінним для складних сценаріїв промислової автоматизації [4].

Simulink, частина Matlab, є графічним середовищем моделювання, яке дозволяє моделювати та імітувати складні системи, включаючи роботизовані системи. Simulink чудово підходить для моделювання динамічних систем, дозволяючи користувачам моделювати залежну від часу поведінку систем. Це має вирішальне значення для розуміння того, як системи розвиваються з часом і як вони реагують на різні вхідні дані, а також Matlab/Simulink підтримує автоматизовану генерацію коду, що дозволяє користувачам генерувати виконуваний код зі своїх моделей. Ця функція полегшує плавний перехід від симуляції до реальної реалізації, підвищуючи ефективність розробки [5].

Webots – це універсальне програмне забезпечення для моделювання роботів, яке широко використовується при розробці та тестуванні різних робототехнічних систем, включаючи промислові роботи. Він створює реалістичне тривимірне середовище для моделювання поведінки і взаємодії робітників.

Програмне забезпечення підтримує широкий спектр уже існуючих моделей роботів, у тому числі тих, які зазвичай використовуються в промисловості. Webots дозволяє моделювати різні датчики, такі як камери, лідари та датчики наближення. Також є змога програмувати контролери роботів, використовуючи різні мови, такі як C, C++, Python і Java [6].

Кожна система має свої унікальні переваги: реалістичне фізичне моделювання, спеціалізовані функції, такі як планування руху, можливості інженерного моделювання або симуляції в реальному часі. Інтеграція з ROS і підтримка симуляції з декількома роботами ще більше підвищують їхню корисність. Вибір системи залежить від конкретних вимог і цілей конкретного проекту в динамічній галузі робототехніки.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Shibata T. Rapid Prototyping of Robot Systems using Software Tools. Journal of the Robotics Society of Japan. 2012. Т. 30, № 9. С. 857–859. URL: https://doi.org/10.7210/jrsj.30.857 (дата звернення: 07.01.2024).

2. Robot Operating System (ROS) / ред. A. Koubaa. Cham : Springer International Publishing, 2021. URL: https://doi.org/10.1007/978-3-030-75472-3 (дата звернення: 07.01.2024).

3. The Dynamic Simulation of Robotic Tool Changer Based on ADAMS and ANSYS / N. Li та ін. 2016 International Conference on Cybernetics, Robotics and Control (CRC), м. Hong Kong, Hong Kong, 19–21 серп. 2016 р. 2016. URL: https://doi.org/10.1109/crc.2016.013 (дата звернення: 12.01.2024).

4. Rohmer E., Singh S. P. N., Freese M. V-REP: A versatile and scalable robot simulation framework. 2013 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS 2013), м. Tokyo, 3–7 листоп. 2013 р. 2013. URL: https://doi.org/10.1109/iros.2013.6696520 (дата звернення: 14.01.2024).

5. Колесник К. Імітаційне моделювання руху промислового робота-маніпулятора в програмі Matlab. Комп'ютерні системи проектування. Теорія і практика. 2021. Т. 3, № 1. С. 17–20. URL: https://doi.org/10.23939/cds2021.01.017 (дата звернення: 14.01.2024).

6. Michel O. Cyberbotics Ltd. Webots™: Professional Mobile Robot Simulation. International Journal of Advanced Robotic Systems. 2004. Т. 1, № 1. С. 5. URL: https://doi.org/10.5772/5618 (дата звернення: 20.01.2024).

УДК 004.94:681.5
Столбухов І.С.[1], Миронова Н.О.[2]
[1] студ. гр. БК-612м НУ «Запорізька політехніка»
[2] канд. техн. наук, доц. НУ «Запорізька політехніка»

ДОСЛІДЖЕННЯ СИСТЕМ ІНТЕРНЕТ РЕЧЕЙ УПРАВЛІННЯ ЗАПАСАМИ

Інтернет речей (IoT) є однією з найвпливовіших технологічних інновацій нашого часу. В основі IoT лежить ідея з'єднання фізичних об'єктів із Інтернетом, що дозволяє їм збирати, обмінюватися даними та взаємодіяти один з одним або з користувачами в реальному часі. Ця концепція радикально змінює традиційне сприйняття об'єктів навколишнього середовища, перетворюючи звичайні предмети на "розумні" пристрої з можливістю збору даних, аналізу та автоматизованого управління.

IoT сприяє ефективному використанню ресурсів, зокрема енергії, за рахунок інтелектуального моніторингу та управління споживанням. Це не тільки зменшує витрати, але й сприяє сталому розвитку, зменшуючи вуглецевий слід і сприяючи екологічно чистим ініціативам.

Інтелектуальні IoT-системи можуть адаптуватися до потреб і переваг користувачів, надаючи персоналізовані послуги та вдосконалюючи користувацький досвід. Це досягається за рахунок аналізу поведінки користувачів і їхніх вподобань.

Але попри численні переваги, розгортання IoT також супроводжується викликами, зокрема питаннями безпеки, конфіденційності, стандартизації та сумісності. Це вимагає постійних зусиль для розробки стандартів, захисних механізмів та політик, що регулюють цю сферу.

Загалом IoT є динамічно розвиваючою технологією, що має потенціал радикально змінити наш підхід до використання технологій, впливаючи на різні аспекти нашого повсякденного життя та ділової діяльності. Водночас, для реалізації повного потенціалу IoT необхідно вирішити ряд викликів, зокрема у сферах безпеки, приватності та міжопераційної сумісності.

Актуальність використання IoT на фірмі з багатьма філіалами по Україні можна описати через зростаючу потребу в ефективному управлінні запасами та оптимізації логістичних процесів. У контексті швидкого розвитку ринкової економіки та збільшення конкуренції, підприємства прагнуть не лише максимізувати прибутки, а й забезпечувати високий рівень задоволеності клієнтів, що неможливо без точного та оперативного управління запасами. IoT дозволяє реалізувати ці завдання за рахунок автоматизації збору даних, їх аналізу та моніторингу в реальному часі, що значно підвищує ефективність управлінських рішень на всіх рівнях. Це особливо актуально для компаній з великою мережею філіалів, де потреба в

синхронізації даних між віддаленими локаціями та центральним офісом є критичною для успішного управління запасами та замовленнями. Впровадження IoT сприяє не тільки зниженню витрат на логістику та зберігання, але й підвищенню загальної прозорості бізнес-процесів, що дозволяє оперативно реагувати на зміни в попиті та пропозиції на ринку.

Апаратна частина системи Інтернет речей управління запасами складається з наступних компонентів:

– RFID теги: для ідентифікації та відслідковування товарів на складі та в торговельному залі (рис.1);

– сенсори: включають температурні сенсори, сенсори вологості, вагові сенсори тощо, для моніторингу стану товарів;

– RFID зчитувачі: для швидкої інвентаризації та обліку товарів (рис.2).

Рисунок 1 – RFID тег

Рисунок 2 – RFID зчитувач

Загалом використання IoT для регулювання кількості товару на фірмі з багатьма філіалами по Україні є досить закономірним, сучасним та ефективним рішенням. За допомогою цієї системи зменшується велика

кількість ризиків та водночас підвищується ефективність управління запасами, що веде до оптимізації витрат і збільшення прибутковості. Ця система дозволяє компанії швидше реагувати на зміни в попиті та пропозиції, а також підвищує задоволеність клієнтів завдяки забезпеченню неперервності постачання та зменшенню ймовірності дефіциту товарів. Крім того, автоматизація процесів та зниження потреби в ручній перевірці запасів зменшують можливість помилок і підвищують точність управління запасами. Отже, інтеграція IoT в управління запасами стає ключовим фактором для підвищення конкурентоспроможності на ринку, дозволяючи компаніям не лише оптимізувати свої внутрішні процеси, але й надавати високий рівень обслуговування своїм клієнтам.

УДК 004.94:681.5
Новіков М.А.[1], Миронова Н.О.[2]
[1] студ. гр. БК-612м НУ «Запорізька політехніка»
[2] канд. техн. наук, доц. НУ «Запорізька політехніка»

ДОСЛІДЖЕННЯ ТА РЕАЛІЗАЦІЯ ПІДХОДІВ ЩОДО ПРОЕКТУВАННЯ РОЗУМНОЇ ТЕПЛИЦІ

Сільське господарство відіграє ключову роль у економіках багатьох країн, забезпечуючи продовольчу безпеку та постачання сировини для інших промислових галузей. Проте, з появою нових викликів, таких як зміна клімату, обмеженість ресурсів та високі стандарти якості, в сільському господарстві виникає потреба в нових технологічних рішеннях для оптимізації виробництва.

Сучасні підходи до автоматизації та комп'ютерно-інтегрованих технологій в сільському господарстві мають великий потенціал для покращення ефективності, збільшення врожайності та зниження витрат. Можна виділити наступні переваги використання смарт-теплиць:

– смарт-теплиці автоматизують процеси поливу, регулювання температури та вологості, що дозволяє оптимізувати використання води, енергії та добрив. Враховуючи загрозу дефіциту води та зміни клімату, це особливо важливо;

– використання сучасних технологій управління середовищем в теплицях дозволяє створювати ідеальні умови для росту рослин навіть там, де традиційні методи можуть бути неефективними. Це підвищує врожайність і гарантує стабільне виробництво продуктів;

– завдяки інноваційним методам виробництва смарт-теплиці зменшують використання пестицидів і хімічних добрив, що сприяє збереженню родючості ґрунту та зменшенню забруднення навколишнього середовища.

– смарт-теплиці дозволяють вирощувати органічні овочі та фрукти без використання шкідливих хімічних речовин у контрольованих умовах;

– впровадження смарт-теплиць може підвищити продуктивність виробництва та знизити витрати, особливо для малих сільськогосподарських підприємств, які зазвичай мають обмежений доступ до ресурсів.

Основні технології та компоненти смарт-теплиць наступні:

– системи моніторингу та управління: використання сучасних сенсорів та систем збору даних дозволяє сільським господарствам отримувати точну інформацію про умови вирощування рослин, такі як вологість ґрунту, температура, рівень CO2 тощо. Це дозволяє точно контролювати та оптимізувати процеси вирощування;

– автоматизація обробки ґрунту та поливу: сучасні технології дозволяють автоматизувати процеси обробки ґрунту та поливу, використовуючи наприклад автономні робочі машини з GPS-навігацією. Це допомагає зберегти час та знизити витрати на робочу силу;

– управління інвентарем та складською справою: системи управління інвентарем та складською справою дозволяють автоматизувати процеси замовлення, поставки та ведення обліку матеріалів і обладнання, що допомагає уникнути недоліків та збільшити ефективність;

– застосування штучного інтелекту та аналіз даних: використання штучного інтелекту та аналізу даних дозволяє прогнозувати урожайність, оптимізувати вирощування, виявляти аномалії та приймати рішення на основі об'єктивних даних;

– інтеграція технологій Інтернету речей (IoT): використання IoT дозволяє підключати різноманітні пристрої та сенсори до однієї мережі, що спрощує збір та аналіз даних, а також взаємодію між різними системами.

Загалом, сучасні підходи до автоматизації та комп'ютерно-інтегрованих технологій у сільському господарстві відкривають широкі можливості для покращення продуктивності, ефективності та стійкості галузі. Важливо, щоб фермери були готові до впровадження таких інновацій та мали доступ до необхідних знань та ресурсів.

УДК 004.94
Половінчук Є.В.[1], Миронова Н.О.[2]
[1] студ. гр. БК-612м НУ «Запорізька політехніка»
[2] канд. техн. наук, доц. НУ «Запорізька політехніка»

ДОСЛІДЖЕННЯ ТА РЕАЛІЗАЦІЯ СИСТЕМИ МОНІТОРИНГУ ЗАЛИШКІВ ПРОДУКТІВ В РЕСТОРАНІ

Розвиток ресторанного бізнесу потребує застосування сучасних технологічних рішень для оптимізації процесів та зниження витрат. В умовах глобалізації та зростання конкуренції, ключовим аспектом стає ефективне управління залишками продуктів, що може значно зменшити втрати і збільшити прибутковість ресторанів. Використання інформаційних технологій та систем IoT в цьому контексті відкриває нові можливості для моніторингу та аналізу, дозволяючи ресторанам оперативно реагувати на зміни запасів.

Онлайн системи моніторингу використання продуктів стають все більш поширеними в ресторанному бізнесі, пропонуючи не тільки трекінг залишків, але й аналітику споживання, що дозволяє оптимізувати закупівельну діяльність та складський облік. Виклик полягає в тому, щоб інтегрувати ці технології таким чином, щоб вони були легкі у використанні, масштабовані та економічно ефективні.

Мета роботи: виконати дослідження та реалізацію системи моніторингу залишків продуктів в ресторані. Система має забезпечувати точне відстеження та аналіз залишків продуктів у реальному часі, покращуючи процеси закупівлі та зменшення втрат.

Для досягнення поставленої мети необхідно вирішити наступні задачі:

– аналіз існуючих систем та методів моніторингу залишків;

– розробка моделі для прогнозування потреб у продуктах з використанням технологій машинного навчання;

– інтеграція IoT-датчиків для автоматизованого збору даних про залишки;

– реалізація та тестування розробленої системи;

– виконати експериментальне дослідження розробленої системи в реальних умовах ресторану.

Дані для дослідження будуть збиратися як з внутрішніх джерел (записи системи моніторингу), так і з зовнішніх джерел (відгуки користувачів, аналітика використання). Аналіз даних включатиме статистичну обробку результатів, кореляційний аналіз та використання методів машинного навчання для прогнозування можливих залишків продуктів.

Розвиток систем моніторингу залишків відкриває широкі можливості для подальших досліджень, особливо у сфері оптимізації ланцюгів постачань,

аналітики великих даних та машинного навчання для прогнозування попиту та поведінки споживачів.

УДК 004.94:681.5
Латипов О.В.[1], Миронова Н.О.[2]
[1] студ. гр. БК-613м НУ «Запорізька політехніка»
[2] канд. техн. наук, доц. НУ «Запорізька політехніка»

ВИКОРИСТАННЯ РОБОТИЗОВАНИХ ТЕХНОЛОГІЙ В БУДІВНИЦТВІ

Використання роботизованих технологій в будівництві є досить актуальною темою через переваги, які воно надає, а саме:

– підвищення продуктивності будівництва за рахунок автоматизації монотонних завдань;

– зменшення витрат на робочу силу;

– зменшення небезпечних ситуацій для людини під час будівництва завдяки можливості віддаленого керування процесом;

– можливість виконувати роботи, недоступні людині.

Метою дослідження є визначення перспективи розвитку та огляд вже існуючих прикладів використання роботизованих технологій в сфері будівництва.

Використання роботизованих технологій в будівництві буде продовжувати зростати в найближчі роки. Роботи можуть бути використані для будівництва складних будівель, які було б важко або неможливо побудувати за допомогою традиційних методів. Для створення будівельних матеріалів та компонентів, що в свою чергу може призвести до більш швидкого та дешевого будівництва, може використовуватися 3D-друк. Автономність будівельних машин зможе дозволити виконання завдань на будівельних майданчиках навіть без втручання людини. Роботизовані технології також можуть бути використані для знесення будівель задля уникнення небезпечних ситуацій працівниками.

Серед прикладів використання роботизованих технологій в будівництві можна виділити будівельний 3D-принтер та промислових роботів.

Будівельний 3D-принтер – це машина, яка може будувати будинки, наносячи матеріал (бетон, наприклад) шар за шаром. По суті, будується тільки каркас будинку. Інші елементи, такі як вікна, електрика або сантехніка, повинні встановлюватися окремо. Однак бетонні 3D-принтери можна використовувати для друку мостів, лавок або просто вуличних прикрас [1].

Рисунок 1 – Будівельний 3D-принтер [1]

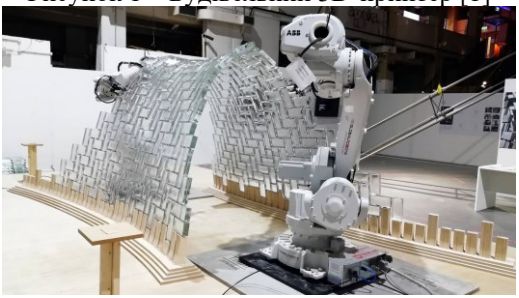


Рисунок 2 – Промислові роботи будують скляну арку[2]

Двоє дослідників з Прінстона, архітектор Стефана Парашо та інженер Сігрід Адріансенс використали двох промислових роботів, наданих британською компанією Global Robots, щоб побудувати сховище висотою 7 футів, 12 футів у поперечнику та довжиною 21 фут, виготовлене з 338 прозорих скляних цеглин [2].

Використання роботизованих технологій в будівництві має потенціал революціонізувати галузь, роблячи її більш продуктивною та безпечною.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Les meilleures imprimantes 3D de maisons en 2023. Aniwaa. – URL: https://www.aniwaa.com/fr/guide-achat/imprimantes-3d/imprimante-3d-construction-maison/

2. Robots and humans collaborate to revolutionize architecture. Princeton University. – URL: https://www.princeton.edu/news/2020/10/21/robots-and-humans-collaborate-revolutionize-architecture

УДК 004.94:681.5
Кузовін Д.С.[1], Миронова Н.О.[2]
[1] студ. гр. БК-613м НУ «Запорізька політехніка»
[2] канд. техн. наук, доц. НУ «Запорізька політехніка»

ІНТЕЛЕКТУАЛЬНІ РОБОТИЗОВАНІ СИСТЕМИ У МЕДИЦИНІ

На сьогоднішній день використання роботизованих систем у медицині є актуальною темою у сучасному медичному контексті. З розвитком технологій та зростанням можливостей штучного інтелекту та робототехніки зростає інтерес до застосування автоматизованих систем у різних галузях, включаючи медицину. Це зумовлено не лише прагненням до поліпшення результатів лікування, а й необхідністю впоратися зі зростаючим навантаженням на медичний персонал. Також застосування роботизованих систем у медицині може покращити точність та результати діагностичних процедур та реабілітації, що призводить до підвищення ефективності лікування та зниження ризиків для пацієнтів.

Впровадження роботизованих систем у медицину може мати потенціал зекономити ресурси та знизити витрати на охорону здоров'я у довгостроковій перспективі. Це пов'язано з покращенням результатів лікування, скороченням часу перебування пацієнта в лікарні та зменшенням ймовірності ускладнень. Дослідження інтелектуальних роботизованих систем у медицині спрямоване на вивчення застосування сучасних технологій робототехніки та штучного інтелекту для покращення медичної практики, реабілітацію та діагностику. У ході дослідження буде проаналізовано різноманітність існуючих роботизованих систем, їх функціональні можливості та застосування у медичних закладах.

В роботі буде розглянуто:

– стан та тенденції розвитку роботизованих систем у медицині: Буде проведено огляд останніх досягнень у галузі робототехніки, а також аналіз сучасних тенденцій розвитку та застосування роботизованих систем у медичних цілях;

– роботизовані системи у реабілітації та фізіотерапії: Вивчиться використання роботизованих пристроїв у процесі реабілітації пацієнтів після травм та операцій, а також у програмі фізіотерапії для покращення моторних функцій та відновлення певних навичок;

– алгоритми управління штучного інтелекту в медичних роботах: Проаналізовано застосування методів машинного навчання та штучного інтелекту для розробки розумних алгоритмів управління медичними роботами, а також їх ролі у підвищенні точності та безпеки процедур.

В якості прикладу роботизованих систем у медицині можна розглянути RehaBot (рис.1). Система RehaBot звільняє фізіотерапевтів від інтенсивного

та повторюваного навчального навантаження та покращує якість медичної допомоги пацієнтам із неврологічними та м'язовими травмами або функціональними порушеннями. Цю систему можна запустити в лікарні під прямим моніторингом та інтерактивним контролем, а також на віддалені за допомогою телеприсутності.

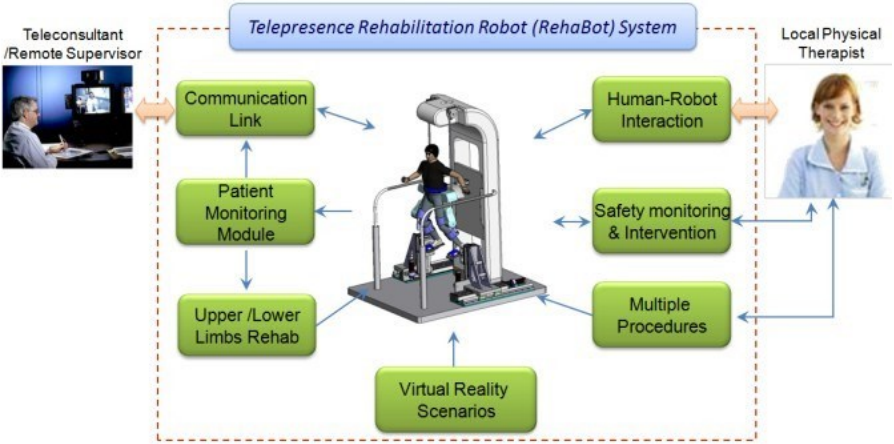


Рисунок 1 – Система RehaBot[1]

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. An advanced rehabilitation robotic system for augmenting healthcare. – URL: https://ieeexplore.ieee.org/abstract/document/6090384 (дата звернення: 15.04.2024).

УДК 004.9
Кондратенко В.Ю.[1], Миронова Н.О.[2]
[1] студ. гр. БК-613м НУ «Запорізька політехніка»
[2] канд. техн. наук, доц. НУ «Запорізька політехніка»

РОЗУМНЕ ВИРОБНИЦТВО

Розумне виробництво – це концепція, яка в останні роки набула значного значення в індустріальному секторі. Ця концепція передбачає використання передових технологій, таких як штучний інтелект, Internet of Things (IoT), аналітику даних та автоматизація процесів для оптимізації виробничих процесів.

Актуальність розумного виробництва полягає в тому, що воно дозволяє підприємствам збільшити ефективність виробництва, знизити витрати, підвищити якість продукції та пришвидшити час виготовлення. Воно також сприяє створенню більш гнучких та адаптивних виробничих систем, які можуть швидко реагувати на зміни в попиті або виробничому середовищі.

У ході дослідження буде проаналізовано розробку та впровадження інноваційних технологічних рішень, які забезпечать підвищення ефективності, продуктивності та конкурентоспроможності у виробництві.

В роботі буде розглянуто розумні системи управління та моніторингу:

– розробка інтегрованих систем моніторингу та управління для автоматизації процесів у промисловості. Буде проведено огляд архітектури системи, включаючи вибір апаратних та програмних засобів, можливості використання різноманітних датчиків, контролерів, промислових комп'ютерів та іншого обладнання;

– дослідження методів обробки великих даних для прийняття рішень у реальному часі на основі даних, зібраних з різних датчиків та пристроїв. Буде проведено огляд методів та технологій для збору даних у реальному часі з різних датчиків та пристроїв, а також можливості їхньої потокової обробки для ефективного аналізу великих обсягів даних, що надходять з різних джерел;

– аналіз можливостей використання IoT для створення розумних систем, здатних адаптуватися до умов і вимог, що змінюються. Це може включати реакцію на зміни в навколишньому середовищі, використання контекстної інформації для прийняття рішень та автоматизацію процесів.

УДК 004.942
Шило А.П[1], Куляба-Харитонова Т.І.[2]
[1] студ. гр. БК-613м НУ «Запорізька політехніка»
[2] старш. викл. НУ «Запорізька політехніка»

РОЗРОБКА СИСТЕМИ ДЛЯ КЕРУВАННЯ РОЗУМНИМ ОФІСОМ

Створення системи розумного офісу передбачає розробку програмного забезпечення для керування пристроями усередині будівлі та візуалізацію роботи офісу у 3D-середовищі для налаштування та тестування роботи [1].

Основним алгоритмом роботи системи розумного офісу є послідовний процес, що включає кілька етапів.

Запуск віртуального середовища, яке відтворює об'єкти та системи розумного офісу. Це розроблене програмне забезпечення, яке дозволяє відображати роботу різних пристроїв у смарт офісі.

Запускається мікроконтролер STM32, який відповідає за керування системами у будівлі. Цей мікроконтролер виконує функцію пульта керування та дозволяє з'єднуватись з обладнанням офісу. З'єднання між мікроконтролером та віртуальним середовищем встановлюється через Ethernet. STM32 підключаєтеся до віртуального середовища за указаним IP адресом та портом. Для передачі даних було обрано протокол Modbus, який широко застосовується в промисловості для організації зв'язку між електронними пристроями.

Після підключення мікроконтролеру до віртуального середовища користувач може взаємодіяти з системою за допомогою розробленого зручного інтерфейсу. Користувач натискає на кнопку, віртуальне середовище отримує відповідний запит та виконує відповідну дію. Наприклад, якщо користувач натискає кнопку "Увімкнути світло", віртуальне середовище відправляє команду на увімкнення відповідного освітлення.

Ця система дозволяє ефективно керувати розумним офісу та тестувати їх роботу у віртуальному середовищі перед впровадженням у реальний офісний простір. Також підвищує швидкість налагодження системи, що дозволяє забезпечити оптимальний функціонал для офісного приміщення з урахуванням потреб користувачів.

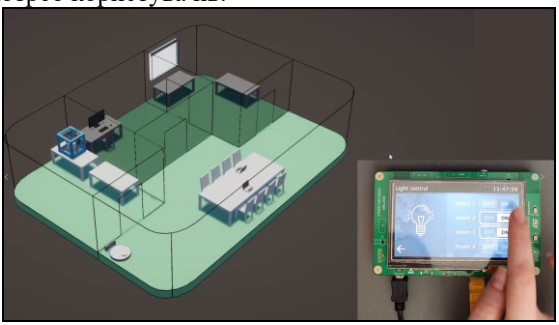


Рисунок 1 – Демонстрація роботи віртуального середовища з пультом керування

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Цифрові двійники для промислового застосування. Визначення, комерційна цінність, аспекти розробки, стандарти та приклади використання//An Industrial Internet Consortium White Paper Version 1.0 2020-02-18. https://atep.kpi.ua/wp-content/uploads/2021/12/iic_digital_twins_industrial_apps_white_paper_2020-02-18-ukr.pdf

УДК 681.5
Кірічков А.А.[1], Тягунова М.Ю.[2]
[1] студ. гр. БК-612м НУ «Запорізька політехніка»
[2] канд. техн. наук, доц. НУ «Запорізька політехніка»

СИСТЕМА АВТОМАТИЗОВАНОГО ПРОЄКТУВАННЯ ТЕХНОЛОГІЧНИХ ПРОЦЕСІВ МЕХАНІЧНОЇ ОБРОБКИ ДЕТАЛЕЙ ПРИСТОСУВАНЬ ОСНАЩЕННЯ

Сучасне виробництво пристосувань оснащення для обробки та складання деталей авіаційних двигунів є мінливою галуззю промисловості, що швидко розвивається.

Використання нового багатофункціонального або модернізація існуючого обладнання для виготовлення пристосувань оснащення, постійна зміна виробничого завдання як за типами оснащення, що виготовляється, так і за його обсягом та термінами виготовлення, зумовлює необхідність розробки нових технологічних процесів (ТП) механообробки деталей пристосувань оснащення.

Виходячи з того, що виробництво пристосувань оснащення найчастіше є дрібносерійним чи одиничним, на його технологічну підготовку витрачається суттєвий час. Актуальним стає завдання скорочення термінів розробки та впровадження ТП та виготовлення часто мінливої номенклатури пристосувань оснащення.

У результаті, посилюються вимоги до скорочення термінів розробки нових ТП, причому зростає складність розробки, оскільки вже при проєктуванні ТП механообробки необхідно враховувати існуючі умови виробництва та швидко адаптуватися до змін виробничої ситуації. Тобто, необхідне створення системи автоматизованої розробки ТП САПР ТП, яка дозволяє значно скоротити час розробки ТП механічної обробки (виготовлення) деталей пристосувань оснащення [1].

САПР ТП має взаємодіяти з іншими системами підприємства, наприклад, у CAD-системі конструктор проєктує деталь, 3D-модель та конструкторську документацію (КД), яка зберігатиметься в базі даних КД.

На основі отриманої 3D-моделі в CAM-системі також за потреби розробляється керуюча програма (КП) для обробки деталей на верстаті з ЧПК, яка зберігатиметься в базі даних ПК.

За наявності інтеграції між CAD-системою та САПР ТП технолог під час створення ТП вказує 3D-модель деталі як об'єкт для зчитування даних про розміри елементів деталі.

Сформована технологічна документація (ТД) зберігається в електронному вигляді у базі даних розроблених ТП.

При розробці ТП використовуються такі бази даних (БД):

БД технологічних можливостей обладнання, що містить у собі всі відомості та параметри про верстати, що використовуються на підприємстві. Вона має містити: максимальні геометричні параметри обробки деталей, потужність, завантаженість та інші технічні та технологічні параметри;

БД інструментів та оснащення, що містить у собі всі відомості та параметри про інструменти та технологічне оснащення, що використовуються на підприємстві. Вона має містити: геометричні параметри та наявність інструменті, матеріал з якого виготовлені інструменти та інші технічні та технологічні параметри;

БД типових ТП (по технологічним типам деталей), що включає всю номенклатуру деталей, які коли-небудь виготовлялися на підприємстві та ТП виробництва яких вже достатньо відпрацьовані та є загальнодоступною базою, матеріал якої може коригуватися у міру оновлення номенклатури виготовляємих деталей та в процесі удосконалення вже розроблених ТП.

При цьому, маючи розроблену ТП на один із технологічних типів деталей, технологи можуть надалі у короткі терміни розробити ТД для деталей цього технологічного типу, які мають схожі конструкції різних типорозмірів та внаслідок цього схожі ТП обробки, звісно з урахуванням ресурсів, досвіду, наявного обладнання та інструментів на підприємстві. При цьому ТП для кожного типу деталей містить всі можливі технологічні операції.

Створення ТП відбувається у певній послідовності: один із типових ТП для наявного технологічного типу приймається за базовий та потім він коригується, наприклад, технолог змінює текст переходу, вибирає інше обладнання чи інструмент, додає нові переходи. Чинники, що впливають на структуру ТП та його зміст, це є особливість конкретної конструкції деталі а також особистість технолога та його творчість. Однак ТП повинен розроблятися з урахуванням усієї інформації, яка використовується в ТД, оскільки результатом формування ТП є отримання комплекту документів, згідно яких буде виготовлено деталь, яка повинна відповідати вимогам КД [2].

Також технолог повинен мати зворотний зв’язок із виробництвом під час виготовлення деталей для можливості своєчасно коригувати ТД при нагальній потребі (наприклад, при виявленні помилок конструктора у КД).

САПР ТП повинен мати модуль для розрахунку режимів різання. Модуль можна використовувати за наявності даних про оброблювані поверхні, інструмент та оснащення, які необхідні для розрахунку режимів. В основі розрахунків у таких модулях треба брати табличні дані із загальномашинобудівних довідників з нормативами режимів різання.

Таким чином, передбачається позбавити технолога від рутинної та монотонної роботи з виправлення документації, та покласти це на систему,

управління якою він буде здійснювати. Застосування САПР дозволяє суттєво спростити технологічну підготовку виробництва деталей пристосувань оснащення.

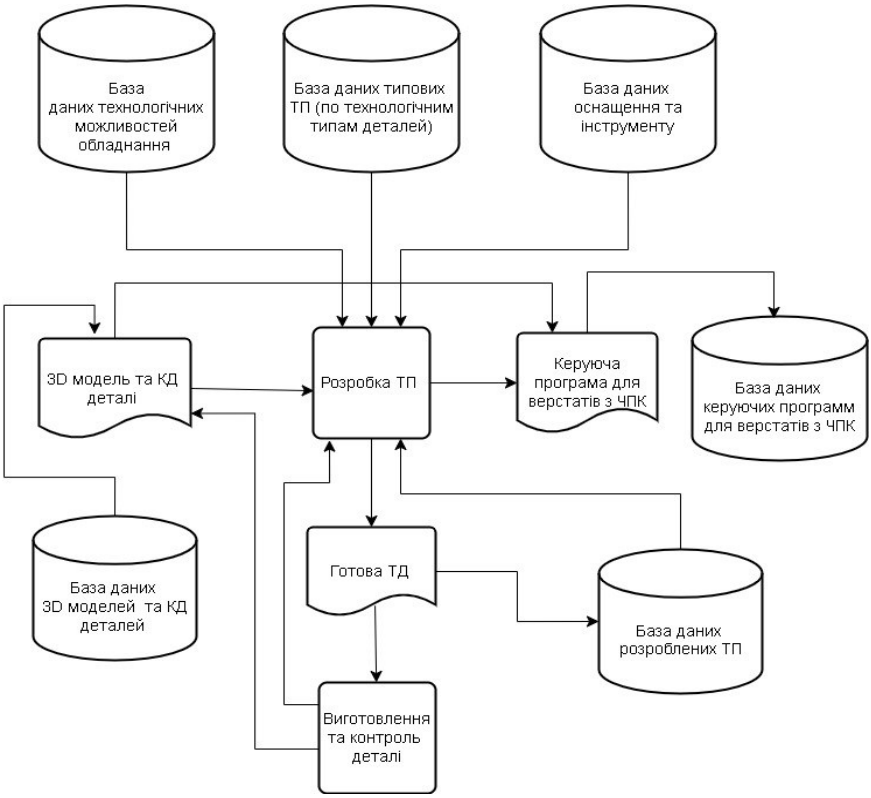


Рисунок 1 – Структура САПР ТП

Отримана структура САПР ТП дозволяє подати внутрішні та зовнішні інформаційні взаємодії під час розробки ТД.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Синтез робототехнічних систем в машинобудуванні / [Л. Є. Пелевін, К. І. Почка, О. М. Гаркавенко]. – К.: Інтерсервіс, 2016. – 258 с.

2. Хлинін А. А., Дербаба В. А. Новітні технології робототехніки в машинобудуванні. – 2023. – с.135 – 137.

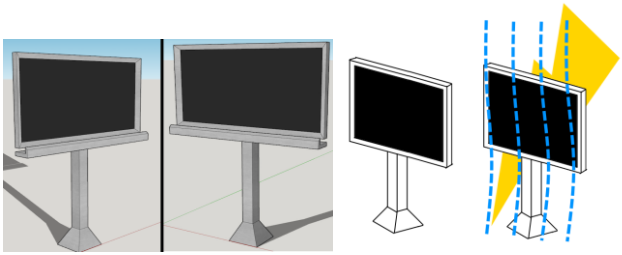
УДК 620.191.2:681.324
Поспєєва І.Є.[1], Резниченко П.О.[2], Савченко О.І.[3]
[1] старш. викл. НУ «Запорізька політехніка»
[2] студ. гр. БК-611 НУ «Запорізька політехніка»
[3] студ. гр. БК-612сп НУ «Запорізька політехніка»

ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ ВУЛИЧНИХ LED-ЕКРАНІВ ВІД ДЕСТАБІЛІЗУЮЧОГО ВПЛИВУ ВОЛОГИ

У сучасному міському середовищі вуличні LED екрани стають все більш популярними для вуличної реклами. Однак, однією з головних проблем, з якою стикаються власники та оператори таких екранів, є забезпечення їх стійкості до вологи та інших погодних умов. Негативний вплив вологості може призвести до несправностей, втрати якості зображення та скорочення терміну служби обладнання.

Для вирішення цієї проблеми проводиться дослідження та розробка ефективних методів захисту вуличних LED екранів-білбордів від дестабілізуючого впливу вологи. З урахуванням важливості цього аспекту у сучасній рекламній індустрії, розробка надійних та інноваційних методів захисту є ключовою.

LED екрани — це екрани, які використовують Light Emitting Diodes (світлодіоди) як джерела світла для створення зображення[1]. Вони використовуються для відображення тексту, зображень та відео і можуть знаходитися у різноманітних місцях, включаючи вулиці, виставкові центри, театри, стадіони та інші сценічні та комерційні простори. LED екрани відрізняються від традиційних екранів на основі рідких кристалів (LCD) або плазми (PDP) за їхньою можливістю працювати в яскравих зовнішніх умовах та високою роздільною здатністю.



а) б)

а) розроблена модель білборду ; б) схематично зображений білборд під впливами вологи.

Рисунок 1

У наукових дослідженнях застосовується комплекс заходів для захисту LED екранів від впливу вологи. Один із таких заходів - герметизація, яка полягає в створенні герметичного ущільнення внутрішніх компонентів екрана, щоб запобігти проникненню вологи та інших шкідливих факторів.

Додатково застосовується спеціальний захист вибраних компонентів екрана, який може включати в себе покриття з водовідштовхувальних матеріалів або захисні оболонки, які ефективно утримують вологу подалі від електронних елементів.

Ці методи дозволяють підвищити стійкість LED екранів до вологи та забезпечити їх надійну роботу в різних погодних умовах, зберігаючи якість зображення та тривалий термін служби обладнання.

Рисунок 2 – приблизний вигляд розробленого білборду в зазначених вологих умовах.

Захист LED екранів[2]. від впливу вологи на вулиці є надзвичайно важливою задачею у забезпеченні тривалої та надійної роботи рекламних засобів. Нижче наведено деякі факти, що підкреслюють важливість цього заходу захисту.

Збереження якості зображення: вологість може спричинити появу конденсату або корозію на електронних компонентах екрана, що призводить до втрати якості зображення та функціональних проблем.

Запобігання несправностям: попадання вологи в електроніку може спричинити коротке замикання, перегрів та інші несправності, які можуть призвести до збоїв у роботі екрана.

Збереження інвестицій: LED екрани є значними інвестиціями для власників та операторів. Захист від вологи допомагає зберегти цінність обладнання та забезпечити його тривалий термін служби.

Мінімізація ризику витрат: ремонт або заміна LED екранів через пошкодження від вологи може бути дорогим та часо- і ресурсозатратним процесом. Ефективний захист може мінімізувати цей ризик.

Забезпечення безперервності реклами: у випадку вуличної реклами, непередбачувані проблеми з екраном можуть призвести до припинення рекламних кампаній та втрати прибутку. Захист від вологи допомагає забезпечити безперервність рекламних показів.

Отже, ефективний захист LED екранів який був розроблений у науковій статті від впливу вологи є критично важливим для забезпечення їхньої стійкості, надійності та тривалої роботи на вулиці.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Автор не вказаний. "Three Protection Standards For Outdoor LED Screen". Asetek. Дата оновлення: Н/Д. URL: https://www.eagerled.com/three-protection-standards-for-outdoor-led-screen/ (дата звернення: 07.04.2024).

2. Julia Jiang. " How to protect your LED displays from moisture and water?". Asetek. Дата оновлення: 28.02.2023. URL:https://www.linkedin.com/pulse/how-protect-your-led-displays-from-moisture-water-julia-jiang (дата звернення: 09.04.2024).

УДК 62-712

Поспеєва І.Є.[1], Савченко О.І.[2], Резниченко П.О.[3]
[1] старш. викл. НУ «Запорізька політехніка»
[2] студ. гр. БК-612сп НУ «Запорізька політехніка»
[3] студ. гр. БК-611 НУ «Запорізька політехніка»

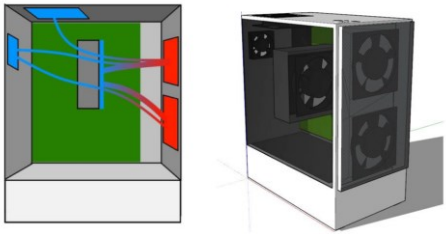
МОДЕЛЮВАННЯ ПОВІТРЯНОГО ОХОЛОДЖЕННЯ ДЛЯ КОМП'ЮТЕРНИХ СИСТЕМ

В сучасному інформаційно-комунікаційному світі комп'ютери та інші електронні пристрої виступають у ролі невід'ємної складової кібернетичної екосистеми. Однак, разом з їх безперечними перевагами постає й низка проблем, що потребує невідкладного вирішення. Однією з найактуальніших є проблема підтримки оптимального теплового режиму, який впливає на продуктивність та тривалість служби цих пристроїв.

Виконуючи складні обчислення та операції, комп'ютери генерують істотну кількість тепла. Цей процес викликає потребу в ефективному відведенні тепла для подальшої роботи систем, оскільки навіть невеликий

перегрів може мати серйозні наслідки від погіршення продуктивності до повного знищення дорогого обладнання.

Тепловий режим — це ключовий аспект функціонування будь-якої електронної системи, що визначає рівень теплових навантажень, які вона генерує та відводить під час роботи. Цей параметр відіграє критичну роль у забезпеченні оптимальних умов для працездатності та довговічності пристроїв. Відповідний тепловий режим дозволяє уникнути перегріву, який може призвести до збоїв у роботі електронної апаратури та зниження її ефективності. Одним з найбільш ефективних способів відведення тепла є конвективний теплообмін, який реалізується з застосуванням перфорованих корпусів (див. рис. 1(а)).



а) б)

а) симуляція циркуляції повітря; б) обраний корпус

Рисунок 1

Для ефективного контролю та вимірювання теплового режиму[1] обраного корпусу (див. рис. 1(б)) електронного пристрою рекомендовано використовувати програмне забезпечення, що забезпечує надійну та точну діагностику температурних показників. Серед різноманітних програмних засобів, призначених для моніторингу теплового режиму обчислювальних систем, варто відзначити досить популярний та добре відомий продукт — AIDA64.

AIDA64 — відомий своєю високою точністю та надійністю вимірів температурного режиму компонентів ПК. Це програмне забезпечення дозволяє в реальному часі моніторити температуру процесора, графічного процесора, твердотільного накопичувача та інших важливих елементів системи. Завдяки широкому спектру функцій та деталізованим звітам, AIDA64 забезпечує користувачу повну інформацію щодо теплового стану його обладнання, що дозволяє оперативно реагувати на будь-які зміни температурних показників. Приклад реального стрес-тесту для розробленого корпусу зображений на рис. 2.

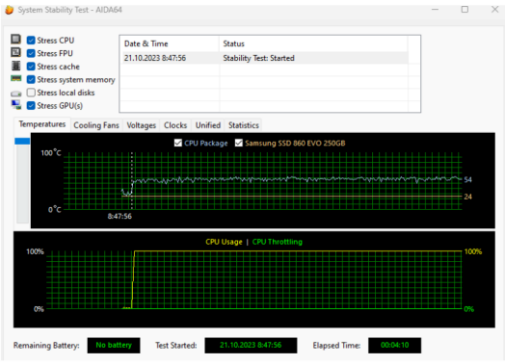


Рисунок 2 – Результати стрес-тесту

Вибір між повітряним та рідинним охолодженням є ключовим аспектом при проектуванні систем охолодження для електронних пристроїв. При вирішенні цього питання необхідно враховувати різноманітні технічні, економічні та функціональні фактори.

Перш за все, враховуючи ефективність та надійність, повітряне охолодження має ряд переваг, які роблять його більш привабливим вибором для багатьох сценаріїв застосування. Порівняно з рідинною, система повітряного охолодження менш складна за конструкцією та використанням, що знижує витрати на підтримку та обслуговування пристроїв. Крім того, системи повітряного охолодження зазвичай мають менше деталей, що зменшує ризик виникнення поломок та збільшує їхню довговічність.[2]

До інших переваг системи повітряного охолодження слід віднести простоту її монтажу та налагодження, а також можливість ефективного використання в широкому спектрі умов експлуатації. Важливим аспектом також є більша стійкість до витоку та корозії, оскільки система повітряного охолодження не має проблем, пов'язаних з рідинами, такими як протікання або замерзання.

Отже, з урахуванням всіх цих переваг, повітряне охолодження виявляється оптимальним вибором для обраного корпусу. Це дає показники температури, що забезпечують оптимальні умови для стабільної роботи обчислювальної системи і підвищать її продуктивність під великим навантаженням.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Win Aung (Editor). Cooling Techniques for Computers: 1st Edition. CRC Press, 1991. - 420 pages.

2. Автор не вказаний. "Liquid Cooling vs Air Cooling – What is the better cooling solution for PC enthusiasts and gamers?". Asetek. Дата оновлення: Н/Д. URL:https://www.asetek.com/liquid-cooling/gaming-enthusiasts/air-vs-liquid/ (дата звернення: 08.04.2024).

УДК 004.896
Фарафонов О.Ю.[1] Лактіонов Є.І.[2]
[1] канд. техн. наук, доц. НУ «Запорізька політехніка»
[2] студ. гр. БК-513м НУ «Запорізька політехніка»

МЕТОД РОЗПІЗНАВАННЯ ОБ'ЄКТІВ ЗА ДОПОМОГОЮ АЛГОРИТМІВ ШІ

У сучасному світі штучний інтелект (ШІ) відіграє ключову роль у розпізнаванні об'єктів. Розвиток алгоритмів навчання і машинного зору відкриває нові можливості, але також стикається з низкою викликів.

Одним із головних викликів є продуктивність при обробці зображень у режимі реального часу, цей процес вимагає швидких та ефективних алгоритмів. Затримки у обробці можуть призвести до втрати важливої інформації або до аварій у випадку дронів.

Є безліч різноманітних алгоритмів розпізнавання образів, але на мій погляд найперспективнішою для рішення проблеми продуктивності при обробці зображень у режимі реального часу є система You Only Look Once (YOLO).

YOLO (J. Redmon et al., 2016) безпосередньо передбачає граничні рамки та ймовірності класів за допомогою однієї мережі за одну одиницю часу. Простота моделі YOLO дозволяє працювати в режимі реального часу.

На рисунку 1 показано спрощений алгоритм роботи системи.

Рисунок 1 – Алгоритм роботи YOLO

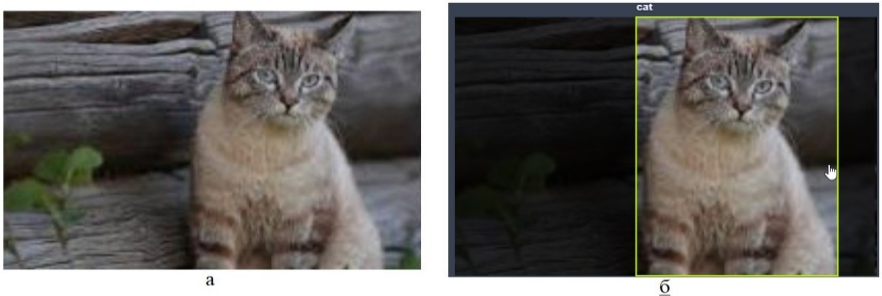
Мережа має 24 згорткових шари, за якими слідують 2 повнозв'язкові шари. Шари скорочення з фільтрами, за якими йдуть згорткові шари 3x3, замінюють вихідні початкові модулі.

Якщо описати роботу моделі максимально просто, то вона ділить зображення на імовірні об'єкти, обводячі їх «рамками», та порівнюючи з базою даних ImageNet.

Плюси YOLO алгоритму, це швидкість, цей алгоритм має високу швидкість виявлення, оскільки виявляє об'єкти у режиму реального часу, висока точність. Але YOLO страждає від помилок з визначенням відстані до об’єкта та має проблеми з ідентифікацією найближчих предметів.

Для прикладу візьмемо довільний наземний дрон, якому потрібно оминати тварин, на дроні встановлена камера, наприклад Escam V380, її роздільної здатність вистачить для даної задачі, на дроні є Wi-fi модуль для зв’язку з комп’ютером з нейромережою Yolo. Після завантаження баз даних у мережу наприклад бази Roboflow-100/animals-ij5d2, все готово до роботи.

При фіксацією камери у режимі відео об’єкта, фото надано на рисунку 2 а. Буде перебрано, деякі класи об’єктів, наприклад курка, корова, собака, лисиця, коза, людина, єнот, та встановлено збіжність з одним з цих об’єктів, після образ буде обведено рамкою з підписом імовірного класу, рисунок 2 б.



а б

а - фото невідомого об’єкта; б - об’єкт ідентифіковано

Рисунок 2 – Обробка фото нейромережою

Гуртуючись на поточному значенні швидкості обробки YOLOV7 досягає 3,5 м\с на кадр у порівнянні з YOLOV4 12 мс або популярним YOLOV3 29 мс. Зверніть увагу на те, як введення YOLO призвело до значного скорочення часу виведення порівняно з будь-якими раніше встановленими методами, наприклад у порівнянні методом Mask R-CNN (333 мс). Відставання останнього у швидкості обробки зображень більше ніж у 10 разів.

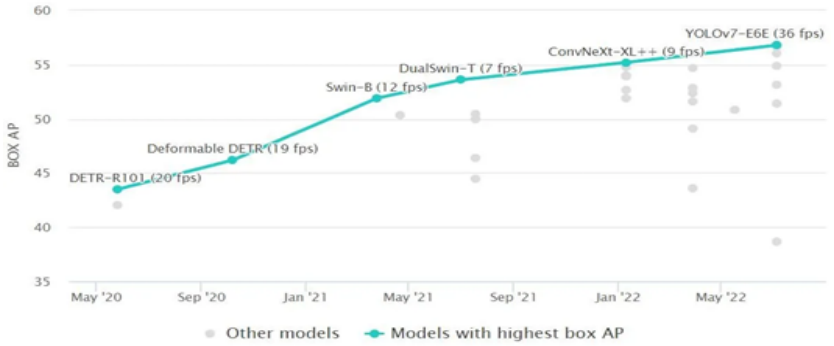


Рисунок 3 - Графік коефіцієнта точності та швидкості різні алгоритмів.

З рисунку 3 можна побачити що алгоритм розпізнавання об’єктів YOLO має найкраще співвідношення точності розпізнавання до швидкості.

Аналізуючи отримані дані використання алгоритму YOLOV7 може значною мірою вирішити питання продуктивності при обробці зображень у режимі реального часу.

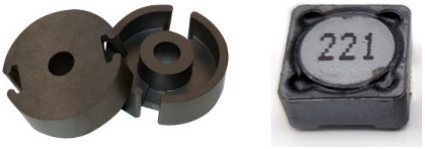
УДК 621.3
Фарафонов О. Ю.[1], Марченко В. Р.[2]
[1] канд. техн. наук, доц. НУ «Запорізька політехніка»
[2] студ. гр. БК-511сп НУ «Запорізька політехніка»

ПОРІВНЯННЯ КОНСТРУКЦІЇ ІНДУКТИВНИХ ДАТЧИКІВ ДЛЯ ВИМІРЮВАЧА ТОВЩИНИ ЛАКОФАРБОВОГО ПОКРИТТЯ

Мета проєкту полягає в створенні простого засобу для вимірювання товщини лакофарбового покриття на автомобілях. Це допоможе оцінити стан кузова перед покупкою або після проведення ремонтних робіт.

Шляхом вимірювання індуктивності котушки, яка змінюється залежно від товщини лакофарбового покриття, і подальшої обробки даних за допомогою Arduino, пристрій виводить інформацію про товщину покриття на дисплей або світлодіодні індикатори.

На рисунку 1 наведено запропоновану конструкцію котушки індуктивності для датчика та дросель.



А - датчик з броньовим осерддям. Б - Дросель

Рисунок 1 - датчики

Формула дозволяє обчислити параметри котушки індуктивності, враховуючи вплив зазору в магнітному контурі.

$$L[\text{мГн}] = \mu_0 \left(\frac{\mu_i}{1+g\mu_i/l_e}\right) N^2 \frac{A_e}{l_e} \quad (1)$$

Де μ_0 - магнітна константа; μ_i - початкова магнітна проникність сердечника; g - зазор в магнітному контурі; l_e - ефективна довжина магнітного контуру; N - кількість витків; A_e - ефективна площа поперечного перерізу магнітного контуру.

У таблиці 1 представлено порівняння параметрів двох типів індуктивних датчиків: котушки індуктивності та дроселя SMD CDRH125-101NC 100мкГн1.

Таблиця 1

Параметр	Котушка індуктивності - 100 витків проволоки 0,1 мм кв. на феритовому сердечнику d=8	Дросель SMD CDRH125-101NC 100мкГн1
μ0	4π * 10^-7 Гн/м	4π * 10^-7 Гн/м
μi	2300	2300
g	0.3 мм = 0.0003 м	0.3 мм = 0.0003 м
le	25.13 мм = 0.02513 м	12.3 мм = 0.0123 м
N	100	500
Ae	50.27 мм² = 0.00005027 м²	12.3 * 6.0 мм² = 0.0000738 м²
Індуктивність	0.002 Гн (або 2 мГн)	0.076 Гн

Таблиця 2 наводить порівняльний аналіз індуктивності котушки індуктивності з різними зазорами.

Дросель SMD CDRH125-101NC 100мкГн1 виявився більш індуктивним порівняно з саморобною котушкою індуктивності. Отже, дросель може бути кращим вибором для використання у вимірювачі товщини лакофарбового покриття на автомобілях, оскільки він має більшу індуктивність та виготовлений за промисловими стандартами, що робить його більш надійним.

Таблиця 2

Зазор (м)	Індуктивність (Гн)
0.0001	0.00569
0.0002	0.00299
0.0003	0.00203
0.0004	0.00153
0.0005	0.00123

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Розрахунок індуктивних котушек [Електронний ресурс]. – Режим доступу: https://coil32.net/ru/pot-core.html

2. CDRH125/LDNP-100NC – Режим доступу: https://eu.mouser.com/ProductDetail/Sumida/CDRH125-LDNP-100NC?qs=mT6umqgwvA2ksaalVYbstQ%3D%3D

УДК 681.396

Фарафонов О.Ю.[1], Назаров Є.О.[2]
[1] канд. техн. наук, доц. НУ «Запорізька Політехніка»
[2] студ. групи БК-513м, НУ «Запорізька Політехніка»

ТЕХНОЛОГІЯ РАДІОЧАСТОТНОЇ ІДЕНТИФІКАЦІЇ (RFID)

Радіочастотна ідентифікація (RFID) являє собою технологію бездротового зчитування і запису даних, що використовує радіочастотні хвилі. Вона зазвичай складається з міток (або транспондерів), які містять електронну інформацію, і зчитувачів, які отримують цю інформацію.

Перша демонстрація сучасних RFID-чипів (на ефекті зворотного розсіювання), як пасивних, так і активних, була проведена в Дослідницькій Лабораторії Лос Аламоса в 1973 році. Портативна система працювала на частоті 915 Мгц і використовувала 12 бітових міток.

Перший патент, пов'язаний власне з назвою RFID, був виданий Чарльзу Валтону в 1983 році.

За типом джерела живлення RFID-мітки діляться на:

– пасивні;

– активні;

– напівпасивні.

За типом використовуваної пам'яті RFID-мітки діляться на:

– RO (Read Only): дані записуються тільки один раз, відразу при виготовленні. Такі мітки придатні тільки для ідентифікації. Ніяку нову інформацію в них записати не можна, і їх практично неможливо підробляти.

– WORM (Write Once Read Many): окрім унікального ідентифікатора такі мітки містять блок одноразово записуваної пам'яті, яку надалі можна багато разів читати.

– RW (Read and Write): такі мітки містять ідентифікатор і блок пам'яті для читання/запису інформації. Дані в них можуть бути перезаписані багаторазово.

Зчитувачі, які читають інформацію з RFID-міток і записують в них дані можуть бути постійно підключеними до облікової системи, або працювати автономно. Залежно від частотного діапазону мітки, дистанція стійкого зчитування і запису даних може бути різна. Розрізняють стаціонарні та мобільні.

Основні переваги RFID-технології:

– для RFID не потрібний контакт або пряма видимість;

– RFID-мітки читаються швидко і точно (наближаючись до сто відсоткової ідентифікації);

– RFID-мітки несуть велику кількість інформації і можуть бути інтелектуальними.

Недоліки RFID-технології:

– в деяких випадках мітки не деактивуються повністю, є можливість повторного спрацьовування;

– мітку можна виявити і в багатьох випадках пошкодити;

– технічно можливо збирати приватну інформацію - національність та інші дані з паспортів, куплену літературу і т. п.

Для забезпечення більшої точності, швидкості та ефективності ідентифікації об’єктів за допомогою систем RFID можна покращити алгоритми зчитування RFID.

Покращення алгоритмів зчитування можна виконати за допомогою наступних шляхів:

– оптимізація параметрів зчитування: розробка алгоритмів, які автоматично оптимізують параметри зчитування, такі як потужність сигналу, частота і швидкість передачі даних, для максимально ефективного зчитування міток у різних умовах. Алгоритми можуть автоматично налаштовувати потужність передачі сигналу в залежності від відстані до міток та характеристик оточуючого середовища. Наприклад, на великих відстанях може знадобитися висока потужність сигналу, а на невеликих - менша, щоб уникнути перешкод. Алгоритми можуть автоматично підбирати оптимальну частоту зчитування в залежності від інтерференції та інших факторів, що можуть впливати на ефективність зчитування. Алгоритми можуть динамічно змінювати швидкість передачі даних для забезпечення оптимальної продуктивності та надійності зчитування, враховуючи фактори, такі як завантаженість мережі та якість зв'язку;

– створення адаптивні алгоритми зчитування: створення алгоритмів, які адаптивно реагують на зміни в середовищі та умовах зчитування, такі як зміни в перешкодах або відстані до міток, для забезпечення стабільного та надійного зчитування. Алгоритми можуть автоматично переключати частоту зчитування для уникнення перешкод та мінімізації втрат сигналу. Наприклад, в разі виникнення інтерференції на одній частоті алгоритм може автоматично перемикнутися на іншу частоту зчитування. Адаптивні алгоритми зможуть використовувати дані з датчиків або зовнішніх джерел, таких як інформація про стан середовища або про рух об'єктів, для адаптації параметрів зчитування. Адаптивні алгоритми можуть також враховувати не лише стабільність зчитування, але й його ефективність. Наприклад, вони можуть динамічно змінювати параметри зчитування для максимізації кількості успішно зчитаних міток або мінімізації часу, потрібного для зчитування;

– управління множинними мітками: Розробка алгоритмів, які ефективно керують багатьма мітками, що знаходяться в полі зчитування одночасно для уникнення конфліктів та максимізації швидкості зчитування за допомогою використання протоколів, які дозволяють зчитувачу взаємодіяти з кількома мітками одночасно, наприклад за допомогою розподілених алгоритмів доступу, таких як протоколи Aloha або слотування. Розробка алгоритмів антиколізії, які дозволяють виявляти та розв'язувати конфлікти між мітками, що відповідають одночасно.

УДК 621.3
Фарафонов О.Ю.[1], Савгачев О.В.[2]
[1] канд. техн. наук, доц. НУ «Запорізька політехніка»
[2] студ. гр. БК-511сп НУ «Запорізька політехніка»

ПОРІВНЯННЯ РІЗНИХ ВИДІВ СКАНЕРІВ ВІДБИТКІВ ПАЛЬЦІВ

Система контролю доступу призначена для захисту цінних ресурсів у окремих приміщеннях. Метою розробки цієї системи є покращення безпеки, якщо для входу у приміщення використовується звичайний замок, до нього легко проникнути. У нашому ж випадку ми додаємо додатковий захист від проникнення за допомогою сканера відбитків пальців.

Для забезпечення безпеки у цьому проекті використовується сканер відбитків пальців R305, яким має інтерфейс підключення UART, та п’ятий клас безпеки, що є найвищім з представлених на ринку. У таблиці 1 наведені різні моделі сканерів відбитків пальців.

Таблиця 1 – Моделі сканерів відбитків пальців та їх характеристики

Характеристики	R305	R502	GT511C3	DigitalPersona U are U 4500	Essl Biometric Nex Touche
Інтерфейс	USB, UART	USB, UART	UART	USB	USB
Сенсор	Оптичний	Оптичний	Напівпровідниковий	Напівпровідниковий	Напівпровідниковий
Розмір сенсора	14x18 мм	20x25 мм	14x25 мм	16x24 мм	12.8x18 мм
Роздільна здатність	512 dpi	500 dpi	512 dpi	508 dpi	500 dpi
Процесор	ARM Cortex-M3	ARM Cortex-M3	Невідомо	Власний процесор	STM32F103CBT6
Швидкість захоплення	15 кадрів/с	15 кадрів/с	16 кадрів/с	20 кадрів/с	8 кадрів/с
Захист	ESD, вологозахист	ESD, вологозахист	ESD, вологозахист	ESD, вологозахист, антистатичний захист	ESD, вологозахист
Сумісність ОС	Windows, Linux, macOS, Android Arduino	Windows, Linux, macOS, Android, Arduino	Windows, Linux, Arduino	Windows, Linux, macOS	Windows, Linux
Програмне забезпечення	FingerVein SDK	FingerVein SDK	ПЗ від виробника	DigitalPersona SDK	Стандартні драйвери та SDK
Додаткові функції	Живе визначення нитки, низьке енергоспоживання	Живе визначення нитки	Живе визначення нитки	Захист від підробок, шифрування даних	Живе визначення нитки
Ціна	30-60$	20-40$	15-35$	80-150$	50-100$

R305 та R502 використовують FingerVein SDK, розроблений компанією Ronly спеціально для їхніх власних сканерів. Це повнофункціональний набір інструментів з бібліотеками для різних мов програмування, що підтримує захоплення, реєстрацію, верифікацію відбитків пальців та виявлення підробок. FingerVein SDK оптимізований для вбудованих систем та низького енергоспоживання.

У GT511C3 та Essl Biometric Nex Touche деталі програмного забезпечення невідомі. Скорі ж за все використовує стандартне ПЗ від виробника з обмеженими можливостями порівняно зі спеціалізованими.

DigitalPersona U are U 4500 постачається з потужним DigitalPersona SDK від відомого виробника біометричних рішень. Який має додаткові функції безпеки, шифрування даних та захисту від підробок відбитків пальців. Ймовірно є найдорожчим ПЗ з наданих сенсорів.

Сканери відбитків пальців з інтерфейсом USB можуть легко підключатися до будь-якого пристрою на базі операційних систем Windows, Linux, macOS та Android, забезпечуючи зручний доступ і безпеку. Тоді як сканери з додатковим інтерфейсом UART відкривають можливості для підключення до широкого спектру пристроїв, включаючи платформи типу Arduino, розширюючи їхню функціональність та застосування.

Таким чином, спеціалізовані SDK, як FingerVein та DigitalPersona, пропонують ширші можливості, кращу безпеку та підтримку різних платформ, але за вищу ціну. Базове програмне забезпечення зазвичай має обмежену функціональність. Професійні біометричні рішення, як правило, використовують потужніші спеціалізовані SDK для інтеграції сканерів відбитків пальців.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. V. Rusyna, S. Subbotinb and A. Sambasc. “Simple Autonomous Security System Based On Arduino UNO Platform and Fingerprint Scanner Module: A Stu dy Case ”, pp 1-10 April 27, 2021,

2. NEUROtechnology [Електронний ресурс]. – Режим доступу: https://www.neurotechnology.com/fingerprint-scanner-digitalpersona-u-are-u-4500.html

3. eSSL [Електронний ресурс]. – Режим доступу: https://www.esslsecurity.com/

4. ZKTeco [Електронний ресурс]. – Режим доступу: https://zkteco.technology/en/product/zkfingervein-sdk-windows/

5. HITACHI [Електронний ресурс]. – Режим доступу: https://www.hitachi.com/products/it/veinid/products/logical_access.html

УДК 621.396.674.1
Фурманова Н.І.[1], Деркач Д.В.[2]
[1] канд. техн. наук, доц. НУ «Запорізька політехніка»
[2] студ. гр. БК-513м НУ «Запорізька політехніка»

ПЛАНАРНІ МІКРОСМУЖКОВІ АНТЕНИ

Мікросмужкові антени (МСА), виготовлені за технологією ІС, забезпечують високу повторюваність розмірів, низьку вартість, малу металоємність, габаритні розміри, масу.

Планарні мікросмужкові антени – являють собою типи антен, які виготовляються на плоских підкладках, таких як плати з мікрополосковими структурами. Вони використовуються для передачі та отримання радіосигналів у бездротових комунікаційних системах. Ці антени мають компактні розміри, високу ефективність та можуть бути легко інтегровані в мікроелектронні пристрої, такі як смартфони, медичні пристрої, безпілотні літальні апарати та інші пристрої інтернету речей.

Типи планарних мікросмужкових антен, які використовуються залежно від конкретних потреб і вимог системи. Найрозповсюджені з них:

– Прямокутні мікросмужкові антени: Це один з найпоширеніших типів планарних антен, що складаються з прямокутної мікросмужки. Вони можуть бути одиночними або складними з декількох мікросмужок;

– Круглі мікросмужкові антени: Такі антени мають форму кола або диска і часто використовуються в аплікаціях, де потрібне кругле або сферичне випромінювання сигналу;

– Планарні спіральні антени: Ці антени мають спіральну форму і зазвичай використовуються у високочастотних діапазонах, таких як GPS та супут–- Планарні антени з подвійним полюсом (Dipole Antennas): Вони складаються з двох провідників, які розташовані паралельно на плоскій підкладці;

– Планарні антени з використанням розсіювачів (Scattering Antennas): Ці антени використовують мікроструктури, що розсіюють сигнал, для отримання бажаної діаграми напрямленості та характеристик випромінювання;

– Планарні фазові антени: Вони використовують елементи змінної фази для створення бажаної діаграми напрямленості та керування напрямком випромінювання.

Планарні мікросмужкові антени мають декілька основних переваг, серед яких:

– Компактність: Вони виготовляються на плоских підкладках, що дозволяє їм бути дуже компактними. Це особливо важливо в сучасних мікроелектронних пристроях, де простір є обмеженим;

– Легка інтеграція: Планарні мікросмужкові антени легко інтегруються з іншими компонентами мікроелектронних пристроїв на одній платі. Це спрощує виробництво та зменшує витрати на виробництво;

– Висока ефективність: Вони можуть мати високу ефективність випромінювання, що дозволяє отримувати сильний сигнал на великі відстані;

- Гнучкість дизайну: Планарні мікросмужкові антени можуть бути легко змінюваними та оптимізованими для різних застосувань та вимог, зокрема для роботи в різних частотних діапазонах та отримання різних діаграм напрямленості;

– Низькі витрати виробництва: Виготовлення планарних антен може бути відносно дешевим, особливо у великих обсягах виробництва;

– Добра сумісність з мікрополосковими структурами: Це дозволяє комбінувати планарні антени з іншими мікрополосковими пристроями та системами для створення інтегрованих мікроелектронних пристроїв.

Оптимізація конструкції планарних антен може бути проведена з метою покращення їх частотних характеристик. Ось деякі стратегії оптимізації:

– Геометрична оптимізація: Зміна геометрії антени, таких як розміри мікросмужок, форма, кут нахилу, може покращити її частотні характеристики. Наприклад, збільшення довжини мікросмужок або зміна їх форми може підвищити ефективність антени у певному частотному діапазоні;

– Матеріали: Використання відповідних матеріалів для планарних антен може покращити їх частотні характеристики. Наприклад, використання матеріалів з низькою діелектричною проникливістю може знизити втрати сигналу та покращити коефіцієнт підсилення;

– Технології виготовлення: Вибір відповідних технологій виготовлення, таких як високоточна фотолітографія або плазмове травлення, може допомогти досягти більш точної геометрії та кращих електричних характеристик антени;

– Керування діаграмою напрямленості: Оптимізація форми та розміру мікросмужок може допомогти керувати діаграмою напрямленості антени, щоб забезпечити бажану напрямленість сигналу;

– Використання апертурного синтезу: Використання апертурного синтезу дозволяє створювати складні мікроструктури антен, що можуть мати покращені частотні та просторові характеристики.

УДК 621.396
Фурманова Н.І.[1], Жулай А.О.[2]
[1] канд. техн. наук, доц. НУ «Запорізька політехніка»
[2] студ. гр. БК-511сп НУ «Запорізька політехніка»

СИСТЕМА МОНІТОРИНГУ ТА ОПОВІЩЕННЯ ПРО БЕЗПЕКУ У ВУГІЛЬНІЙ ШАХТІ

Система моніторингу головних показників призначена для попередження аварійних ситуацій у шахті. Причиною розробки такої системи є велика кількість проблем, які призводять до травмування та до більш гірших наслідків.

Система збирає дані про рівень метану та задимленість під землею, а також показники вологості повітря та температуру. Потім дані передаються до оператора, й у випадку, якщо якісь показники перевищують нормальні значення, то сповіщають працівників напряму. Основні заміри робляться в декількох ключових місцях таких як: лава, де є великий ризик виникнення аварійних ситуацій, шлях транспортування вугілля та ділянку, де здійснюється підйом видобутого на поверхню чи підйомника для працюючих. На рисунку 1 наведено приклад екрану для оператора, із відображенням усіх показників, які вимірюються в шахті.

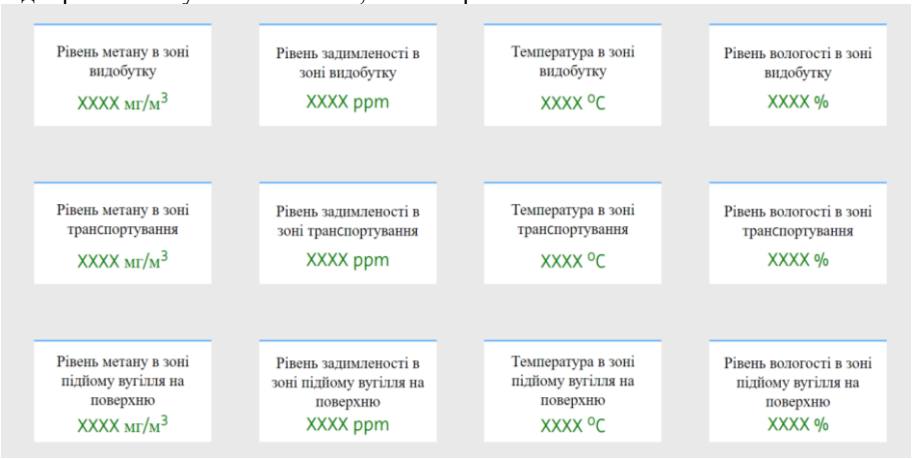


Рисунок 1 – Екран оператора

Системи зв'язку, що використовуються в підземному видобутку розділяються на телефоні системи, радіозв’язок та локальний зв’язок. Найбільш пріоритетним є радіозв’язок, через мобільність, тобто такий різновид зв’язку необмежений наявність проводів.

На дальність проходження сигналу проводилися досліди, де досліджувалися такі частоти як, 455 і 915 МГц та 2,45 і 5,8 ГГц, де дійшли до висновку, що високі частоти краще себе показують в обох поляризаціях [1]. Подібні випробування проводили також на пострадянському просторі, в цьому випадку використовувалися частоти 1,8 та 1,9 ГГц, де прийшли до висновку, що ці частоти ефективний, коли капітальні виробки великого перерізу, більше ніж 10 м.

Радіозв'язок обмежений дальністю передачі сигналу, тому для збільшення дальності використовують ретранслятори. Проаналізувавши результати досліджень, можна сказати, що відстань між ретранслятором та джерелом сигналу чи приймачем, залежить від перешкод, які трапляються на шляху. Тому для умов досліду, де досліджувалися частоти 2,4 та 5,8 ГГц, ретранслятор потрібно розташовувати на відстані 350 – 390 м, для досліду із частотами 1,8 та 1,9 ГГц – 700 м, тільки за умови, що невелика кількість металевих перешкод.

Основним параметром, на який потрібно орієнтуватися, що вберегти працюючих, є рівень метану. Загазованість повітря на різних ділянка різна, але в середньому допустимий вміст метану в гірничих виробках не вище, чим 1% [2].

Також важливо враховувати вологість повітря та температуру у шахті. Невідповідність стандартам кліматичних умов може спричинити замерзання шахтних штолень та проходів, пошкодження каналів вентиляційних систем, а також зсуви та обвали [3].

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. C. Zhou, T. Plass, R. Jacksha and J. A. Waynert, "RF Propagation in Mines and Tunnels: Extensive measurements for vertically, horizontally, and cross-polarized signals in mines and tunnels," in IEEE Antennas and Propagation Magazine, vol. 57, no. 4, pp. 88-102, Aug. 2015, doi: 10.1109/MAP.2015.2453881

2. Мала гірнича енциклопедія : у 3 т. / за ред. В. С. Білецького. — Д. : Донбас, 2007. — Т. 2 : Л — Р. — С. 138-139.

3. Тепловий режим та тепловий баланс шахт і рудників [Електронний ресурс]. – Режим доступу: https://studfile.net/preview/6308693/page:2/

УДК 621.372.543.3
Фурманова Н.І.[1], Худзій Б.С.[2]
[1] канд. техн. наук, доц. НУ «Запорізька політехніка»
[2] студ. гр. БК-513м НУ «Запорізька політехніка»

МОДЕЛЮВАННЯ С-ПОДІБНИХ МІКРОСМУЖКОВИХ ФІЛЬТРІВ

Смуговий фільтр з характеристиками мікрокомпактності, хорошими характеристиками, низькою вартістю та простотою використання був у центрі увазі при мініатюризації пристроїв.

Тому розробка двосмугових фільтрів з низькою вартістю та високими характеристиками наразі представляє великий інтерес. Мікросмужкові фільтри можуть бути легко змонтовані на діелектричній підкладці і забезпечують більш гнучке проектування схеми.

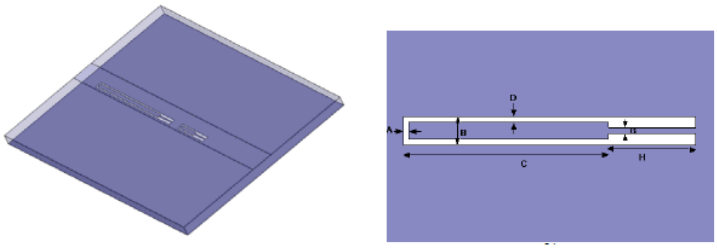
Традиційна топологія цього типу мікросмужкових фільтрів – це фільтр другого порядку з асиметричною структурою. Фільтр складається з двох розімкнутих резонаторів у С-подібній конфігурації, що забезпечує одну резонансну частоту. Але використовуючи дві структури однакової форми з різними розмірами, можна спроектувати двосмуговий фільтр.

Частотними характеристиками даного фільтру можна керувати, змінюючи параметри дефектної заземлювальної структури (Defected Ground Structure), такі як ширина і довжина обох С-подібних решіток. Крім того, відстань між двома структурами можна регулювати для отримання необхідних частотних характеристик.

Структури з дефектним заземленням були представлені у 1999 році. Ці нові структури, які були виявлені на фотонних заборонених зонах, можуть бути застосовані при проектуванні микрохвильових планарних схем таких, як фільтри.

Розподіл струму заземлення мікросмужкового контуру може бути суттєво змінений шляхом травлення структури, що призводить до зміни параметрів лінії передачі. DGS-структури компактні, мають невеликі розміри та пристосовані до мініатюризації планарних мікрохвильових схем. Крім того, ці структури можна моделювати за допомогою простих резонансних контурів, а отже, їхні параметри легко вирахувати, що дає перевагу при проектуванні мікрохвильових та міліметрових схем.

Тривимірне зображення фільтра показано на рис. 1. Видно, що фільтр складається з двох С-подібних структур з різними розмірами (табл. 1), що резонують на різних частотах.



а б

а – 3-D вигляд; б – елементарна комірка.
Рисунок 1 – Геометрія С-подібного DGS-фільтра.

Характеристики відкидання залежать не тільки від розмірів кожної комірки, але й від відстані між двома комірками, що впливає на АЧХ фільтру.

Таблиця 1 – Розміри комірок С-подібного фільтру(всі розміри у мм).

	Комірка 1 (2,4 ГГц)	Комірка 2 (5,7 ГГц)
A	0.2	0.2
B	1	1
C	14.2	3.4
D	0.2	0.2
G	0.2	0.2
H	3	2.5

Можна зробити висновок , що збільшення відстані між двома комірками призводить до зниження резонансної частоти і смуги пропускання першої резонансної частоти. Для другої резонансної частоти при збільшенні вище згаданого параметру: резонансна частота зменшується, а смуга пропускання майже не змінюється.

Даний двосмуговий фільтр має малі розміри і вузьку смугу пропускання. Такий фільтр доцільно використовувати при проектуванні мікрохвильових схем, антенних решіток, де потрібне придушення кількох смуг частот та мініатюризації схем.

Зав. кафедри Олександр МАЛИЙ

Відповідальний на факультеті Станіслав ШАПТАЛА

СЕКЦІЯ «ІНФОРМАЦІЙНА БЕЗПЕКА ТА НАНОЕЛЕКТРОНІКА»

УДК 539.21
Pogosov V.V.[1]
[1] Doctor of Physical and Mathematical Sciences, professor NU «Zaporizhzhia Polytechnic»

EFFECT OF SURFACE STATES ON ELECTRON FIELD EMISSION FROM SEMICONDUCTORS

In the process of developing new technologies of solid-state and vacuum electronics, a particular problem is the creation of new efficient semiconductor emitters. The final theory of the laws of the emission current of semiconductors has not yet been developed.

In experimental studies for semiconductors, both elementary and binary, with an atomically clean surface, it has been shown that the field emission current is generated by electrons from the valence band, and in some cases surface states located in the band gap and valence bands of the semiconductor take part in the emission [1-3].

In [1], the energy distribution of electrons from a field emitter made of an *n*-GaAs single crystal coated with a thin layer of its own oxide was experimentally studied. Further, the energy distribution of electrons from the (111) plane of a germanium single crystal during field emission and the dependence of the energy spectra on the external field strength were experimentally studied. The main peak corresponds to energies below the bottom of the valence band E_c.

Traditional field emission calculations neglected to the semiconductor surface potential profile in the presence of an external field. In this case, no attention is paid to the presence of a narrow potential well formed by the polarization potential near the surface

$$V_p(x) = \left(\frac{\varepsilon - 1}{\varepsilon + 1}\right)\frac{e^2}{4x}, \tag{1}$$

where ε is the dielectric constant of material, and e is the elementary positive charge. Eq. (1) is exactly the image charge potential at the plane surface of a dielectric.

In this work, the one-dimensional Schrödinger equation for the ABDFG potential at the Figure (the case of no field) for germanium and gallium arsenide is solved. The image potential (1) is cut off at a distance x_0 (in the Bohr radii a_0)

from the surface. Then the electron momentum component is quantized along the normal to the surface ($x-$axis), and parallel to the surface ($yz-$plane), the spectrum of values of the momentum components is continuous. Figure shows an energy diagram that corresponds well to zero temperature, when a semiconductor turns into a dielectric.

The presence of a surface subband (SS) was discovered, the bottom E_{ss} of which lies bellow the valence band one E_v (see Table). At a non-zero temperature, as well as the presence of an electric field and band bending, the ACDFJ-potential profile will be even more favorable for the formation of the deeper band. Thus, the presence of a surface band below the Fermi level and E_v qualitatively explains the shift in the energy spectrum of emitted electrons discovered in [1, 2].

Table – Imput data and calculated the surface subband bottom E_{ss}.

Material	E_c, eV	E_v, eV	ε	x_0, a_0	E_{ss}, eV
Ge	-4,00	-4,75	16,0	0,15	-6,59
GaAs	-4,07	-5,50	12,5	0,15	-6,37

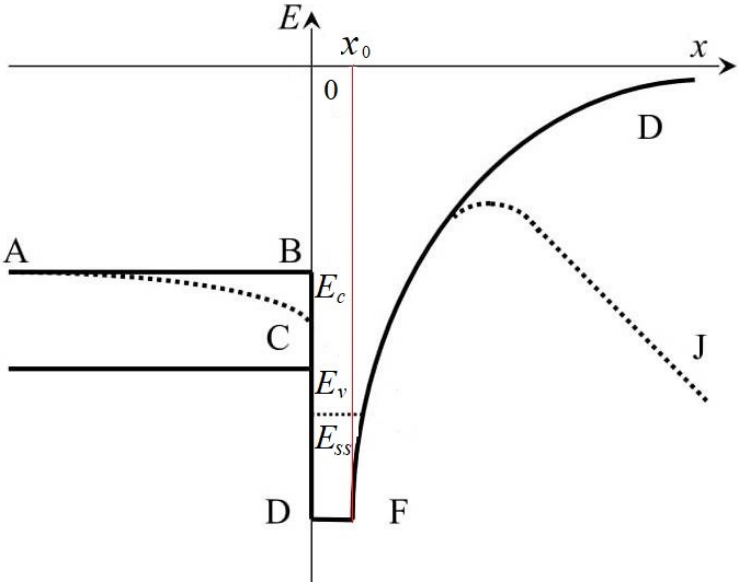


Figure – Energy diagram for electrons near the surface

REFERENCES

1. V.D. Kalganov, N.V. Mileshkina, and S.A. Sapronov, Vacuum, 46, 559-574 (1995).

2. T. Deck, A.O. Moscardini, V.D. Kalganov, N.V. Mileshkina, J. Phys.: Condens. Matter, **20**, 395002-9 (2008).

3. L. Lin, R. Jacobs, T. Ma, D. Chen, J. Booske, D. Morgan, Appl. Phys. Rev. 19, 037001-39 (2023).

УДК 539.219.3
Матюшин В.М.[1]
[1] д-р фіз.-мат. наук, проф. НУ ”Запорізька політехніка”

МЕХАНІЗМИ СТИМУЛЮВАННЯ ДИФУЗІЙНИХ ПРОЦЕСІВ В ТВЕРДОМУ ТІЛІ ПРИ ПРОТІКАННІ НА ЙОГО ПОВЕРХНІ ЕКЗОТЕРМІЧНОЇ ХІМІЧНОЇ РЕАКЦІЇ

Задача стимулювання дифузійних процесів є актуальною в електронній технології. Одним із напрямків стимулювання є дія енергії, що виділяється в результаті протікання на поверхні напівпровідникового кристала екзотермічної хімічної реакції. Енергія при цьому виділяється поблизу поверхні, тобто локально, що дуже зручно при створенні складних напівпровідникових структур.

В якості модельної було вибрана реакція рекомбінації атомів водню в молекули, в результаті якої виділяється 4,48 Ев на один акт рекомбінації. Виділення такої великої енергії в малому об’ємі (приблизно 10 $нм^2$) приводить до того, що локальна температура різко підвищується до декілька тисяч градусів. Це може привести до протікання різноманітних фізичних процесів, в т.ч. до розпиленню, збудженню електронної підсистеми, амортизації, рекристалізації, генерації вакансії, виникненню дефектів по Шотткі і Френкелю, що може привести до прискоренню гетеродифузії.

Інтенсивність рекомбінації суттєво підвищує присутність невеликих кількостей металевих домішок на поверхні кристала-каталізатора. Частина енергії, що виділяється, понесеться молекулою. Але більша частина передається кристалу. Ця енергія приводить до виникнення локальних коливальних станів атомів градки, які релаксують шляхом генерації фононів. Все це приводить до стимуляції дифузійних процесів в локальних приповерхневих шарах напівпровідникових структур.

В якості модельних використовувались структури металева плівка-напівпровідник. Використовувались метали: мідь, нікель, срібло, золото та індій. Ці метали дифундують в германії і кремнії різними механізмами: міжвузільним, дисоціативним і вакансійним, які можуть протікати одночасно, але з перевагою одного із них (все залежить від температури кристала).

На стимуляцію гетеродифузії впливають наступні процеси.

Генерація фононів.

Час виділення енергії хімічної взаємодії атомів водню $\tau \sim 10^{-10}$ с (час обмінної взаємодії), тому механізм виділення й дисипації енергії укладається в уявлення про Θ-спалах. Оскільки температура в області Θ-спалаху велика (порядку температури плавлення матеріалу), то це приводить до збільшення інтенсивності процесу дефектоутворення. Генерація фононів може призвести

до переходу атома із вузла градки в міжвузілля, тобто виникнення пари вакансія-межвузільний атом (дефект по Френкелю). Розпилення атома з поверхні приводить до виникнення поверхневої вакансії (дефект по Шотткі), яка може втягуватися в об'єм. Підвищена дефектність та висока локальна температура в області Θ-спалаху ускладнюють відвід тепла. При цьому зростає роль багатофононних процесів, що прискорює дифузію атомів. Прискорюється дифузія домішкок, які переміщуються по вакансійному (нікель, срібло, золото, індій), міжвузільному (мідь – при високих температурах), дисоціативному (нікель, срібло, золото) механізмам.

Виникнення градієнту температур.

При дії атомарного водню в приповерхневих шарах кристала виникає значний градієнт температур. Це приводить к прискоренню дифузії домішок, особливо тих, що дифундують по міжвузільному та дисоціативному механізмам.

Збудження електронної системи.

Збудження електронної підсистеми навівпровідникових кристалах приводить до виникнення потоку електронів з поверхні в об'єм ("електронний вітер"), яка протикає при початку процесу обробки Н, а також виникненню електричних полів в приповерхневих шарах навівпровідника. Це прискорює гетеродифузію домішок, які дифундують у вигляді позитивних іонів, особливо по міжвузільному та дисоціативному механізмам (мідь, срібло, золото).

Таким чином, комплексна дія всіх механізмів приводить до значного стимулювання гетеродифузії всіх перерахованих домішок в навівпровідниковому кристалі.

УДК 621.382
Кривоус А.С.[1], Сніжной Г.В.[2], Солодовник А.І.[3]
[1] асп. НУ «Запорізька політехніка»
[2] д-р. техн. наук, проф. НУ «Запорізька політехніка»
[3] директор ТОВ «Елемент-Перетворювач»

АНАЛІЗ ФІЗИКО-ТЕХНОЛОГІЧНИХ ПРОБЛЕМ, ПОВ`ЯЗАНИХ З ВИМОГАМИ ДО МАТЕРІАЛІВ ДЛЯ СИЛОВОЇ ЕЛЕКТРОНІКИ

Основою енергоефективної економіки є високотехнологічна силова електроніка. Використання якісних та надійних силових напівпровідникових приладів (СНП) та силових напівпровідникових модулів (СНМ) сприяє заощадженню електроенергії в транспорті та промисловості. Якість СНП та СНМ залежить здебільшого від використання якісних матеріалів при виготовлені цих виробів. До основних матеріалів, що використовуються для виготовлення СНП та СНМ, відносяться монокристалічний кремній, мідь, молібден, матеріали для пасивації краєвого профілю напівпровідникової структури та металізовані керамічні підкладки.

Для виготовлення напівпровідникових структур використовується монокристалічний кремній різних діаметрів, який отримується методами Чохральського, безтигельної зонної плавки (БЗП) та БЗП з нейтронним легуванням кремнію. Кремній отриманий методом Чохральського значно дешевше кремнію отриманого БЗП та нейтронно-легованого кремнію, але він має суттєві недоліки – великий розмах значень та нестабільність питомого опору, обмеження по максимальному значенню питомого опору (не вище 100 Ом·см), великий вміст кисню та вуглецю. Через це, кремній отриманий методом Чохральського, використовують лише в приладах напругою до 1200 В та на струми до 100-200 А. Для приладів на більші напругу та струм використовують кремній отриманий методом БЗП. Він має відносно високу термостабільність та малий розмах значень питомого опору (≤5-7%). До недоліків можна віднести велику вартість.

Через велику різницю коефіцієнта теплового розширення кремнію та міді складно паяти напівпровідникову структуру одразу до мідного електроду. В якості термокомпенсаторів в СНП та СНМ використовують диски та пластини з молібдену. В термокомпенсаторах, які виготовляються з листового прокату, часто спостерігаються розшарування по краю диску. Це призводить до потрапляння хімічних реактивів до ущелин з ускладненням видалення їх під час технологічних процесів та збільшенню теплового опору СНП. У випадку виготовлення молібденових термокомпенсаторів способом порошкової металургії виникають проблеми виготовлення дисків малої товщини, пористості та міцності при механічній обробці.

Для виготовлення електродів для подання струму в СНП та СНМ використовують мідь. Для з`єднання електродів з керамічним корпусом, або з напівпровідниковою структурою, переважно використовується пайка в середовищі з високою концентрацією водню при високій температурі. Для запобігання утворенню «водневої крихкості» в струмопровідних електродах повинна використовуватись мідь з низьким вмістом кисню (<0,001%). Така мідь після процесу пайки залишається м`якою та не викликає великого механічного напруження в кремнії, що в багатьох випадках є корисними властивостями такої міді. Але у випадку, коли в СНП використовуються притискні контакти з зусиллям стиску >250 кг/см$^2$ або різьбові з`єднання з охолоджувачем, мідь починає «текти», через що параметри приладів можуть погіршуватися. Зокрема, відбувається послаблення зусилля стиску в притискних контактах та ін. Тому в мідь необхідно вносити зміцнюючи домішки, але ці домішки не повинні суттєво погіршувати електро- та теплопровідність міді.

Для утворення гальванічної розв`язки струмопровідних електродів в СНМ використовують діелектричні керамічні підкладки на основі Al_2O_3 та AlN з тонким (до 10-20 мкм) або з товстим (до 300 мкм) шаром міді. Існують проблеми недостатньої міцності адгезії металізації до керамічної поверхні, особливо до кераміки з AlN. Підкладки з AlN хоч і суттєво дорожче за підкладки з Al_2O_3, але мають теплопровідність у 8 разів більшу в порівнянні з Al_2O_3, а це дуже важливо при використанні в СНМ на великий струм. Останнім часом, в силовій електроніці поширення набули DBC (Direct Bonded Copper) підкладки з мідною фольгою на кераміці, але це накладає низку вимог до технологічних процесів під час виробництва силових напівпровідникових модулів: температура пайки обмежена 400℃ в середовищі водню. Крім того, товщина кераміки з DBC повинна бути до 0,5 мкм при товщині міді 0,3 мкм, а це зменшує електроміцність СНМ.

Для пасивації краєвого профілю фаски напівпровідникових структур використовують кремнійорганічні компаунди та багатокомпонентне скло. Головні проблеми цієї технологічної операції – це чистота захисних матеріалів, стабільність їх захисних властивостей, збереження заряду заданої величини на поверхні кремнію, який вони утворили, а також міцність адгезії захисного матеріалу до кремнію. Оскільки під час тривалої експлуатації СНП та СНМ піддаються циклічним тепловим навантаженням, які можуть погіршувати ВАХ приладів, необхідно забезпечувати високу міцність адгезії та стабільність захисного покриття на кремнії.

Наведені вище проблеми не можливо вирішити на виробництвах без залучення науковців за різним фахом освіти, підготовкою яких займається НУ «Запорізька політехніка».

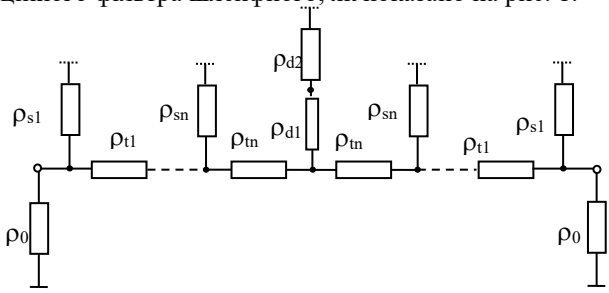
УДК 621.372.852.1
Карпуков Л.М.[1], Воскобойник В.О.[2], Савченко Ю. В.[3], Ісаченко Д.О.[4]
[1] д-р техн. наук, проф. НУ «Запорізька політехніка»
[2] канд. техн. наук, проф. НУ «Запорізька політехніка»
[3] канд. техн. наук, доц. Університету митної справи та фінансів
[4] студ. гр. БК-713сп НУ «Запорізька політехніка»

МЕТОД ПІДВИЩЕННЯ ВИБІРКОВОСТІ ШЛЕЙФНОГО ФІЛЬТРА НИЗЬКИХ ЧАСТОТ

Шлейфні фільтри знаходять широке застосування в системах передачі, прийому та захисту інформації завдяки простоті конструкції, можливості реалізації в мікросмужковому виконанні та технологічності при масовому виготовленні.

Традиційні структури шлейфних фільтрів, які складені з чвертьхвильових розімкнених шлейфів і відрізків ліній передачі, не мають достатньої вибірковості.

Підвищити вибірковість можна шляхом додавання двосекційного шлейфу, що забезпечує нуль коефіцієнта передачі в смузі загородження, до структури традиційного фільтра шлейфного, як показано на рис. 1.



.

Рисунок 1 – Структура фільтра з нулем коефіцієнта передачі

На рисунку ρ0, ρt, ρS - хвильові опори вхідного та вихідного портів, відрізків ліній та односекційних шлейфів, відповідно; ρd1, ρd2 – хвильові опори двосекційного шлейфу.

Мета роботи полягає у розробці методу синтезу фільтрів зі структурою на рис. 1 і рівнохвильовою характеристикою смуги пропускання.

Елементи структури фільтра характеризуються матрицями передачі:

– для відрізка лінії

$$T_t(\theta) = \cos(\theta)\,E + j\frac{\sin(\theta)}{2R_t}\begin{bmatrix} R_t^2+1 & -\left(R_t^2-1\right) \\ R_t^2-1 & -\left(R_t^2+1\right) \end{bmatrix}, A_{21_t} = 1; \qquad (1)$$

– для розімкнутого на кінці шлейфу

$$T_s(\theta) = \cos(\theta)E + j\frac{\sin(\theta)}{2R_s}\begin{bmatrix} 1 & 1 \\ -1 & -1 \end{bmatrix}, A_{21_s} = \cos(\theta); \qquad (2)$$

– для двосекційного розімкнутого на кінці шлейфу

$$\left.\begin{aligned} T_d(\theta) &= \left(\cos^2(\theta) - \cos^2(\theta_0)\right)E + j\frac{\sin(2\theta)}{4R_{d_1}}\begin{bmatrix} 1 & 1 \\ -1 & -1 \end{bmatrix}, \\ A_{21_d}(\theta) &= \cos^2(\theta) - \cos^2(\theta_0). \end{aligned}\right\} \qquad (3)$$

де E – поодинока матриця, $R_i=\rho_i/\rho_0$ – нормовані опори ліній; $j=\sqrt{-1}$ – уявна одиниця, θ-електрична довжина, θ_0 – кут, що відповідає нулю передачі.

Функція фільтрації цієї структури, що отримана при перемноженні матриць передач (1) - (3) її елементів, має вигляд:

$$F(\theta) = j\frac{\sin(\theta)\sum_{k=0}^{n_s} a_k \sin^{2k}(\theta)}{\cos^{n_s-1}(\theta)\left[\cos^2(\theta) - \cos^2(\theta_0)\right]}, \qquad (4)$$

де n_s - число односекційних шлейфів.

Функцією такого виду може бути представлена Чебишевська функція

$$F_a(\theta) = \cos\left\{ n_s \arccos\left[\frac{\sin(\theta)}{\sin(\theta_c)}\right] + (n_s - 1)\arccos\left[\frac{tg(\theta)}{tg(\theta_c)}\right] + 2\cos\left[\eta(\theta, \theta_0)\right]\right\}, \quad (5)$$

Яка має рівнохвильову характеристику в смузі від нуля до θ_c та має полюс при $\theta_0 > \theta_c$.

Тут

$$\eta(\theta, \theta_0) = h_0 \frac{\sin(\theta)}{\sin(\theta_c)} \Big/ \sqrt{1 - S(\theta)^2 / S(\theta_0)^2},$$

$$h_0 = \sqrt{1 - S(\theta_c)^2 / S(\theta_0)^2}.$$

Наприклад, для структури з трьох шлейфів (n_s=3) і двох ліній (n_t=2) при θ_c=0,7, θ_0=0,8 функція (5) набуде наступного вигляду:

$$F_a(\theta) = \frac{\sin(\theta)\sum_{k=0}^{2} b_k \sin^{2k}(\theta)}{\cos(\theta)\left[\cos^2(\theta) - \cos^2(\theta_0)\right]} \quad (6)$$

зі значеннями коефіцієнтів b=2,911; -20,816; 33,94.

Визначення оптимальних значень хвильових опорів фільтра, при яких його функція фільтрації збігається з (6), здійснюється з вирішення оптимізаційної задачі з цільовою функцією, що мінімізує різницю функцій $F(\theta)$ і $F_a(\theta)$ в діапазоні кутів від нуля до θ_c.

Для умов прикладу та для згасання α=0,1 Дб отримані такі нормовані значення хвильових опорів: R=0,823; 1,49; 2,081.

На рис. 2 для цих значень R наведена аплітудно-частотна характеристика фільтра (суцільна лінія). Пунктирною лінією на рисунку відзначено характеристику фільтра, що складається з трьох простих односекційних шлейфів та двох ліній з опорами R=0,746; 1,953; 0,447, отриманими з розв'язання аналогічного оптимізаційного завдання. У верхній

частині рисунку представлені рівнохвильові характеристики фільтрів у смузі пропускання.

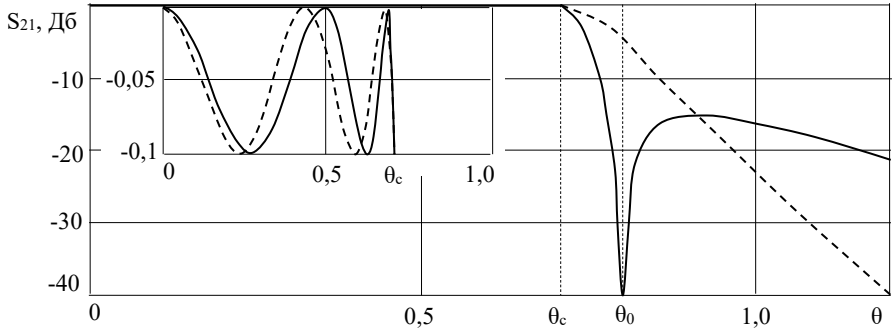


Рисунок 2 – Амплітудно-частотні характеристики фільтрів

Таким чином, введення двосекційного шлейфу в традиційну структуру шлейфного фільтра забезпечило істотне підвищення крутості спаду частотної характеристики в перехідній області.

УДК 539
Березовський О.Д.[1], Смирнова Н.А.[2], Рева В.І.[3], Коротун А.В.[4]
[1] студ. гр. БК-310 НУ «Запорізька політехніка»
[2] старш. викл. НУ «Запорізька політехніка»
[3] канд. фіз.-мат. наук, доц. НУ «Запорізька політехніка»
[4] канд. фіз.-мат. наук, проф. НУ «Запорізька політехніка»

ЗБУДЖЕННЯ ПЛАЗМОННИХ РЕЗОНАНСІВ У КОНІЧНИХ МЕТАЛІЧНИХ ОСТРІВЦЯХ НА ДІЕЛЕКТРИЧНІЙ ПІДКЛАДЦІ

У зв’язку з широким практичним використанням підсиленого поверхнею раманівського розсіювання (SERS) важливим є дослідження оптичних і плазмон них властивостей металічних острівців різної форми на діелектричній підкладці. Треба відмітити, що в основному теоретично та експериментально досліджувалися властивості плівок із острівцями напівсферичної [1] та еліпсоїдальної форм [2], а оптичні властивості острівців інших форм практично не досліджувалися.

Розглянемо металічний наностровець у формі конусу висотою h та з радіусом основи R, розташований на діелектричній підкладці з проникністю ε_d, а проникність оточуючого середовища дорівнює ε_m. Оскільки розміри

наноконусу набагато менші за довжину світлової хвилі, то оптичні властивості досліджуваної наносистеми можна вивчати в квазістатичному наближенні, в якому співвідношення для частотних залежностей діагональних компонент тензора поляризовності наноконусу на підкладці мають вигляд:

$$\alpha_{\perp(\parallel)}(\omega)=\frac{3\kappa_{\perp(\parallel)}V\bar{\alpha}_{\perp(\parallel)}(\omega)}{\kappa_{\perp(\parallel)}-\frac{\check{n}_d-\check{n}_m}{\check{n}_d+\check{n}_m}\bar{\alpha}_{\perp(\parallel)}(\omega)}, \qquad (1)$$

де $\kappa_\perp=4$, $\kappa_\parallel=8$, об'єм конусу $V=\frac{1}{3}\pi R^2 h$, $\bar{\alpha}_{\perp(\parallel)}(\omega)$ – діагональні компоненти тензора поляризовності поодинокого металічного конусу.

Умовою збудження поверхневих плазмонних резонансів у конічному наноострівці в бездисипативному наближенні буде рівність нулю знаменника виразу (1). У цьому випадку отримуємо наступні вирази для частот поверхневого плазмонного резонансу

$$\omega_{sp}^{\perp(\parallel)}=\frac{\omega_p}{\sqrt{\check{n}^\infty+\mathscr{L}_{\perp(\parallel)}\check{n}_m}}, \qquad (2)$$

де ω_p – плазмова частота; $\check{n}^\infty$ – внесок кристалічної ґратки в діелектричну проникність металу, а перенормовані фактори деполяризації визначається співвідношеннями

$$\mathscr{L}_{\perp(\parallel)}=\frac{\left(1-\mathcal{L}_{\perp(\parallel)}\right)\kappa_{\perp(\parallel)}\frac{\check{n}_d-\check{n}_m}{\check{n}_d+\check{n}_m}+1}{\kappa_{\perp(\parallel)}\mathcal{L}_{\perp(\parallel)}\frac{\check{n}_d-\check{n}_m}{\check{n}_d+\check{n}_m}-1}. \qquad (3)$$

Розмірні залежності факторів деполяризації мають вигляд

$$\mathcal{L}_\parallel=\frac{4-\acute{n}^2}{4+\acute{n}^2}, \qquad \mathcal{L}_\perp=\frac{\acute{n}^2}{4+\acute{n}^2}, \qquad (4)$$

де аспектне відношення для конусу $\acute{n}=2R/h$.

Таким чином, одержано розмірні залежності частот поздовжнього і поперечного поверхневого плазмонного резонансу. Розрахунки показали збільшення розщеплення частот поверхневого плазмонного резонансу зі зменшенням величини аспектного відношення для конічного острівця.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Коротун, А. В. Поляризовність металевої напівсфери на діелектричній підкладці / А. В. Коротун // Український фізичний журнал. – 2022. – Т. 67. – №12. – С. 858–868.

2. Wind M.M., Bobbert P.A., Vlieger J., Bedeaux D. The polarizability of a truncated spheres and oblate spheroids on a substrate comparison with experimental results // Thin Solid Films (1988). - V. 164. – P. 57 – 62.

УДК 512.21:621.391

Нагорна Н.М.[1]

[1] старш. викл. НУ «Запорізька політехніка»

РЕАЛІЗАЦІЯ КОДЕРІВ У САПР QUARTUS II

Виконані дослідження включають синтез моделей кодерів на основі генераторів псевдовипадкових послідовностей (ПВП), реалізацію розроблених кодерів на ПЛІС і оптимізацію їх параметрів.

При передаванні інформації по каналам зв’язку с завадами в прийнятих даних можуть виникати помилки. У роботі К. Шенона «Математична теорія зв’язку» стверджується: якщо швидкість створення джерелом повідомлення не перевищує пропускну здатність каналу, то при відповідному кодуванні і декодуванні можна звести ймовірність помилок в каналі до нуля. У зв’язку з цим постійно ведуться пошуки ефективних кодів, створення практично реалізовуваних схем кодування, які по своїм характеристикам наближались би до передбачених теоретично.

Задача кодера полягає у представленні передачі даних в максимально компактній і по можливості неспотвореній формі. Згортальний код створюється проходженням переданої інформаційної послідовності через лінійний регістр зсуву з кінцевим числом станів. Регістр зсуву складається з K (k-бітових) комірок та лінійного перетворювача, що складається з n функціональних генераторів і виконує алгебраїчні функції (рис.1).

Вхідні дані до кодера, які вважаються двійковими, просуваються уздовж регістра зсуву по k біт за період синхросигналу. Число вихідних бітів для кожної k-бітової вхідної послідовності дорівнює n. Отже, кодова швидкість, визначена як $R_c = k / n$, узгоджується з визначенням швидкості блокового коду. Параметр K називається кодовим обмеженням згортального коду.

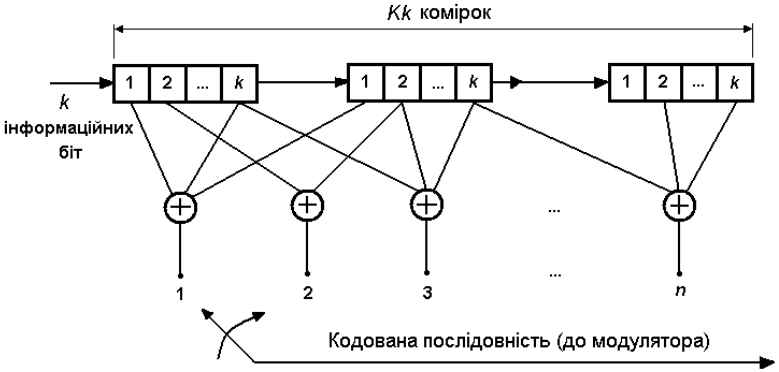


Рисунок 1 –Узагальнена структура згортального кодера

При дослідженнях на основі генераторів ПВП були розроблені дискретні моделі наступних кодерів: 1) з кодовим обмеженням 3, і швидкістю коду 1/3 (K = 3, k = 1, n = 3); 2) з кодовим обмеженням 2, і швидкістю коду 1/3 (K = 2, k = 2,n = 3; 3) з кодовим обмеженням 2, і швидкістю коду 1/2 (K=2, k = 2, n = 4), де K – кодове обмеження згортального коду, яке показує зі скількох комірок складається регістр зсуву, k –бітові комірки, n – кількість вихідних бітів, k / n – кодова швидкість. На основі розроблених моделей зазначених кодерів створювались їх моделі у вигляді цифрових автоматів Мура.

Для реалізації моделей складені програми, що описують алгоритми робіт кодерів на мові VHDL. Такий підхід дозволяє не робити прив'язку до конкретної технології реалізації кодерів, як цифрових пристроїв. За розробленими програми були реалізовані пристрої кодерів на базі ПЛІС. У САПР Quartus II за допомогою заданих критеріїв оптимізації було виконано оптимізацію проєктів кодерів за критеріями максимальної швидкодії і мінімального об'єму ресурсів ПЛІС.

Для прикладу, на рис. 2. показана діаграма станів згортального кодера з параметрами K = 2, k = 2, n = 4. На рис. 3 показана його часова діаграма.

Затримки розповсюдження між синхронізуючим сигналом і виходами вказаного кодера дорівнюють 4 нс.

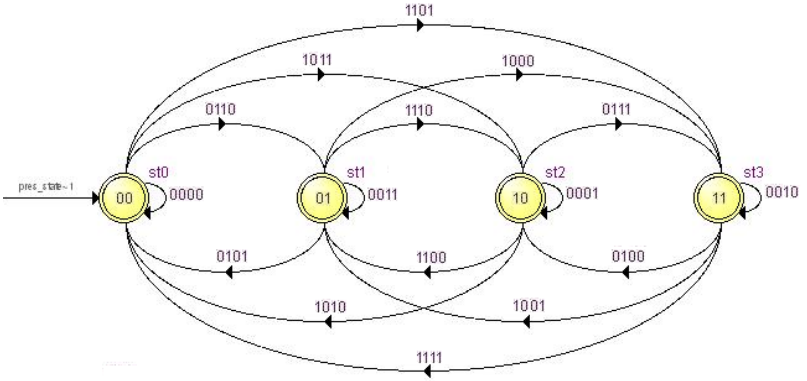


Рисунок 2 – Діаграма станів кодера згортального коду $K = 2$, $k = 2$, $n = 4$

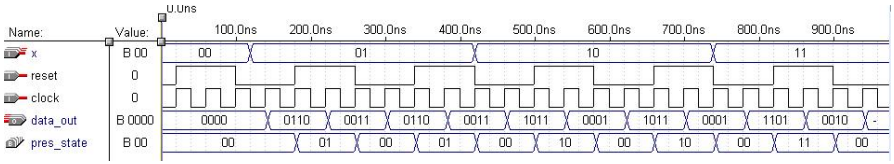


Рисунок 3 – Часова діаграма кодера загортального коду $K = 2$, $k = 2$, $n = 4$

Отже, практична цінність досліджень полягає у тому, що ці розробки можуть бути використані для збільшення завадостійкості і ймовірності безпомилкового прийому сигналу, що передається по каналу зв'язку з завадами.

УДК 004.67
Лізунов С. І.[1], Філобок Є.В.[2]
[1] канд. техн. наук, доц НУ «Запорізька політехніка»
[2] асп. НУ «Запорізька політехніка»

АНАЛІЗ МОЖЛИВОСТЕЙ ВИКОРИСТАННЯ ІНТЕГРОВАНИХ СИСТЕМ МОНІТОРИНГУ ІНФРАСТРУКТУРИ

Сучасний розвиток інформаційних технологій зумовлює необхідність надійного моніторингу інфраструктури для забезпечення стабільності та ефективності функціонування систем. Інтегровані системи моніторингу є одним з ключових інструментів управління інфраструктурою, які дозволяють оперативно виявляти, аналізувати та вирішувати проблеми, що виникають у роботі обладнання та програмного забезпечення. У цій статті буде розглянуто

можливості таких систем і їх більш детальну структуру, на прикладі системи Centeron.

Аналіз існуючих інтегрованих систем моніторингу

Доречність використання певної системи моніторингу (далі СМ) на підприємстві або у компанії залежить від деяких факторів, таких як достатність ресурсів, кількість інфраструктури, яку потрібно моніторити та ризик менеджмент.

Nagios

Nagios, як одна з перших і найбільш відомих СМ, має значні переваги, такі як широка спільнота користувачів, яка надає великий обсяг документації, підтримки та розширень. Багато користувачів відзначають його надійність і гнучкість у конфігурації, а також можливість інтеграції з іншими інструментами моніторингу (рис 1). В умовах швидко зростаючої інфраструктури, недоліки Nagios, такі як складність налаштування та нестабільність у високонавантажених середовищах, можуть стати суттєвими перешкодами [1].

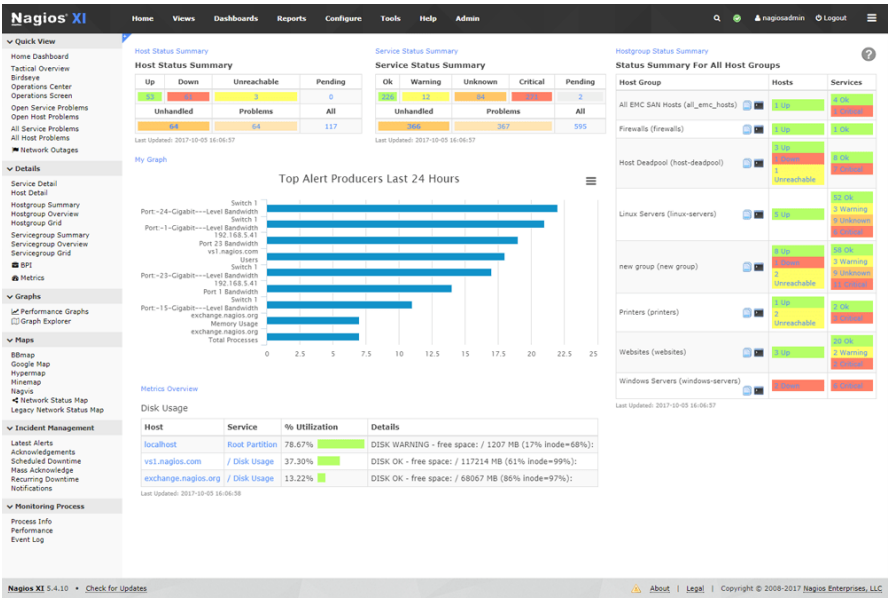


Рисунок 1 – Інтерфейс системи Nagios

Zabbix

Zabbix відзначається простотою в налаштуванні, що робить його привабливим для використання навіть для початківців. Він має широкий

функціонал, включаючи моніторинг мережі, серверів та додатків. Потужна система аналітики дозволяє виявляти та передбачувати проблеми ще до того, як вони виникнуть. Використовується загалом для моніторингу мережевих систем та обладнання (рис 2). Відсутність підтримки деяких специфічних пристроїв і складність в налаштуванні опцій сповіщення можуть стати проблемою для деяких організацій [2].

Рисунок 2 – Інтерфейс системи Nagios

Prometheus

Prometheus є системою моніторингу з відкритим кодом, яка зосереджена на моніторингу великих розподілених систем. Однією з його ключових переваг є здатність до масштабування і гнучкості налаштування, що дозволяє ефективно моніторити складні інфраструктурні середовища. Prometheus відзначається потужними засобами збору метрик та аналізу даних, що дозволяє виявляти проблеми та аналізувати їхні причини, використовується для створення графологічного представлення даних (рис 3).

Недоліком є те, що успішного впровадження Prometheus може знадобитися додатковий час і зусилля для налаштування та розгортання [3].

Centreon

Centreon є однією з найбільш повних та функціональних інтегрованих систем на ринку. Вона надає широкі можливості моніторингу різноманітних компонентів інфраструктури, включаючи сервери, мережеве обладнання, бази даних та додатки.

Centreon має зручний інтерфейс користувача (рис.4), що робить її привабливим вибором для багатьох організацій [4].

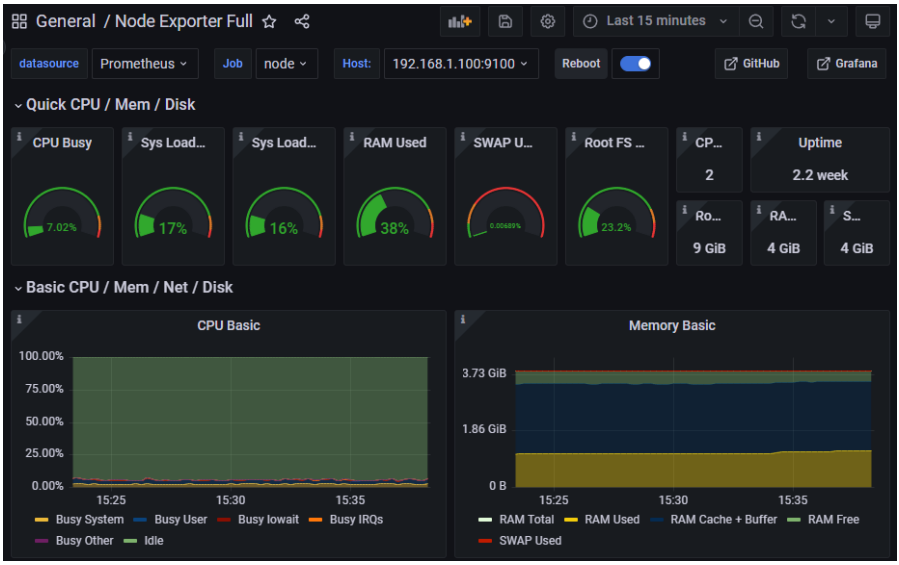


Рисунок 3 – Інтерфейс системи Prometheus

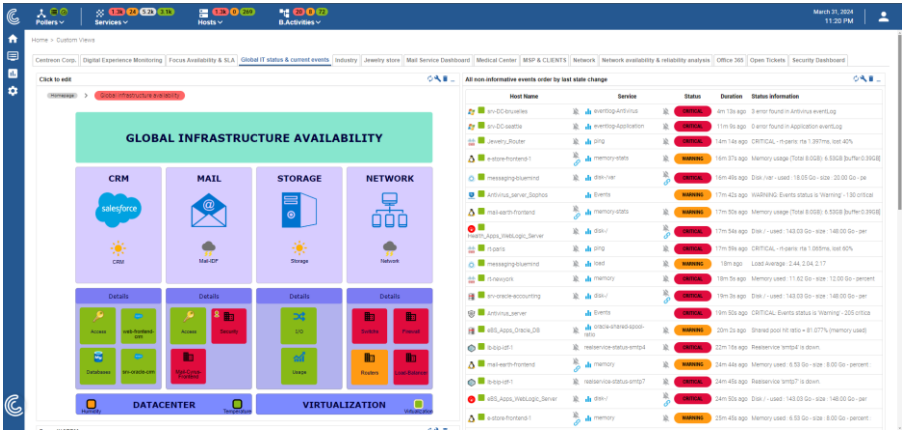


Рисунок .4 – Інтерфейс системи Centreon

Структура СМ

Архітектура системи Centreon може бути гарним прикладом для розуміння того, як саме працює СМ. Основні складові цієї архітектури включають (рис 5):

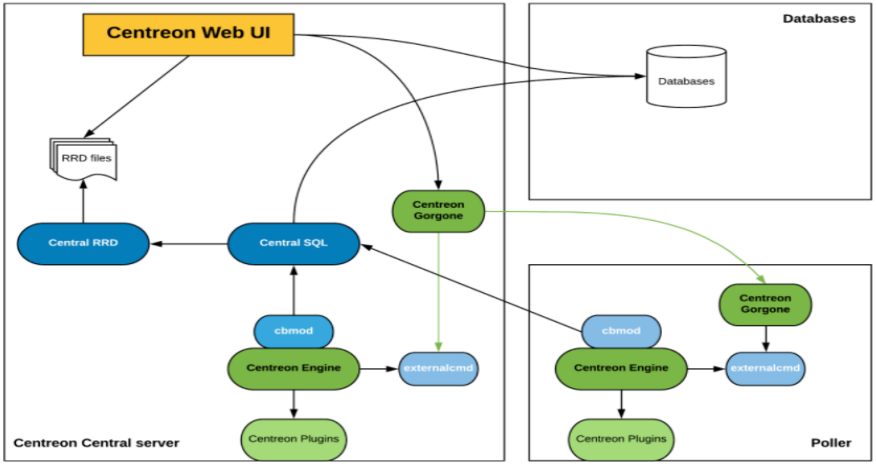


Рисунок 5 – Архітектура СМ Centreon

Центральний сервер Centreon: Це головний вузол системи, який відповідає за відображення та управління даними моніторингу. Він містить веб-інтерфейс для взаємодії з користувачем, моніторинговий двигун для збору даних, а також брокер для обміну інформацією між різними компонентами.

Сервер баз даних: Це місце, де зберігаються всі конфігураційні дані та зібрані метрики. Це допомагає забезпечити надійність та безпеку інформації.

Поллери: Це вузли, які відповідають за збір даних з об'єктами, що моніторяться, такими як сервери або мережеве обладнання. Вони виконують функцію збору даних і передачі їх до центрального сервера для подальшої обробки.

Коли мова йде про відображення стану сервісів у Centreon, процес починається зі збору даних. Поллери, що розташовані в мережі, активно моніторять різні компоненти та сервіси інфраструктури. За допомогою протоколу SNMP вони звертаються до мережевих пристроїв, щоб отримати необхідну інформацію про їх стан. Отримані дані надсилаються на центральний сервер Centreon, де вони аналізуються та обробляються. Центральний сервер визначає статус кожного сервісу на основі зібраних даних. Наприклад, якщо сервер недоступний або навантаження перевищує порогове значення, система встановлює статус "помилка" для цього сервісу.

Інформація про стан сервісів відображається на головній панелі веб-інтерфейсу Centreon (рис 6). Користувач може побачити список всіх сервісів, що моніторяться та їх стан, який представлений за допомогою кольорового кодування. Зелений колір означає, що сервіс працює нормально, червоний - що виникла помилка, а жовтий - що сервіс перебуває в стані попередження або відстежується. Крім того, Centreon може генерувати графіки та діаграми, які відображають зміни у стані сервісів з часом. Це допомагає адміністраторам відстежувати тенденції та вчасно реагувати на будь-які проблеми. Таким чином, завдяки інтегрованому підходу до збору та відображення даних, Centreon забезпечує зрозумілий та зручний інтерфейс для моніторингу стану інфраструктури.

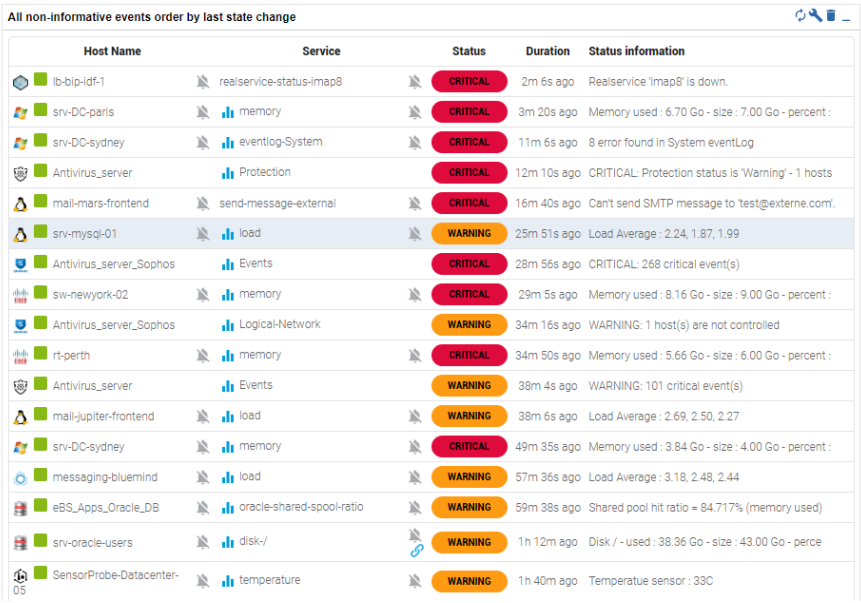


Рисунок 6 – Веб інтерфейс інцидентів

Крім візуалізації стану сервісів, Centreon також надає можливості налаштування сповіщень про виявлені проблеми або події в інфраструктурі. Коли будь-який сервіс переходить у стан помилки або попередження, або коли досягається певний поріг важливих метрик, система автоматично відправляє сповіщення адміністраторам або відповідальним особам, за допомогою Email або іншого виду сповіщення, наприклад у Slack (рис 7).

Centreon може моніторити різні типи об'єктів інфраструктури, включаючи сервери, мережеве обладнання, бази даних, хмарні сервіси тощо.

Більшість популярних та затребуваних сервісів-перевірок вже вбудовані в базу Centreon, але відміною перевагою є можливість створенні власних сервісів, написаних під певні потреби користувачів. Це дозволяє компаніям отримувати повну картину стану своєї інфраструктури та вчасно реагувати на будь-які проблеми чи загрози.

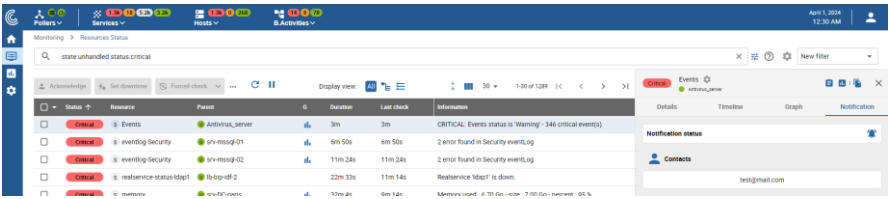


Рисунок 7 – Конфігурація сервісу зі сповіщенням через email

Також ця СМ надає інструменти для аналізу зібраних даних та створення звітів про продуктивність та ефективність інфраструктури (рис 8). Ці звіти допомагають адміністраторам та керівництву розуміти тенденції в розвитку інфраструктури, виявляти проблемні аспекти та приймати обґрунтовані рішення з покращення ефективності.

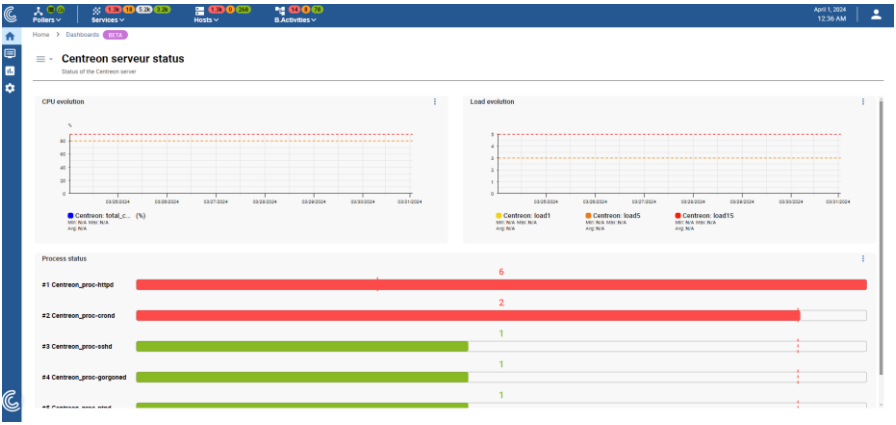


Рисунок 8 – Приклад дашборду у Centeron

У цілому, системи моніторингу є незамінним інструментом для сучасних компаній, які прагнуть забезпечити надійність, ефективність та безпеку своєї інфраструктури. Інтеграція таких систем у робочий процес дозволяє забезпечити ефективне управління та контроль за інфраструктурою, знизити ризики виникнення непередбачених ситуацій та збільшити загальну продуктивність бізнесу.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Nagios – система IT моніторингу [Електронний ресурс]. – Режим доступу: https://idealsoft.com.ua/vendory/vendors-more/nagios/
2. Що таке Zabbix | Основні функції та можливості. [Електронний ресурс]. – Режим доступу: https://lvivservice.com.ua/sysadmin/chto-takoe-zabbix-osnovnye-funkczii-i-vozmozhnosti/
3. Prometheus vs Zabbix: відмінне та подібне цих систем моніторингу [Електронний ресурс]. – Режим доступу: https://itedu.center/ua/blog/comparisons/prometheus_vs_zabbix/
4. Centreon | IT Infrastructure Monitoring Software [Електронний ресурс]. – Режим доступу: https://www.centreon.com/

УДК 004.056

Корольков Р.Ю.[1], Рева В.І.[2]

[1] канд. техн. наук, доц. НУ «Запорізька політехніка»

[2] канд. фіз.-мат. наук, доц. НУ «Запорізька політехніка»

ВИКОРИСТАННЯ GOOGLE DORKING/HACKING ДЛЯ ПОКРАЩЕННЯ СТРАТЕГІЙ ЗАХИСТУ

Використання операторів розширеного пошуку пошукової системи Google відомо як "Google Dorking/Hacking". Ця техніка дозволяє знаходити конфіденційні дані та вразливі веб-сайти без необхідності використання спеціалізованих програмних інструментів. До операторів розширеного пошуку відносяться cache, link, related, info, define, stocks, site, allintitle, intitle, allinurl, inurl та ін. Деякі з них можуть надати цінну інформацію для зловмисників. У більшості випадків зловмисники можуть шукати каталоги для перегляду, конфіденційну інформацію, таку як імена користувачів, паролі, журнали помилок, архіви резервних копій та ін [1].

Наприклад, "filetype:sql intext:username password" – запит який зловмисники можуть використовувати для пошуку файлів баз даних зі словами "username" і "password" в тексті. Запит "filetype:xlsx email" дозволить знайти файли Excel, які містять адреси електронної пошти. Зловмисники можуть використовувати його для пошуку списків розсилки або баз даних з контактами. "site:example.com inurl:admin" – це запит, який зловмисники можуть використовувати для пошуку панелей адміністратора, які не захищені паролем. Запит "intitle:"index of" знайде веб-сторінки, які містять фразу "index of" і часто відображають список всіх файлів, які знаходяться в певній директорії на веб-сервері. Зловмисники можуть використовувати їх для пошуку конфіденційних файлів, які не повинні бути доступні публічно.

"ip:192.168.1.0/24" - цей запит зловмисники можуть використовувати для сканування локальних мереж з метою пошуку вразливих пристроїв, та ін.

Всі ці ризики виникають внаслідок небезпечної конфігурації сервера. Тисячі веб-сайтів знаходяться під загрозою через базові помилки в налаштуванні безпеки, а деякі сервери навіть дозволяють необмежений доступ до файлових каталогів.

Сьогодні існує велика база даних пошукових запитів Google Hacking Database (GHDB), яка була зібрана та опублікована спільнотою експертів з кібербезпеки та ентузіастами [2]. GHDB містить близько 8000 різноманітних пошукових запитів для Google і оновлюється майже щодня новими запитами, які дозволяють виявляти різні вразливості, конфіденційну інформацію та інші цікаві ресурси в мережі Інтернет.

Важливо відзначити, що техніку розширених пошукових запитів можна застосовувати не тільки в Google, але й в інших пошукових системах. Будь-яка пошукова система, така як Bing, Yahoo та DuckDuckGo, може прийняти пошуковий запит та повернути відповідні результати. Однак, навіть якщо дві пошукові системи підтримують однакові оператори, вони часто повертають різні результати пошуку через різницю в індексації кожної пошукової системи.

Техніка Google Hacking може допомогти досліднику безпеки знайти кращі способи зробити веб-сайт більш безпечним, оскільки дуже важливо перевіряти конфігурацію сервера та вживати всіх необхідних заходів для захисту файлів і даних.

Для запобігання індексації конфіденційної інформації пошуковими системами рекомендується: захистити приватні зони за допомогою автентифікації користувачів та паролів, а також за допомогою обмеження за IP-адресами; шифрувати конфіденційну інформацію, таку як дані користувачів, паролі, номери кредитних карток, електронні листи, адреси, IP-адреси, номери телефонів тощо; регулярно проводити сканування вразливостей сайту, використовуючи популярні запити Google Dorks з бази даних Exploit DB Dorks [2], що можуть ефективно виявляти найбільш поширені вразливості; застосовувати блокування конфіденційного контенту за допомогою файлу robots.txt, розташованого в кореневому каталозі веб-сайту.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Messier R. CEH V12 Certified Ethical Hacker Study Guide. – John Wiley & Sons, Incorporated, 2023. – 768 p.

2. База даних OffSec Exploit Database Archive. Exploit Database - Exploits for Penetration Testers, Researchers, and Ethical Hackers – https://www.exploit-db.com/

УДК 004.428
Неласий О.В.[1], Самойлик С.С.[2], Неласа Г.В.[3]
[1] асп. НУ «Запорізька політехніка»
[2] канд. фіз.-мат. наук, доц. НУ «Запорізька політехніка»
[3] канд. техн. наук, доц. НУ «Запорізька політехніка»

РОЗРОБКА АРХІТЕКТУРИ ВЕБ ЗАСТОСУНКУ ПЛАТІЖНОЇ СИСТЕМИ У ПАРАДИГМІ WEB3

Зростання попиту на використання електромобілів в останній час обумовлено як турботою про довкілля так і загальним трендом переходу суспільства на відновлювані джерела енергії. Це збільшує коло потенційних постачальників енергії одночасно зі зменшенням їх масштабу. Тому доцільно розглянути можливість розробки розподіленої інформаційної системи оплати послуг заряджання електромобілів у парадигмі Web3[1] – нової концепції розвитку Інтернету, що є децентралізованим та базується на блокчейнах.

При проектуванні архітектури програмного застосунку авторами було прийняте рішення використання технологій:

- React JS;
- бібліотека Web3 JS[2];
- смарт-контракти на Solidity;
- блокчейн мережа Ethereum.

React - це JavaScript-бібліотека загального призначення для розробки інтерфейсу користувача. Оскільки серверна частина при такому підході замінюється розподіленою блокчейн мережею, необхідно використовувати JavaScript бібліотеку Web3 для роботи з Ethereum. Логіка застосунку реалізується смарт-контрактами на мові Solidity.

Застосунок, що розробляється, допоможе вирішити проблеми, притаманні централізованій клієнт-серверній архітектурі, за рахунок використання в якості back-end сучасних технологій смарт-контрактів, що виконуються в децентралізованому блокчейні Ethereum. При цьому засоби front-end розробки залишаються звичними.

В ході роботи розроблена архітектура застосунку децентралізованої платіжної системи та протестоване поєднання зазначених вище технологій в одному проекті.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. The Father of Web3 Wants You to Trust Less – [Електронний ресурс]. – Режим доступу: https://www.wired.com/story/web3-gavin-wood-interview/

2. A JavaScript library for building on Ethereum – [Електронний ресурс]. – Режим доступу: https://web3js.org/

УДК 004.056
Лізунов С.І.[1], Верещака М.П.[2]
[1] канд. техн. наук, доц. НУ «Запорізька політехніка»
[2] асп. НУ «Запорізька політехніка»

ВІРУСИ В МАРШРУТИЗАТОРІ: ЧИМ НЕБЕЗПЕЧНІ, ЯК ЇХ ВИЯВИТИ ТА УСУНУТИ

У світі, де цифрові технології проникають в усі сфери життя, інформаційна безпека стає пріоритетом. Багато користувачів добре обізнані про віруси, які можуть потрапити в комп'ютери і ноутбуки, але далеко не всі знають, що вони можуть також вражати домашній маршрутизатор. Маршрутизатори, ключовий елемент сучасних мереж, дедалі частіше стає мішенню для кіберзлочинців.

Способів заразити маршрутизатор досить багато, але з найпоширеніших на практиці можна навести наступні:

Вразливості програмного забезпечення. Якщо маршрутизатор не оновлюється і використовує застаріле програмне забезпечення, зловмисники можуть скористатися вразливостями в цьому програмному забезпеченні, щоб отримати доступ до маршрутизатора і заразити його вірусом.

Пароль. Якщо пароль для маршрутизатора дуже простий, зловмисники можуть легко його підібрати і отримати доступ, всіляко налаштувавши його і завантаживши шкідливі програми. Це стосується не тільки мережевого пароля, але і пароля до панелі адміністратора маршрутизатора.

Фішинг. Зловмисники можуть надсилати фішингові електронні листи або повідомлення в соціальних мережах, які виглядають як справжні. У них користувачів просять надати свої дані для входу в різні сервіси, в тому числі у адміністративну панель маршрутизатора. Це може призвести до того, що зловмисники отримають доступ і заразять маршрутизатор вірусом.

Зараження маршрутизатора вірусом може призвести до серйозних наслідків. Ось деякі з них:

Витік персональних даних. Вірус може перехоплювати дані, що передаються через маршрутизатор, включаючи дані банківських карток, паролі, особисту інформацію тощо.

Спам. Заражений маршрутизатор може бути використаний зловмисниками для розсилки спаму.

Доступ до пристроїв у вашій мережі. Зловмисники можуть отримати доступ до пристроїв у вашій мережі, таких як комп'ютери, принтери та інші пристрої, і використовувати їх у своїх цілях.

Уповільнення роботи мережі. Заражений маршрутизатор може входити у масштабні ботнет-мережі для організації DDoS-атак. Використання значної

частини мережевих ресурсів призводить до уповільнення та погіршення якості інтернет-з'єднання.

Зазвичай користувач не відразу розуміє, що проблеми пов'язані з маршрутизатором. Однак є кілька ознак, які можуть вказувати на проблему:

Несподівано низька швидкість інтернету або проблеми зі з'єднанням. Ця ознака може мати інтервальний період, коли канал зв’язку зайнятий зловмисниками.

Поява незрозумілих повідомлень веб-браузера, таких як попередження про безпеку (недійсний сертифікат HTTPS), банерна реклама тощо.

Незвичайна активність на маршрутизаторі, наприклад, несподівана зміна налаштувань або поява нових пристроїв у списку підключених пристроїв до маршрутизатора.

Якщо ви помітили одну з цих ознак, негайно перевірте свій комп'ютер, ноутбук, телефон або інший пристрій, з якого ви виходите в інтернет, на наявність вірусів. Найчастіше проблема криється саме в пристрої. Якщо ви впевнені в "чистоті" свого пристрою, а "симптоми" вірусу з’являються на всіх інших гаджетах, то шкідливе програмне забезпечення, ймовірно, знаходиться в маршрутизаторі. Необхідно переходити до процесу його видалення.

Видалення вірусу з маршрутизатора може вимагати великих знань і досвіду, оскільки різні програми мають свої властивості та особливості. Ось кілька кроків, які допоможуть вам впоратися з більшістю випадків:

Скиньте маршрутизатор до заводських налаштувань за замовчуванням і необхідно налаштувати його заново. Зазвичай це робиться натисканням і утриманням клавіші Reset протягом 15 секунд.

Змініть пароль (як панелі адміністратора маршрутизатора, так і мережі) на більш складний і надійний.

Оновіть прошивку маршрутизатора до останньої версії. Універсальної інструкції не існує. Зазвичай, необхідно перейти на офіційну веб сторінку виробника маршрутизатора та завантажити останню версію програмного забезпечення для маршрутизатора.

Використовуйте антивірусне програмне забезпечення для перевірки мережі на наявність вірусів та інших шкідливих програм.

Найефективніший метод протидії будь-якому вірусу полягає у його своєчасній профілактиці. Розглянемо наступні кроки:

Регулярно оновлювати програмне забезпечення для маршрутизатора до останньої версії. Необхідно перевіряти знайдені CVE (Поширені вразливості та ризики) у останніх версіях програмних забезпечень і, у разі наявності, додавати додатковий захист від знайдених вразливостей якщо ці вразливості ще не закриті розробниками.

Використовуйте надійні паролі, які важко вгадати або підібрати. Перевіряйте у відкритих базах даних наявність відомих паролів та використовуйте складний пароль із цифрами, буквами в різному регістрі та іншими символами.

Не відповідайте на фішингові електронні листи та не надавайте особисту інформацію, якщо ви не впевнені, що це справжній запит. Завжди перевіряйте адреси та назви посилань.

Використовуйте антивірусне програмне забезпечення для захисту ваших пристроїв і мережі в цілому. Оновлюйте базу сигнатур до останньої версії

Встановіть файрвол. Файрвол — це програма або пристрій, що контролює вхід та вихід мережевого трафіку. Він може блокувати небажаний доступ до мережі та допомагати блокувати потенційно шкідливі підключення.

Відключити віддалений доступ до налаштувань маршрутизатора. Якщо за замовчуванням цей функціонал відкритий – його необхідно закрити, але в більшості сучасних маршрутизаторів віддалений доступ закритий від початку.

Використовуйте безпечні протоколи зв'язку для підключення по Wi-Fi. Замість застарілих протоколів, таких як WEP (Wired Equivalent Privacy), використовуйте більш безпечні протоколи, наприклад, WPA2 (Wi-Fi Protected Access 2) або WPA3. Вони забезпечують більшу захищеність мережі Wi-Fi.

Встановіть VPN (віртуальну приватну мережу). VPN шифрує ваш мережевий трафік і забезпечує конфіденційність та безпеку під час передачі даних через інтернет, навіть на відкритих мережах Wi-Fi.

Увімкніть двофакторну автентифікацію. Двофакторна автентифікація зміцнює безпеку вашої мережі, вимагаючи додаткового підтвердження, крім пароля, для входу в адміністративну панель маршрутизатора.

Перед підключенням до мережі перевірте всі підключені пристрої на наявність вірусів та інших шкідливих програм.

Додатково, важливо періодично проводити аудит безпеки мережі, щоб виявити можливі вразливості та вчасно їх усунути. Також слід регулярно резервувати дані, щоб у разі інциденту мати можливість відновлення інформації та налаштувань.

Захист вашого маршрутизатора від вірусів та інших кіберзагроз є важливою складовою забезпечення вашої інформаційної безпеки.

УДК 004.056
Савченко Ю. В.[1], Карпуков Л.М.[2], Воскобойник В.О.[3], Івахова Ю.В.[4]
[1] канд. техн. наук, доц. Університету митної справи та фінансів
[2] д-р техн. наукт.н., проф. НУ «Запорізька політехніка»
[3] канд. техн. наук, проф. НУ «Запорізька політехніка»
[4] студ. гр. Б21-1 Університету митної справи та фінансів

МОДЕЛЮВАННЯ ПРОЦЕСІВ НАПАДУ НА ІНФОРМАЦІЮ ТА ЇЇ ЗАХИСТУ

Кібербезпека залишається головною проблемою в сучасному IT-світі оскільки кількість хакерських інцидентів зростає. Багато аспектів нашого життя перемістилися в Інтернет, що комерційний і приватний світи можуть багато втратити через порушення безпеки.

У відповідь спеціалісти з кібербезпеки розгортають арсенал засобів захисту та протидії, щоб забезпечити безпеку транзакційних даних і конфіденційної інформації. Враховуючи величезну кількість і різноманітність доступних сьогодні атак, це величезне завдання.

Ціллю даної роботи є моделювання загроз та захисту інформації на основі аналізу процесів моделювання нападу на інформацію і доступні методології, а також існування яких моделей спрямоване на захист інформації і на основі чого ці моделі розроблені.

Модель безпеки конкретно визначає основні аспекти безпеки та їх зв'язок із продуктивністю операційної системи. Жодна організація не може захистити свою конфіденційну інформацію чи дані, не маючи ефективних і ефективних моделей безпеки. Можна сказати, що основною метою моделі безпеки є забезпечення необхідного рівня розуміння для успішної та ефективної реалізації ключових вимог захисту. Моделі інформаційної безпеки — це процедури, які використовуються для перевірки політик безпеки, оскільки вони передбачають надання точного набору вказівок, яким комп'ютер може слідувати для реалізації життєве важливих процесів безпеки, процедур і концепцій, що містяться в програмі безпеки. Ці моделі можуть бути інтуїтивно зрозумілими або абстрактними. Моделі безпеки керують напрямками безпеки операційних систем.

Існують деякі моделі безпеки, які найчастіше використовуються для пояснення вказівок і правил, які керують конфіденційністю, захистом і цілісністю інформації. Основною причиною та фокусом на реалізації моделі безпеки є конфіденційність, яка не враховує контролю доступу та цілісності інформації. За допомогою цих моделей безпеки, які є основними компонентами, на які слід звернути увагу при розробці політик і систем інформаційної безпеки. Ці моделі розповідають про правила доступу,

необхідні для створення екземпляра визначеної політики та виділення об'єктів, які керуються політикою компанії.

Ось деякі з важливих моделей, які ми обговорюємо нижче, щоб зрозуміти функції та важливість моделей інформаційної безпеки в сучасному діловому світі.

Модель Bell-LaPadula спочатку стала розробкою Міністерства оборони США (DoD). Ця модель є початково математичною моделлю багаторівневої політики безпеки, яка пояснює концепцію безпечного стану та обов'язкових методів доступу. Це гарантує, що дані передаються лише таким чином, щоб не порушувати політику системи та зосереджено на конфіденційності.

Деякі проблеми, пов'язані з реалізаціями Bell-LaPadula, пов'язані з тим, що користувачі, звичайно, не можуть спілкуватися з користувачами з низьким рівнем. З одного боку, коли модель BLP звертається до конфіденційності, вона не враховує приховані канали чи контроль доступу, з іншого боку. Крім того, будь-хто може створити об'єкт вищої класифікації, що також є проблемою. Спочатку модель Белла-ЛаПадули мала завершити потреби Міністерства оборони для InfoSec, наразі військові прагнуть і досягають цілей, практикуючи забезпечення дискретної сегрегації та контролю доступу.

Модель Clark Wilson має справу з двома видами об'єктів, один з яких ми назвали CDI та UDI, тобто елементи даних з обмеженнями та елементи даних без обмежень. Він також має два типи зв'язків: перший – IVP, що означає процедуру перевірки цілісності, а другий – TP, тобто процедура транзакції. Робота IVP полягає в тому, щоб переконатися, що TP, які спричиняють CDI, перебувають у правильному стані, і дійсні сертифікати перетворення для всіх TP. Тут лише авторизовані TP можуть контролювати CDI. Іншими словами, щоб захистити цілісність інформації та забезпечити правильно відформатовані транзакції, ця модель цілісності повинна бути добре реалізована.

Модель Biba трохи схожа на BLP, хоча вона не наголошує на конфіденційності, основна увага моделі Biba зосереджена на цілісності, і її часто використовують для цілісності, де конфіденційність важливіша. Ми можемо дивитися на це просто як на протилежну реалізацію BLP. Конфіденційність є головною проблемою багатьох урядів, але більшість підприємств хочуть забезпечити цілісність безпеки даних на найвищому рівні. Biba є зразком вибору, коли безпека цілісності життєве важлива.

Два основних правила моделі *Biba*:

Проста аксіома цілісності: (без зчитування) суб'єкт на рівні дозволу не може прочитати інформацію з нижчою класифікацією. Це допомагає особам отримати доступ до важливих даних на нижчому рівні цілісності. Це гарантує цілісність, запобігаючи впливу поганої інформації з нижчих рівнів цілісності.

Аксіома цілісності: (без запису) суб’єкт на рівні дозволу не може записати інформацію до вищої класифікації. Це допомагає суб’єктам передавати важливу інформацію до вищого рівня цілісності, ніж дозвіл на зміни. Це гарантує цілісність, запобігаючи переміщенню поганого матеріалу на вищі рівні цілісності.

Brewer and Nash модель також відома як модель «китайської стіни» і використовується для уникнення конфлікту інтересів шляхом заборони окремій особі, наприклад консультанту, входити до кількох COI, тобто категорій конфлікту інтересів. Зміна політик контролю доступу залежить від поведінки користувача. Це означає, що якщо особа, яка отримує доступ до інформації, що стосується однієї сторони, не може отримати доступ до даних іншої сторони або дані для тієї самої особи недоступні.

Модель *Harrison Ruzzo Ullman* також вважається доповненням до моделі BLP. Модель Белла-ЛаПадули не має системи для зміни привілеїв доступу або для створення та видалення суб'єктів і об'єктів. Модель вирішує ці проблеми шляхом авторизації структури для розподілу прав доступу та перевірки відповідності даній політиці, що припиняє несанкціонований доступ. Модель Harrison Ruzzo Ullman може бути реалізована за допомогою контролю доступу або списку можливостей.

Одним із найважливіших завдань у сфері інформаційної безпеки є якісна оцінка загроз. Саме достовірний результат такої оцінки є основою для раціонального вибору засобів і методів захисту інформації. Існує кілька відомих інструментів для оцінки інформаційної безпеки, моделювання заходів безпеки та можливих типів загроз інформаційній безпеці, основні з яких представлені в [1-5]. Ці моделі побудовані на основі теорії ймовірностей та математичної статистики, нечіткі множин, теорії ігор, теорії графів, теорії цифрових автоматів , мережі Петрі, теорії випадкових процесів тощо.

Ці методології утворюють набір інструментів для аналізу продуктивності досліджуваних інформаційних систем протягом обмеженого цензурованого періоду часу. Аналіз відбувається в контексті визначення: періоду час між відмовами в досліджуваній системі; кількості відмов у досліджуваній системі за цензурований період її роботи; реакції досліджуваної системи на спровоковані збої; реакції досліджуваної системи на комплексні тестові впливи.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. S. Colabianchi, F. Costantino, G. Di Gravio, F. Nonino, R. Patriarca Discussing resilience in the context of cyber physical systems Comput Ind. 2021, 10.1016/j.cie.2021.107534

2. H.S. Lallie, K. Debattista, J. Bal A review of attack graph and attack tree visual syntax in cyber security Computer Science Review. 2020, 10.1016/j.cosrev.2019.100219

3. George, P.G., Renjith, V.R., 2021. Evolution of Safety and Security Risk Assessment methodologies towards the use of Bayesian Networks in Process Industries. *Process Safety and Environmental Protection*. 10.1016/j.psep.2021.03.031

4. L. Zhang, V.L.L.Three decades of deception techniques in active cyber defense – Retrospect and outlook Computers & Security. 2021, 10.1016/j.cose.2021.102288

5. D. Bhamare, M. Zolanvari, A. Erbad, R. Jain, K. Khan, N. Meskin Cybersecurity for industrial control systems: A survey Computers & Security10.1016/j.cose.2019.101677

УДК 004.056.55

Постоленко М.О.[1], Романенко С.М.[2]
[1] студ. гр. БК-713м НУ «Запорізька політехніка»
[2] канд. фіз.-мат. наук, доц. НУ «Запорізька політехніка»

КРИПТОГРАФІЧНІ РІШЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Криптографія була однією з перших дисциплін у рамках інформаційної безпеки. Починаючи з античних часів, військові, дипломати та шпигуни використовували різні пристрої та засоби шифрування, дешифрування та передачі секретної інформації. У середні віки криптографія продовжила розвиток і стала складнішою й різноманітнішою, включаючи різні форми транспозиційних та підстановочних шифрів. Із початку XX століття технології криптографії еволюціонували безперервним потоком механічних, електронних та математичних інновацій, досягнувши такого ступеню розвитку, що тепер вони вкоренилися в нашому повсякденному житті скрізь, ставши непомітною, але невід'ємною частиною практично будь-якої роботи із цифровою інформацією. Сучасні криптографічні рішення відіграють ключову роль у захисті даних та систем їхньої обробки. Криптографічні технології присутні в багатьох системах інформаційної безпеки. У цій роботі коротко описуються деякі криптографічні рішення із загальноприйнятими абревіатурами, а для неусталених абревіатур використовуються повні назви.

Криптографічні рішення

Можна виділити кілька класів загальних та спеціалізованих криптографічних рішень, серед яких такі:

ES (Encryption Solutions) – загальний клас рішень, що захищають дані, перетворюючи їх на зашифровану форму, доступ до якої можливий лише за

допомогою правильного ключа. Рішення щодо шифрування з'явилися в докомп'ютерну епоху. Вони охоплюють широкий спектр інструментів і технологій, призначених для шифрування даних, що перебувають у стані спокою, так і переданих. Це може включати в себе програми шифрування, протоколи шифрування для безпечного зв'язку (наприклад, SSL/TLS для інтернет-трафіку) і сервіси шифрування, що надаються хмарними провайдерами. Ціль цих рішень – забезпечити конфіденційність та цілісність даних шляхом перетворення читаних даних у нечитаний формат, який можна звернути тільки за допомогою правильних ключів розшифровки.

FDE (Full Disk Encryption) – це клас програмних чи апаратних рішень, призначених для шифрування всіх даних на жорсткому диску комп'ютера чи іншого пристрою. Такий підхід забезпечує захист інформації на рівні диска, включаючи системні файли, програми та дані. Основна мета FDE – забезпечення конфіденційності та захисту даних на пристрої від несанкціонованого доступу, особливо у разі втрати або крадіжки. Різновиди FDE – програмні та апаратні рішення. Системи FDE пов'язані з технологією TPM (див. далі). Одна з перших систем FDE Jetico BestCrypt була розроблена у 1993 році. Найпоширенішими рішеннями FDE, вбудованими в операційні системи, є Microsoft BitLocker та Apple FileVault.

Password Management Tools (Password Managers) – інструменти, призначені для спрощення та покращення процесів створення та зберігання паролів. Функції менеджерів паролів – генерація сильних паролів, зберігання та впорядкування паролів, автоматичне заповнення форм, зміна паролів. Різновиди інструментів управління паролями – персональні менеджери паролів; менеджери паролів для команд, що надають функціонал спільного використання паролів у робочих групах; менеджери привілейованих паролів; корпоративні менеджери паролів (EPM) Перший програмний менеджер паролів Password Safe був створений Брюсом Шнайєром в 1997 році як безкоштовна утиліта для Microsoft Windows 95. Станом на 2023 рік найчастіше використовуваним менеджером паролів був вбудований менеджер паролів Google Chrome.

EPM (Enterprise Password Management) – це розвиток менеджерів паролів у застосуванні на всю організацію. Ці рішення призначені для централізованого управління паролями, надаючи управління, моніторинг та захист привілейованих облікових записів як власних, так і сервісних облікових записів в організаціях. Функції EPM – централізоване керування паролями, автоматичне оновлення паролів, відстеження активності паролів, регулярний аудит для забезпечення відповідності політикам безпеки, керування доступом на основі ролей. Різновиди EPM – наземні та хмарні. Рішення для управління паролями в корпоративному середовищі почали розвиватися на початку 2000-х років.

TRSM (Tamper-Resistant Security Module) – це загальна назва пристроїв, призначених для особливої стійкості до фізичного втручання та несанкціонованого доступу. Ці модулі часто включають додаткові заходи фізичної безпеки, такі як: механізми самознищення, щоб запобігти фізичним атакам або несанкціонованому доступу до ключів шифрування та криптографічних операцій, які вони виконують. TRSM необхідні у середовищах, де безпека є основною турботою, таких як: військові чи фінансові установи. Найпростішими прикладами TRSM є платіжні смарт-картки, які з'явилися у 1970-х роках. Також прикладами TRSM є POS-термінали та пристрої HSM.

HSM (Hardware Security Module) – фізичний обчислювальний пристрій, який захищає секрети та керує ними. HSM з'явилися наприкінці 1970-х років. Апаратні модулі безпеки зазвичай забезпечують безпечне керування найважливішими криптографічними ключами та операціями. HSM використовуються для генерації, зберігання та керування ключами шифрування в безпечній формі, пропонуючи більш високий рівень безпеки, ніж програмне керування ключами, оскільки ключі зберігаються у захищеному від злому апаратному пристрої. HSM широко використовуються у середовищах з високим рівнем безпеки, таких як: фінансові установи, державні агенції та великі підприємства, де захист чутливих даних має вирішальне значення.

KMS (Key Management Systems) – це рішення, призначені для централізованого управління криптографічними ключами, які використовуються для шифрування даних. Основним їхнім завданням є забезпечення безпеки, доступності та управління життєвим циклом ключів. KMS автоматизують процеси створення, розподілу, зберігання, ротації та знищення ключів. Вони інтегруються з різними програмами та інфраструктурою, надаючи централізований контроль над шифруванням у підприємствах. Ідея централізованого управління криптографічними ключами почала розвиватися у 1970-х роках разом із зростанням використання криптографії, але конкретні системи KMS почали активно розроблятися та впроваджуватися у 1990-х та 2000-х роках.

PKI (Public Key Infrastructure) – це система, яка використовується для створення, керування, розподілу, використання та зберігання цифрових сертифікатів та відкритих криптографічних ключів. Вона забезпечує безпечне цифрове підписування документів, шифрування даних та автентифікацію користувачів або пристроїв в електронних системах. PKI є ключовим елементом у забезпеченні безпеки мережевих комунікацій та транзакцій, дозволяючи учасникам конфіденційно обмінюватися даними та підтверджувати справжність один одного. PKI надає набір інструментів для управління асиметричними ключами та сертифікатами як у рамках окремих

організацій, так і цілих держав. Цим рішення PKI відрізняються від рішень KMS, які зосереджені на гнучкішому управлінні ключами, проте зазвичай лише в рамках одного підприємства. Історія PKI розпочалася у 1970-х роках з розробки асиметричного шифрування. Концепція PKI у сучасному розумінні була розроблена та стандартизована у 1990-х роках. З появою блокчейну Ethereum у 2015 році почали розвиватись децентралізовані PKI.

SSE (Server-Side Encryption) – метод шифрування даних, що зберігаються на стороні сервера, що використовується з початку 2000-х років для підвищення безпеки даних. Шифрування на стороні сервера є шифрування даних на накопичувачах сервера. Ключі шифрування керуються самим сервером або центральною системою керування ключами. Це гарантує доступ до даних лише уповноважених осіб. SSE особливо ефективний для захисту конфіденційних даних у хмарному сховищі, оскільки запобігає несанкціонованому доступу навіть у разі компрометації фізичних пристроїв зберігання.

TPM (Trusted Platform Module) – це апаратний компонент, який забезпечує безпечне зберігання криптографічних ключів, що використовуються для шифрування та захисту інформації на комп'ютері або іншому пристрої. TPM встановлюється на материнську плату пристрою або вбудований процесор. Уперше концепція TPM була представлена консорціумом Trusted Computing Group (TCG) та стандартизована ISO у 2009 році. З того часу TPM став стандартним компонентом у багатьох комп'ютерах, особливо в корпоративному секторі, де вимоги до безпеки особливо високі.

ZKP (Zero-Knowledge Proof) – технологія доказу з нульовою довірою використовується для виконання завдання комунікацій, коли одній стороні потрібно переконати іншу сторону, що перша знає якусь таємницю, не розкриваючи цієї таємниці, крім достовірного факту її наявності. У розвиток технології ZKP у 1980-х роках зробили внесок Сільвіо Мікалі, Шафі Голдвассер, Одед Голдрейх, Аві Вігдерсон та Чарльз Ракофф. Починаючи з 2020 року, у рамках методу ZKP створено пост-квантові системи безпеки, тобто системи, стійкі до криптоаналізу на квантових комп'ютерах. Технологія ZKP знаходить все більше застосувань, від безпеки транзакцій та автентифікації до забезпечення конфіденційності в блокчейн-системах та інших додатках, де важливий захист особистих даних та конфіденційності.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Горбенко, І.Д., Горбенко, Ю.І. Прикладна криптологія. Теорія. Практика. Застосування: підручник для вищих навч. закладів. – Харків: Форт, 2013. – 880 с.

УДК 004.056(075)
Ковальов І.Є.[1], Козіна Г.Л.[2]
[1] студ. гр. БК-813м НУ «Запорізька політехніка»
[2] канд. фіз.-мат. наук, доц. НУ «Запорізька політехніка»

ОГЛЯД КРИТЕРІЇВ ОЦІНКИ ВЛАСТИВОСТЕЙ ФУНКЦІЙ ХЕШУВАННЯ

Всі геш функції можна розділити та порівняти за наступними характеристиками: довжина гешу, довжина блоку обробки даних.

Це характеристики, які відомі і без дослідження, можна дізнатися з документації функції. А також, є властивості, функції які слід встановлювати вже методом аналізу, серед них швидкість обчислення, стійкість до 0000-0002-4787-6865, аваланшний ефект.

При дослідженні властивостей функцій гешування дуже важливо, щоб умови виконання цих функцій, а також спосіб їх реалізації був максимально однаковим.

Для цього було обрано саме бібліотечну реалізацію цих функцій, а саме бібліотеку Bouncy Castle.

Для порівняння було обрано функцію гешування «Купина», яка описана в ДСТУ 7564:2014, також було розповсюджені функції, так і національні стандарти інших країн: SM3, MD5, родина SHA, BLAKE2, Whirlpool (табл.1).

Таблиця 1 – Загальна характеристика

Функ-ція	Купи-на	SM 3	Whirlpo ol	BLAKE2	MD 5	SHA3	SH A	SHA 1
Дов-жина гешу (біт)	256/51 2	256	512	256/384/5 12	128	256/ 384/51 2	256 / 512	160
Дов-жина блоку (біт)	1024	512	512	512-1024	512	512-1024	512 - 102 4	512

Вимір характеристик відбувався за допомогою програми, яка написана на мові C# і використовує бібліотеку BouncyCastle для реалізації цих функцій. Результати було зведено до таблиці 2.

За даними таблицями можна зробити висновки що до вибору хеш-функцій для різних ситуацій.

Купина-256/512 – як національний стандарт України, найкраще підходить саме для внутрішнього ринку, де потрібна досить висока швидкість та надійність.

Таблиця 2. Результати вимірювання

Функція	Швидкість обчислення (біт/с)	Стійкість до колізій (спроб до колізії)	Аваланшний ефект (біт)
Купина-256	84450,84	2545517993	127,97
Купина-512	2612244,89	4247515242	255,95
SM3	247701,98	3754245964	127,985
Whirlpool	363946,54	4154245697	255,98
BLAKE2-256	9350759,13	2456795431	127,95
BLAKE2-384	9434889,43	2705943256	191,99
BLAKE2-512	9578638,94	3654245678	255,97
MD5	110382,89	137729200	63,68
SHA3-256	247056,55	3245117215	127,98
SHA3-384	25430463,57	3821954021	191,98
SHA3-512	26806282,72	4651256780	255,96
SHA-256	372147,11	155289240	128,00
SHA-512	542085,75	253256975	255,99
SHA-1	298340,48	11564249	79,98

Функція гешування SM3 оптимальна для цілісності та цифрових підписів.

Функція гешування Whirlpool – повільна.

Функція гешування BLAKE2 оптимальна для швидкості та безпеки.

Функція гешування MD5 застаріла та небезпечна.

Функція гешування SHA3 надає баланс швидкості та безпеки.

Функція гешування SHA-256/512 широко використовуються; а SHA-1 не рекомендується.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Євсеєв С. П., Йохов О. Ю., Король О. Г., Гешування даних в інформаційних системах: монография — К.: «ХНЕУ», 2013. — 312 с.

2. ДСТУ ISO 7564:2014 Інформаційні технології. Криптографічний захист інформації. Функція гешування [Чинний від 2015-04-01]. Київ, 2015. 39 с. (Інформація та документація).

УДК 003.26:004.421:004.428
Кацюба М.В.[1], Неласа Г.В.[2]
[1] студ. гр. БК-710 НУ «Запорізька політехніка»
[2] канд. техн. наук, доц. НУ «Запорізька політехніка»

РЕАЛІЗАЦІЯ НЕІНТЕРАКТИВНОГО ПРОТОКОЛУ ДОКАЗУ З НУЛЬОВИМ РОЗГОЛОШЕННЯМ В СХЕМАХ АВТЕНТИФІКАЦІЇ

Одним із сучасних методів автентифікації є автентифікація з використанням систем доказів з нульовим розголошенням.

Доказ із нульовим розголошенням — це криптографічний протокол, який дозволяє стороні, що доводить, підтвердити істинність твердження іншій стороні (верифікатору), при цьому не розкриваючи ніякої додаткової інформації про нього (ні змісту, ні джерела, з якого доказуючий дізнався про правдивість) [1].

Приклади проектів, що використовують докази з нульовим розголошенням в автентифікаційних схемах:

Proton Mail – сервіс веб-пошти із шифруванням. Для автентифікації використовує протокол парольної автентифікації SRP (Secure Remote Password), який дозволяє користувачеві доводити серверу, що знає пароль, не розкриваючи його. На етапі реєстрації клієнт обчислює та відправляє на сервер верифікатор. При генерації верифікатора використовується пароль, але пароль ніколи не потрапляє на сервер. Відновити пароль за допомогою верифікатора неможливо [2].

Iden3 – це рішення SSI (Self-Sovereign Identity), яке дозволяє користувачам використовувати свої вже існуючі перевірені ідентифікатори. Завдяки SSI вони можуть довести, що вони є тими, за кого себе видають, на основі доказів нульового знання.

Одним із прямих застосувань технології iden3 є дозвіл веб-додаткам використовувати ці ідентифікатори для автентифікації. Зокрема для систем автентифікації використовує принцип неінтерактивної взаємодії, тобто після запиту автентифікації від сервера клієнт самостійно генерує доказ і один раз відправляє його серверу (верифікатору) на перевірку.

Iden3 підтримує Groth16 для генерації та перевірки доказів [3].

Процес автентифікації, який реалізовано в iden3, можна поділити на кроки:

Крок 1. Сервер генерує запит на автентифікацію. Він може бути доставлений користувачеві через різні канали зв’язку: QR-код, електронну пошту, Deep Links тощо.

Крок 2. Клієнт аналізує запит, генерує доказ і надсилає відповідь на URL-адресу зворотного виклику.

Крок 3. Сервер перевіряє доказ і, в залежності від результату перевірки, приймає або відхиляє авторизацію.

Метою даної роботи є реалізація схеми автентифікації від iden3 з використанням одного із сучасних протоколів з нульовим розголошенням.

Для реалізації у якості протоколу з нульовим розголошенням для генерації та перевірки доказів було обрано сучасний протокол Plonky2 [4].

Його основні риси: використовує FRI [5] замість схем на еліптичних кривих; є рекурсивним протоколом: розбиває доказ на окремі докази, які обчислюються паралельно, і потім об'єднуються в один доказ; використовує основне просте поле Галуа за модулем $p = 2^{64} - 2^{32} + 1$, яке дозволяє оптимізувати обчислення на апаратному рівні.

Завдяки цим рисам Plonky2 є швидким протоколом, який можна використовувати у системах, де необхідна швидкодія.

У якості мови програмування була обрана мова програмування Rust. Він є сучасним аналогом C++, проте, на відміну від нього, реалізовує автоматичне керування пам'яттю, що захищає від проблем, які виникають через низькорівневу роботу з пам'яттю.

Також для Rust існує бібліотека plonky2, який дозволяє зручно вбудовувати цей протокол у проекті.

На даний момент розробляється практична реалізація даної системи автентифікації.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Goldwasser S., Micali S., Rackoff C. The knowledge complexity of interactive proof systems. SIAM journal on computing. 1989. Т. 18, № 1. С. 186–208.

2. Butler B. Improved authentication for email encryption and security | Proton. Proton. URL: https://proton.me/blog/encrypted-email-authentication.

3. Login protocol - iden3 documentation. Iden3 Documentation. URL: https://docs.iden3.io/protocol/zklogin/.

4. GitHub - 0xPolygonZero/plonky2. GitHub. URL: https://github.com/0xPolygonZero/plonky2.

5. Eli Ben-Sasson, Iddo Bentov, Yinon Horesh, Michael Riabzev. Fast Reed-Solomon Interactive Oracle Proofs of Proximity. Electronic Colloquium on Computational Complexity. 2018. № 2. С. 12–19.

УДК 004.05
Синюшкіна М.Д.,[1], Неласа Г.В.[2]
[1] студ. гр. БК-813м НУ «Запорізька політехніка»
[2] канд. техн. наук, доц. НУ «Запорізька політехніка»

АВТОМАТИЗОВАНИЙ АУДИТ СМАРТ-КОНТРАКТІВ MARKETPLACE ЗАСТОСУНКУ: СТРАТЕГІЇ БЕЗПЕКИ

З роками концепція Web 3.0 проходила крізь етапи еволюції, від початкової ідеї про семантичну мережу до більш децентралізованої версії Інтернету, побудованої за допомогою блокчейну. Однією з головних ідей Web 3.0 є переклад усього веб-контенту, написаного людськими мовами, у машиночитану форму, що дозволить алгоритмам і програмам визначати значення повідомлень і встановлювати з'єднання на їх основі [1].

У Web3 кожен вміст є цифровим активом. Завдяки Web3 більше нікому не ділитеся своїми конфіденційними даними. Навіть купувати або продавати банкам [1]. З цієї причини з'явилися криптовалюти – ще одне відоме та всюдисуще явище. Платежі в криптовалюті пропонують сторонам свободу, якої не існувало в Web 2.0 – не потрібно нікому звітувати, хто це робить і на що витрачаються гроші.

При розробці додатків «нового покоління» дотримуються децентралізації організації даних, у тому числі їх зберігання. Децентралізація, у свою чергу, є ключем до успішного впровадження криптовалют і смарт-контрактів в економіку: усуває потребу в довірі, а отже, в посередниках і централізованих структурах.

Тому ідеальний стан Web3 – це ефективна бізнес-модель, яка не використовує ієрархічні структури та традиційні фінансові інструменти.

При аудиті смарт-контрактів у контексті Web3, однією з ключових вимог є забезпечення безпеки та надійності системи [2]. Децентралізація організації даних та їх зберігання є однією з основних стратегій, яка використовується для забезпечення цілісності та невід'ємності смарт-контрактів у розподіленій мережі.

Під час аудиту смарт-контрактів важливо перевірити, чи відповідає код вимогам безпеки. Для цього використовуються різноманітні техніки, включаючи аналіз потенційних вразливостей, перевірку наявності захисту від атак, валідацію вхідних даних та інші методи аналізу [3]. Важливо також переконатися, що механізми захисту даних та конфіденційності реалізовані належним чином та враховують усі можливі ризики.

Крім того, у контексті Web3 велика увага приділяється використанню криптовалют та забезпеченню безпеки та відповідності регуляторним вимогам у цій сфері. Такі аспекти, як захист приватності користувачів, безпека транзакцій та відповідність нормативним вимогам, викликають

особливий інтерес при аудиті смарт-контрактів, оскільки вони безпосередньо впливають на фінансову та особисту безпеку користувачів.

При аудиті смарт-контрактів, особливу увагу зазвичай приділяють вразливостям, що стосуються контрактів, таким як переповнення, відмова в обслуговуванні, викладення конфіденційних даних та інші [3]. OWASP Top 10 може служити важливим джерелом для визначення потенційних загроз безпеці та розробки стратегій їх усунення.

Крім того, існують інші стандарти та рекомендації, спрямовані на забезпечення безпеки програмного забезпечення, які можуть бути застосовані при аудиті смарт-контрактів. Наприклад, CERT Secure Coding Standards включає набір практик з безпеки програмування, які можуть допомогти у виявленні та усуненні потенційних вразливостей у смарт-контрактах.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Introduction to smart contracts – [Електронний ресурс]. – Режим доступу: https://ethereum.org/en/developers/docs/smart-contracts/

2. Comparison of smart contract generation methods. – [Електронний ресурс]. – Режим доступу https://www.researchgate.net/figure/Comparison-ofsmart-contract-generation-methods_tbl1_360503282

3. H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, J. J. Kishigami, ‘‘Blockchain contract: A complete consensus using blockchain,’’ in Proc. IEEE 4th Global Conf. Consum. Electron. (GCCE), Жовтень, 2015, с. 577–578.

УДК 681.518.3.01

Василенко О.В.[1], Сніжной Г.В.[2], Зайцев І.Д.[3]
[1] канд. техн. наук, доц. НУ «Запорізька політехніка»
[2] д-р. техн. наук, проф. НУ «Запорізька політехніка»
[3] студ. гр. БК-310 НУ «Запорізька політехніка»

МЕХАТРОНІКА ЯК ОСНОВА КІБЕРФІЗИЧНИХ СИСТЕМ

Як відомо, мехатронна система – це синергетична комбінація механіки, енергетичної та інформаційної електроніки для скоординованого руху в робототехнічних системах. Маніпулятори, роботи, пристрої адитивних технологій (3D-принтери, наприклад), навіть більшість верстатів з ЧПК (комп'ютерне числове керування) є в основному мехатронними системами.

Передові мехатронні системи включають інтелектуальні датчики, які використовують технології Інтернету речей (IoT) або промислового Інтернету речей (IIoT) для передачі відповідних даних до систем керування, SCADA, інтерфейсів людина-машина (HMI) та інших цифрових платформ. З

переходом до технології четвертої промислової революції, так званої Industry 4.0 (I4.0) [1], ці датчики почали надсилати дані для створення Digital Twin, для машинного навчання, для аналізу великих даних для прийняття рішень за допомогою штучного інтелекту та хмарних сервісів.

Оцифровка продуктів (автомобілів, побутової техніки), підприємств, організацій, інфраструктури робить їх більш автономними [2]. Вплив на ці об'єкти інформаційних технологій, зокрема IoT, плюс повна автоматизація та використання модельного підходу перетворює їх на кіберфізичні системи (CFS). Можна сказати, що CPS поєднує фізичний і віртуальний світи.

У CFS процеси реального світу відбуваються майже паралельно з процесами віртуального світу. Іноді ці процеси випереджають один одного, наприклад, при прогнозному аналізі віртуальна модель CFS попереджає про аномальну поведінку контрольованого фізичного об'єкта.

Цифрове виробництво [3], яке є CFS і основним драйвером I4.0, базується на роботизованих системах, які керуються CAM (Computer-aided Manufacturing) і CADAM (Computer-augmented Design and Manufacturing). Дані процесів надсилаються до цифрових платформ SAP (системні додатки та продукти в обробці даних), які надсилають дані до хмарних служб для обробки, прогнозування та планування. SAP включає спеціалізоване прикладне програмне забезпечення: EPR – Enterprise Resource Planning, MES – Manufacturing Execution Systems, QMS – Quality Management Systems, CRM – Customer Relationship Management) тощо.

Модель цифрового виробництва у вигляді CFS з мехатронними підсистемами має п'ять ієрархічних рівнів. Два нижніх рівня тяжіють до фізичного світу, і, власне, до виробничих процесів, два верхніх рівні більш актуальні для віртуального світу, вони використовуються для автоматизації бізнес-процесів.

На середньому (третьому) рівні зв'язок віртуального і фізичного світів здійснюється шляхом тотальної інтеграції та автоматизації (TIA). Портал TIA поєднує дані на всіх рівнях і перетворює завод / організацію / підприємство в CFS.

Аналіз сучасних мехатронних систем і технологій I4.0 показав, що мехатронні системи є основою кіберфізичних систем і забезпечують роботу з фізичними активами з передачею даних для створення віртуального Digital Twin з використанням технологій IIoT. Таким чином, у мехатронних системах, які входять як базові підсистеми CFS, роль IT-технологій більш значна. Апаратне забезпечення таких мехатронних систем також змінилося, щоб забезпечити повну автоматизацію та інтеграцію на основі Інтернету речей.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Vasylenko O. Design of information and measurement systems within the Industry 4.0 paradigm / O. Vasylenko, S. Ivchenko, H. Snizhnoi // Radioelectronic and Computer Systems. – 2023. – N. 1. – P. 45–54. doi: 10.32620/reks.2023.1.04

2. Василенко О. В. Концепція моделювання електромобілів для оптимізації запасу ходу в різних патернах руху / О. В. Василенко, Г. В. Сніжной, С. А. Івченко // Матеріали VIII Міжнар. наук.-техн. конф. Комп'ютерне моделювання та оптимізація складних систем, 1-3 лист. 2023 р. – Дніпро: УДХТУ, 2023. – С. 155-156.

3. Василенко О. В. Менеджмент цифрового виробництва: монографія / О. В. Василенко, Г. В. Сніжной, Ю. С. Ямненко – Запоріжжя: Національний університет «Запорізька політехніка», 2022. – 120 с. ISBN 978-617-529-374-4.

УДК 043.5

Нагорна Н.М.[1], Гарбуз С.В.[2]

[1] старш. викл. НУ «Запорізька політехніка»

[2] студ. гр. БК-313м НУ «Запорізька політехніка»

ОПТИМІЗАЦІЯ ІНТЕРФЕЙСУ ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНИХ СИСТЕМ ТИПУ «СТРУМОВА ПЕТЛЯ»

Основна мета досліджень – це отримання характеристик та мінімізація похибок при вимірюваннях, що виникають в інтерфейсах промислової автоматики типу «струмова петля 4…20 мА», за рахунок використання перетворювачів «напруга-струм» та «струм-напруга» на базі сучасних спеціалізованих надвеликих інтегрованих схем (НВІС).

Актуальність досліджень підтверджується тим, що розробки в області промислових телекомунікацій особливо необхідні для України, тому що на сьогодення застаріле обладнання на промислових підприємствах підлягає або заміні, або модернізації. При цьому модернізація вимагає менших грошових вкладень. При виконанні досліджень саме розглядалися питання, що стосуються модернізації інтерфейсів типу «струмова петля».

Широке використання вказаних інтерфейсів при вимірюваннях пов'язане з такою властивістю цих інтерфейсів, як незалежність струму, що протікає по замкнутому контуру (петлі), ні від активного опору контуру, ні від струму навантаження, ні від ЕРС індуктивної завади в контурі.

Для більш детального розгляду процесів, що відбуваються при передаванні даних від вимірювальних перетворювачів до контролерів при віддалених вимірюваннях, була проаналізована робота системи «передавач-струмова петля 4…20 мА – приймач», де у якості перетворювача напруги у струм (U/I) була використана НВІС XTR115.

Мікросхема XTR115 є прецизійним струмовим перетворювачем. На виході XTR115, що приєднується до струмової петлі, створюється струм величиною 4 мА при нульовому вхідному струмі на вході HBIC (до якого приєднується джерело виміряної напруги з деяким внутрішнім опором).

Характеристики системи зі струмовою петлею оцінювалися на основі моделі струмової петлі, що містить передавач, перетворювач напруги у струм (U/I), приймач (рис. 1).

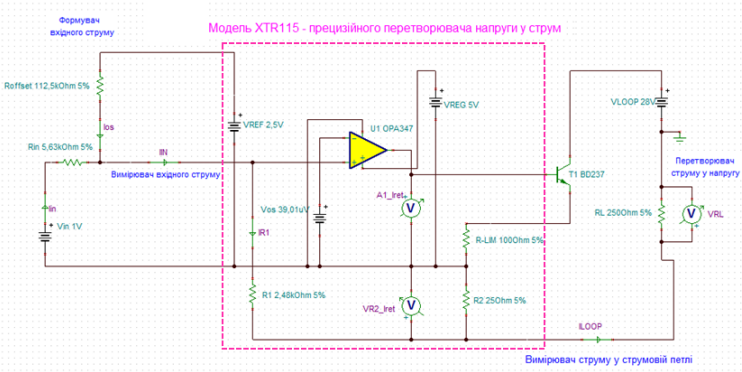


Рисунок 1 – Модель струмової петлі на основі блоків: передавача, перетворювача напруги у струм, приймача

Аналіз перехідних процесів показав значну інерційність струмової петлі при вхідних сигналах з крутими фронтами.

У другій досліджуваній схемі перетворювача струму у напругу (I/U) інтерфейсу системи використовувалися дві мікросхеми: вимірювального підсилювача INA213 та прецизійного джерела напруги REF2030. Дослідження вказаного перетворювача проводилися на основі моделі, показаної на рис. 2.

При дослідженнях обчислювалися похибки точності та похибки внаслідок дрейфу температури перетворювача *I*/*U*. В результаті отримані похибки: сумарна мультиплікативна за параметрами точності, середньоквадратична за параметрами точності, сумарна мультиплікативна за параметрами дрейфу, сумарна мультиплікативна та сумарна середньоквадратична похибки пристрою, які мають значення (2,09, 1,17, 2,52, 1,624, 4,61, 2,00)·10^{-3} відповідно.

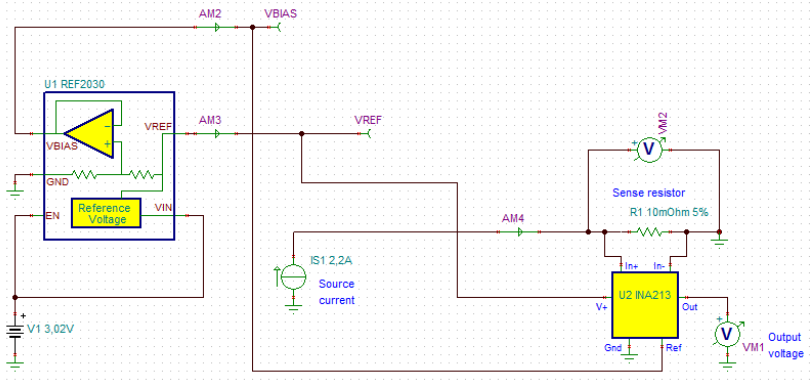


Рисунок 2 – Модель перетворювача струму інтерфейсу інформаційно-вимірювальної системи у напругу

Результати аналізів перетворювача *U*/*I* показали, що розроблений пристрій має параметри, які відповідають вимогам інтерфейсу "струмова петля"; пристрій має лінійну залежність вихідного струму від вхідної напруги.

При зміненні вхідних струмів перетворювача *I*/*U* від мінус 2,5 А до плюс 2,5А діапазон вихідної напруги змінюється від 250 мВ до 2,75 В.

Також отримано, що середня квадратична похибка перетворювача *I*/*U* не перевищує $2{,}00 \cdot 10^{-3}$ в.о., тобто є малою.

УДК 519.7
Юрченко П.Ю.[1], Нагорна Н.М.[2]
[1] студ. гр. БК-313м НУ «Запорізька політехніка»
[2] старш. викл. НУ «Запорізька політехніка»

АПРОКСИМАЦІЯ КІНЦЕВОЇ МНОЖИНИ ВИМІРЮВАНИХ ДАНИХ, СПОТВОРЕНИХ ШУМОМ

У каналах вимірювальних систем виникають випадкові адитивні завади, які динамічно змінюються. Такого типу завади зазвичай описуються моделлю адитивного білого гаусівського шуму з дискретним часом. Даний вид шуму притаманний багатьом вимірювальним системам, а особливо системам з радіозв'язком. Білий шум імітує ефекти багатьох природних випадкових процесів.

Характерною особливістю білого шуму є рівномірна на усіх частотах спектральна густина потужності шуму. Білий шум статистично не залежить

від корисного сигналу, що передається по каналу, а також має нормально розподілені у часі значення.

Суть представленого алгоритму апроксимації кінцевої множини вимірюваних даних полягає у використанні адаптивної нейрон-нечіткої системи для розпізнавання прийнятого корисного сигналу з адитивним білим шумом, причому потужність завади у вигляді шуму може бути більше потужності корисного сигналу.

Система апроксимує залежністю прийнятий сигнал з шумом як шумову складову сигналу. Потім з прийнятого сигналу віднімається апроксимована залежність.

В результаті отримується корисний сигнал з дуже зниженим рівнем шуму, тобто потужність шуму значно зменшується, і шум майже не впливає на форму корисного сигналу. При необхідності подавити цю шумову складову можна легко за допомогою фільтра.

Алгоритм складається з наступних етапів:

1) генерація множини пар ”вхід-вихід” за заданим аналітичним описом функції, яка підлягає апроксимації (тобто генерація корисного сигналу);

2) генерація вектора n_1 нормально розподілених випадкових чисел за допомогою функції ***randn*** (генерація шуму);

3) припущення, що сигнал завади (шуму), який генерується у каналі, є випадковим і описується (для прикладу) невідомим для системи нелінійним рівнянням, залежним від n_1: $n_2 = 4 \cdot \sin(n_1(k)) \cdot n_1(k\text{-}1)/(1+n_1(k\text{-}1)^4)$, де k – номер точки дискретизованої залежності; формування сітки (функція ***mechgrid***) та відображення (функція ***surface***) 3D-графіка сигналу завади;

4) формування виміряного сигналу, в який додається шум: $m = x + n_2$, графічне представлення сигналу m в залежності від часу;

5) створення початкової нейронної мережі (функція ***genfis1***) під назвою ”in_fismat” з чотирма функціями приналежності (для подальшого навчання мережі) та двома входами;

6) за допомогою функції ***anfis*** виконується остаточне формування структури нейрон-нечіткої мережі, її навчання, також відбувається точне налаштування параметрів 16 функцій приналежності;

7) тестування налаштованої мережі з навчаючими даними, виконання обчислення нечіткого висновку (оцінка вихідних значень за допомогою функцій приналежності) проводиться з використанням функції ***evalfis***;

8) вихідним сигналом мережі є оцінена завада n_2, визначення оціненого корисного сигналу x: $x = m – n_2$; 9) візуалізація графічних залежностей.

Вказаний алгоритм побудований на основі використання адаптивної нейро-нечіткої мережі.

На основі програмної реалізації приведеного алгоритму в системі Matlab виконані розрахунки; результати показані на рис. 1 та рис. 2.

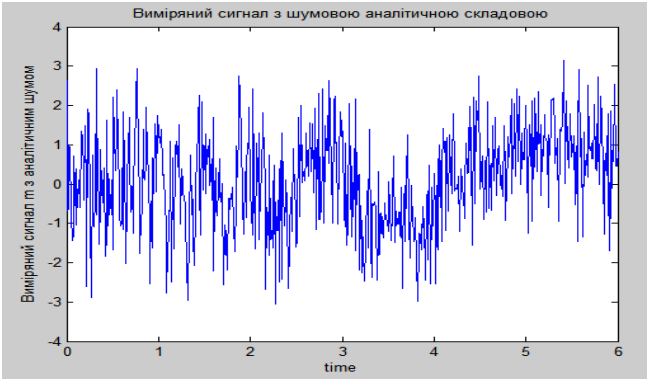


Рисунок 1 – Корисний сигнал з шумовою складовою на приймальному кінці каналу до обробки його нейро-нечіткою мережею

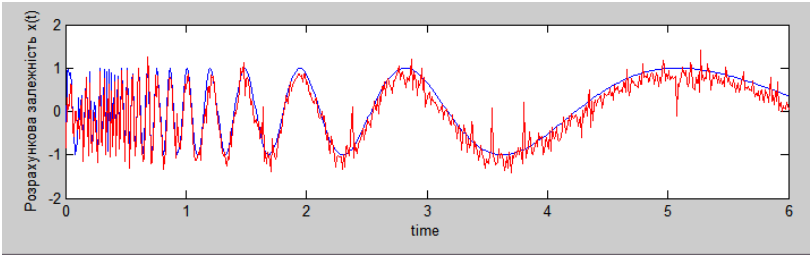


Рисунок 2 – Корисний сигнал зі значно зменшеною шумовою складовою на приймальному кінці каналу після обробки його нейро-нечіткою мережею (червоний колір графіка)

Таким чином, отримана структура системи ANFIS нечіткого висновку типу Сугено з двома входами, одним виходом, яка виконує фазифікацію функціями Гауса; сформовано чотири апріорних функції приналежності; при дефазифікації використаний метод зваженого середнього; створена нейро-нечітка мережа виконує роль апроксиматора експериментальних залежностей з шумовою компонентою.

УДК 004.056
Піківець Г.М.[1], Корольков Р.Ю.[2]
[1] студ. гр. БКз-813м НУ «Запорізька політехніка»
[2] канд. техн. наук, доц. НУ «Запорізька політехніка»

ОГЛЯД МЕТОДІВ OSINT ТА ЇХ РОЛЬ У РОЗСЛІДУВАННІ КІБЕРІНЦИДЕНТІВ

Кіберзлочинність стрімко еволюціонує, перетворюючись на одну з найбільш актуальних проблем сучасності. Зловмисники постійно удосконалюють свої методи, завдаючи шкоду як приватним особам, так і великим компаніям. У цьому контексті, розслідування кіберінцидентів стає все більш важливим завданням, оскільки від його успіху залежить не лише компенсація завданих збитків, але й запобігання майбутнім атакам.

Звичайні методи розслідування не завжди є ефективними у віртуальному просторі, де зловмисники використовують складні інструменти та методи для приховування своїх дій. Розвідка з відкритих джерел стає все більш ефективним інструментом у боротьбі з кіберзлочинністю та кіберінцидентами [1]. В контексті протидії кіберзлочинності методи розвідки з відкритих джерел набувають все більшого значення, що дозволяє збирати інформацію про зловмисників, їхні методи та цілі, а також моніторити кіберзагрози.

Open Source Intelligence (OSINT) – це концепція, методологія та технологія для отримання та використання військової, політичної, економічної та іншої інформації з відкритих джерел без порушення чинного законодавства. OSINT використовується для прийняття рішень у сфері національної оборони та безпеки, у розслідуваннях кіберзлочинів, терористичних актів та інших подій, що включає збір інформації, реєстрацію, облік та аналіз, аналітичну та синтетичну обробку первинної інформації, зберігання та поширення інформації, інформаційну безпеку та подання результатів дослідження. Після того, як первинна інформація з відкритих джерел пройде аналіз та обробку, вона може стати корисною і ,якщо ця інформація не відноситься до категорії, що є державною таємницею, вона може бути розголошена [2].

Щоб максимізувати ефективність OSINT, вкрай важливо застосовувати різноманітні методи та використовувати відповідні інструменти. Ці техніки можна умовно розділити на пасивні та активні [3].

Пасивні OSINT-методи передбачають збір інформації без безпосереднього звернення до джерел, використовуючи інформацію, доступну для загального ознайомлення.

Деякі поширені методи включають:

1. Аналіз соціальних мереж: Facebook, Twitter, LinkedIn, Instagram та інші. Аналізуючи профілі користувачів, публікації та зв'язки, аналітики можуть отримати цінну інформацію про людей, організації та тенденції.

2. Запити в пошукових системах Google, Bing, DuckDuckGo та інших. Використовуючи оператори розширеного пошуку такі як Google Dork можливо уточнювати пошуки та отримувати цільову інформацію.

3. Дослідження веб-сайтів і доменів є важливою частиною методів OSINT і може надати цінну інформацію про підприємства, організації чи навіть окремих користувачів. Такі методи, як записи WHOIS, аналіз IP-адрес і веб-скрапінг, можуть розкрити важливу інформацію.

Активні методи OSINT передбачають безпосередню взаємодію з джерелами та активний збір даних, а також вимагають від користувача значних зусиль, в тому числі фінансових витрат.

До таких методів належать:

1. Сканування веб-сайтів та індексація каталогів що включає безпосередню взаємодію з веб-сайтами шляхом сканування їх структури, пошуку вразливостей та визначення характеристик, таких як доступні служби чи ресурси.

2. Звернення до джерел із запитами про інформацію ВКЛЮЧАЮЧИ направлення запитів до компаній, організацій або громадських установ для отримання конкретної інформації.

3. Активне спостереження і взаємодія в соціальних мережах. Цей підхід передбачає безпосереднє спостереження за активністю користувачів у соціальних мережах та взаємодію з ними для отримання додаткової інформації.

4. Тестування на проникнення та збір інформації про безпеку мережі передбачає активне тестування систем та мереж на предмет наявності потенційних вразливостей шляхом спроби проникнення в них.

5. Дослідження публічних архівів, таких як судові документи, реєстрація бізнесу та майнові записи, що надають цінну інформацію про окремих осіб, організації та їх діяльність.

6. Аналіз зображень і відео, що часто містять цінну інформацію, яка може сприяти збору розвідувальних даних. Такі методи, як реверсивний пошук зображень, аналіз метаданих і відеокриміналістика, допомагають отримати інформацію з візуального вмісту.

У розслідуванні кіберінцидентів OSINT відіграє важливу роль, допомагаючи: ідентифікувати зловмисників; визначити інструменти та методи які використовуються зловмисниками, та способи захисту від них; зібрати докази; моніторити кіберзагрози.

Хоча OSINT є потужним інструментом для розслідування кіберзлочинів та забезпечення кібербезпеки, його використання вимагає уважного

врахування етичних аспектів. Якість отриманих даних не завжди є достатньою, що потребує критичного аналізу та перевірки. Крім того, використання Open Source Intelligence може порушувати юридичні обмеження, особливо у випадках, коли стосується конфіденційної інформації або національної безпеки. Отже, при використанні OSINT необхідно дотримуватися етичних принципів та враховувати можливі ризики і обмеження, щоб забезпечити ефективність та законність проведених дій [4].

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Мамедова Л.Ш. Особливості використання спеціальних знань під час розслідування кіберзлочинів: міжнародний досвід. Юридичний науковий електронний журнал. 2021. № 12. С. 392–395. URL: https://doi.org/10.32782/2524-0374/2021-12/99 (дата звернення: 09.04.2024).
2. Електронна енциклопедія Wikipedia. Українськомовна версія URL: https://uk.wikipedia.org/w/index.php?title=Розвідка_на_основі_відкритих_джерел&stable=0 (дата звернення: 09.04.2024)
3. THE OSINT FRAMEWORK: UNVEILING THE ART OF INFORMATION GATHERING URL: https://www.pvt365.net/the-osint-framework-unveiling-the-art-of-information-gathering (дата звернення: 09.04.2024).
4. Open Source Intelligence (OSINT): A Powerful Tool for Information Gathering URL: https://www.linkedin.com/pulse/open-source-intelligence-osint-powerful-tool-information-t-w96pc (дата звернення: 09.04.2024)

Зав. кафедри Андрій КОРОТУН

Відповідальний на факультеті Станіслав ШАПТАЛА

Наукове електронне видання
Можна використовувати в локальному та
мережному режимах

ТИЖДЕНЬ НАУКИ-2024

Факультет інформаційної безпеки та електронних комунікацій

Збірник тез доповідей щорічної
науково-технічної конференції серед студентів,
викладачів, науковців, молодих вчених та аспірантів

15–19 квітня 2024 року

Один електронний оптичний диск (DVD-ROM); супровідна
документація.
Тираж 100 прим. Зам. №608

Видавець і виготовлювач
Національний університет «Запорізька політехніка»
Україна, 69063, м. Запоріжжя, вул. Жуковського, 64
Тел.: (061) 769–82–96, 220–12–14

Свідоцтво суб'єкта видавничої справи ДК № 6952 від 22.10.2019.