МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
РАДІОЕЛЕКТРОНІКИ

МАТЕРІАЛИ
V ФОРУМУ
«Автоматизація, електроніка та робототехніка. Стратегії розвитку та інноваційні технології»
AERT-2023

29 - 30 листопада 2023 р.

Харків 2023

Збірник матеріалів V форуму «Автоматизація, електроніка та робототехніка. Стратегії розвитку та інноваційні технології» AERT-2023. – Харків, ХНУРЕ, 2023. – 149 стр.

В збірник включені матеріали V форуму «Автоматизація, електроніка та робототехніка. Стратегії розвитку та інноваційні технології» AERT-2023.

V форум «Автоматизація, електроніка та робототехніка. Стратегії розвитку та інноваційні технології» AERT-2023 проведено кафедрами:

- мікропроцесорних технологій і систем (МТС),
- комп'ютерно-інтегрованих технологій, автоматизації та робототехніки (КІТАР).

Видання підготоване
кафедрою мікропроцесорних технологій і систем (МТС)
Харківського національного університету радіоелектроніки (ХНУРЕ)

61166 Україна, Харків, просп. Науки, 14
Тел. +38 (057) 755 0220
E-mail:
iryna.svyd@nure.ua

КОМІТЕТ ФОРУМУ

Голова комітету форуму:

Романенков Ю.О. д.т.н., проф., проректор з наукової роботи ХНУРЕ, м. Харків, Україна.

Програмний комітет форуму:

Свид І.В. к.т.н., доц., зав. каф. МТС ХНУРЕ, м. Харків, Україна.

Обод І.І. д.т.н., проф., проф. каф. МТС ХНУРЕ, м. Харків, Україна.

Новоселов С.П. к.т.н., доц., проф. каф. КІТАР ХНУРЕ, м. Харків, Україна.

Воргуль О.В. к.т.н., доц., доц. каф. МТС ХНУРЕ, м. Харків, Україна.

Зубков О.В. к.т.н., доц., доц. каф. МТС ХНУРЕ, м. Харків, Україна.

Горелов Д.Ю. к.т.н., доц., доц. каф. КРіСТЗІ ХНУРЕ, м. Харків, Україна.

Сичова О.В. к.т.н., доц. каф. КІТАР ХНУРЕ, м. Харків, Україна.

Секретаріат комітету форуму:

Теслюк С.І. старший викладач каф. КІТАР ХНУРЕ, м. Харків, Україна.

Чумак В.С. асистент каф. МТС ХНУРЕ, м. Харків, Україна.

Бойко Н.В. завідувач лабораторії каф. МТС ХНУРЕ, м. Харків, Україна.

РОЗРОБЛЕННЯ ВІРТУАЛЬНОЇ ЛАБОРАТОРНОЇ РОБОТИ З ДОСЛІДЖЕННЯ ОСНОВ РОБОТИ АЦП

професор, к.т.н., Новоселов С.П., доцент, к.т.н., Сичова О.В.
Харківський національний університет радіоелектроніки,
кафедра комп'ютерно-інтегрованих технологій, автоматики і робототехніки, м. Харків, Україна
e-mail: sergiy.novoselov@nure.ua, oksana.sychova@nure.ua

Abstract. The analysis of the structural diagram of the real layout was performed and the algorithm of its operation was described for the further creation of a program of virtual laboratory work. The prototype for virtual laboratory work was a model of a modular industrial controller based on a Raspberry PI mini-PC. A software tool for virtual laboratory work on the study of the basics of ADC operation has been developed. The graphic interface of virtual laboratory work is described.

Ключові слова: АЦП, віртуальна лабораторія, ПЛК, LDmicro.

Вступ. Використання віртуальних лабораторних робіт у навчанні має багато переваг. Це ефективний і зручний інструмент для вивчення програмно-технічних комплексів та інших технічних дисциплін. Вони допомагають студентам більш ефективно виконувати практичну роботу та отримувати реальний досвід, що забезпечує краще розуміння та запам'ятовування матеріалу.

Віртуальні лабораторні роботи дозволяють викладачам створювати різні сценарії та завдання для студентів різного рівня складності. Це допомагає викладачу персоналізувати навчання та забезпечити ефективніше засвоєння матеріалу студентами.

Віртуальні лабораторні роботи є важливим інструментом для дистанційного навчання, оскільки вони дають можливість студентам виконувати практичну роботу з будь-якого місця з доступом до Інтернету.

Загалом, віртуальні лабораторні роботи мають багато переваг у навчанні технічних дисциплін та можуть забезпечити більш ефективне засвоєння матеріалу та отримання реального досвіду.

Метою даної роботи є вдосконалення навчального процесу завдяки розробці програми для виконання віртуальної лабораторної роботи з дослідження принципів роботи з АЦП за допомогою ПЛК та технологічних мов програмування.

Основна частина. При створенні програми для виконання віртуальної роботи в якості аналога реального макету обрано макет модульного промислового контролеру з модулем введення аналогових сигналів, що зображено на рис. 1.

Алгоритм роботи модуля вводу аналогових сигналів показано на рис. 2.

1 – центральний процесорний модуль на базі міні-ПК Raspberry;
2 – модуль аналогового вводу; 3 – модуль дискретного вводу-виводу

Рисунок 1 – Зовнішній вигляд модульного ПЛК

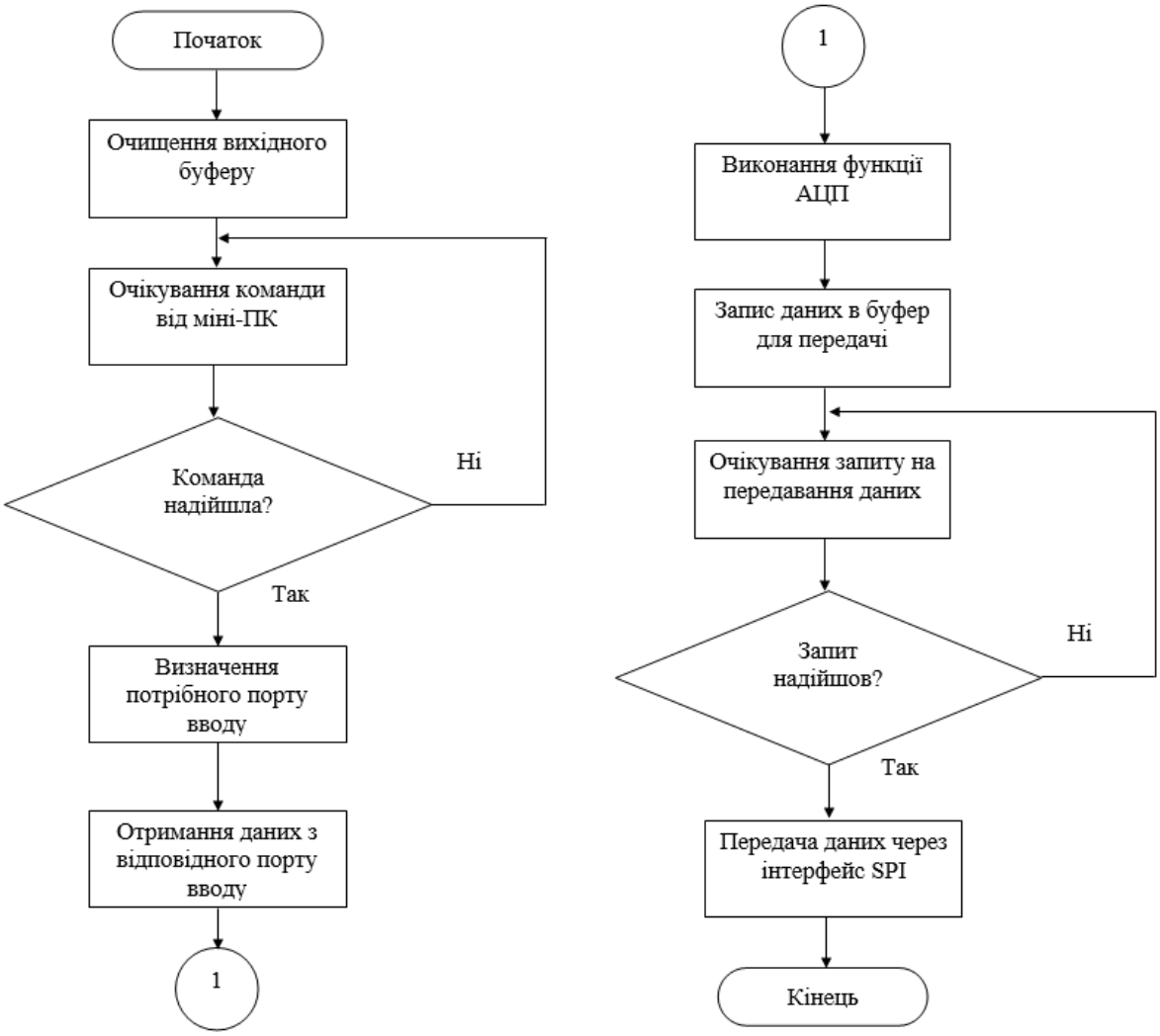


Рисунок 2 – Алгоритм роботи модуля вводу аналогових сигналів

Робота модуля починається з очищення буферу обміну даними та скидання всіх регістрів в початковий стан. Після початкової ініціалізації модуль переходить в режим очікування команди від міні-ПК, яка повинна надійти через інтерфейс SPI.

Після надходження команди виконується визначення потрібної адреси вхідного порту вводу. Коли номер порту буде з'ясовано, видається команда на внутрішній комутатор для підключення потрібного порту до блоку АЦП.

Блок АЦП виконує перетворення поточного значення напруги на вході модуля в його цифрове значення. Отримане значення вхідного сигналу записується до вихідного буфера, де очікує запиту на передавання. Після отримання запита на обмін даними модуль передає на міні-ПК визначене значення через послідовний інтерфейс SPI.

Інтерфейс користувача віртуального макету «Аналого-цифровий перетворювач» показано на рис. 3. Верхня частина робочого вікна програми представляє собою окремий віртуальний прилад «Семисегментний чотирьох розрядний цифровий індикатор». Він може використовуватись як самостійно, так і в комплексі із аналого-цифровим перетворювачем. Нижня частина має необхідні органи керування для виконання дослідження методів введення аналогових сигналів за допомогою ПЛК.

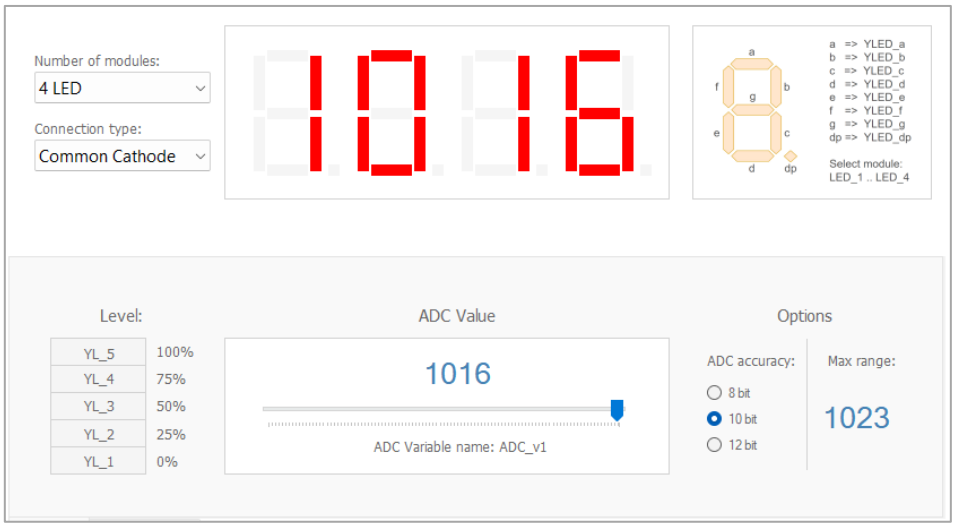


Рисунок 3 – Інтерфейс користувача віртуального макету «Аналого-цифровий перетворювач»

Верхня частина віртуальної лабораторної роботи «Семисегментний чотирьох розрядний цифровий індикатор» призначений для відображення поточної інформації засобами ПЛК та дослідження методів організації динамічної індикації при роботі з багаторозрядними цифровими індикаторами.

За допомогою кнопок Simple ADC і Voltage Regulation можна перемикати режим роботи віртуального приладу: простий АЦП або регулятор напруги. Зовнішній вигляд приладу в режимі регулятора напруги показано на рис. 4. Даний режим призначений для дослідження методів перетворення вхідної інформації від АЦП в реальне значення вимірюваної величини.

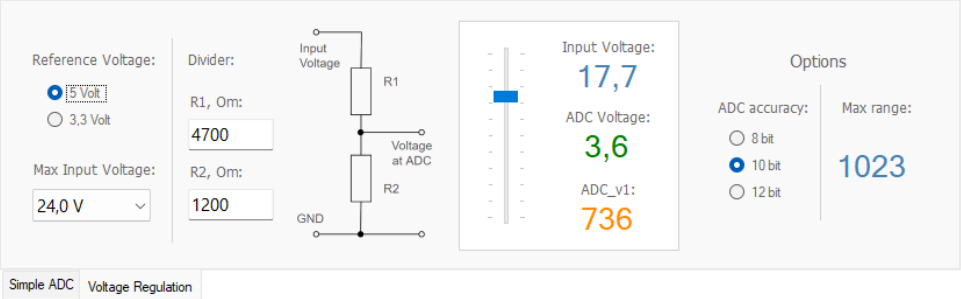


Рисунок 4 – Зовнішній вигляд приладу в режимі регулятора напруги

Віртуальна лабораторна робота створена в інтегрованому середовищі розробки програм Visual Studio 2022. При розробці була застосована мова програмування C# та технологія Named Pipes для поєднання з іншою програмою LDmicro.

Висновки. Дана робота присвячена створенню програми віртуальної лабораторної роботи, прототипом якої став макет модульного промислового контролеру на базі міні-ПК Raspberry PI. Розроблена віртуальна лабораторна робота для дослідження основ роботи АЦП в технічних засобах автоматизації надає широкі можливості для виконання різних практичних завдань в області автоматизації технологічних процесів та програмування ПЛК.

Список використаних джерел.

1. Novoselov S., Sychova O. Technology of using digital twins in the control of industrial equipment. – Information systems in project and program management: Collective monograph edited by I. Linde. European University Press. Riga: ISMA, 2023. – P. 173-181.

2. Новоселов С. П., Сичова О. В. Принцип використання віртуальних приладів в управлінні промисловим обладнанням. Міжнародна науково-практична конференція «Інтелектуальні інформаційні системи в управлінні проєктами та програмами», Коблево, 12–15 вересня 2023 р. Збірник праць. – Харків: ХНУРЕ, 2023. - с.155-158.

3. Невлюдов І. Ш. Застосування цифрових двійників технічних засобів автоматизації для розроблення програмно-технічних комплексів АСУ ТП : Навчальний посібник / І. Ш. Невлюдов, С. П. Новоселов, О. В. Сичова. – Харків: Видавництво Іванченка І. С., 2023. – 267 с. ISBN 978-617-8059-95-8, DOI: 10.30837/978-617-8059-95-8.

РЕАЛІЗАЦІЯ ЦИФРОВИХ ФІЛЬТРІВ НА МІКРОКОНТРОЛЕРАХ STM32 З ВИКОРИСТАННЯМ КІЛЬЦЕВИХ БУФЕРІВ

доцент, к.т.н. Зубков О.В., студент Яковенко О.С.
Харківський національний університет радіоелектроніки,
кафедра мікропроцесорних технологій і систем, м. Харків, Україна
e-mail: oleh.zubkov@nure.ua, oleksandr.iakovenko@nure.ua

Abstract. The analysis of digital filters in electronics and their software implementation on general-purpose microcontrollers was completed in this work. A real-time digital filtering algorithm has been developed for STM32 microcontrollers with support for DSP instructions and the use of ring buffers. A study of the proposed algorithm performance was carried out using the example a digital low-pass filter with a finite impulse response implementation. A comparative analysis of performance measurement results and comparisons with the results of using the standard library proved the effectiveness of the proposed algorithm.

Ключові слова: цифровий фільтр, мікроконтролер, буфер, швидкодія.

Вступ. Наразі розробка цифрових фільтрів на мікроконтролерах залишається актуальною та корисною в багатьох сферах. Цифрові фільтри застосовуються для обробки сигналів у реальному часі в різноманітних пристроях, від медичних приладів до комунікаційних систем. В контексті "Інтернету речей" (IoT) цифрові фільтри застосовуються для фільтрації шумів, видалення спотворень та покращення якості отриманих сигналів. В медичних пристроях, наприклад, в електрокардіографах (ЕКГ) чи електроенцефалографах (ЕЕГ), використання цифрових фільтрів дозволяє відокремлювати корисний сигнал від шумів. У бездротових комунікаційних системах, таких як Wi-Fi, Bluetooth, цифрові фільтри можуть використовуватися для покращення якості сигналу та підвищення швидкості передачі даних. Враховуючи зростаючі можливості мікроконтролерів та їх обробки, розробка цифрових фільтрів на мікроконтролерах залишається актуальною та значущою у багатьох сферах, де потрібна обробка сигналів у реальному часі.

Основна частина. Усі сучасні процесори за їх апаратними можливостями реалізації цифрової фільтрації умовно можна поділити на 2 групи: спеціалізовані та загального призначення. Спеціалізовані процесори, такі як Shark, мають високу вартість і їх використовують при створенні професійної віщальної, локаційної, навігаційної і т.д. апаратури. Менші за ціною процесори загального призначення, такі як STM32, завдяки вбудованому DSP модулю можуть бути використані для реалізації цифрових фільтрів [1, 2]. Математичні підходи до синтезу цифрових фільтрів дуже добре відомі і описані у сучасній літературі [3]. Такі математичні пакети, як Matlab, мають навіть вбудовані спеціалізовані

утиліти для візуального проектування цифрових фільтрів [4]. Основною проблемою реалізації цифрових фільтрів на мікроконтролерах загального призначення є необхідність виконувати багато інших різноманітних задач крім цифрової фільтрації. Якщо для зберігання коефіцієнтів фільтру, відліків сигналу, що обробляється, і результатів фільтрації достатньо незначного об'єму оперативної пам'яті (близько 1 кбайт при порядках фільтра до 100), то об'єм математичних операцій значний і необхідно мати значну швидкодію процесора для втілення алгоритму цифрової фільтрації або розробляти оптимальні за часом виконання алгоритми обробки, які використовують апаратні можливості сучасних процесорів і мов програмування. Тому метою дослідження був аналіз швидкодії існуючих алгоритмів та досягнення зменшення часу обробки.

Найбільш поширеними на практиці є фільтри з кінцевою імпульсною характеристикою (FIR) [3, 4]. FIR фільтри мають скінчену відповідь на імпульс, що означає, що їх відповідь на вхідний сигнал залежить лише від обмеженої кількості минулих вхідних сигналів. Це дає їм хорошу лінійність та стійкість до коливань. Загальна структура таких фільтрів наведена на рис. 1, а математичний опис сигналу на виході фільтра представлено формулою 1.

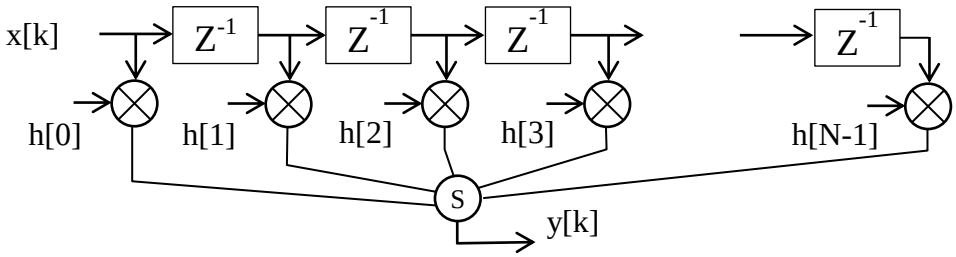


Рисунок 1 – Узагальнена схема цифрового FIR фільтра

$$y[k] = \sum_{i=0}^{N-1} h(i) \cdot x[k-i], \quad (1)$$

де N – порядок фільтру; h(i) – коефіцієнти фільтру; x[k-i] – відліки вхідного сигналу.

Задача створення алгоритмів цифрової фільтрації сигналів на мікроконтролерах з ARM архітектурою не є новою. Існують спеціалізовані бібліотеки CMSIS, які містять набір функцій реалізації цифрової фільтрації. Наприклад, для реалізації FIR фільтрів існують функції: arm_fir_f32, arm_fir_q31, arm_fir_q15. Перша з функцій призначена для виконання обчислень з плаваючою комою. При таких обчисленнях поведінка фільтра завжди стабільна і результат реальної фільтрації відповідає теоретичним розрахункам. Дві інші функції призначені для реалізації обчислень з фіксованою комою. Вони мають більшу швидкодію, але результат фільтрації може значно відрізнятись від очікуваного. Кожна з функцій має 3 вхідних параметри: набір коефіцієнтів фільтру, масив відліків вхідного сигналу і масив для формування результатів фільтрації.

Функції забезпечують високу швидкодію завдяки використанню усіх 32 регістрів загального призначення ARM ядра. У багатьох Internet джерелах є порівняльний аналіз швидкодії цих функцій при заданій частоті дискретизації та кількості коефіцієнтів фільтру. Але реальна реалізація фільтрації сигналу значно складніша, бо передбачає взаємодію з аналого-цифровим (АЦП) та цифро-аналоговим (ЦАП) перетворювачем.

У таких сучасних мікроконтролерах, як STM32 існує вбудований контролер прямого доступу до пам'яті, який забезпечує паралельно з роботою ядра процесору передавання даних між оперативною пам'яттю та периферійним пристроєм. Найбільша швидкодія передавання даних досягається при використанні кільцевих буферів разом з контролером DMA та АЦП і ЦАП. З урахуванням апаратних можливостей мікроконтролерів STM32 були запропоновані наступні: структурна реалізація цифрової фільтрації та алгоритм програмної реалізації фільтрації.

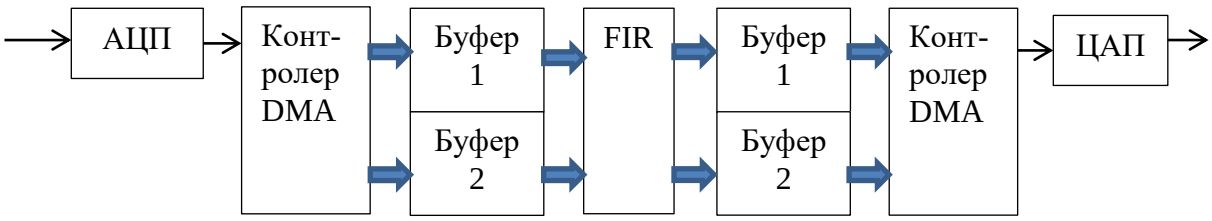


Рисунок 2 – Апаратна реалізація цифрової фільтрації у мікроконтролерах STM32

В системі на рис. 2 АЦП виконує періодичні перетворення вхідного сигналу у цифрову форму, а контролер DMA передає ці значення у 2 буфера. Спочатку накопичуються дані у перший буфер. Коли починається накопичення у другий виконується цифрова фільтрація, що використовує кінцеву частину другого буфера і значення із першого буфера. Результат фільтрації одразу записується у перший вихідний буфер для їх відтворення за допомогою контролеру DMA та ЦАП. АЦП та ЦАП працюють синхронно, а синхронізацію забезпечує на апаратному рівні таймер, що подає на них команди запуску перетворень. Після заповнення буферу 2 йде фільтрація частини даних із буферу 1 і даних із буферу 2, а у цей час відтворюються дані із першого буферу. Далі процес повторюється циклічно по колу. Для досліджень були створені дві програми. Перший алгоритм фільтрації був реалізований у обробниках переривань від контролеру DMA по закінченню заповнення кожного з буферів. Він використовував безпосередньо результати аналого-цифрового перетворення із буферів. Друга програма використовувала стандартні функції бібліотеки CMSIS-DSP для фільтрації. Але для їх використання необхідно було додатково формувати масив вхідних даних бо функції не

вміють працювати із кільцевими буферами, тобто було необхідно копіювати значення із буферів у додатковий масив. Для аналізу швидкодії розробленого алгоритму було синтезовано цифровий фільтр у середовищі Matlab із наступними характеристиками: полоса пропускання 7.5кГц, частота дискретизації 50кГц, гранична частота полоси затримування 9кГц, порядок фільтру 63 (кількість коефіцієнтів 64). Результати дослідження представлені на рис. 3.

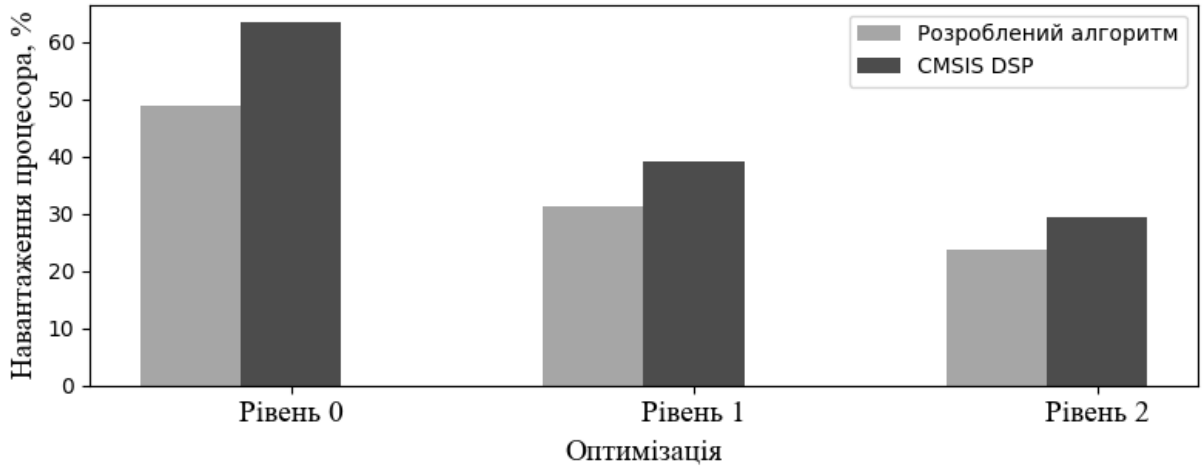


Рисунок 3 – Результати аналізу швидкодії алгоритмів реалізації DSP фільтрів

Аналіз отриманих даних показує, що при відсутності оптимізації запропонований алгоритм дає виграш у 14.5% від загальної швидкодії мікрокотнролера. При використанні першого рівня оптимізації програмного коду виграш зменшується до 5.6%, але все одно є достатньо значним.

Висновки. Запропонований алгоритм цифрової фільтрації сигналу з безпосереднім використанням кільцевих буферів АЦП та ЦАП забезпечує швидкодію більшу ніж у функцій бібліотеки CMSIS DSP, бо ця бібліотека не враховує апаратних можливостей мікроконтролерів серії STM32F4 та вищих. Завдяки запропонованому алгоритму вдалося досягти зростання швидкодії до 14.5%.

Список використаних джерел.

1. Simona-Daiana Sim; Zsófia Lendek; Petru Dobra Implementation and Testing of Digital Filters on STM32 Nucleo-64P 2022 IEEE International Conference on Automation, Quality and Testing, Robotics pp.1-6.

2. Програмування мікроконтролерів STM32 в середовищі STM32CubeIDE в прикладах і задачах: Навч. посіб. / О. В. Зубков, І. В. Свид, О. В. Воргуль, В. В. Семенець. Дніпро : ЛІРА ЛТД, 2022. 144 с.

3. Проектування цифрових фільтрів: навчальний посібник / Г.Є. Філатова. Х. : НТУ «ХПІ», 2017. 120 с.

4. Lars Wanhammar, Tapio Saramäki Digital Filters Using MATLAB 1st ed.- Springer, 2020, 821 p.

РОБОТИЗОВАНА СИСТЕМА ДЛЯ ЕКОНОМІЧНОГО АВТОМАТИЗОВАНОГО НАНЕСЕННЯ ПАЯЛЬНОЇ МАСКИ ТА ЗАХИСНОГО ПОКРИТТЯ НА ПІДКЛАДКАХ З ТЕКСТОЛІТУ

аспірант Костін Д.О.
Харківський національний університет радіоелектроніки, кафедра мікроелектроніки, електронних приладів та пристроїв, м. Харків, Україна
e-mail: denys.kostin@nure.ua

Abstract. This work is dedicated to modern developments in the field of automation of instrument engineering and instrument production technologies. A robotic system for economically automated application of solder mask and protective coating on fiberglass substrates is an innovative solution in the electronics manufacturing sector. It ensures high precision and speed in applying materials, contributing to increased productivity and production quality. This system allows efficient resource utilization, reducing material costs and ensuring time-saving.

Ключові слова: роботизована система, паяльна маска, текстоліт.

Вступ. Паяльна маска – це матеріал, який використовується при паянні електроніки для захисту від непотрібних припоїв. Це зазвичай тонкий шар полімерного матеріалу, який наносять на плату або виріб перед процесом паяння. Маска залишається на місці паяльного з’єднання, захищаючи навколишні елементи від надмірного паяльного матеріалу. На підкладці зі склотекстоліту можуть бути нанесені паяльною маскою зони, які залишаються відкритими для паяльного матеріалу, а інші – закриті. Це дозволяє точно контролювати місця з'єднань і запобігає надмірному розплавленню припою, яке може призвести до коротких замикань або інших проблем. Особливо важливим є цей процес в сферах виготовлення електроніки, де потрібно точно розташовувати і паяти дрібні компоненти.

Основна частина. Нанесення паяльної маски на підкладку – це процес, який включає кілька етапів. Паяльна маска наноситься на підкладку (т. зв. маскація) в областях, де не потрібно паяти. Це може бути зроблено різними способами, такими як друк, фотолітографія або нанесення за допомогою трафарету.

Після нанесення маски підкладку висушують, щоб видалити розчинник або воду, які можуть бути використані в процесі нанесення, та опромінюють, використовуючи трафарети. Цей процес дозволяє створити точні області на підкладці, які залишаються відкритими для паяльного матеріалу.

Автоматизовані друкарські системи можуть використовувати спеціальні друкарські головки для нанесення паяльної маски на підкладку. Цей метод ефективний для великих обсягів виробництва і дозволяє точно контролювати товщину шару маски.

Фотолітографія – це процес, що включає використання світлочутливої паяльної маски та маскувальної плівки. За допомогою світлочутливого шару, який змінює свої властивості під впливом світла, можна створювати точні малюнки на підкладці. Однак використання трафарету для нанесення паяльної маски не завжди дозволяє отримати високу точність та швидкість виробництва. Кожен зі вказаних методів має свої переваги і застосовується в залежності від конкретних вимог виробництва.

Враховуючи ці особливості, розроблено систему з числовим програмним керуванням (ЧПК) для автоматизації процесу нанесення та затвердіння паяльної маски. Вона спроектована таким чином, щоб об’єднати всі необхідні технологічні операції нанесення паяльної маски та її подальшої полімеризації з урахуванням особливостей топології друкованої плати.

Для організації технологічного процесу запропоновано симбіоз принципів 3D друку та лазерного гравірування з додаванням до ЧПК додаткової операції з усунення дефектів друку фотополімерної паяльної маски на платі (рис. 1).

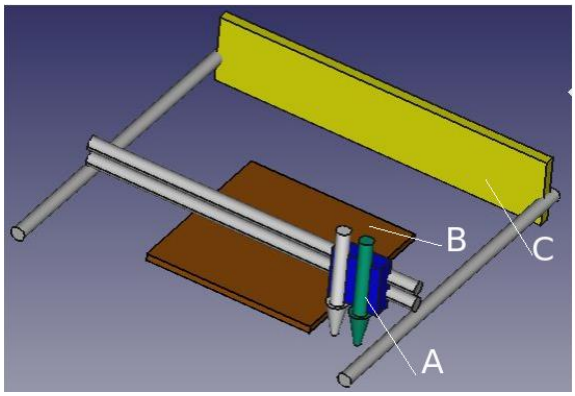


Рисунок 1 – 3D модель розробленої системи ЧПК за кінематикою Core-XY

Механізм друкувальної каретки (A) складається з двох основних компонент: екструдера, через який подається паяльна маска, та джерела ультрафіолетового випромінювання з можливістю фокусування світлової плями. Система має нерухомо зафіксовану підкладку з текстоліту (B). Додаткова рухома платформа (C) призначена для переміщення вздовж надрукованої паяльної маски, з метою вирівнювання нанесеного шару полімеру (рис. 2 – 4).

Таким чином, процес нанесення паяльної маски за допомогою принципу 3D друку та подальшого її розподілення шляхом переміщення додаткової площини надає рівномірність покриттю підкладки. Після цього технологічний процес переходить до опромінення нанесеного фотополімеру шляхом лазерного візирування. Однак слід зазначити, що для коректного створення топології паяльної маски треба використовувати опромінювач з функцією автоматичного фокусування світлової плями.

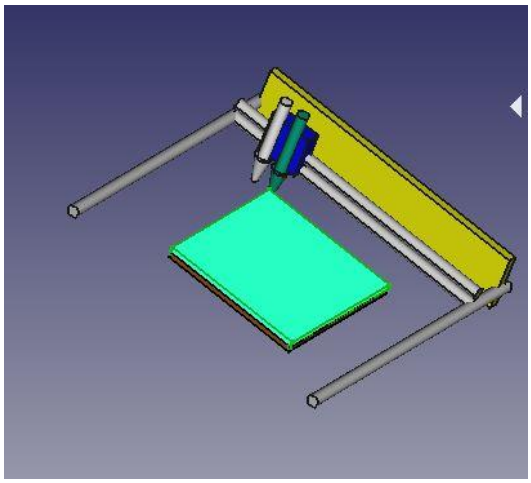


Рисунок 2 – 3D модель надрукованої паяльної маски

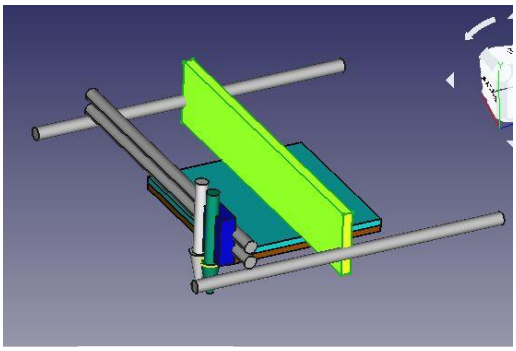


Рисунок 3 – Переміщення механізму з метою рівномірного розподілення надрукованої паяльної маски

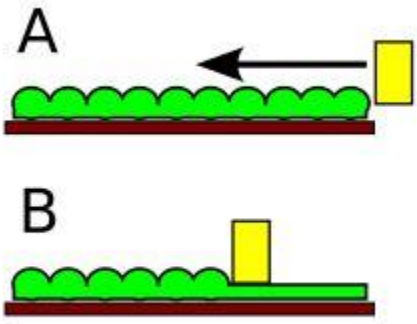


Рисунок 4 – Ілюстрація процесу рівномірного розподілення надрукованої паяльної маски за рахунок оптимально підібраного мінімального зазору між шпателем та підкладкою

Технічно автоматичне фокусування світлової плями можливо реалізувати за принципом CD-ROM пристроїв, де це реалізовано шляхом переміщення котушки в магнітному полі. Фокусуюча лінза в такому випадку закріплена на самій котушці, а фокусування світлової плями

досягається переміщенням лінзи з котушкою вгору та вниз, в залежності від зміни магнітного поля (рис. 5).

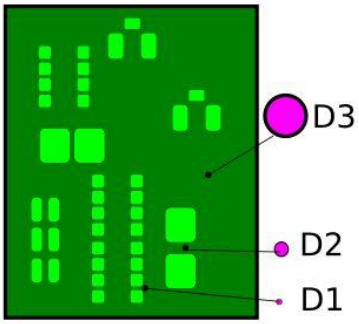


Рисунок 5 – Зміна діаметру світлової плями для відтворення топології паяльної маски задля уникнення необхідності використання спеціальних трафаретів

Висновки. На мікроскопічних масштабах, з якими мають справу мікроелектронні технології (де потрібна висока точність), друкарські методи можуть виявитися більш ефективними порівняно з іншими. Налаштування і керування друкарським обладнанням з розробленою системою з ЧПК кінематикою не вимагатиме кваліфікованого персоналу. Вказані особливості цілком задовольняють потреби сучасного електронного виробництва.

Обладнання, створене за розробленою технологією для автоматизованого друку, може бути значно дешевшим у встановленні та обслуговуванні, що повинно знизити додаткові витрати для виробників. Друкарські головки та інші компоненти обладнання не вимагатимуть регулярного обслуговування та заміни. Розроблена друкарська система може значно розширити спектр матеріалів, що використовуватимуться для нанесення маски.

Список використаних джерел.

1. Montrose, Mark I. Printed circuit board design techniques for EMC compliance: a handbook for designers. 2nd ed. IEEE Press series on electronics technology. IEEE Electromagnetic Compatibility Society, sponsor. Hoboken, NJ: Wiley, 2000. ISBN 0-7803-5376-5.

ЗАСТОСУВАННЯ РОБОТИЗОВАНОЇ ТЕХНІКИ, ОСНАЩЕНОЇ ВОГНЕПАЛЬНОЮ ЗБРОЄЮ, ДЛЯ ЗНИЩЕННЯ ВИБУХОНЕБЕЗПЕЧНИХ ПРЕДМЕТІВ

к.т.н., доцент Толкунов І.О., курсант Куркурін І.П.
Національний університет цивільного захисту України,
кафедра піротехнічної та спеціальної підготовки, м. Харків, Україна
e-mail: nuczu@dsns.gov.ua, tolkunov_ia@ukr.net

Abstract. The study proposes one of the ways to solve the current scientific and technical task of improving the existing methods and technical means intended for the neutralization and destruction of the most dangerous explosive objects for the population - anti-personnel and anti-tank engineering mines with tension, electromagnetic, infrared, acoustic and seismic sensors of the target by the use of robotic equipment equipped with firearms, while simultaneously ensuring the safety of personnel involved in the humanitarian demining of the territory of Ukraine.

Ключові слова. Вибухонебезпечний предмет, розмінування, роботизована техніка.

Вступ. Історія існування людства на Землі завжди була пов’язана із веденням воєн та воєнних конфліктів, які супроводжувалися широким застосуванням протиборчими сторонами різноманітних типів боєприпасів: систем залпового вогню і керованої зброї, авіаційних, артилерійських і мінометних боєприпасів, протитанкових і протипіхотних мін, касетних боєприпасів, засобів ближнього бою, саморобних вибухових пристроїв (СВП) та багатьох інших. Країни, на території яких велися або ведуться бойові дії, обов’язково стикаються з проблемами гуманітарного розмінування. Одною з таких країн на сьогоднішній день є Україна. Територія нашої держави визнана одною із найзабрудненіших вибухонебезпечними предметами (ВНП) у світі. З огляду на вищезазначене, нагальним та актуальним є вирішення науково-технічних завдань щодо розробки нових та удосконалення існуючих методів та технічних засобів, призначених для знешкодження та знищення різноманітних вибухонебезпечних предметів з одночасним забезпеченням безпеки персоналу, який залучається до виконання робіт з гуманітарного розмінування території України.

Як доводить аналіз виконання робіт з гуманітарного розмінування на території України урядовими організаціями та міжнародними операторами, з огляду на щільність забруднення та складність рельєфу, ці роботи в основному здійснюються ручними методами, однак міжнародний досвід підтверджує необхідність створення робототехнічних засобів та систем військового (подвійного) призначення. В Україні та світі проведено ряд досліджень теоретичного та експериментального характеру, в

результаті яких розроблені дослідні зразки таких засобів, в тому числі і для проведення гуманітарного розмінування, та проведена їх апробація [1,2]. Застосування подібної роботизованої техніки обумовлюється прагненням усіх країн світу до збереження життя людей, як в бойових умовах (в контексті якого використання подібних засобів та систем дозволяє досягти позитивних результатів), а також в процесі гуманітарного розмінування територій, на яких знаходяться ВНП.

Основна частина. Найбільшу небезпеку як для цивільного населення, так і для фахівців піротехнічних або інженерно-саперних підрозділів становлять протипіхотні та протитанкові міни у зв'язку із їх підступністю і масовістю застосування, необізнаністю пересічних громадян. Особливо це стосується протипіхотних мін осколкової і фугасної дії та протитанкових мін фугасної і кумулятивної дії із натяжними, сейсмічними, акустичними, інфрачервоними, оптичними та електромагнітними датчиками цілі, наприклад, таких як: протипіхотні – ПОМ-2 «Отьок», ПОМ-3 «Медальйон»; протитанкові – ТМ-83, ПТМ-1, ПТМ-3, ПТМ-4, ПТКМ-1Р та інші [4].

Особливістю цих та подібних ним інженерних боєприпасів є їх висока ефективність, з одного боку, та надзвичайна небезпечність у поводженні – з іншого. Вони не підлягають знешкодженню, а знищеними можуть бути або шляхом доставки до них зарядів для знищення (з використанням маніпуляторів, наземних або повітряних роботизованих засобів), або шляхом дистанційного знищення з використанням стрілецької зброї. Останній метод широко використовується військовими підрозділами в ході ведення бойових дій та виконанні бойових завдань.

Перспективним варіантом виконання подібних завдань представляється використання наземних роботів, оснащених вогнепальною зброєю. Прикладом тому можуть слугувати роботи канадської компанії ICOR Technology, модель CALIBER з різновидами, які можуть бути оснащені подібними системами та мають високі показники щодо швидкості, спритності та маневреності, призначені для буксирування та перетягування вантажів, ведення розвідки на місцевості та в будівлях, мають широкий перелік навісного обладнання [5].

На рис. 1,а) показано модель роботу CALIBER MK4 – це самий потужний з серії роботів CALIBER, максимальна маса вантажу, який може підняти робот – 90 кг (200 фунтів). На рис. 1,б) зображений «найрозумніший» робот із сімейства CALIBER FLEX, який має вантажопідйомність 36 кг. Їхні блоки управління забезпечують автоматичне попередньо встановлене позиціонування для полегшення швидкого розгортання, а 3D-аватар забезпечує зворотний зв'язок та позиціонування фактичного положення робота у реальному часі. Модульна конструкція робота дозволяє зменшити витрати на технічне обслуговування за рахунок легкої та швидкої модернізації та

переоснащення платформи, ремонту та заміни деталей безпосередньо на місці (в районі) виконання бойового завдання.

а) *б)*

Рисунок 1 – Роботи наземні серії CALIBER:
а) – модель MK4; б) – модель FLEX

Технічні характеристики роботів наведені у табл. 1.

Таблиця 1 – Технічні характеристики роботів наземних серії CALIBER

№ з/п	Найменування показника	Характеристики робота	
		модель MK4	модель FLEX
1.	Час безперервної роботи (виконання завдання), год.	2…5 і більше (в залежності від місії)	2…4 і більше (в залежності від місії)
2.	Габаритні розміри, мм (дюйми):		
	- довжина: у розгорнутому стані у складеному стані	 1400 (55) 990 (39)	 1400 (55) 990 (39)
	- ширина	750 (29,5)	610 (24)
	- висота	870 (34,5)	690 (27)
3.	Вага, з елементами живлення, кг	333	107
4.	Кут підйому по сходах, °	40	45
5.	Стійкість до погодних умов за IP65	екологічно герметичний; можливість хімічного біозмивання	

Роботи оснащені: системою управління із гнучким і точним контролем; IP-радіоприймачем; вдосконаленим лазерним далекоміром з вбудованим датчиком відстані LIDAR; 2-швидкісною PTZ-камерою з можливістю управління її просторового положення в автоматичному і ручному режимах.

Висновки. Запропонована в дослідженні роботизована техніка канадського виробництва, або їй подібна, забезпечить в складних умовах сьогодення виконання бойових завдань фахівцями піротехнічних підрозділів ДСНС України (за умови законодавчого вирішення питання щодо можливості використання цими підрозділами зазначеного обладнання) або особовим складом інженерно-саперних чи вибухотехнічніх підрозділів інших силових структур щодо знешкодження та знищення різноманітних вибухонебезпечних предметів, в тому числі і досліджених в роботі протипіхотних та протитанкових інженерних мін, а також врятувати ще не одне життя.

Список використаних джерел.

1. Янушкевич Д.А., Іванов Л.С. Роботизовані засоби спеціального призначення: аналіз міжнародних нормативних документів [Електронний друк]. / Виробництво & Мехатронні Системи-2021. // Матеріали V Міжнародної конференції. – Харків: ХНУРЕ, 21-22.10.2021. – С.176-179.

2. Толкунов І.О., Янушкевич Д.А., Губар С.В., Гайовий О.О. Підвищення ефективності робіт з гуманітарного розмінування шляхом застосування сучасних робототехнічних систем. // Матеріали круглого столу «Об'єднання теорії та практики – запорука підвищення готовності оперативно-рятувальних підрозділів до виконання дій за призначенням». – Х.: НУЦЗ України, 28.10.2022. – 153 с. – С.132-134.

3. Fedorenko Gennadiy, Fesenko Herman, Kharchenko Vyacheslav, Kliushnikov Ihor, Tolkunov Ihor. Robotic-biological systems for detection and identification of explosive ordnance: concept, general structure, and models. / Journal «Radioelectronic and Computer Systems» (журнал «Радіоелектронні і комп'ютерні системи») (ISSN 1814-4225 (print), ISSN 2663-2012 (online)). Series: Information security and safety (DOI: 10.32620/reks.2023.2.12). – Х.: ХНАКУ ім. М.Є. Жуковського («ХАІ»), 2023. – Вип. №2(106). – С.143-159.

4. Tarhan M. Invisible Death: Antipersonnel mines continue to claim thousands of lives. Anadolu agency. 2021. [Режим доступу – URL: https://bit.ly/352MG61].

5. Робототехнічні комплекси для розмінування. Сайт «Пост-1». [Режим доступу – URL: http://www.post-01.com.ua/ua/catalog/oborudovanie-i-spetssredstva-dlya-armii-i-politsii/razminirovanie/icor_robots/].

QSPICE – ПОПОВНЕННЯ В РЯДУ СИМУЛЯТОРІВ

асистент Пятайкіна М.І., асистент Горбенко Є.О.,
старший викладач Карнаушенко В.П.
Харківський національний університет радіоелектроніки, кафедра мікроелектроніки, електронних приладів та пристроїв, м. Харків, Україна
e-mail: mariia.piataikina@nure.ua, yevhen.horbenko@nure.ua, vladimir.karnaushenko@nure.ua

Abstract. Since the beginning of automation of the process of development of new electronic devices and systems, software products that simplified design procedures were used by large manufacturers for their own production. Over time, such applications became an independent commercial product that took its place in the chain of production of semiconductor devices and systems. One of these products was the Spice simulator (Simulation Program with Integrated Circuit Emphasis), designed for simulating the operation of electronic circuits.

Ключові слова: автоматизація, Spice, симулятори, моделювання.

Вступ. З початку автоматизації процесу розробки нових електронних приладів і пристроїв програмні продукти, що спрощували проектні процедури, застосовувались великими виробниками для власного виробництва. З часом такі додатки стали самостійним комерційним продуктом, який зайняв своє місце в ланцюгу виробництва напівпровідникових приладів і пристроїв. Одним з цих продуктів став симулятор Spice (Simulation Program with Integrated Circuit Emphasis), призначений для моделювання роботи електронних схем. Безліч розробників представили свої версії стимуляторів, які існують, як самостійні додатки, так і входять до складу складних, потужних програм наскрізного проектування електроніки.

На сьогодні існують як комерційні продукти програм – симуляторів, так і безкоштовні, такі, як LTSpice.

Основна частина. Нову версію безкоштовного симулятора Qspice в липні цього року представив виробник напівпровідникових приладів і пристроїв компанія Qorvo. Qorvo, будучи одним з провідних постачальників продуктів для зв’язку та джерел живлення, надав нову версію програмного забезпечення для моделювання схем, яке забезпечує розробникам силової електроніки значно вищій рівень продуктивності проектування завдяки покращеній швидкості моделювання, функціональності та надійності.

На додаток до вдосконалення сучасної технології аналогового моделювання, QSPICE дозволяє розробникам моделювати складні цифрові схеми та алгоритми. Нове поєднання сучасного схемного проектування та швидкого змішаного моделювання робить його ідеальним інструментом для вирішення дедалі складніших апаратних і програмних завдань, з якими

стикаються сучасні системні розробники.

SPICE вже давно є основним інструментом для інженерів, який використовується для моделювання аналогових схем. Однак із зростаючою доступністю інструментів моделювання, багато з яких є відкритими або безкоштовними для використання, виникли питання, такі як їх здатність підтримувати новітні широко зонні пристрої. Пристрої з широкою забороненою зоною мають унікальні характеристики, але вони також створюють проблеми з точки зору моделювання схеми. Одним із помітних обмежень є те, що існуючі програми SPICE можуть не мати рівнянь пристроїв, необхідних для правильного моделювання пристроїв із SiC та GaN.

QSPICE має деякі вдосконалення порівняно зі старими інструментами аналогового моделювання. Ці покращення включають:

- повна підтримка розширеного моделювання аналогових і цифрових систем, наприклад тих, що використовуються в програмах штучного інтелекту та машинного навчання;
- оновлений та оптимізований механізм моделювання, який використовує вдосконалені чисельні методи для сучасного обчислювального обладнання, включаючи інтерфейс користувача, що відтворюється графічним процесором, і керування пам’яттю з підтримкою SSD, щоб забезпечити значно вищу швидкість і точність;
- скорочений загальний час моделювання та 100% відсоток завершення на основі порівняльних тестів Qorvo із набором складних тестових схем;
- наявність регулярно обновлюваної бібліотеки моделей QSPICE, що містить карбід кремнію Qorvo та розширені рішення керування живленням, що полегшує розробникам верифікацію та проектування.

Крім того, нова версія аналогового симулятора може спростити розробку керування двигунами для силових агрегатів електромобілів та інших транспортних засобів. Пристрої з широкою забороненою зоною мають унікальні характеристики, але вони також створюють проблеми з точки зору моделювання схеми. Одним із помітних обмежень є те, що існуючі програми SPICE можуть не мати рівнянь пристроїв, необхідних для правильного моделювання пристроїв із SiC та GaN. Як приклад, розробник приводить моделювання схеми трифазного тягового інвертора потужністю 150 кВт з використанням каскодних пристроїв Qorvo.

Основні покращення, застосовані в QSPICE:

1) повна підтримка розширеного моделювання аналогових і цифрових систем, наприклад тих, що використовуються в програмах штучного інтелекту та машинного навчання;

2) оновлений механізм моделювання, який використовує вдосконалені чисельні методи та оптимізований для сучасного обчислювального обладнання, включаючи інтерфейс користувача, що відтворюється

графічним процесором, і керування пам'яттю з підтримкою SSD, щоб забезпечити значно вищу швидкість і точність;

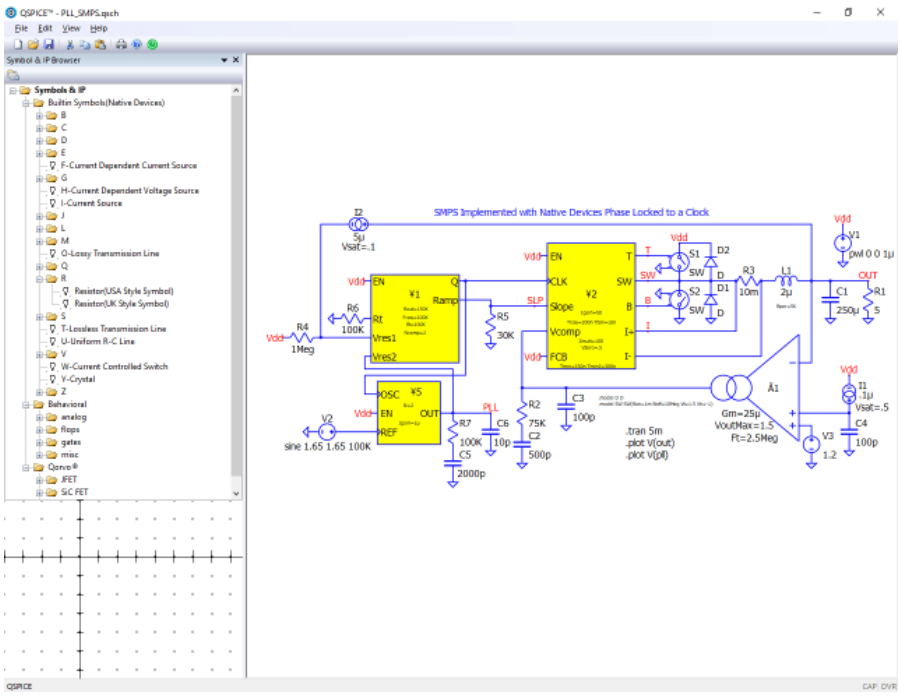


Рисунок 1 – Робоче вікно симулятора QSPICE

3) скорочений загальний час роботи та 100% відсоток завершення на основі порівняльних тестів Qorvo із набором складних тестових схем. Це можна порівняти з частотою відмов до 15% з тими самими тестовими схемами з використанням інших популярних симуляторів SPICE;

4) Наявність регулярно обновлюваної бібліотеки моделей QSPICE, що містить карбід кремнію та розширені рішення керування живленням, що полегшує клієнтам оцінку та проектування за допомогою Qorvo power.

5) усунення розривів кривої вольт-амперної характеристики пристрою, було зроблено вдосконалення для забезпечення плавних і безперервних ВАХ для пристроїв у моделюванні SPICE, що призводить до кращої точності та стабільності;

6) вирівнювання ітерації Ньютона та кроку симуляції: алгоритми розв'язування рівнянь кіл, наприклад ітерації Ньютона-Рафсона були вдосконалені для досягнення швидшої конвергенції та скорочення часу моделювання;

7) виправлення реалізації хеш-таблиці та таблиці рядків**:** структури даних, які використовуються в лексиконі SPICE, такі як хеш-таблиці та таблиці рядків, були оптимізовані для покращення операцій пошуку та вилучення під час моделювання;

8) виправлення помилок у рівняннях каналу польового транзистора: рівняння, що використовуються для моделювання польових транзисторів (FET), були виправлені, щоб підвищити точність моделювання SPICE із залученням пристроїв польового транзистора;

9) впровадження каскодного польового транзистора SiC, як елемента рідної схеми: додано підтримку каскодного польового транзистора з карбіду кремнію, як вбудованого елемент у SPICE, що підвищує точність моделювання схем, які використовують цей компонент;

10) виправлення обчислення стохастичного шуму. Помилки в моделюванні та обчисленні стохастичного шуму в схемах були усунені, щоб підвищити точність моделювання схем, чутливих до шуму;

11) впровадження зарядової моделі Янга-Чаттерджі для МОП-транзисторів: модель заряду Янга-Чаттерджі була інтегрована в SPICE, щоб забезпечити більш точне представлення поведінки заряду в МОН польових транзисторах (MOSFET);

13) підвищена надійність: спрощення представлення спеціалізованих пристроїв SiC JFET і cascode FET як власних елементів схеми може призвести до більш стабільного та надійного моделювання;

14) перехід до кількох процесів для покращеного керування пам’яттю: перехід від багато потокового підходу до кількох процесів покращив керування пам’яттю та використання кешу, що призвело до загального підвищення продуктивності для завдань, пов’язаних з обчисленнями.

Ці комбіновані чисельні методи та оптимізація обчислювального обладнання значно покращили можливості SPICE, зробивши його більш надійним та ефективним інструментом для моделювання електронних схем.

Висновки. QSPICE вирішує унікальні проблеми моделювання, пов’язані з широко зонними (WBG) напівпровідниками, такими як SiC і нітрид галію (GaN). Він вирішує рівняння пристрою для моделювання GaN і SiC як власних елементів схеми, враховуючи такі аспекти, як витоки затвора, підпорогова провідність і лінійні області для точного моделювання.

Крім того, QSPICE представляє можливість розрізняти струми зміщення та струми розсіювання, що дозволяє докладно та точно розраховувати потужність розсіювання у пристроях, що має вирішальне значення для силових приладів і пристроїв.

Можливості змішаного моделювання QSPICE дозволяють інженерам легко інтегрувати та симулювати складні цифрові алгоритми разом із аналоговими схемами. Загалом QSPICE надає комплексні інструменти для обробки цілісності живлення, моделювання шуму та вирішення рівнянь складних напівпровідникових. Також, вагомим фактором для навчальних закладів є безкоштовний доступ до продукту.

Список використаних джерел.

1. https://www.powerelectronicsnews.com/qspice-a-new-simulator-for-electronic-circuits-part-1/
2. https://www.elektormagazine.com/news/exploring-qspice
3. https://www.powerelectronicsnews.com/gen-4-sic-fets-provide-lowest-on-resistance-in-toll-package/

ВИКЛИКИ П'ЯТОЇ ІНДУСТРІАЛЬНОЇ РЕВОЛЮЦІЇ

асистент Пятайкіна М.І., асистент Горбенко Є.О., старший викладач Васильєв Ю.С., старший викладач Карнаушенко В.П.
Харківський національний університет радіоелектроніки, кафедра мікроелектроніки, електронних приладів та пристроїв, м. Харків, Україна
e-mail: mariia.piataikina@nure.ua, yevhen.horbenko@nure.ua, yurii.vasyliev@nure.ua, vladimir.karnaushenko@nure.ua

Abstract. Industry 5.0 is a term used to describe the next phase of the industrial revolution, which focuses on the relationship between humans and machined in industry. It is a concept based on the achievements of Industry 4.0, which emphases the integration of robotic system, the Internet of Things (IoT) ant the use of big data analytics to improve production processes. However, Industry 5.0 goes even further, emphasizing the importance of the involvement and interaction of man and machine in production processes. The evolution of industry is characterized by great revolution. In this sense, Industry 5.0 is part of these revolutions, referring to the fifth industrial revolution.

Ключові слова: Industry 5.0, IoT, промислова революція, кібербезпека

Вступ. Будь яка промислова трансформація є соціотехнічною, тобто вона пов'язує технічні аспекти з нагальними потребами людства. Враховуючі цей фактор, виникають нові виклики для системи вищої освіти в галузі підготовки фахівців, здатних якісно опановувати швидкозмінні процеси в технічній і соціальній сфері.

«Індустрія 5.0» – один із останніх термінів для опису явища, яке визначається як гуманізоване бачення технологічних перетворень у промисловості, збалансування поточних і майбутніх потреб працівників і суспільства зі сталою оптимізацією енергоспоживання, обробки матеріалів і життєвих циклів продукції.

Індустрія 5.0 – це термін, який використовується для опису наступного етапу промислової революції, який зосереджується на стосунках між людьми та машинами в промисловості. Це концепція, заснована на досягненнях Індустрії 4.0, яка акцентувала увагу на інтеграції роботизованих систем, Інтернету речей (IoT) і використанні аналітики великих даних для вдосконалення виробничих процесів. Проте Індустрія 5.0 йде ще далі, підкреслюючи важливість залучення та взаємодії людини і машини у виробничих процесах.

Основна частина. Еволюція промисловості характеризується великими революціями. У цьому сенсі Індустрія 5.0 є частиною цих революцій, посилаючись на п'яту промислову революцію. Історично ми розрізняємо чотири етапи розвитку промисловості: Перша промислова революція характеризувалася переходом від ручної праці до машинного виробництва, що рухалося водою та парою. У цей період з'явилися

текстильні фабрики, парові двигуни та фабрична система. Друга промислова революція ознаменувалася появою масового виробництва та електрифікації. Нові технології, такі як складальна лінія , телеграф і телефон, уможливили масове виробництво товарів і розширення мереж зв'язку. Третя промислова революція, також відома як цифрова революція, ознаменувалася широким впровадженням комп'ютерних технологій і автоматизації. У цей період з'явилися персональні комп'ютери, Інтернет і автоматизація багатьох виробничих процесів. Четверта промислова революція дуже схожа на попередню, але в основному характеризується інтеграцією роботизованих систем, Інтернету речей (IoT) і використанням аналітики великих даних для вдосконалення виробничих процесів. Крім того, Індустрія 4.0 також підкреслює використання автономних роботів, 3D-друку та доповненої реальності для створення більш гнучких і ефективних виробничих систем.

Індустрія майбутнього – це вдосконалення сучасної Індустрії 4.0. Вона зосереджена насамперед на симбіотичних стосунках між людьми та машинами для підвищення можливостей людей та покращення умов праці. Крім того, наголошується на стійкості та використанні передових технологій, таких як штучний інтелект і когнітивні виробничі системи, для створення більш гнучких, адаптивних і ефективних виробничих процесів.

Термін Індустрія 5.0 вперше з'явився в 2017 році в науковій статті під назвою «Індустрія 5.0 – симбіоз людини та технологій та ін. Автори стверджують, що, незважаючи на те, що Індустрія 4.0 значно підвищила ефективність виробництва, вона також викликала занепокоєння щодо впливу автоматизації на робочу силу та втрати людської участі у виробничому процесі. Наступний етап спрямований на вирішення цих проблем, підкреслюючи важливість співпраці людини та машини та створюючи більш природні та інтуїтивно зрозумілі способи взаємодії людей із машинами. Найважливіша відмінність від Індустрії 4.0 полягає в тому, що вона ставить на перше місце благополуччя працівників.

Поняття «Суспільство 5.0» та «Індустрія 5.0» пов'язані. Обидва стосуються фундаментального зрушення нашого суспільства та економіки до нової парадигми. Суспільство 5.0 намагається збалансувати економічний розвиток із вирішенням соціальних та екологічних проблем. Він не обмежується виробничим сектором, але вирішує більші соціальні проблеми на основі інтеграції фізичного та віртуального просторів. Суспільство 5.0 – це суспільство, в якому передові IT-технології, Інтернет речей, роботи, штучний інтелект і доповнена реальність активно використовуються в повсякденному житті, промисловості, охороні здоров'я та інших сферах діяльності для економічної вигоди, вигоди та зручності кожного громадянин.

Отже, важливість Індустрії 5.0 є значною, оскільки пропонує можливість створення більш стійкої та гуманної промисловості.

Приділяючи більше уваги людському фактору у виробничому процесі, вона може допомогти створити більш повноцінні та корисні робочі місця для працівників і покращити умови праці, підвищуючи потенціал для створення більш ефективних і гнучких виробничих процесів, які краще адаптуються до мінливих вимог ринку та збоїв у ланцюжках поставок.

Основні характеристики і найважливіші функції Індустрії 5.0.

Когнітивні виробничі системи, які можуть вчитися на досвіді та адаптуватися до мінливих умов, що призводить до більш компетентних виробничих процесів.

Людино-машинна взаємодія, зосереджена на створенні більш природних та інтуїтивно зрозумілих способів взаємодії людини з машинами. Наприклад, завдяки розпізнаванню голосу та жестів, що покращує безпеку та продуктивність працівників. Людиноцентричний підхід ставить основні людські потреби та інтереси в центр виробничих процесів. Він надає працівникам можливості за допомогою цифрових пристроїв, схвалюючи орієнтований на людину підхід до технологій. Техніка служить людям. Йдеться не лише про те, що ми можемо зробити з новою технологією, а про використання технології для адаптації виробничих процесів до потреб працівників. Це все про те, як підтримати, допомогти та розширити можливості працівників за допомогою інформації про завдання та середовище, що веде до покращення безпеки. У той же час, людина звільняється їх від малоцінних завдань. Працівник отримує більше можливостей, а робоче середовище стає більш інклюзивним. Щоб досягти цього, працівники мають бути тісно залучені до розробки та впровадження нових промислових технологій, зокрема робототехніки та штучного інтелекту.

Індустрія 5.0 приділяє більшу увагу співпраці «людина-машина» з технологіями, призначеними для розширення людських можливостей, а не заміни їх.

Використання передових технології, щоб створити більш гнучкі, адаптивні та стійкі виробничі системи.

Екологічна відповідальність, виробничі процеси спрямовані на мінімізацію відходів і забруднення, а також на ефективне використання природних ресурсів.

Тут ми маємо низку кроків, які необхідно виконати перед адаптацією до Індустрії 5.0:

- забезпечення кібербезпеки та конфіденційності даних. З інтеграцією технологій і процесів виникає потреба в посилених заходах кібербезпеки та захисту конфіденційних даних. Компанія повинна переконатися, що вона має надійні заходи кібербезпеки, щоб захистити себе від потенційних кіберзагроз і забезпечити конфіденційність даних співробітників і клієнтів;

- інвестиції в навчання та освіту співробітників. Індустрія 5.0 вимагає нового набору навичок і знань від працівників, тому важливо інвестувати в

навчання та освіту працівників, щоб підготувати їх до нових технологій і процесів. Це допоможе забезпечити плавний перехід і максимізувати переваги, які можна отримати.

Здійснюючи ці кроки, виробнича компанія може підготуватися до інтеграції в Індустрію 5.0 і забезпечити плавний і успішний перехід до нових технологій і процесів

Висновки. Галузь майбутнього має бути обладнана для швидкої адаптації до мінливих обставин для ланцюжків створення вартості, щоб забезпечити свою роль сталого двигуна процвітання. Стійка галузь може мати справу з уразливістю на багатьох рівнях, включаючи рівні виробництва, промислових систем та мережі постачання.

Особливу роль відіграватимуть цифрові технології. У той час як цифровий взаємозв'язок забезпечить безліч стійких технологій, включаючи збір даних, автоматизований аналіз ризиків і автоматизовані заходи керування, зростання залежності від цифрових технологій наражає галузь на проблеми через збої в роботі. Розробка засобів, необхідних для стійкої промисловості майбутнього, також відіграватиме ключову роль. Бачення індустрії 5.0 стає реальністю завдяки технологічним рішенням і продуктам, які закладають основу сучасної промислової революції.

Список використаних джерел.

1. A. Akundi, D. Euresti, S. Luna, et al. State of Industry 5.0 – Analysis and Identification of Current Research Trends" Applied System Innovation, 2022, v.5(1), PP. 1-14.

2. M.J. Ávila-Gutiérrez, S. Suarez-Fernandez de Miranda, F. Aguayo-González Occupational Safety and Health 5.0 – A Model for Multilevel Strategic Deployment Aligned with the Sustainable Development Goals of Agenda 2030 Sustainability, 2022, v. 14 (11), p. 6741.

3. E.G. Carayannis, K. Christodoulou, P. Christodoulou, et al. Known Unknowns in an Era of Technological and Viral Disruptions – Implications for Theory, Policy, and Practice Journal of the Knowledge Economy, 2022, v. 13(1), PP. 587-610.

4. E. Coronado, T Kiyokawa, GAG Ricardez, et al. Evaluating quality in human-robot interaction: A systematic search and classification of performance and human-centered factors, measures and metrics towards an industry 5.0 Journal of Manufacturing Systems, 2022, v.63, PP. 392-410.

5. K. Dhawan, J.E. Tookey, A Ghaffarian Hoseini, et al. Greening Construction Transport as a Sustainability Enabler for New Zealand: A Research Framework Frontiers in Built Environment, 2022, v.8, PP. 1-19.

6. AS Duggal, PK Malik, A Gehlot, et al. A sequential roadmap to Industry 6.0: Exploring future manufacturing trends IET Communications, 2022, v. 16(5), PP. 521-531.

ОГЛЯД БАЗОВИХ ЕЛЕМЕНТІВ АВТОМАТИЗОВАНОЇ СИСТЕМИ КОНТРОЛЮ НАВКОЛИШНЬОГО СЕРЕДОВИЩА ПОРТАТИВНОЇ ДІЛЯНКИ ЗЕЛЕНОГО ПОБУТУ

доцент, к.т.н., Сотник С.В., студент Кирпота Ф.В.
Харківський національний університет радіоелектроніки,
кафедра комп'ютерно-інтегрованих технологій, автоматизації та робототехніки, м. Харків, Україна
e-mail: svetlana.sotnik@nure.ua, fedir.kyrpota@nure.ua

Abstract. The article discusses use of automation, in particular, in agriculture, where automated environmental control system for growing plants is important. The basic elements of such system are discussed. The structure and principles of green living system operation, which should be used in various conditions, including horticulture, experimental plots, farms, growing flowers and rare plants, are analyzed in detail. The study includes analysis of market analogs and focused development design.

Ключові слова: автоматизація, теплиця, зелений побут, базові, елементи.

Вступ. На сьогодні в різних секторах актуальність автоматизації проявляється через збільшення ефективності, зниження витрат і поліпшення якості виконання завдань, сприяючи загальному зростанню продуктивності та конкурентоспроможності [1-5]. Наприклад, автоматизація завдяки застосуванню роботів забезпечує збільшення продуктивності, зниження ризиків для працівників, підвищення якості продукції, що випускається, а також розширює можливості у сфері інновацій та розвитку технологій. Також для автоматизації активно застосовуються: програмне забезпечення, Інтернет речі (IoT), системи автоматичного управління (SCADA), штучний інтелект (ШІ), розпізнавання образів і комп'ютерний зір, безпілотні транспортні засоби.

Автоматизація стосується всіх сфер, в тому числі вирощування рослин і таке інше, тому, саме про автоматизовану систему контролю навколишнього середовища та її компоненти присвячене це дослідження.

В цій роботі є ключове поняття – зелений побут під яким будемо мати на увазі портативний засіб для вирощування рослин в домашніх і не тільки умовах. Портативні «теплиці» чи піддони та програмне забезпечення для них будемо називати системою зеленого побуту (СЗП). Така система достатньо мобільна та здатна створювати оптимальні умови для росту рослин, забезпечуючи гнучкість в управлінні мікрокліматом і продовжуючи сезон вирощування, а це підкреслює актуальність теми.

Основна частина. СЗП вказує на принципи екологічної та сталих методів ведення сільського господарства, зокрема, вирощування овочів та інших культур у тепличних умовах.

Перед тим, як проектувати СЗП було визначено її базові елементи:

- каркас, який може бути металевою або пластиковою конструкцією, яка забезпечує форму теплиці та підтримує інші компоненти;
- полікарбонатні або поліетиленові стінки – прозорі матеріали, які пропускають сонячне світло, створюючи теплий і захищений мікроклімат усередині теплиці;
- система вентиляції, яка може включати вентиляційні вікна або системи автоматичної вентиляції для регулювання температури і вологості всередині теплиці;
- система поливу, яка включає різні елементи для ефективного та регульованого поливу рослин;
- освітлення – додаткові джерела світла можуть використовуватися для забезпечення оптимальних умов у періоди нестачі сонячного світла.

Що стосується програмного забезпечення, воно може містити в собі:

- системи моніторингу – датчики температури, вологості, освітленості та інші збирають дані, які потім аналізуються для забезпечення оптимальних умов зростання;
- автоматизація поливу – програмне забезпечення може керувати системою поливу, ґрунтуючись на параметрах, таких як вологість ґрунту і вимоги до води рослин;
- управління кліматом – системи, які регулюють температуру, вологість і вентиляцію в теплиці в реальному часі;
- управління освітленням – програмне забезпечення може керувати джерелами і часом освітлення в теплиці.

Перед тим як розробляти корпус було проаналізовано аналоги: COSTWAY, SmartGarten S, GrowIt Farm Smart Indoor Garden, GreenYou [7-10]. В результаті, визначено, що, наприклад, COSTWAY не має оптимальної системи підігріву; SmartGarteS також не має системи підігріву, поливу та вентиляції; GrowIt Farm та GreenYou – мають все необхідне, але ціновий діапазон таких розробок від 172 до 400 Евро, бо виробники використовують різні матеріали, датчики, сенсори, які також впливають на якість проекту та на ціну.

Приклад такої розробки-аналога на рис. 1.

Рисунок 1 – Конструкція найпростішої «системи зеленого побуту»

Тобто, при розробці власної конструкції стало визначено, що необхідно проаналізувати умови застосування СПЗ і тоді буде більш зрозуміло чи потрібні полікарбонатні або поліетиленові стінки і т.п. Тож, всі можливі умови наведені в таблиці 1.

Таблиця 1 – Умови застосування СПЗ

Умова	Опис
Садівництво та городництво	Дає змогу садівникам і городникам подовжувати сезон вирощування, створюючи оптимальні умови для рослин і захищаючи їх від несприятливих погодних умов.
Міські умови	У міських умовах портативні теплиці можуть бути розміщені на балконах, дахах будівель або навіть усередині приміщень, що дає змогу містянам займатися вирощуванням свіжих овочів і зелені.
Експериментальні ділянки	У наукових та освітніх цілях для проведення експериментів з вирощування рослин у різних умовах і під різними параметрами.
Фермерські господарства	Для оптимізації умов вирощування певних культурних рослин, особливо в тих регіонах, де кліматичні умови можуть бути несприятливими.
Вирощування квітів	Для професійних квітникарів або любителів квітів, які бажають забезпечити оптимальні умови для цвітіння та прикраси саду.
Вирощування рідкісних або екзотичних рослин	Дає змогу створювати спеціалізовані умови для вирощування рідкісних і вимогливих до умов зростання рослин.

Після визначення з умовами та основною концепцією будемо проектувати дизайн СПЗ (рис. 2).

Рисунок 2 – Орієнтований дизайн розробки

Висновки. Таким чином, автоматизовані теплиці, використовуючи передові технології, надають оптимальні умови для росту рослин. Порівняння різних моделей теплиць вказує на їхні переваги та недоліки, враховуючи індивідуальні потреби користувачів.

В результаті, з врахуванням умов застосування нашої розробки та сучасних екологічних викликів і потреб споживачів визначено фінальний варіант конструкції СПЗ. Базовими елементами розробки будуть: корпус з пластику; система вентиляції; система поливу та освітлення.

Список використаних джерел.

1. Sotnik S. V. Design features of control panels and consoles in automation systems // 9th International scientific and practical conference “Science and innovation of modern world” (May 18-20, 2023) Cognum Publishing House, London, United Kingdom / S. V. Sotnik, K. S. Redkin. – 2023, pp. 201-205.
2. Sotnik S. Modern Integrated Software Development Environments // International Journal of Academic and Applied Research (IJAAR) / S. Sotnik, V. Lyashenko, T. Schakurova. – 2021. – Vol. 5, Issue 10. – pp. 157-161.
3. Sotnik S. Nano Devices and Microsystem Technologies: Brief Overview // International Journal of Engineering and Information Systems (IJEAIS) / S. Sotnik, V. Lyashenko, T. Shakurova. – 2021. – Vol. 5, Issue 11. – pp. 74-82.
4. Mohammad A. S. Y. Generalized Procedure for Determining the Collision-Free Trajectory for a Robotic Arm // Tikrit Journal of Engineering Sciences, 2023. – 30 (2) / A. S. Y. Mohammad, AT. Abu-Jassar, S. Sotnik, V. Lyashenko. – pp. 142-151.
5. Sotnik S. Overview of Modern Accelerometers // International Journal of Engineering and Information Systems (IJEAIS) / S. Sotnik, V. Lyashenko. – 2022. – Vol. 6, Issue 1. – pp. 57-64.
6. Sotnik S. V. Safe cobots in development of industrial robotics // 8th International scientific and practical conference “European scientific congress” (September 4-6, 2023) Barca Academy Publishing, Madrid, Spain / S. V. Sotnik, Y. S. Usenko, P. V. Shakhov. 2023, pp. 80-84.
7. Pithadiya B. An IoT Based Greenhouse Control System Employing Multiple Sensors, for Controlling Soil Moisture, Ambient Temperature and Humidity // Proceedings of the 2nd International Conference on Electronics, Biomedical Engineering, and Health Informatics: ICEBEHI 2021, 3–4 November, Surabaya, Indonesia. – Singapore: Springer Nature Singapore / B. Pithadiya et al., 2022. – pp. 405-416.
8. Solichatiningsih S. N. Web monitoring smart gardening tanaman cabai berbasis IoT: дис. – Politeknik Harapan Bersama Tegal, 2021. – 159 p.
9. 13 Best Portable Greenhouses to Buy Today (ourendangeredworld.com) [Електроний ресурс]. – Режим доступу до ресурсу: http://www.ourendangeredworld.com/portable-greenhouses.
10. Portable mini greenhouse [Електроний ресурс]. – Режим доступу до ресурсу: Amazon.com: portable mini greenhouse

АНАЛІЗ СИСТЕМ АВТОМАТИЗАЦІЇ ВИЗНАЧЕННЯ УМОВ У ЖИТЛОВИХ ТА РОБОЧИХ ПРИМІЩЕННЯХ З ВИКОРИСТАННЯМ КОМП'ЮТЕРНО-ІНТЕГРОВАНИХ РІШЕНЬ

доцент, к.т.н., Сотник С.В., студент Халімонов Я.І.
Харківський національний університет радіоелектроніки,
кафедра комп'ютерно-інтегрованих технологій, автоматизації та робототехніки, м. Харків, Україна
e-mail: svetlana.sotnik@nure.ua, yan.khalimonov@nure.ua

Abstract. The article analyzes various technologies, such as smart home, smart lighting systems, smart thermostats, and building management systems, which promote innovation, efficiency, and resource savings. The main emphasis is on importance of implementing computer-integrated solutions to automate measurement of indoor conditions in order to improve quality of life and work. Based on analysis, we plan to implement additional measures to address shortcomings aimed at reducing costs and simplifying installation and maintenance processes. As result, it is planned to develop system for determining climatic conditions for both residential and workspaces.

Ключові слова: система, автоматизація, умови, приміщення, модуль.

Вступ. Автоматизація та робототехніка трендові напрямки 21 століття, які відіграють ключову роль у сучасному житті, забезпечуючи не тільки зручність, а й підвищення ефективності, економію часу та ресурсів. Вони проникає в різні сфери, включно з виробництвом, транспортом, охороною здоров'я і навіть повсякденними аспектами, як-от розумний дім [1-3]. Автоматизація сприяє інноваціям, скороченню трудовитрат, поліпшенню якості життя і забезпечує швидкий технологічний прогрес, який стає невід'ємною частиною сучасного суспільства [4-6]. Автоматизація, будучи важливим елементом сучасного життя, не обмежується лише сферою технологій. Вона також впливає на нашу повсякденність, включно з аспектами, такими як контроль клімату та освітлення. Зокрема, важливість автоматизації проявляється в тому, як ми можемо оптимізувати умови всередині будинку і на виробництві за допомогою систем розумного будинку і промислової автоматизації. Ці технології не тільки забезпечують комфорт і ефективність використання ресурсів, а й роблять внесок в екологічну стійкість, даючи змогу ретельніше контролювати енергоспоживання, підтримувати оптимальні умови для роботи і приводити до більш ефективного виробничого процесу.

Комп'ютерно-інтегровані рішення для автоматизації визначення умов у приміщеннях є актуальним і стратегічно важливим напрямком, спрямованим на покращення ефективності, комфорту та сталості життя та роботи людей.

Основна частина. В даній роботі мова буде йти про розробку автоматизованого модуля, але перед розробкою треба провести аналіз аналогів. Якщо узагальнити такі системи, то основні види представлені в табл. 1.

Таблиця 1 – Основні види систем для контролю та визначення умов у житлових та робочих приміщеннях

Назва виду системи	Опис
Системи розумного будинку	Містять у собі широкий спектр пристроїв і сенсорів, які можуть контролювати й керувати умовами в будинку, включно з безпекою, температурою, вологістю, а також системами відеоспостереження та домофонами.
Системи розумного освітлення	Дають змогу автоматично регулювати яскравість і колір освітлення, а також створювати попередньо встановлені сценарії освітлення залежно від часу доби або діяльності.
Розумні термостати	Ці пристрої автоматично регулюють температуру в приміщенні відповідно до заданих параметрів, а також можуть враховувати звички та вподобання користувачів.
Системи вентиляції з рекуперацією тепла (HRV)	Деякі системи вентиляції обладнані сенсорами вологості, які регулюють рівень вологості повітря в приміщенні.
Системи управління будівлею (BMS)	Використовуються в комерційних і промислових будівлях для централізованого контролю та управління різними системами, як-от опалення, вентиляція, кондиціювання повітря (HVAC), освітлення та енергоспоживання.

Проаналізувавши ці види систем можна визначити їх плюси та мінуси (табл. 2).

В ході проведеного аналізу можна сказати , що впровадження розумних технологій, як-от розумні термостати, системи розумного освітлення, розумні будинки, системи управління будівлею та метеостанції, надає ефективні інструменти для підвищення комфорту, безпеки та енергоефективності в житлових і робочих приміщеннях, хоча з їхніми перевагами, також супутні високі витрати та можливі складнощі у встановленні та обслуговуванні.

Таблиця 2 – Аналіз систем для контролю та визначення умов у житлових та робочих приміщеннях

Вид системи	Плюси	Мінуси
Системи розумного будинку	1. Інтеграція функцій. Одночасне керування різними аспектами будинку, підвищуючи зручність. 2. Безпека бо такі системи відеоспостереження, домофони та сигналізації забезпечують додатковий рівень безпеки.	1. Складність встановлення, бо потребує навичок і часу для встановлення та налаштування. 2. Висока вартість оскільки повна автоматизація може бути витратною.
Системи розумного освітлення	1. Енергозбереження так, як автоматичне вимкнення світла за відсутності людей або регулювання яскравості може знизити енергоспоживання. 2. Налаштовані сценарії, які дають можливість створення різних сценаріїв освітлення для різних діяльностей або часу доби.	1. Висока вартість початкового встановлення бо введення системи розумного освітлення може потребувати заміни обладнання, що дорого. 2. Потрібна технічна підтримка оскільки іноді може знадобитися професійне встановлення та налаштування.
Розумні термостати	1. Енергозбереження так, як автоматичне регулювання температури може знизити енергоспоживання і, отже, рахунки за електроенергію. 2. Користувацький комфорт – з огляду на вподобання та звички користувачів, вони створюють більш комфортні умови проживання. 3. Дистанційне керування дає можливість керувати температурою здалеку через смартфон.	1. Висока вартість оскільки розумні термостати можуть бути дорогими порівняно зі звичайними термостатами. 2. Залежність від технології так, як працездатність може бути порушена в разі збоїв у мережі або технічних проблем.
Системи вентиляції з рекуперацією тепла (HRV)	1. Централізоване управління бо може координувати різні системи для оптимальної ефективності. 2. Енергозбереження оскільки розумне керування опаленням, вентиляцією та кондиціонуванням повітря.	1. Висока вартість впровадження так, як потребує значних інвестицій. 2. Потребує спеціальних навичок – необхідність навчання персоналу для ефективного використання.
Системи управління будівлею (BMS)		

У світлі проведеного аналізу, планується активно взятися за усунення виявлених недоліків, впроваджуючи додаткові заходи та технологічні рішення, спрямовані на зниження витрат, підвищення доступності та спрощення процесів встановлення й обслуговування, з метою максимально оптимізувати функціональність та ефективність використання розумних технологій у наших житлових і робочих просторах.

Висновки. Отже, автоматизовані системи моніторингу умов у приміщеннях є перспективним напрямком, який значно підвищить комфорт і безпеку в наших домівках та офісах. Ключове, щоб ці технології стали доступнішими та надійно захищеними. Потенціал автоматизованих систем моніторингу дуже великий. Головне – забезпечити їх доступність, надійність та відповідність етичним нормам. Тоді вони стануть важливою складовою для створення комфортних і безпечних умов праці та побуту.

Список використаних джерел.

1. Sotnik S. V. Design features of control panels and consoles in automation systems // 9th International scientific and practical conference “Science and innovation of modern world” (May 18-20, 2023) Cognum Publishing House, London, United Kingdom / S. V. Sotnik, K. S. Redkin. – 2023, pp. 201-205.

2. Sotnik S. Nano Devices and Microsystem Technologies: Brief Overview // International Journal of Engineering and Information Systems (IJEAIS) / S. Sotnik, V. Lyashenko, T. Shakurova. – 2021. – Vol. 5, Issue 11. – pp. 74-82.

3. Mohammad A. S. Y. Generalized Procedure for Determining the Collision-Free Trajectory for a Robotic Arm // Tikrit Journal of Engineering Sciences, 2023. – 30 (2) / A. S. Y. Mohammad, AT. Abu-Jassar, S. Sotnik, V. Lyashenko. – pp. 142-151.

4. Sotnik S. Overview of Modern Accelerometers // International Journal of Engineering and Information Systems (IJEAIS) / S. Sotnik, V. Lyashenko. – 2022. – Vol. 6, Issue 1. – pp. 57-64.

5. Sotnik S. Modern Integrated Software Development Environments // International Journal of Academic and Applied Research (IJAAR) / S. Sotnik, V. Lyashenko, T. Schakurova. – 2021. – Vol. 5, Issue 10. – pp. 157-161.

6. Sotnik S. V. Safe cobots in development of industrial robotics // 8th International scientific and practical conference “European scientific congress” (September 4-6, 2023) Barca Academy Publishing, Madrid, Spain / S. V. Sotnik, Y. S. Usenko, P. V. Shakhov. 2023, pp. 80-84.

7. Zhang L. Recent Advances in Smart Lighting Control Systems for Smart Buildings: A Review // IEEE Access / L. Zhang, S. Wang. – 2020. – 8. – pp. 22051-22063.

8. Vijayan D. S. Automation systems in smart buildings: a review // Journal of Ambient Intelligence and Humanized Computing / D. S. Vijayan et al. – 2020. – С. 1-13.

АНАЛІЗ КОМП'ЮТЕРНОГО ЗОРУ В СУЧАСНИХ СИМУЛЯТОРАХ РОБОТІВ

студент Поддубняк І.А., доцент, д.т.н., Цимбал О.М.
Харківський національний університет радіоелектроніки,
кафедра комп'ютерно-інтегрованих технологій, автоматизації та робототехніки, м. Харків, Україна
e-mail: illia.poddubniak@nure.ua, oleksandr.tsymbal@nure.ua

Abstract. As one of the fields of emerging technologies of Industry 4.0 and Industry 5.0, robotics received tremendous advancements thanks to integration of latest hardware and software, such as high-fidelity cameras and computer vision systems. Sensory input from cameras can be a rich data source of information for computer vision of robotic systems, and, with the need to minimize risks and expenses involved with testing robots in real world, functional principles of cameras also found their use in robotics simulation environments. This work investigates the current state of utilization of computer vision in modern robotics simulator environments.

Ключові слова: робототехніка, робот, комп'ютерний зір, симуляція, моделювання.

Вступ. Будучи частиною сфери новітніх технологій Industry 4.0 та Industry 5.0, робототехніка досягла значних розвинень завдяки інтеграції такого сучасного апаратного та програмного забезпечення, як якісні камери та системи комп'ютерного зору. Щоб взаємодіяти з реальним світом, роботам потрібні різноманітні дані про їх оточення – зір є ефективним способом збору таких даних, тому камери та обробка даних з них знайшли широке розповсюдження в робототехніці. А через необхідність в мінімізації ризиків і витрат, пов'язаних з тестуванням роботів у реальному світі, комп'ютерний зір для робототехніки також знайшов свою нішу і у середовищах симуляції функціоналу роботів.

У цій роботі досліджується поточний стан галузі використання комп'ютерного зору в сучасних пакетах програмного забезпечення (ПЗ) робототехнічних симуляторів.

Основна частина. Як показують результати аналізу публікацій з галузі, дослідники та розробники мають успіх для використання симуляцій для впровадження дій що відповідають цілям застосування роботів, станам роботів та таких даних про середовища навколо роботів, що отримуються з камери. Це стосується й успіху у розробці процесів, які були перевірені й на апаратних виконань роботів, що були модельовані: виявлення цілі, відстеження цілі, пошук шляху, маніпуляція об'єктом, прогнозування майбутніх станів за необробленими сенсорними показаннями, автономне приземлення, контроль групи роботів у формації лідер-послідовник, оцінка погляду, оцінка руху, точна взаємодія з руками людини тощо [1].

Більшість моделювань, процеси яких названо вище, мали спрощені вигляди рендерінгу об’єктів, але результати моделювання з них мали продуктивні співвідношення з результатами використання роботів у справжньому виконанні, де камери вловлювали зображення саме реальних середовищ. З точки зору застосування симуляцій, успіхи таких типів є можливими завдяки особливостям ходу обробки зображень в програмній частині комп’ютерного зору – як зазначено публікаціями з галузі [2-3], це пов’язано з тим, що, для більшості цілей розробок, видима фотографічна реалістичність відображення симуляцій має другорядне значення – для правильних програмних опрацювань систем комп’ютерного зору, для знятих зображень потрібний саме реалізм даних, який не обов’язково має повне співвідношення з фотореалізмом.

Першорядність реалізму даних варто пам’ятати та враховувати при оцінюванні рівня потреб у апаратному забезпеченні, що буде проводити рендерінг для розробника, бо фотореалістичний рендерінг вимагає більш потужних та коштовних апаратних компонентів.

Для подальшого аналізу необхідно окреслити різновиди камер, що використовуються у робототехніці – вони приведені у таблиці 1.

Таблиця 1 – Типові види камер, що використовуються в робототехніці для комп’ютерного зору

Пристрій	Тип знімання	Приклади застосування
Камера RGB	Зображення з широким діапазоном кольорів за низької вартості	Виявлення об'єктів
Камера дальнісного зображення	Поєднання RGB зображень з даними відстані з далекоміру	Система керування з точною взаємодію з людиною
Стереокамера	Імітація двоокого зору людини кількома лінзами	Навігація роботів зі спрощеним розпізнаванням об'єктів
Ендоскопічні, мікроскопічні камери	Роздільні зображення у важкодоступних місцях	Керування мікроботами та роботами з м’якими компонентами
Монокулярна камера	Цілісні зображення з широким полем зору за низької вартості та маленької ваги	Відстеження цілі, швидкий аналіз місцевості «сферичними зображеннями»
Інфрачервона (IR) камера	Знімання зображень за IR випромінюванням	Перевірка на перегрівання, нічний зір, відстеження очей по IR відблиску

Щодо обмежень застосувань камер, варто зазначити, що, у порівнянні з датчиками зображення, людська зорова система більш чутлива та краще здатна до адаптацій – штучний датчик зору не зможе надійно виявляти

об’єкти, якщо середовище піддається впливу незвичайного освітлення. Але для проблеми освітлення є багато рішень, які можна впроваджувати у апаратне виконання та моделювати у симуляційному ПЗ з оновленнями:

− застосування активного освітлення, джерело якого може бути вбудоване в сам датчик зору;

− застосування IR освітлення та камери;

− застосування фіксованого освітлення навколишнього середовища;

− застосування додаткових оптичних технологій, які використовують світло іншими методами, наприклад LIDAR.

Отже, відповідно особливостей використання комп’ютерного зору для реалістичного розв’язання різних задач робототехніки на рівні симуляцій, можна привести такі пакети ПЗ симуляцій, що відповідають різним функціональним вимогам у галузі [3-9]:

– Project Chrono (через Chrono::Sensor) – підтримка RGB, мап глибин, LIDAR. Краще орієнтований на комплексні фізичні симуляції типу багатокомпонентних транспортів, ґрунту, температур тіл тощо;

– Webots – підтримка RGB, датчику відстані, вимірювача відстані, LIDAR. Краще орієнтований на універсальність, оптимізоване використання комп’ютерних ресурсів та простоту використання;

– Gazebo (та Gazebo Ignition) – підтримка RGB, термальної камери, датчиків відстані, мап глибин, LIDAR. Краще орієнтований на інтеграцію ROS2 (що, серед іншого, необхідно для паралельної роботи між симульованим та апаратним виконанням робота);

– MuJoCo (через OpenAI Gym) – підтримка RGB, IR, датчику відстані, мап глибин, LIDAR. Орієнтований на машинне навчання;

– NVIDIA Isaac Sim – підтримка RGB, IR, LIDAR. Орієнтований на машинне навчання та фотореалізм рендерінгу;

– CoppeliaSim (V-REP) – підтримка RGB, IR, LIDAR. Орієнтований на простоту використання та універсальність;

– PyBullet – підтримка RGB, мап глибин, LIDAR. Орієнтований на машинне навчання та комплексні фізичні симуляції (наприклад, м’які об’єкти).

Варто зазначити, що симуляція стереоскопічних камер, камер с широким кутом огляду, камер-далекомірів та камер зі змінним масштабуванням є можливою й непрямими способами – наприклад, використання кількох камер для стереоскопічної камери, зміна параметрів масштабування та куту огляду для змінної камери та ширококутової камери, використання значень позицій об’єктів симуляції чи використання модулів далекомірів (чи LIDAR) для поєднання з модулем камери для отримання камери-далекоміра тощо.

Так як центр прийняття зображень камер в симуляціях – це абстрактна точка в координатах, то можна моделювати роботу камери будь-яких габаритів та апаратних виконань – обмеження існують тільки на рівні

результатів оптичних принципів роботи, які можна відобразити у симуляції.

Висновки. Під час вибору сучасного симуляційного ПЗ, розробнику варто пам'ятати як особливості використання камер та комп'ютерного зору у симуляціях, так й те, що різні середовища мають свої відмінності як в плані типів камер, симуляції яких можуть бути підтримані, так й в плані загальних можливостей моделювання різних процесів, на яких будуть опиратись розроблені системи комп'ютерного зору. З подальшими розробками пакетів симуляційного ПЗ, відмінності між їх інтеграціями комп'ютерного зору можуть зменшитися, а функціонал – розширитися.

Список використаних джерел.

1. M. T. Shahria, M. S. H. Sunny, M. I. I. Zarif, J. Ghommam, S. I. Ahamed, and M. H. Rahman, "A Comprehensive Review of Vision-Based Robotic Applications: Current State, Components, Approaches, Barriers, and Potential Solutions," Robotics, vol. 11, no. 6, p. 139, Dec. 2022, doi: https://doi.org/10.3390/robotics11060139.

2. A. Elmquist, R. Serban, and D. Negrut, "Camera simulation for robot simulation: how important are various camera model components?," arXiv (Cornell University), Nov. 2022, doi: https://doi.org/10.48550/arxiv.2211.08599.

3. A. Elmquist, R. Serban, and D. Negrut, "A Sensor Simulation Framework for Training and Testing Robots and Autonomous Vehicles," Journal of Autonomous Vehicles and Systems, vol. 1, no. 2, Feb. 2021, doi: https://doi.org/10.1115/1.4050080.

4. M.-A. Blais and M. A. Akhloufi, "Reinforcement learning for swarm robotics: An overview of applications, algorithms and simulators," Cognitive Robotics, vol. 3, pp. 226–256, Jan. 2023, doi: https://doi.org/10.1016/j.cogr.2023.07.004.

5. Z. Chen, J. Yan, B. Ma, K. Shi, Q. Yu, and W. Yuan, "A Survey on Open-Source Simulation Platforms for Multi-Copter UAV Swarms," Robotics, vol. 12, no. 2, pp. 53–53, Apr. 2023, doi: https://doi.org/10.3390/robotics12020053.

6. V. Křivánek, V. Starý, and Y. Bergeon, "Optical Sensor Placement Optimization for Unmanned Ground Vehicles by the Simulation," in IEEE Xplore, IEEE, Jul. 2023. doi: https://doi.org/10.1109/icmt58149.2023.10171309.

7. T.-W. Kang, J.-B. Yi, D. Song, and S. Yi, "High-Speed Autonomous Robotic Assembly Using In-Hand Manipulation and Re-Grasping," Applied sciences, vol. 11, no. 1, pp. 37–37, Dec. 2020, doi: https://doi.org/10.3390/app11010037.

8. A. Ma'arif, A. A. Nuryono, and Iswanto, "Vision-Based Line Following Robot in Webots," in IEEE Xplore, IEEE, Nov. 2020, pp. 24–28. doi: https://doi.org/10.1109/FORTEI-ICEE50915.2020.9249943.

9. A. S. Priambodo, F. Arifin, A. Nasuha, Muslikhin, and A. Winursito, "A Vision and GPS Based System for Autonomous Precision Vertical Landing of UAV Quadcopter," Journal of Physics: Conference Series, vol. 2406, no. 1, p. 012004, Dec. 2022, doi: https://doi.org/10.1088/1742-6596/2406/1/012004.

СУЧАСНІ ТЕНДЕНЦІЇ МІКРОПРОЦЕСОРНОЇ ТЕХНІКИ

студентка Натарова В.С., доцент, к.т.н., Чала О.О.
Харківський національний університет радіоелектроніки,
кафедра комп'ютерно-інтегрованих технологій, автоматизації та робототехніки, м. Харків, Україна
e-mail: viktoriia.natarova@nure.ua, olena.chala@nure.ua

Abstract. The article discusses in detail the main trends in the development of microprocessors and microcomputers. The article analyzes the convergence of structures, the placement of circuits and devices on crystals, and technological advances in the density of element placement. As well as expanding the functionality of devices for managing peripherals. Aspects of increasing the clock speed, expanding memory, and increasing the number of parallel actuators are discussed. The role of single-chip systems (SoCs) and the latest technologies are also highlighted. In particular, the design of memory with cut-out cells. The importance of these trends for creating powerful and compact electronic devices such as routers, computers, phones, and video game consoles is highlighted. The study also points to significant prospects for using new technologies to create reliable and efficient microprocessors, contributing to the development of high-speed and energy-efficient electronic systems.

Ключові слова: мікропроцесори, мікроЕОМ, структури МП, технологічні покращення, щільність розміщення, периферійні пристрої.

Вступ. Розвиток технології мікропроцесорів (МП) та мікроЕОМ (мікроелектронних обчислювальних машин) – це постійний об'єкт вивчення та вдосконалення у світі сучасної електроніки. Основні тенденції в цьому контексті свідчать про зближення структур МП і мікроЕОМ, що зумовлене розміщенням на кристалах різноманітних схем та пристроїв. Це відбувається завдяки удосконаленню технології виготовлення МП, що дозволяє досягти вражаючої щільності розміщення елементів на кристалі та розширює можливості управління периферійними пристроями.

Розвиток не обмежується лише МП, оскільки мікроЕОМ також відчуває вплив визначальних тенденцій. Особливо слід відзначити оснащення мікроЕОМ розширеним спектром периферійних пристроїв та можливість їх підключення до каналів зв'язку. Відбувається зближення функціональних можливостей мікро- та міні-ЕОМ, що відкриває нові перспективи для розвитку цих обчислювальних систем.

Основна частина. Сучасні тенденції розвитку мікропроцесорної техніки визначаються швидким темпом змін у цьому секторі. По-перше, спостерігається тенденція до збільшення кількості ядер у мікропроцесорах. Це відбувається через потребу у високопродуктивних системах, таких як сервери та робочі станції, які використовують паралельні обчислення для розв'язання складних задач.

По-друге, зростає увага до оптимізації споживаної енергії

мікропроцесорами. У зв'язку з ростом популярності портативних пристроїв та інтернету речей, важливо забезпечити ефективне використання енергії для продовження тривалості роботи батарей та зменшення впливу на довкілля [1].

По-третє, збільшується використання технологій штучного інтелекту в мікропроцесорній техніці. Інтеграція нейромереж та спеціалізованих прискорювачів дозволяє покращити продуктивність у завданнях, пов'язаних із штучним інтелектом, таких як розпізнавання образів, обробка природної мови та автономні системи. Ці тенденції свідчать про постійний розвиток та адаптацію мікропроцесорної техніки до вимог сучасного інформаційного суспільства.

Крім того, збільшується роль вбудованих систем і відкритих стандартів у розвитку мікропроцесорної техніки. Розширення використання вбудованих систем спрямоване на створення інтегрованих рішень для різноманітних застосувань, включаючи автомобільну промисловість, медицину, промисловість та сферу енергетики. Відкриті стандарти дозволяють розробникам спільно працювати та використовувати загальноприйняті протоколи, що сприяє сумісності та обміну інформацією між різними пристроями та системами.

Однією з ключових тенденцій є також посилення фокусу на безпеці в мікропроцесорній техніці. З огляду на зростання кількості зв'язаних мереж та обробку важливої конфіденційної інформації, виробники стають більш уважними до захисту від кіберзагроз та зломів. Розробка вбудованих механізмів безпеки, шифрування та інших заходів допомагає забезпечити надійність та захищеність мікропроцесорних пристроїв в умовах сучасного цифрового середовища [2].

Основні тенденції у розвитку виробництва мікропроцесорів можна узагальнити наступним чином: наближення структур мікропроцесорів і мікроЕОМ проявляється у розміщенні на кристалах не лише мікропроцесорів, але й схем запам'ятовуючих пристроїв, таймерів, інтерфейсів пам'яті та введення-виведення. Це досягається завдяки удосконаленню технології виготовлення мікропроцесорів, що дозволяє розміщувати до 100000 елементів на кристалі, а також розширенню функціональних можливостей мікропроцесорів для управління периферійними пристроями.

Основні напрямки розвитку мікроЕОМ включають збільшення набору периферійних пристроїв, можливість підключення їх до каналів зв'язку та зближення мікро- та міні-ЕОМ за функціональними можливостями.

Розвиток мікропроцесорів визначається наступними основними напрямками:

– збільшення тактової частоти за допомогою удосконаленого технологічного процесу, збільшення числа шарів металізації та оптимізації схемотехніки;

– розширення обсягу та пропускної здатності підсистеми пам'яті, що реалізується різними методами, такими як використання зовнішніх кеш-пам'ятей та окремих кристалів кеш-пам'яті: час двотактного доступу до зовнішніх даних і кешу команд від 256 Кб до 2 Мб при часу доступу HP PA-8000 за 2 такта; окремий кристал кеш-пам'яті другого рівня, розташований в тому ж корпусі, що і Pentium Pro;

– збільшення кількості паралельно працюючих виконавчих пристроїв для поліпшення характеристик і функціональності мікропроцесорів;

– використання систем на одному кристалі (System On Chip) та нових технологій, таких як конструкція пам'яті з врізаними осередками, що дозволяють створювати потужніші та компактніші мікропроцесори.

Зокрема, технологічний прорив в області System On Chip відзначається реалізацією об'єднання логічної частини мікропроцесора та оперативної пам'яті на одному кристалі, що відкриває перспективи для створення більш потужних та компактних електронних пристроїв[3].

Висновок. У світі мікропроцесорів та мікроЕОМ наразі спостерігається вражаючий розвиток, заснований на технологічних інноваціях та сталому прагненні до удосконалення функціональних можливостей. Перехід від простих мікропроцесорів до складних систем на одному кристалі, таких як SOC (System On Chip), свідчить про стрімкий розвиток галузі. Підвищення тактової частоти, розширення обсягу пам'яті та збільшення кількості виконавчих пристроїв стають стандартними вимогами до нових продуктів.

Реалізація технології SOC корпорацією IBM відкриває нові перспективи для створення компактних, потужних і високоефективних електронних пристроїв. Такий напрям розвитку дозволяє виготовляти продукти, які поєднують у собі високу продуктивність і економічність. Загалом, тенденції розвитку світу мікропроцесорів вказують на постійне стремління до інновацій та вдосконалення, що визначає майбутнє цієї важливої галузі інформаційних технологій.

Список використаних джерел.

1. Ельперін, І. В. Сучасні тенденції впровадження мікропроцесорних систем управління в харчовій промисловості / І. В. Ельперін // Матеріали засідання технічної ради. – К.: НАЦУ «УКРЦУКОР». – 2003. – С. 13-16.

2. V. Bortnikova, V. Yevsieiev, S. Maksymova, I. Nevliudov, O. Chala and K. Kolesnyk, "Mathematical Model of Equivalent Stress Value Dependence from Displacement of RF MEMS Membrane," *2019 IEEE XVth International Conference on the Perspective Technologies and Methods in MEMS Design (MEMSTECH)*, Polyana, Ukraine, 2019, pp. 83-86, doi: 10.1109/MEMSTECH.2019.8817394.

3. Невлюдов І. Ш.Трансфер технологій у сучасній науці, освіті та виробництві в умовах четвертої промислової революції «ІНДУСТРІЯ 4.0» / Невлюдов І. Ш., Чала О. О., Олександров Ю. М. // Сучасний рух науки: тези доп. VIII міжнародної науково-практичної інтернетконференції, 3-4 жовтня 2019 р. – Дніпро, 2019. – Т.2 С.: 604-608

РОЗРОБЛЕННЯ АВТОМАТИЗОВАНОЇ СИСТЕМИ УПРАВЛІННЯ ДЛЯ ЗНЕШКОДЖЕННЯ ВИБУХОНЕБЕЗПЕЧНИХ ПРЕДМЕТІВ

доцент, к.т.н. Янушевич Д.А., студент Мірошніченко С.Ю.
Харківський національний університет радіоелектроніки,
кафедра комп'ютерно-інтегрованих технологій, автоматизації та робототехніки, м. Харків, Україна
e-mail: dmytro.ianushkevych@nure.ua, serhii.miroshnichenko1@nure.ua

Abstract. The deployment of robotic complexes in humanitarian settings is planned by the military forces of all countries in order to save human lives both during combat operations and during the removal of unsafe facilities iв in obstructed territories. One of the main tasks of humanitarian development is the identification of the visceral characteristics on the basis of their signs in order to embrace their nature.

Ключові слова: розмінування, вибуховий пристрій, технічні роботи, технічні маніпулятори.

Вступ. Робототехнічні рішення з відповідною модульною структурою та правильно адаптовані до місцевих умов небезпечних неструктурованих зон можуть значно підвищити безпеку персоналу, а також ефективність роботи, продуктивність і гнучкість. У цьому сенсі мобільні системи, оснащені маніпуляторами для виявлення та визначення місцезнаходження протипіхотних мін, вважаються найважливішими для автономного/напівавтономного визначення мін у професійний, надійний, безпечніший та ефективний спосіб.

Технології виявлення та класифікації вибухонебезпечних предметів. Технології виявлення та класифікації вибухонебезпечних предметів є важливими для забезпечення безпеки та попередження можливих інцидентів з вибуховими матеріалами. Ось детальний розгляд цих технологій:

1. Рентгенівська томографія:

Принцип роботи: Використовується рентгенівське випромінювання для проникнення через об'єкт і створення зображення на основі різниці в поглинанні променів різними матеріалами.

Застосування: Виявлення складних вибухових пристроїв, які можуть містити різні компоненти.

2. Магнітна резонансна томографія (МРТ):

Принцип роботи: Використовує магнітне поле та радіочастотні хвилі для створення зображення внутрішньої структури об'єкта.

Застосування: Виявлення металевих частинок або предметів у вибухових пристроях.

3. Детектори за допомогою рентгенівського випромінювання:

Принцип роботи: Використовується рентгенівське випромінювання для створення зображення вмісту багажу або предмета.

Застосування: Контроль на точках доступу, таких як аеропорти, для виявлення прихованих вибухових пристроїв у багажі.

4. Теплові інфрачервоні камери:

Принцип роботи: Реєструють інфрачервоне випромінювання, що виділяється від об'єктів з різною температурою.

Застосування: Виявлення теплової активності, яка може бути пов'язана з хімічними реакціями вибухових матеріалів.

5. Сенсори для хімічного аналізу:

Принцип роботи: Виявлення особливих хімічних речовин, які можуть бути характерними для вибухових матеріалів.

Застосування: Виявлення залишків вибухових речовин або газів, що можуть вказувати на можливу загрозу.

6. Акустичні сенсори:

Принцип роботи: Виявлення акустичних сигналів, таких як звуки механічних частин вибухового пристрою або тикання годинника.

Застосування: Виявлення несподіваних звуків або шумів, що можуть вказувати на можливий вибух.

7. Візуальні системи розпізнавання образів:

Принцип роботи: Використовують алгоритми машинного навчання та обробку зображень для виявлення об'єктів на відео або фотографіях.

Застосування: Виявлення підозрілих об'єктів на великих площах або у великому потоці даних.

8. Системи штучного інтелекту і машинного навчання:

Принцип роботи: Застосовуються для аналізу великих обсягів даних та автоматичної класифікації вибухонебезпечних предметів.

Застосування: Виявлення нових, раніше невідомих вибухових матеріалів або пристроїв за допомогою аналізу патернів та ознак.

Ці технології можуть використовуватися окремо або в поєднанні, залежно від конкретної ситуації та завдань безпеки. Вони грають ключову роль у попередженні та виявленні можливих загроз від вибухових матеріалів і забезпечують безпеку на публічних місцях, в транспорті та важливих інфраструктурних об'єктах. Також виявлення вибухонебезпечних предметів є критично важливим завданням для забезпечення безпеки в громадських місцях та на важливих об'єктах. Для цього використовуються різні методи та технології. Ось деякі з них:

Рентгенівське сканування: використовується рентгенівське випромінювання для створення деталізованих зображень внутрішньої структури предметів. Це дозволяє виявляти незвичайні або підозрілі об'єкти в багажі, сумках та інших контейнерах.

Детектори металу: використовуються для виявлення металевих об'єктів, таких як ножі, пістолети або інші збройні предмети. Це допомагає виявити можливі загрози в областях забороненої зброї.

Сенсори для хімічного аналізу: ці сенсори можуть виявляти хімічні речовини або гази, що можуть бути характерними для вибухових матеріалів. Вони використовуються для виявлення можливих загроз, пов'язаних із хімічними вибуховими речовинами.

Теплові камери: інфрачервоні камери виявляють теплове випромінювання, що виділяється від об'єктів з різною температурою. Це може допомогти виявити підозрілу активність або термічні джерела, пов'язані з вибуховими матеріалами.

Рентгенівська флуоресценція: цей метод використовується для аналізу хімічного складу предметів на основі рентгенівського випромінювання, яке виникає при впливі на об'єкт рентгенівського випромінювання.

Магнітні детектори: виявляють магнітні об'єкти або феромагнетичні матеріали, які можуть бути складовими вибухових пристроїв або їхніми компонентами.

Акустичні сенсори: виявляють акустичні сигнали, такі як шум або вибухи, пов'язані зі справжніми або підозрілими вибуховими пристроями.

Системи візуального виявлення: використовуються відеокамери та системи розпізнавання образів для виявлення підозрілих об'єктів або осіб.

Системи штучного інтелекту і машинного навчання: застосовують алгоритми машинного навчання для аналізу даних та автоматичної класифікації підозрілих об'єктів.

Ці методи і технології часто використовуються в поєднанні для максимальної ефективності виявлення вибухонебезпечних предметів на різних точках доступу та важливих об'єктах з метою забезпечення безпеки громадськості.

Дизайн та прототип. Розробка автоматизованої системи управління для знешкодження вибухонебезпечних предметів є складним та многогранним процесом, який включає в себе низку послідовних етапів, виконаних з великою уважністю до деталей. Кожен із цих етапів є важливим для досягнення успішного результату - надійної та ефективної системи, призначеної для забезпечення безпеки громадських місць та важливих об'єктів.

Висновки. Розробка автоматизованої системи управління для знешкодження вибухонебезпечних предметів є актуальною і важливою задачею в галузі безпеки та робототехніки. Дана система має великий потенціал у підвищенні рівня безпеки на громадських місцях, важливих об'єктах та в зоні бойових дій.

Головними висновками з цієї теми є.

Необхідність і важливість: зростання загрози вибухонебезпечних предметів вимагає розробки та впровадження автоматизованих систем, які допомагатимуть виявляти та знешкоджувати такі загрози.

Методи виявлення і класифікації: важливо досліджувати і використовувати різні методи виявлення та класифікації вибухонебезпечних предметів, щоб система була надійною та точною.

Робототехнічні рішення: використання робототехнічних компонентів, таких як маніпулятори та сенсори, є важливою складовою для успішної реалізації системи.

Інтеграція і тестування: процес інтеграції та тестування всіх компонентів системи є критичним для забезпечення її ефективності та надійності.

Перспективи: розробка автоматизованих систем управління для знешкодження вибухонебезпечних предметів є перспективною галуззю, яка має потенціал сприяти підвищенню рівня безпеки і запобіганню небажаним подіям.

У цілому, розробка такої системи вимагає інтердисциплінарного підходу, співпраці фахівців з різних галузей і великої уваги до деталей. Запровадження автоматизованих систем управління для знешкодження вибухонебезпечних предметів може позитивно вплинути на безпеку суспільства та захищати життя та майно.

Список використаних джерел.

1. Янушкевич Д. А., Кирпота Ф. В. (2021). Роботизовані системи та їх застосування у гуманітарному розмінуванні. Матеріали всеукраїнської науково-практичної конференції здобувачів вищої освіти і молодих учених «Комп’ютерно-інтегровані технології автоматизації технологічних процесів на транспорті та у виробництві», Харків, ХНАДУ, С. 104-109.

2. Nevliudov I., Yanushkevych D., Ivanov L. (2021). Analysis of the state of creation of robotic complexes for humanitarian mining. Technology Audit and Production Reserves, 6/2 (62), 47-52.

3. Толкунов І. О., Попов І. І., Янушкевич Д. А. Застосування сучасних роботизованих систем і комплексів у гуманітарному розмінуванні (2022). *Матеріали міжнародної науково-практичної конференції «Problems of Emergency Situations»*. Харків: НУЦЗУ. С. 112-114.

4. Ata A. A. Alexandria University (2015). Autonomous mobile robot for mine detection, May 2015, pp. 607-608.

5. Ata, A. A. (2010) Dynamic analysis of a non-holonomic wheeled mobile manipulator for mine detection, International Journal of Mechanics and Materials in Design, Vol. 6, No. 3, August 2010, pp. 209-216.

ПОРІВНЯЛЬНИЙ АНАЛІЗ АНТЕН КОХА ТА ГІЛЬБЕРТА ДЛЯ ПРИЙОМУ СИГНАЛІВ НА ЧАСТОТІ 2100 МГЦ

доцент, к.т.н. Іванова О.О., студент Сердюк С.Л.
Харківський національний університет радіоелектроніки,
кафедра комп'ютерної радіоінженерії та систем технічного захисту інформації, м. Харків, Україна
e-mail: serhii.serdiuk@nure.ua

Abstract. A comparative study of Koch and Hilbert antennas at a frequency of 2100 MHz will identify common technological challenges, as well as reveal the advantages and limitations of each antenna type, contributing to a deeper understanding of their potential in modern wireless communications.

Ключові слова: фрактал, крива Коха, крива Гільберта, сигнал, антена.

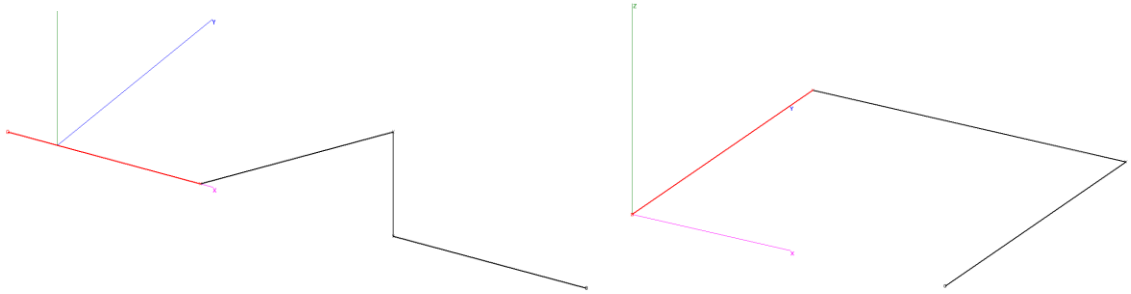
Вступ. У зв'язку із розвитком мобільних технологій, вибір оптимальної антени стає стратегічно важливим завданням. Важливим аспектом нашого дослідження є розуміння впливу антен на якість бездротового зв'язку. У нашому дослідженні ми порівнювали дві антени - Гільберта та Коха для з'ясування їхньої ефективності у бездротових комунікаціях. Обидві антени, Гільберта та Коха, можуть забезпечити стабільний прийом на частоті 2100 МГц, але їхні технічні особливості визначатимуть їхню ефективність у конкретних умовах. Важливо враховувати особливості топології місцевості, вимог системи для точного вибору антени і т.д.

Основна частина. Враховуючи практичні виміри та результати теоретичних розрахунків для антен Коха та Гільберта, отримані дані надають можливість конкретизувати ефективність різних типів антен у сучасних мобільних мережах. Фрактальні антени відрізняються від традиційних антен своєю геометричною складністю та самоподібністю на різних масштабах. Антена Коха базується на кривій Коха, яка є самоподібною і має багато вузьких відгалужень, що дозволяє отримувати кумулятивні зв'язки із сигналом. Антена Гільберта використовує подібний підхід, використовуючи фрактальні криві Гільберта.

Однією з переваг фрактальних антен є їхня компактність і можливість працювати на багатьох частотах, що особливо важливо для мультисмугових систем, таких як 3G та 4G. Також вони можуть мати високу ефективність та низьку область затухання.

Антени Гільберта та Коха викликають інтерес у сфері бездротових комунікацій. Розглянемо їхні ключові параметри.

Коефіцієнт підсилення (Ga) є важливим показником ефективності антени. У Гільберта цей параметр досягає 8.23 дБ, вказуючи на високу здатність антени концентрувати сигнал. У порівнянні, Коха має трошки менший коефіцієнт - 7.58 дБ, але все ще на високому рівні продуктивності.



а) б)

Рисунок 1 - Геометрія першої ітерації кривої Коха (а), кривої Гільберта (б)

Таблиця 1 – Зведена таблиця результатів моделювання

		Крива Гільберта		Крива Коха	
Номер ітерації	0	1	2	1	2
R, Ом	225.8	87.08	236.5	68.11	257
jX, Ом	-462.5	-303.9	159.9	-183.9	-367.4
КСХ	23.6	23.5	6.96	11.9	15.8
Ga	10.03	8.23	7.81	7.58	6.83
F/B	-0.06	-0.4	-0.21	-2.62	0.16
Elev	86.3	78	77.9	78	86.3
Поляризація	горизонтальна				

Відношення підсилення до задньої напрямленості (F/B) визначає, наскільки добре антена фокусує сигнал в передньому напрямку порівняно з заднім. У Гільберта це відношення складає -0.4 дБ, вказуючи на високу точність направленого прийому. Для Коха це значення -2.62 дБ, що може бути важливим у задачах з меншою концентрацією сигналу.

Обидві антени мають однаковий кут елевації - 78 градусів, вказуючи на схожі характеристики щодо вертикального прийому. Це важливо для ситуацій, де потрібне широке охоплення. Антена Гільберта має опір 87.08 Ом та реактивний опір -303.9 Ом. З іншого боку, опір антени Коха становить 68.11 Ом, а реактивний опір -183.9 Ом. Опір визначає ефективність взаємодії антени з системою передачі та прийому сигналів, а реактивний опір вказує на фазове зміщення між струмом і напругою.

Висновки. Ці параметри важливі для розуміння того, як добре антени можуть приймати сигнали на частоті 2100 МГц. Слід зазначити, що для зниження опору і КСХ необхідно використовувати узгоджуючи пристрої. Аналіз даних пристроїв проводився за допомогою програми MMANA-GAL. Діаграми спрямованості двох антен дуже близькі за формою у горизонтальній площині. У вертикальній площині мають велику кількість максимумів і мінімумів. Коефіцієнти підсилення у антен близькі за значеннями.

Список використаних джерел.

1. Fractal Antenna Applications Mircea V. Rusu and Roman Baican ,University of Bucharest, Physics Faculty, Bucharest „Transilvania” University, Brasov Romania. 2016.

2. Fractal Geometry in Electromagnetics Applications - from Antenna to Metamaterials Wojciech J. Krzysztofik.

АПАРАТНИЙ МОДУЛЬ РОБОТОТЕХНІЧНОГО КОМПЛЕКСУ ДЛЯ ПОШУКУ ВИБУХОНЕБЕЗПЕЧНИХ ПРЕДМЕТІВ

студент Вирвихвост О.В., доцент, к.т.н. Янушкевич Д.А.
Харківський національний університет радіоелектроніки,
кафедра комп'ютерно-інтегрованих технологій, автоматизації та робототехніки, м. Харків, Україна
e-mail: oleh.vyrvykhvost@nure.ua

Abstract. The relevance of the topic of creating a hardware module for searching for explosive objects of the robotic complex of humanitarian demining is presented. The definition of humanitarian demining is given. The composition of the equipment, its advantages and disadvantages are analyzed.

Ключові слова: гуманітарне розмінування, РКВП, роботизована система.

Вступ. У період найбільших війн, таких як Перша та Друга світова, Україна опинялася в епіцентрі подій, і проблеми, пов'язані з мінуванням та розмінуванням у мирний час, стосувалися її території та населення. Навіть після закінчення Другої світової війни сапери ДСНС щоденно виявляють вибухонебезпечні предмети, а внаслідок випадкових знахідок гинуть люди.

Сучасні воєнні конфлікти часто супроводжуються широким використанням протипіхотних мін та вибухонебезпечних предметів (ВНП). Однією з проблем, які виникають у всіх регіонах, де велись бойові дії або існують воєнні конфлікти, є проблема гуманітарного розмінування.

Гуманітарне розмінування – це заходи, які проводяться з метою ліквідації небезпек, пов'язаних із ВНП, включаючи нетехнічне та технічне обстеження територій, забруднених ВНП, їх картографування, маркування, пошук, ідентифікація та знешкодження тощо [1]

Гуманітарне розмінування має на меті зменшення негативного впливу вибухових речовин на життєдіяльність людей. Основна ціль розмінування полягає в тому, щоб знизити рівень мінної небезпеки до такого рівня, при якому люди можуть безпечно жити, а економічний, соціальний і фізіологічний розвиток може відбуватися безперешкодно, не обмежуючись впливом обмежень, спричинених наземними мінами.

Для досягнення цієї мети важливим є використання робототехнічних комплексів та систем військового, спеціального та подвійного призначення (РКВП). Це визначається зусиллями всіх країн світу за збереженням людських життів, і використання РКВП дозволяє досягти позитивних результатів.

Розв'язання вищезазначених проблем вимагає комплексного підходу, який включає в себе організаційно-технічні заходи, розділені на дві основні частини:

– використання мережно-центричної концепції ведення бойових дій;

– створення РКВП для здійснення гуманітарного розмінування.

Аналіз сучасного стану створення роботизованих систем. Виділимо низку основних параметрів, за якими будемо здійснювати аналіз сучасного стану створення роботизованих систем військового призначення. Незважаючи на зміну підходів із часом, можна виокремити деякі загальні умовні характеристики, за якими ми зможемо дати оцінку сучасному етапу розвитку робототехніки в світі та підбити деякі підсумки діяльності в цій галузі. До таких характеристик належать: автономність (рішення приймається роботом автономно або оператором дистанційно); адаптивність – наявність експертної системи, реагування на ситуаційні зміни; обробка та розпізнавання мовних і зорових образів; створення мовних інтерфейсів; мобільність; навігація; вогнева міць.

Сьогодні робота над роботизованими системами проводиться цілою низкою воєнних та наукових установ. Особливі успіхи слід відзначити в сфері створення провідними країнами світу, насамперед США, безпілотних літальних апаратів (БЛА), здатних виконувати завдання з інформаційного забезпечення, а також здійснювати пуски високоточних ракет по наземних цілях.

Роботи по створенню роботтотехнічних комплексів у сфері гуманітарного розмінування ведуться в Україні і за кордоном [1]. В Україні та світі виконано значний обсяг досліджень теоретичного та експериментального характеру, які стосуються розробки мобільних роботів. Наявні окремі дослідження статичних характеристик, розроблені дослідні зразки робототехнічних комплексів у сфері гуманітарного розмінування та проведена їх апробація [2].

Сухопутні війська поповнюють свій арсенал низкою моделей високоінтелектуальних систем. Вони здатні переміщуватись у просторі за допомогою дистанційного керування людини та виконувати деякі функції, небезпечні або важкі для солдатів: пошук вибухових речовин та їхня нейтралізація, розвідка тощо. Деякі моделі вже активно використовуються в умовах бойових дій в Іраку та Афганістані. Так, широке використання знайшла модель Packbot (рис. 1) яка широко застосовується для розроблена для пошуку та знешкодження ВНП.

В Україні, проектування й виробництво роботизованих систем, зокрема, БЛА, є одним із найбільш актуальних напрямів розвитку сучасної військової справи. Враховуючи можливості наукової школи, яка досі залишається на належному рівні, вирішення цього завдання виглядає цілком можливим. Так, за твердженням деяких фахівців, достатньо 2-3 роки та 30-50 млн дол., щоб створити вітчизняну операційну систему (ОС). Саме стільки часу і коштів достатньо для розробки власної системи управління базами даних (СУБД). Одним з перспективних й необхідних кроків в напрямі розробки високотехнологічних систем є певне розширення сфери їх використання. Існують певні «критичні» сектори,

система управління якими повинна мати підвищений ступінь безпеки, від надійності функціонування якої залежить безпека країни – електроенергетичні системи постачання, атомні станції, фінансова сфера, хімічне виробництво, міністерство надзвичайних ситуацій. Привертання уваги провідних установ суміжних сфер із відповідним залученням коштів здатне зрушити проблему з місця. З цією метою, а також для зацікавленості комерційного сектору можливе також виробництво на цій базі спрощених зразків, що виконуватимуть спеціальні цивільні завдання.

Рисунок 1 – Робототехнічний комплекс Packbot

Аналіз та побудова апаратного модуля пошуку вибухонебезпечних предметів робототехнічного комплексу гуманітарного розмінування. Метою даної роботи є створення робототехнічних комплексів військового призначення. Прикладом може бути комплекс для пошуку вибухонебезпечних предметів.

Створення РКВП потребує опрацювання ядра критичних технологій, які необхідні для створення всієї номенклатури перспективних РКВП. При цьому типовий зразок РКВП може бути представлений у вигляді сукупності функціонально пов’язаних елементів. Зокрема [1, 2]:

1. Базовий носій – це може бути мобільна платформа, шасі чи корпус будь-якої конфігурації, призначені до застосування у різних середовищах.

2. Спеціалізоване навісне (вбудовуване) обладнання у вигляді набору знімних модулів корисного (цільового) навантаження.

3. Засоби забезпечення та обслуговування, що використовуються при підготовці до застосування та технічної експлуатації робота.

Склад спеціалізованого обладнання встановлюється, виходячи з функціонального призначення РКВП і може включати: засоби розвідки та озброєння, навігаційні пристрої, технологічне обладнання, засоби зв'язку та телекомунікацій, спеціалізовані обчислювачі із програмно-алгоритмічним забезпеченням, засоби радіоелектронної боротьби тощо.

Така побудова РКВП дозволяє виділити технології для розробки перелічених елементів. Технології можна декомпозувати на: основні, тобто розроблювані безпосередньо для РКВП; допоміжні – розроблювані для широкої номенклатури зразків озброєння та перспективи застосування під час створення РКВП [1, 2].

До основних можуть бути віднесені технології систем прийняття та обробки інформації, оцінки ситуації та планування дій, систем дистанційного управління, автоматичного розпізнавання образів (цілей), аналізу ситуацій та динамічних сцен, штучного інтелекту та навчання, людино-машинного інтерфейсу, інтелектуальних систем керування [3].

До допоміжних можна віднести технології живлення, системи геоінформаційного та глобального позиціонування тощо.

Технічним результатом справжнього виробу є надійне виявлення мін в ґрунті, в тому числі пластикових, протипіхотних, малогабаритної апаратури доступній для переноски сапером. В своїй роботі пропоную розглянути робототехнічний комплекс для пошуку протипіхотних мін та вибухонебезпечних предметів. Принцип дії оснований на виявленні мін за допомогою опромінення ґрунту джерелом НВЧ-енергії і вимірюванні температури поверхні ґрунту, яка утворюється в наслідок опромінення шару ґрунту на опромінюваній ділянці з подальшим аналізом про тип вибухонебезпечного предмету.

Принциповою відмінністю способу є вимірювання сигналу іншої природи ніж ту, яку ми відправили, а саме вимірювання наслідків опромінення НВЧ хвилею. При цьому реєструють лише приріст температури, який становиться не рівномірним, якщо на шляху хвилі з’явиться якийсь предмет, який відрізняється температурними показниками від ґрунту навколо нього. Фіксуючи контур в якому з'явився сторонній предмет і зрівнюючи цей контур з певними деталями предмета якого ми шукаємо ми можемо визначити міну. Суть виробу реалізується набором відомих технічних засобів, які задовольняють комплекс вимог до поставленої задачі. Оцінка таких вимог приводить до наступних параметрів апаратури: частота розігріваючого ґрунт НВЧ-променя; потужність НВЧ-променя; чутливість виявлення; характеристики габаритів.

Висновки. Сьогодні в Україні має місце технологічна відсталість та відсутність необхідної елементної бази, але збережений науковий потенціал дозволяє в Україні створювати конкурентоспроможну оборонну продукцію. Основою успішних перетворень має стати розширення сфери використання роботизованих систем. У перспективі така політика здатна привернути увагу інших «критичних» секторів держави та приватного сектору, що надасть можливості для залучення коштів, необхідних для створення конкурентоспроможної продукції.

Список використаних джерел.

1. Analysis of the state of creation of robotic complexes for humanitarian mining. / Nevliudov, I., Yanushkevych, D., Ivanov,.L. ; Technology Audit and Production Reserves, 6/2 (62), 47-52, 2021.

2. Робототехнічні комплекси військового призначення - сучасний стан і перспективи розвитку, / Макаренко С. І. , Systems of Control, Communication and Security, № 2, 73-129, 2016.

3. Сучасні тенденції застосування роботизованих систем для гуманітарного розмінування, / Янушкевич Д. А., Іванов Л. С. , Збірник матеріалів III форуму «Автоматизація, електроніка та робототехніка. Стратегії розвитку та інноваційні технології» AERT-2021, 27 – 31, 2021.

МОДЕЛЮВАННЯ РОБОТОТЕХНІЧНОЇ СИСТЕМИ ДЛЯ ДИСТАНЦІЙНОГО ЗНЕШКОДЖЕННЯ ВИБУХОНЕБЕЗПЕЧНИХ ПРЕДМЕТІВ

студент Лузан М.С., к.т.н., с.н.с. Янушкевич Д.А.
Харківський національний університет радіоелектроніки,
кафедра комп'ютерно-інтегрованих технологій, автоматизації та робототехніки, м. Харків, Україна
e-mail: maksym.luzan@nure.ua, dmytro.ianushkevych@nure.ua

Abstract. The modern world needs safe and effective robotic systems for decontamination of explosive objects. The study of technical requirements, development and mathematical modeling of the system are key stages. Optimization of parameters and a systematic approach determine the basis for the development of effective systems.

Ключові слова: безпека, оптимізація, розробка та моделювання, системний підхід, технічні вимоги.

Вступ. Сучасний світ стикається з постійними викликами безпеки в зв'язку із зростанням кількості вибухонебезпечних об'єктів, якими забруднена територія України. Проблема дистанційного знешкодження цих об'єктів є важливою складовою системи безпеки. Відповідь на ці виклики полягають у розробці та оптимізації робототехнічних систем, які можуть ефективно та безпечно знешкоджувати вибухонебезпечні предмети.

Робототехнічні системи вже здавна використовуються для різноманітних завдань, включаючи знешкодження вибухонебезпечних предметів та пристроїв. Проте, наразі існуючі технології та конструкції не завжди відповідають вимогам ефективного та безпечного знешкодження. Продовження досліджень у цьому напрямку стає надзвичайно важливим для вдосконалення існуючих підходів та розробки нових, відповідних вимогам часу.

Основна частина. Технічні вимоги, які визначають ефективність і безпеку робототехнічної системи, розробленої для ефективного знешкодження вибухонебезпечних предметів. Визначення обсягу та функціональних характеристик системи залежить від цього аналізу.

Характеристики вибухонебезпечних предметів вимагають уваги до розмірів, форм та фізичних властивостей об'єктів. Аналіз параметрів вибуху, хімічного складу та чутливості до впливу надасть базовий набір вимог до системи.

Оцінка технічних параметрів робототехнічної системи включає вивчення можливостей та обмежень існуючих технологій. Визначення оптимальних операційних параметрів, таких як діапазон роботи,

маневреність, швидкість та точність, є ключовим для розробки ефективної системи для дистанційного знешкодження вибухонебезпечних предметів.

Для роботи в умовах підвищеного ризику важливі питання безпеки та надійності. Оцінка можливих ризиків для оператора та працівника дозволяє створювати системи безпеки та превентивні заходи.

На першому етапі аналізу технічних вимог визначаються основні параметри робототехнічної системи. Розгляд характеристик вибухонебезпечних предметів дає важливу інформацію для розробки вимог. Оцінка технічних можливостей і безпеки робототехнічної системи стане основою для подальшої оптимізації та проєктування.

Враховуючи технічні вимоги та особливості вибухонебезпечних об'єктів, ми спочатку визначаємо ідею робототехнічної системи. Необхідно вибрати технології, які забезпечать найвищу ефективність і безпеку в різних умовах впливу. Розглядаючи такі речі, як надійність, маневреність і вага. Створення ефективного пристрою залежить від вибору матеріалів, створення механічних та електронних компонентів і розробки систем керування. Після цього, використовуються сучасні програмні інструменти для математичного та фізичного моделювання робототехнічної системи. Це дозволяє детально вивчати роботу системи в різних умовах, передбачати її поведінку та визначати потенційні місця для вдосконалення.

На останньому етапі результати математичного моделювання засовуються для оптимізації розробленої робототехнічної системи.

Висновки. Таким чином розробка робототехнічної системи із застосуванням сучасних програмних інструментів математичного та фізичного моделювання дозволяє детально вивчати роботу системи в різних умовах, передбачати її поведінку та визначати потенційні місця для її удосконалення.

Список використаних джерел.

1. Янушкевич Д. А., Кирпота Ф. В. (2021). Роботизовані системи та їх застосування у гуманітарному розмінуванні. Матеріали всеукраїнської науково-практичної конференції здобувачів вищої освіти і молодих учених «Комп'ютерно-інтегровані технології автоматизації технологічних процесів на транспорті та у виробництві», Харків, ХНАДУ, С. 104-109.

2. Nevliudov I., Yanushkevych D., Ivanov L. (2021). Analysis of the state of creation of robotic complexes for humanitarian mining. Technology Audit and Production Reserves, 6/2 (62), 47-52.

3. Толкунов І. О., Попов І. І., Янушкевич Д. А. Застосування сучасних роботизованих систем і комплексів у гуманітарному розмінуванні (2022). Матеріали міжнародної науково-практичної конференції «Problems of Emergency Situations». Харків: НУЦЗУ. С. 90-110.

КРЕАТИВНІ ПІДХОДИ УПРАВЛІННЯ ЯКІСТЮ У СФЕРІ ГУМАНІТАРНОГО РОЗМІНУВАННЯ ІЗ ЗАСТОСУВАННЯМ РОБОТОТЕХНІЧНИХ СИСТЕМ

к.т.н., Янушкевич Д.А., к.т.н., Іванов Л.С., к.т.н., доцент Толкунов І.О.
Харківський національний університет радіоелектроніки, кафедра КІТАР,
Національний університет цивільного захисту, кафедра ПСП,
e-mail: dmytro.ianushkevych@nure.ua,: tolkunov_ia@ukr.net

Abstract. Currently, about 160,000 m2 of land in the territory of Ukraine needs to be examined for the presence of explosive objects. In Ukraine, within ten years, the goal is to examine 80% of the territories for the presence of explosive objects, which should be safe for the civilian population. This goal can be achieved and should be based on a creative approach. The creative approach involves the use of the latest means, in particular, unmanned aerial vehicles, ground robotic complexes and systems, systems with artificial intelligence, which can determine the presence of danger without human intervention by studying the results of UAV territory survey and managing the quality of demining.

Ключові слова: гуманітарне розмінування, робототехнічні системи, пошук, вибухонебезпечні предмети, управління якістю.

Вступ. Унаслідок російського вторгнення Україна стала однією з найзамінованіших країн у світі. І тому важливо необхідні креативні підходи до розв'язання питань гуманітарного розмінування із застосуванням робототехнічних комплексів та систем зі штучним інтелектом, які можуть без втручання людини визначати наявність вибухонебезпечних предметів (ВНП) та здійснювати їх знешкодження.

На даний час близько 160 000 м^2 території України потрібно обстежити на наявність ВНП. В Україні ставиться за мету на протязі десяти років 80 % територій обстежити на наявність вибухонебезпечних предметів, які повинні бути безпечними для мирного населення. Ця мета може бути досягнута та повинна базуватися на креативному підході. Креативний підхід передбачає застосування новітніх засобів, зокрема безпілотних літальних апаратів, наземних робототехнічних комплексів та систем, систем зі штучним інтелектом, які можуть без втручання людини визначати наявність небезпеки шляхом дослідження результатів обстеження території БПЛА та управлінням якістю розмінування.

Система управління якістю розмінування складається з двох частин:

– це гарантія якості, тобто впевненість у тому, що оператор, який заявив свою спроможність розмінувати, дійсно на це спроможний;

– контроль якості.

Пріоритетними для розмінування є об’єкти електро-, водо-, газо-, теплопостачання, критичної й транспортної інфраструктури, сільськогосподарські землі тощо.

Перший етап гуманітарного розмінування розпочинається з оцифровування супутникових даних на предмет кратерів, окопів, траншей, аномалій та інших неоднорідностей по всій території України.

Другий рівень даних – це візуальна інспекція за допомогою БПЛА, який виявляє ВНП на землі.

Третій рівень даних – це вибухонебезпечні предмети під землею. Їх шукають з допомогою магнітометрів, термокамер, мультиспекторальних камер, хімічних сенсорів і металошукачів.

Незважаючи на значну кількість наукових робіт із даної тематики, на сьогодні склалася тенденція розмежування зазначених питань.

Роботи по створенню робототехнічних комплексів у сфері гуманітарного розмінування ведуться в Україні і за кордоном [1]. В Україні та світі виконано значний обсяг досліджень теоретичного та експериментального характеру, які стосуються розробки мобільних роботів. Наявні окремі дослідження статичних характеристик, розроблені дослідні зразки робототехнічних комплексів у сфері гуманітарного розмінування та проведена їх апробація [2].

Тому проблема розроблення креативного підходу до застосування робототехнічних комплексів у сфері гуманітарного розмінування є актуальним завданням.

Основна частина. Еволюція розвитку робототехнічних засобів показує, наскільки швидким є розвиток даної галузі. Від появи першого робота, який міг виконувати самі прості операції, до масового виробництва робототехнічних комплексів пройшло не більше 70 років. Як показує статистика, зростання в індустрії робототехніки продовжує бути вибуховим. Сьогодні існує величезна різноманітність роботів, які застосовуються у гуманітарного розмінування.

Гуманітарне розмінування – комплекс заходів, які проводяться з метою ліквідації небезпек, пов’язаних із ВНП, включаючи нетехнічне та технічне обстеження територій, складення карт, виявлення, знешкодження та/або знищення ВНП, маркування, підготовку документації після розмінування, надання громадам інформації щодо протимінної діяльності та передачу очищеної території [1].

Гуманітарне розмінування спрямоване на зменшення шкідливого фактору дії ВНП на життєдіяльність людей. Мета розмінування полягає в тому, щоб знизити мінну небезпеку до рівня, при якому люди можуть жити безпечно; при якому економічний, соціальний і фізіологічний розвиток може здійснюватися безперешкодно, не наражаючись впливу обмежень, що викликаються впливом забруднення території України ВНП. Гуманітарне розмінування, на відміну від військового, передбачає

комплексний огляд усієї території, де тривали бойові дії, визначення небезпечних районів, виявлення забруднених вибухонебезпечними предметами ділянок та їх очищення, після чого місцевість стає повністю придатною для використання [2].

Пошук та ідентифікація ВНП для гуманітарного розмінування з метою зменшення ризиків з питань безпеки людей, які його здійснюють, є комплексним завданням та вимагають застосування РТК для його проведення. РТК для проведення гуманітарного розмінування повинні бути оснащені відповідними детекторами (сенсорами, датчиками), засобами прийняття рішень та застосовуватись на етапах розвідки, пошуку, локації, маркування, ідентифікації, знешкодження та знищення ВНП [4].

ВНП можна виявляти за рахунок трьох факторів:

– наявність зосередженої маси вибухової речовини;

– характерна конструкція мін та ВНП (форм, матеріал корпусу, колір тощо);

– порушення однорідності навколишнього фону (кольору рослинності, щільності ґрунту тощо).

Основні етапи процесу гуманітарного розмінування можна розділити на етапи, які наведені у табл. 1.

Таблиця 1 – Етапи процесу гуманітарного розмінування

Номер етапу	Зміст етапу
1-й етап	Нетехнічне обстеження
2-й етап	Технічне обстеження
3-й етап	Розмінування території, забруднених ВНП та очищення районів ведення бойових дій
4-й етап	Утилізація (знищення, знешкодження) ВНП
5-й етап	Контроль якості розмінування та передача територій, забруднених ВНП їх користувачам

Нетехнічне обстеження (НТО) передбачає збір, аналіз та оцінювання інформації стосовно території для подальшої її класифікації за статусом небезпеки, без використання технічних засобів пошуку ВНП.

Технічне обстеження включає збір та аналіз даних про наявність, тип, розподіл та навколишні умови знаходження мін та вибухонебезпечних предметів із застосуванням технічних засобів, щоб точніше визначити місце, де присутні міни та вибухонебезпечні боєприпаси, а де їх немає, для сприяння пріоритизації вивільнення земель та забезпечення прийняття рішень шляхом надання фактів [3].

Розмінування полягає у здійсненні операцій виявлення, видалення або знищення мін та вибухонебезпечних боєприпасів, а для операцій з

розмінування може також бути потрібне забезпечення доступу, діагностування, приведення в безпечний стан, остаточна утилізація та (у разі потреби) захисні роботи.

Очищення районів ведення бойових дій передбачає виявлення та знешкодження в певних районах, на яких велися бойові дії і які можуть включати оборонні позиції та місця, де були випущені або скинуті авіаційні або артилерійські боєприпаси, включаючи касетні боєприпаси.

Утилізація, знешкодження (знищення) мін та вибухонебезпечних предметів включає всі аспекти виявлення та знешкодження боєприпасів, що не розірвалися, шляхом проведення операцій з розмінування. Виконання операції зі знешкодження та знищення ВНП варіюється від відносно простих методик знешкодження та відкритого підриву до дуже складних промислових процесів із залученням відповідних фахівців.

Контроль якості розмінування – елемент процесу управління якістю розмінування, який забезпечує повне дотримання вимог щодо ліквідації небезпек, пов'язаних з вибухонебезпечними предметами, а також контроль за дотриманням вимог щодо якості розмінування.

Висновки. Проведений аналіз дає змогу дійти висновку про існування та складність проблеми гуманітарного розмінування, яка потребує креативності та комплексного підходу до її розв'язання. Креативний підхід передбачає застосування новітніх робототехнічних засобів, зокрема БПЛА, наземних робототехнічних комплексів та систем, систем зі штучним інтелектом, які можуть без втручання людини визначати наявність небезпеки шляхом дослідження результатів обстеження території БПЛА та управлінням якістю розмінування.

Список використаних джерел.

1. Nevliudov, I., Yanushkevych, D., Ivanov,. L. Analysis of the state of creation of robotic complexes for humanitarian demining. / I. Nevliudov, D. Yanushkevych, L. Ivanov // Technology Audit and Production Reserves, 6/2 (62). – 2021. – P. 47-52.

2. Підвищення ефективності робіт з гуманітарного розмінування шляхом застосування сучасних робототехнічних систем / Толкунов І. О., Янушкевич Д. А., Губар С. В., Гайовий О. О. // Об'єднання теорії та практики – запорука підвищення готовності оперативно-рятувальних підрозділів до виконання дій за призначенням. Матеріали круглого столу. – Харків: Національний університет цивільного захисту України, 28 жовтня 2022. – С. 130-132.

3. Кириленко В. А., Нероба В. Р. // Глобальна проблема розмінування: стан та підходи до розв'язання Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського № 2(66). – 2019.– С. 115-119.

ANALYSIS OF DESIGN PROCESS OF AUTOMATED FIRE PROTECTION SYSTEM

Associate professor, Ph. D., Sotnik S.V., student Vasylchenko Y.R.
Kharkiv National University of Radioelectronics, Department of computer-integrated technologies, automation and robotics, Kharkiv, Ukraine
e-mail: svetlana.sotnik@nure.ua, yelyzaveta.vasylchenko@nure.ua

Abstract. This work addresses topical issue of fire safety, identifying its importance in various spheres of life and emphasizing potential threats to people and property. The importance of automating fire safety systems and developing modern fire protection systems (FPS) as key element for minimizing risks and responding effectively to fire situations is discussed. The work provides details of fire protection system design process, including choice of system type, equipment brand, integration with other systems, and development of equipment layouts. Taking into account the various features of facilities, work recommends optimal approaches to selection and development of fire alarm system, helping to ensure complete control and safety at facilities of various nature.

Key words: system, fire alarm, detector, room, plan.

Introduction. Today, fire safety is becoming subject of serious attention and research, as fire incidents can occur in various areas of our lives, threatening not only human health and life but also causing significant material damage. Ensuring effective fire safety system is critical task to protect communities, businesses and other facilities from potential hazards.

In this context, it is important to consider automation capabilities that can significantly increase efficiency and speed of response to fire threats [1-3].

The development of automated fire protection systems (AFS) that combine modern fire detection, tracking, and response technologies is becoming necessity to ensure complete control and safety at facilities.

A security and fire alarm system is set of jointly operating technical means for detecting signs of intruder at protected facilities and/or fire at them, transmitting, collecting, processing and presenting information in given form.

Such systems can ensure rapid detection and localization of fire, as well as effective timely response, minimizing risks to people and property, so topic is relevant.

Main part. The fire alarm design procedure consists of various equipment, is very laborious and requires certain level of knowledge, skills, and attention to location of all devices, so let's take closer look at design process.

The project is plan that is used to make number of calculations necessary for:

- determining optimal number of devices;
- determining their optimal location during use.

The project indicates route for laying cable communications and takes into

account details that may arise during implementation of alarm system.

Before starting to develop system, it is necessary to conduct pre-design studies of facility and take into account

- building area;
- planning features. Types of premises in accordance with need for FPS (Fig. 1);
- number of floors and complexity of metal structures.

The result will be division of entire building into zones, each of which is subject to control and monitoring.

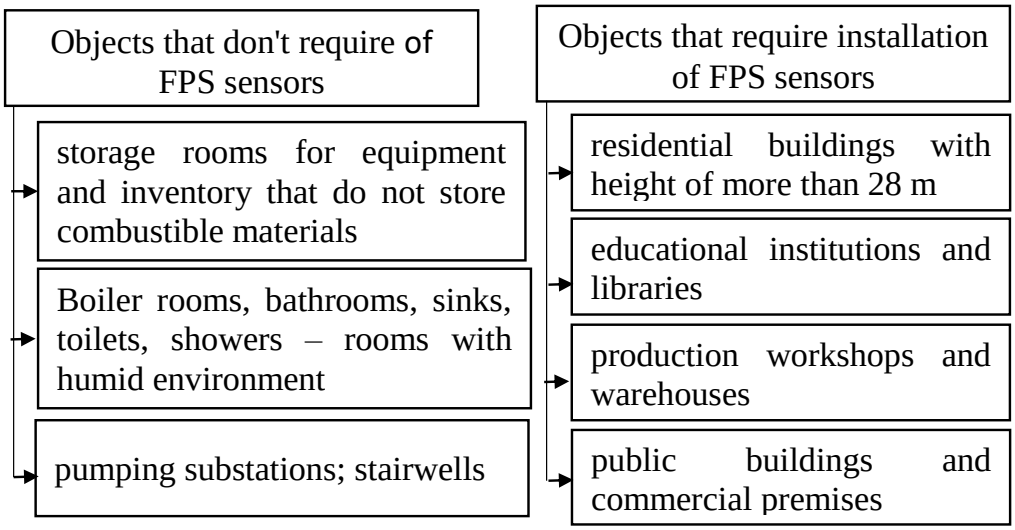


Figure 1 –Types of premises according to need of FPS

Further, stages of designing FPS include:

1. The choice of type (autonomous, centralized or combined) of FPS is strategic step to ensure that security system best meets specific needs and conditions of facility [4].

Here we should pay attention to:

- adaptation to specifics of facility, as different buildings have different characteristics, structures, and sizes. The choice of system type depends on specific features of facility. For example, stand-alone systems may be more suitable for smaller facilities, while centralized or combined systems can provide greater control and management over large areas. The need for centralized management – if centralized management of all security system components is required, including monitoring, data analysis, and decision-making, then centralized system is logical choice;
- scalability requirements, because if building is expected to expand further or change in structure, system choice should provide for ability to scale and adapt to changes in security needs;
- level of security, as security is extremely important issue in these difficult times, and different types of systems provide different levels of security.

Centralized systems, for example, can provide centralized management and monitoring, which is important for high-security facilities such as banks or large enterprises;

- integration with other systems because choice of system type is also related to ability to integrate with other security systems at facility, such as video surveillance, access control, and building management systems. This ensures that different aspects of security are coordinated and interoperable.

2. Selection of fire alarm system type. Currently, 3 types of fire alarm systems are being actively implemented at facilities: addressless, addressable, and address-analog. They differ in principle of operation and specifics of installation in building.

Addressless devices usually use inexpensive alarms with primitive circuit; they recognize fire, loop breakage, and short circuit conditions. Budget devices require large number of cables during installation; latter are usually placed in metal hoses and hidden in walls.

Addressable devices here receive information from all sensors distributed in premises to be serviced, they read characteristics of surrounding space. The control devices analyze dynamics of changes in these parameters, on basis of which it can be concluded that fire has occurred – corresponding signal is sent.

Addressed-analog systems use receiving and control circuit rather than detector directly, as in addressless systems, to process information and make decision about emergency.

3. Selection of brand of equipment for fire protection system.

Selection of fire safety detectors according to the type of premises:

- industrial buildings: heat, smoke, flame;
- premises used for distributors and transformers: heat, smoke, flame;
- buildings for domestic, administrative, public purposes: smoke;
- administrative and economic facilities: heat, smoke;
- hospital wards, catering establishments, hostels and hotels, commercial facilities, office premises: heat, smoke. FPS equipment (Fig. 2).

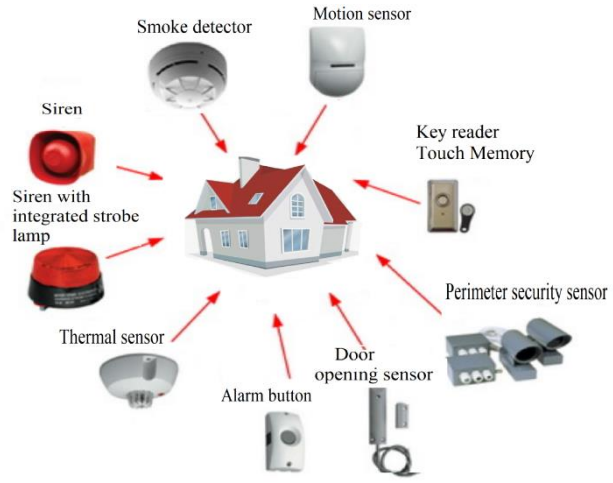


Figure 2 – FPS equipment

4. Design of alarm system. The structure of alarm system is developed, including types of signals, their distribution by zones, and means of notification.

5. Designing access control system. If necessary, system includes access control mechanism that determines access rights to different areas of building.

6. Backup power supply. The system takes into account measures to ensure uninterrupted power supply for main components of security system.

7. Development of equipment layouts. Schemes for location of all system components at facility are created, taking into account optimal coverage and efficiency.

Conclusions. Thus, designing fire and security system requires careful analysis and integrated approach to ensure maximum efficiency and safety of facility.

The selection and design of fire protection system is complex process that requires careful consideration of facility's characteristics and identification of specific security needs. Important aspects include adapting to characteristics of building, selecting type of system based on its size and structure, and considering need for centralized management and integration with other security systems. Pre-design studies that cover ability of system.

Important design stages include selecting type of security system, choosing brand of equipment, designing structure of alarm and access control system, taking into account backup power supply, and developing equipment layout plans.

This comprehensive approach ensures optimal facility security and system efficiency in face of various potential threats.

References.

1. Sotnik S. V. Design features of control panels and consoles in automation systems // 9th International scientific and practical conference “Science and innovation of modern world” (May 18-20, 2023) Cognum Publishing House, London, United Kingdom / S. V. Sotnik, K. S. Redkin. – 2023, pp. 201-205.

2. Sotnik S. Modern Integrated Software Development Environments // International Journal of Academic and Applied Research (IJAAR) / S. Sotnik, V. Lyashenko, T. Schakurova. – 2021. – Vol. 5, Issue 10. – pp. 157-161.

3. Sotnik S. Nano Devices and Microsystem Technologies: Brief Overview // International Journal of Engineering and Information Systems (IJEAIS) / S. Sotnik, V. Lyashenko, T. Shakurova. – 2021. – Vol. 5, Issue 11. – pp. 74-82.

4. Lee W. Development of building fire safety system with automatic security firm monitoring capability // Fire safety journal / W. Lee et al. – 2013. – T. 58. – C. 65-73.

АНАЛІЗ СИСТЕМИ СЕЛЕКЦІЇ РУХОМИХ ЦІЛЕЙ В РЛС

аспірант Головатенко С.В., д.т.н., проф. Обод І.І., к.т.н., доц. Свид І.В.
Харківський національний університет радіоелектроніки, кафедра мікропроцесорних технологій і систем, м. Харків, Україна
e-mail: serhii.holovatenko@nure.ua

Abstract. Modern radar systems provide the formation of a target's radar mark and automatic tracking of its trajectory based on received reflection signals. The information system calculates the course of movement of the tracked object, its speed and other parameters depending on the purpose of the radar. The rapid development of technologies requires the improvement of system performance.

Ключові слова: РЛС, аналіз, система, селекція, траса, супровід.

Вступ. Сучасні радіолокаційні системи (РЛС) забезпечують формування радіолокаційної відмітки цілі та автоматичне супроводження її траєкторії на основі прийнятих сигналів відбиття. Інформаційна система розраховує курс руху супроводжуваного об’єкту, його швидкість та інші параметри залежно від призначення радіолокатора.

Основна частина. Супроводження траєкторій особливо ускладнюється у випадках маневрування цілі, впливу пасивних та активних радіолокаційних завад, при пропусках цілі та хибних тривогах (виявленнях). Через необхідність формування траєкторій радіолокаційних цілей майже в реальному масштабі часу, якість супроводження обмежується наявними інформаційними, технічними та обчислювальними ресурсами [1-4]. В процесі роботи система супроводження визначає, які з нових відміток цілей слід використовувати для оновлення вже наявних траєкторій цілей. Для цього спочатку виконується приведення всіх наявних траєкторій цілей до поточного моменту часу. Ця операція виконується шляхом екстраполяції положення цілі з використанням оцінки її попереднього положення та даних про її курс, швидкість, прискорення та інші наявні дані. Екстраполяція виконується на основі прийнятої на поточний момент часу моделі руху цілі (наприклад, рівномірний, рівноприскорений рух та інше). Після приведення траєкторій цілей до єдиного часу система супроводження починає прив’язку до них нових радіолокаційних відміток цілей. Дана операція може бути виконана одним з декількох способів, а саме: 1) шляхом формування стробу супроводження навколо поточного положення траєкторії та аналізу відміток, що потрапили в нього, при цьому, якщо в строб супроводження потрапляє декілька відміток, то серед них вибирається: відмітка, найближча до прогнозованого (екстрапольованого) положення цілі; відмітка з найбільшою потужністю; 2) застосуванням статистичної обробки, коли найбільш імовірне положення відмітки визначається статистичною

комбінацією всіх можливих відміток, - цей підхід показує гарну ефективність під час роботи в сильних завадах [5-7].

Представляє інтерес проведення аналізу системи селекції рухомих цілей та виявлювачів трас повітряних об’єктів.

В оглядових радіолокаційних системах спостереження супровід повітряних об'єктів зазвичай здійснюється за інформацією первинних радіолокаційних систем спостереження [8, 9], а вторинні радіолокаційних систем спостереження використовуються, як джерела додаткової радіолокаційної інформації [10]. З переходом на автоматичне залежне спостереження [9-11] передбачається обов'язкова наявність лише вторинних радіолокаційних систем спостереження.

Послідовність виконуваних процедур виявлення дозволяє реалізувати виявлювачі трас повітряних об'єктів з проміжними прийняттями рішень про виявлення сигналів відповіді, виявлення повітряних об’єктів та виявлення траси повітряних об’єктів.

Можна реалізувати виявлювач, в якому рішення про виявлення траси повітряних об’єктів приймається на основі перевищення суми одиничних рішенні про виявлення сигналів відповіді запитальних радіолокаційних систем спостереження.

Модульність побудови виявлювача трас повітряних об’єктів дозволяє розглядати цю структуру в наступних послідовностях попередніх виявлень:

1) виявлювач повітряних об’єктів - виявлювач сигналів відповіді - виявлювач траси повітряних об’єктів;

2) виявлювач сигналів відповіді - виявлювач повітряних об’єктів - виявлювач траси повітряних об’єктів;

3) виявлювач повітряних об’єктів - виявлювач траси повітряних об’єктів - виявлювач сигналів відповіді.

До основних характеристик будь-якої системи селекції рухомих цілей (СРЦ) відносяться:

1) швидкісна характеристика;

2) якість подавлення пасивних завад;

3) коефіцієнт відношення сигнал-завада;

4) коефіцієнт підзавадової видимості;

5) коефіцієнт зміни втрат при включенні системи СРЦ.

Висновки. Для досягнення заданих характеристик роботи щодо селекції рухомих цілей необхідно покращувати характеристики системи кожну окрему і дивитися на загальний вплив на систему. Або ввести інтегральний показник якості селекції рухомих цілей, що значно спростить розуміння впливу параметрів характеристик на кінцевий результат.

Список використаних джерел.

1. Свид І. В. Обробка радіолокаційної інформації систем спостереження повітряного простору: монографія. Дніпро : ЛІРА ЛТД, 2022. 224 с.

2. І.І. Обод, І.В. Свид, О.С. Мальцев. Обробка даних радіолокаційних систем спостереження повітряного простору: навчальний посібник. – Харків: Друкарня Мадрид, 2021. – 255 с.

3. І.В. Свид, І.І. Обод. Завадостійкість радіолокаційних систем ідентифікації за ознакою «свій-чужий»: монографія. Харків : Друкарня Мадрид, 2021. 254 с.

4. I. Svyd, I. Obod and O. Maltsev, "Interference Immunity Assessment Identification Friend or Foe Systems", Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 69. Springer, Cham, pp. 287-306, 2021. doi: 10.1007/978-3-030-71892-3_12.

5. V. Semenets, I. Svyd, I. Obod, O. Maltsev and M. Tkach, "Quality Assessment of Measuring the Coordinates of Airborne Objects with a Secondary Surveillance Radar", Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 69. Springer, Cham, pp. 105-125, 2021. doi: 10.1007/978-3-030-71892-3_5.

6. І.І. Обод, І.В. Свид. Порівняльний аналіз якості виявлення повітряних об’єктів запитальними системами спостереження. Тематичний збірник «Системи обробки інформації» Випуск 9 (90) – Харків, видавництво ХУПС, 2010 – С. 74-76.

7. Обод І.І., Свид І.В., Штих І.А. Завадозахищеність запитальних систем спостереження повітряного простору: монографія. / За заг. ред. І.І. Обода. Харків: ХНУРЕ, 2014. 312 с.

8. І.І. Обод, І.В. Свид, І.В. Рубан, Г.Е. Заволодько. Математичне моделювання інформаційних систем: навчальний посібник. / За редакцією І.І. Обода. Харків : Друкарня Мадрид, 2019. 270 с.

9. I. Obod, I. Svyd, O. Maltsev, O. Vorgul, G. Maistrenko and G. Zavolodko, "Optimization of the Quality of Information Support for Consumers of Cooperative Surveillance Systems", Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 48. Springer, Cham, pp. 133-155, 2020. doi: 10.1007/978-3-030-43070-2_8.

10. I. Obod, I. Svyd, O. Maltsev, G. Zavolodko, D. Pavlova and G. Maistrenko, "Fusion the Coordinate Data of Airborne Objects in the Networks of Surveillance Radar Observation Systems", Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 48. Springer, Cham, pp. 731-746, 2020. doi: 10.1007/978-3-030-43070-2_31.

11. I. Svyd, I. Obod, O. Maltsev, V. Andrusevich, B. Bakumenko and O. Vorgul. Optimal Measurement of Signal Data Parameters of Requesting Radar Systems. // 2021 IEEE 3nd Ukraine Conference on Electrical and Computer Engineering, Lviv: 2021. – P. 138-141. doi: 10.1109/UKRCON53503.2021.9575235.

ОГЛЯД ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ВИКОНАННЯ ПРОЕКТІВ НА ПЛІС

студент Беззабарний Д.І., канд. техн. наук, доц. Воргуль О.В.
Харківський національний університет радіоелектроніки,
кафедра мікропроцесорних технологій і систем, м. Харків, Україна
e-mail: dmytro.bezzabarnyi@nure.ua

Abstract. The purpose of this work is to provide an open source overview of the FPGA software which can be found on the Internet. Some comparison by complexity of operation, possibilities and usability is performed.

Ключові слова: ПЛІС, програмне забезпечення, проет.

Вступ. Щоб навчитися складати моделі електронних цифрових систем мовою HDL, необхідна практика. Під час навчання мови програмування необхідний базовий інструмент програміста. Таким же чином, для того, щоб вивчити мову HDL, майбутньому спеціалісту потрібен інструмент розробника. Потрібно отримувати практику, а політика фірм розробників, наприклад, Xilinx згодом краще не стає. І софт у них усім добрий, але важкий, і точно не компактний [1-4].

Зі звичайним програмуванням легше. У самому спартанському випадку програмування можна вивчати, маючи текстовий редактор, компілятор, можливо, відладчик, і процесор. Звичайно ж, зараз усі звикли до середовищ розробника, щоб з описом команд, щоб редактор із підсвічуванням синтаксису та вбудованою допомогою. І так, це зручно.

Основна частина. А як для вивчення мови HDL? Роль процесора у цій ситуації може зіграти або симулятор, або живий кристал ПЛМ чи ПЛІС. Особливістю ПЛІС є те, що результатом є модель електронного приладу, який не є самодостатнім. Для його повноцінної перевірки він повинен бути вбудований у схему або тестовий стенд [5-8].

Адже з програмуванням як. Сидиш за комп'ютером та пишеш програму. І відразу її запускаєш і перевіряєш. А якщо ми створюємо модель електричного приладу? Який мінімальний набір програмного забезпечення потрібен?

З 80-х років минулого століття, часом – бурхливо, часом – неквапливо, розвиток цієї галузі відбувався у різних напрямках [1]. Спочатку пропонувалося в ході створення моделі паралельно створювати тестову програму - тест бенч. Виходить, що модель перевіряється моделлю. У світі HDL інструментом може бути симулятор.

Симулятори створювалися як розробниками апаратного забезпечення – великими фірмами, і фірмами чи співтовариствами, які займаються випуском власних ПЛМ і ПЛІС.

Що робить симулятор для мови HDL? Aria, ChatGPT з Opera [2] інформує:

Симулятор HDL (мова опису обладнання) – це програмний інструмент, який використовується при цифровому проектуванні та перевірці для моделювання та тестування цифрових схем та систем, що описуються з використанням HDL, таких як VHDL (мова опису апаратного забезпечення надшвидкісних інтегральних схем) або Verilog . Основна мета симулятора HDL – дати розробникам можливість перевірити правильність та функціональність своїх цифрових проектів до їх реалізації на апаратному рівні.

Ось що може симулятор HDL:

1. Поведінкове моделювання. Симулятор HDL може моделювати поведінку цифрової схеми чи системи більш високому рівні абстракції. Це дозволяє розробникам описувати функціональність схеми за допомогою конструкцій HDL та моделювати її поведінку з часом. Це дозволяє їм тестувати та налагоджувати проект, перш ніж переходити до реалізації нижчого рівня.

2. Часовий аналіз та аналіз продуктивності. Симулятори HDL можуть аналізувати часову поведінку проекту, щоб переконатися, що він відповідає бажаним вимогам щодо продуктивності. Вони можуть виконувати аналіз критичного шляху та виявляти потенційні проблеми синхронізації, такі як гонки чи надмірні затримки, які можуть вплинути на загальну функціональність схеми.

3. Генерація тест бенча (тестового стенду). Це HDL модель, що є набором стимулів, що використовуються для управління вхідними даними цифрового проекту під час моделювання. Симулятори HDL надають інструменти автоматичного або ручного створення тестових стендів. Ці тестові стенди дозволяють розробникам перевіряти поведінку своїх проектів у різних вхідних умовах та тестувати різні сценарії, щоб гарантувати правильну функціональність.

4. Налагодження та перегляд сигналів: симулятори HDL надають можливості налагодження, дозволяючи розробникам відстежувати та аналізувати поведінку своїх проектів. Вони можуть встановлювати точки зупинки, покроково виконувати моделювання та перевіряти значення сигналів та змінних у різні моменти часу. Засоби перегляду сигналів – поширена функція HDL-симуляторів, що дозволяє розробникам візуалізувати сигнали та їх переходи з часом.

5. Перевірка та аналіз покриття. Симулятори HDL підтримують методологію перевірки, що дозволяє гарантувати, що проект відповідає зазначеним вимогам. Вони можуть виконати аналіз функціонального покриття, щоб визначити повноту процесу перевірки та виявити будь-які неперевірені частини проекту.

Загалом, симулятор HDL є найважливішим інструментом у процесі цифрового проектування та перевірки, що дозволяє розробникам моделювати, тестувати, налагоджувати та перевіряти поведінку та

продуктивність своїх цифрових схем та систем, описаних з використанням HDL.

Xilinx пропонує Vitis, Vivado та ISE. Ці версії мають вбудовані різні симулятори. ISE легше, простіше, але на нових версіях операційних систем працює лише на віртуальній машині з підтримкою Windows 7. Xilinx вміло керує популярністю більш свіжих продуктів, встановивши більш потужні стимулятори в Vivado та Vitis.

Altera, яка тепер зветься Intel, пропонувала Altera Max Plus та Quartus II. На сайті Intel пропонується Quartus Prime, підтримка попередніх вище згаданих програм припинена.

Крім пари грандів, інтерес становлять ще два розробники.

Model Sim. Раніше існувала фірма Mentor Graphics випустила симулятор, що використовується досі, якийсь час з ним можна було ознайомитись через altera.com. Оскільки великі фірми до своїх продуктів включають кілька симуляторів.

У фірми Aldec Active-HDL можна завантажити програму та файли, необхідні для моделювання. Для зручності використання та скачування, є можливість вибрати, ПЛМ і ПЛІС, яких саме фірм бажає завантажити користувач. У переліку виробників – Altera, LatticeSemi, Xilinx.

Висновки. Таким чином, можна здійснити вибір програмного забезпечення для моделювання. Щоправда, підтримка апаратного забезпечення буде неповною. Лише моделювання.

Список використаних джерел.

1. https://en.wikipedia.org/wiki/Hardware_description_language

2. ChatGPT Aria for Opera https://www.opera.com/ua/features/browser-ai.

3. ModetSim https://eda.sw.siemens.com/en-US/ic/modelsim/

4. Aldec Active-HDL https://www.aldec.com /en/products/fpga_simulation /active_hdl_student

5. I. Svyd, O. Vorgul, V. Semenets, O. Zubkov, V. Chumak, N. Boiko. Special Features of the Educational Component “Design of Devices on Microcontrollers and FPGA”. // II International Scientific and Practical Conference Theoretical and Applied Aspects of Device Development on Microcontrollers and FPGAs (MC&FPGA), Kharkiv, Ukraine, 2020, pp. 55-57. doi: 10.35598/mcfpga.2020.017

6. O. Vorgul, I. Svyd, O. Zubkov, V. Semenets. Teaching microcontrollers and FPGAs in Quarantine from Coronavirus: Challenges and Prospects. // II International Scientific and Practical Conference Theoretical and Applied Aspects of Device Development on Microcontrollers and FPGAs (MC&FPGA), Kharkiv, Ukraine, 2020, pp. 14-17. doi: 10.35598/mcfpga.2020.005

7. I.V. Svyd, O.V. Litvinenko, O.G. Bilotserkivets. Features of designing digital devices based on Xilinx FPGA in CAD Vivado HLx Design Suite. // Specialized Exhibition "KharkivProm Days. Production and efficiency". Collection of materials of the forum section "Automation, electronics and robotics. Development Strategies and Innovative Technologies". - Kharkiv, KNURE, Exhibition Company ADT, 2019, pp. 43-44.

8. В. Чумак, І. Свид. Створення модуля VHDL-опису при проектуванні цифрових систем на ПЛІС в Xilinx ISE Design Suite. // Перспективні напрямки сучасної електроніки, інформаційних і комп'ютерних систем (MEICS-2019). – Дніпро, Дніпровський національний університет імені Олеся Гончара, Кременчук: ПП Щербатих О. В., 2019. – С. 94-95.

ОГЛЯД ВІЗУАЛЬНИХ МОВ ПРОГРАМУВАННЯ

ст. викл. Шафроненко Є.О., викладач Нестерук О.Г, викладач Бабич А.О.
Харківський національний університет радіоелектроніки,
кафедра медіаінженерії та інформаційних радіоелектронних систем,
м. Харків, Україна;
Відокремлений структурний підрозділ «Полтавський політехнічний фаховий коледж Національного технічного університету «Харківський політехнічний інститут», м. Полтава, Україна
e-mail: yevhenii.shafronenko@nure.ua

Abstract. This paper reviews the programs of visual programming. It classifies visual programming languages into three categories based on how they use graphics to represent the syntax of the language. It also divides visual programming languages that rely on flowcharts into four subcategories: data flow programming, state machines, behavior trees, and event-based rules. We suggests that the best way to learn the main types of visual programming languages is to start with languages like Blockly and end with the LabVIEW language.

Ключові слова: візуальні мови програмування, Blockly, LabVIEW, CASE-системи, SCADA-системи.

Вступ. Сучасне програмування використовує візуальні методи для спрощення та пришвидшення створення програм. Візуальні мови програмування (ВМП) – це підхід, за яким програми будуються з візуальних компонентів, наприклад, блоків та стрілок, а не з текстового коду. Цей етап в історії програмування дав розробникам більше можливостей та зробив програмування доступнішим. Зараз існує понад 70 різноманітних візуальних мов програмування, які мають різне призначення, функції та сфери застосування.

Основна частина. Візуальне програмування, яке включає створення програм за допомогою графічних засобів та автоматичну генерацію програмного коду, може бути реалізоване через різноманітні інструменти та підходи. Цей метод відділяє процес програмування від прямого написання тексту програм та дозволяє використовувати візуальні елементи для визначення структури програми та її функціональності.

Існують різні системи та середовища, які впроваджують концепції візуального програмування. Деякі з них спрямовані на спрощення процесу створення програм для початківців, тоді як інші ставлять за мету полегшити взаємодію між розробниками та замовниками.

Однак на етапі класифікації можуть виникати питання через неоднозначність та величезний асортимент інструментів візуального програмування. Вони можуть різнитися за концепціями та рівнем складності. Класифікація ускладнюється через різні підходи та філософії,

які вони втілюють. Важливо враховувати, що хоча візуальне програмування може полегшити розробку (для певних завдань), ускладнення може виникнути при роботі над складними або масштабними проектами.

Візуальні мови програмування поділяються за рівнем складності та функціональністю. Залежно від характеристик, візуальні мови можна розділити на кілька категорій, як показано на рисунку 1.

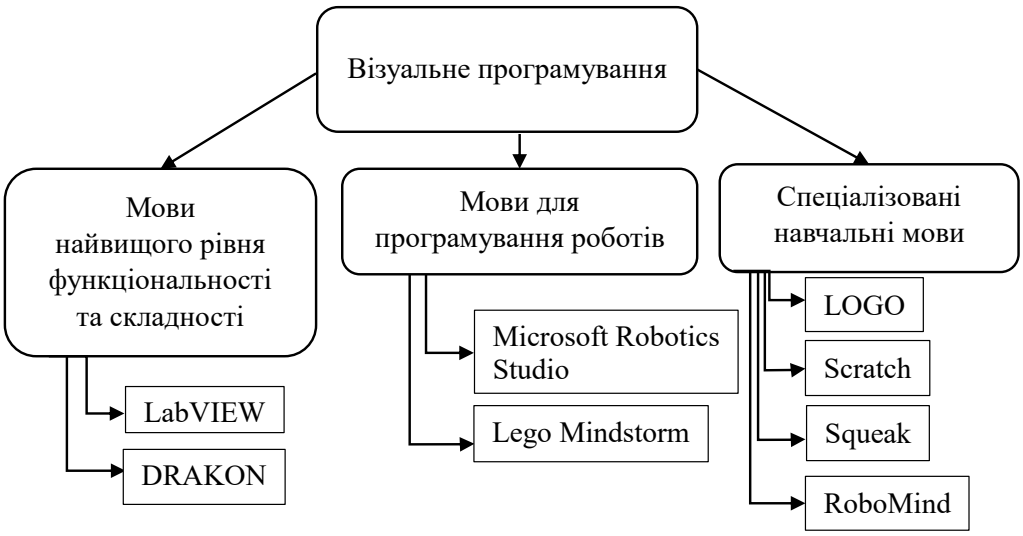


Рисунок 1 – Класифікація візуальних мов програмування

Ці категорії відображають відмінності, спрямованість та особливості візуальних мов програмування, а також їхню придатність для конкретних завдань та цільових аудиторій. Візуальне програмування може розглядатись в двох аспектах:

- графічна мова програмування, яка використовує графічні елементи для конструювання програми. Кожен графічний елемент представляє конкретну операцію або дію, а їх поєднання визначає послідовність виконання програми. Приклади таких мов – LabVIEW, Blockly тощо;
- візуальні засоби розробки, які включають інструменти та середовища для створення програм або розробки додатків, такі як CASE-системи, системи швидкої розробки додатків, SCADA-системи для програмування мікроконтролерів та інші.

Такі інструменти дозволяють інженерам і програмістам розробляти програми, не працюючи безпосередньо з кодом. Незалежно від використаного інструменту та обраної мови, використовуються графічні елементи, але їх функції та застосування можуть значно відрізнятися.

Візуальні мови програмування знаходять широке застосування у сфері навчання програмуванню, особливо серед початківців. Прикладами таких мов є App Inventor, Blockly, Scratch, Snap!, які спрощують процес навчання

та роблять його доступнішим.

У візуальних мовах програмування, основні елементи програми представлені у вигляді блоків, які користувач складає разом, визначаючи потік виконання програми. Блоки зазвичай групуються за типами у каталозі, що забезпечує зручний доступ до функцій без необхідності вивчення документації. Такий підхід розв'язує проблеми, пов’язані з вивченням синтаксису текстових мов програмування, дозволяючи зосередитися на логіці програми. Середовище розробки для таких мов зазвичай має спрощений інтерфейс, за допомогою якого користувач може легко запускати свій код на виконання та переглядати отримані результати. Для деяких візуальних мов є можливим «переклад» коду в текстові мови програмування, такі як JavaScript, Python, PHP, Lua, Dart, або збереження створеної логіки у вигляді XML-файлу.

Існують також візуальні мови, які використовують графічні елементи аналогічні тим, що використовуються у блок-схемах. Прикладами таких мов є Bonita BPM, Discovery Machine, Flowgorithm, Flowhub, Grafcet, Raptor, WebML, Widget Workshop тощо. Програми, створені за допомогою цих мов, являють собою послідовність дій заданих стандартними блоками, включаючи розгалуження з умовами для вибору подальших блоків виконання.

Такий метод використання візуальної граматики спрощує розуміння синтаксису мови, однак логічні конструкції, створені цим способом, можуть бути обмеженими в порівнянні з традиційними мовами програмування. Також важливо мати усвідомлення того, що саме міститься всередині блоків програми (дані, команди, дії), і цей вміст не завжди можна змінити за допомогою графічного інтерфейсу.

При програмуванні кінцевих автоматів у графічному вигляді, блоки являють собою стани, а зв’язки між ними відображають переходи. Програміст визначає стани і переходи між ними, ініційовані умовами. При зміні стану, спрацьовує відповідна інструкція, тобто створюється потік виконання у відповідності до блок-схеми, яка з’єднує стани, і визначає тригери для їх зміни. Таким чином, логіка керування контролюється безпосередньо через переходи і їх умови, замість фокусування на внутрішніх деталях блоків, що дозволяє створювати складніші інструкції, використовуючи інкапсульовану поведінку блоків. До таких мов можна віднести EKI One, NodeCanvas, Unity3D Mecanim Animator Controller, xaitControl тощо.

Мови програмування поведінки на основі дерев використовують візуальну граматику, яка складається з блоків і зв’язків між ними. Ці зв’язки визначають потік виконання і обробляють та повертають статус до попереднього блоку, що схоже на генеалогічне дерево. Такий підхід дозволяє визначати логіку програми через графічний інтерфейс, не вимагаючи додаткової візуальної граматики або редагування тексту.

Приклади таких мов – RAIN, AngryAnt Behave, Behavior3, NodeCanvas.

Ще одним типом візуальних мов програмування є мови, що базуються на правилах, побудованих на подіях. У таких мовах програміст визначає правила типу «якщо відбудеться ця подія, виконати такі дії». Правила спрацьовують кожен раз, коли умова виконується, і виконують вказані інструкції. Зазвичай такий підхід використовується під час розробки комп'ютерних ігор та симуляторів. Прикладами таких мов є Blender Game Engine, Construct 2, Kodu, Zapier тощо.

Висновки. В роботі виконано аналіз візуальних мов програмування, класифікація їх за форматом графічного представлення, та виділено дві основні категорії: мови, що використовують блоки, та мови, що базуються на блок-схемах. Висвітлено різні підтипи, такі як ті, що використовують потік даних, кінцеві автомати, дерева поведінки та правила на основі подій.

При розгляді основних типів візуальних мов програмування рекомендується починати з мов, таких як Blockly, і поетапно продовжувати вивчення, переходячи до складніших мов, наприклад, LabVIEW.

Список використаних джерел.

1. Dehouck, R. E. M. I. (2015). The maturity of visual programming. Режим доступу: http://www. craft. ai/blog/the-maturity-of-visualprogramming.

2. Завадський, І. О., & Заболотний, Р. І. (2009). Основи візуального програмування. К.: Видавнича група BHV, 272.

3. Семеренко, В. П. (2010). Візуальне програмування.

4. Вакалюк, Т. А. (2013). Візуальне програмування. Навчально-методичний посібник для студентів фізико-математичного факультету.

5. Лозовська, Л. І., Бандоріна, Л. М., Савчук, Р. В., & Климкович, Т. О. (2022). Візуальне програмування. Український державний університет науки і технологій, Дніпро.

6. Круглик, В. С., & Марчук, М. С. (2022). Сучасні тенденції у вивченні візуального програмування майбутніх інженерів-програмістів. In Мехатронні системи: інновації та інжиніринг. Київський національний університет технологій та дизайну.

7. Tsai, C. Y. (2019). Improving students' understanding of basic programming concepts through visual programming language: The role of self-efficacy. Computers in Human Behavior, 95, 224-232.

АНАЛІЗ ТЕХНОЛОГІЙ ВІДДАЛЕНОГО ДОСТУПУ ДО ПРИСТРОЇВ НА МІКРОКОНТРОЛЕРАХ

к.т.н., доцент Зубков О.В., викладач Олійник В.В., студентка Павлій С.С.
Харківський національний університет радіоелектроніки,
кафедра медіаінженерії та інформаційних радіоелектронних систем,
м. Харків, Україна
e-mail: oleh.zubkov@nure.ua

Abstract. An analysis of modern remote access technologies for monitoring the status and control of modern electronic devices based on microcontrollers was carried out. The economic and technical infeasibility of deploying embedded servers based on microcontrollers when accessed from the Internet is shown. An analysis of modern Docker technology for applications containerization and their deployment on local or cloud servers was carried out. The effectiveness of the technology has been proven by the example of deploying a web application for monitoring and controlling a home heating system.

Ключові слова: мікроконтролер, віддалений доступ, протокол, мережа.

Вступ. Віддалений доступ до пристроїв на мікроконтролерах стає все більш актуальним і важливим з розвитком Інтернету речей (IoT) та потребою віддаленого керування вбудованими системами [1]. Віддалений доступ особливо актуальний для вирішення наступного кола проблем:

1. Моніторинг та управління постійно зростаючою кількістю підключених пристроїв і систем в рамках Інтернету речей, промисловості, медичних пристроїв та інше.

3. Для віддаленого налагодження, діагностики помилок та підтримки користувачів.

4. Націлений віддалений доступ може забезпечувати захист та безпеку, забороняючи несанкціонований доступ до систем та дозволяючи контролювати права доступу.

5. Можливість отримати швидкий доступ до вбудованих систем для реагування на події або зміну параметрів в реальному часі.

У цілому, актуальність віддаленого доступу до пристроїв на мікроконтролерах стає все більш важливою з поглибленням цифрової трансформації у багатьох галузях, де важливо не лише зібрати дані, а й здійснювати контроль та управління пристроями здалеку.

Основна частина. На апаратному рівні віддалений доступ означає поєднання мережних інтерфейсів з підтримкою сучасних протоколів передавання даних та вбудованих чи хмарних серверних технологій. Хоча сучасні мікроконтролери мають багато інтерфейсів передавання даних (USB, CAN, USART та ін.), але для глобального дистанційного доступу в

основному використовують інтерфейс дротового Ethernet з'єднання або бездротову технологію WiFi. В обох цих інтерфейсах на комунікаційно-програмному рівні передавання даних забезпечують протоколи: HTTP (Hypertext Transfer Protocol), MQTT (Message Queuing Telemetry Transport), CoAP (Constrained Application Protocol), SSH (Secure Shell), Telnet, SNMP (Simple Network Management Protocol) [2]. Найпростішим рішенням дистанційного доступу є розгортання вбудованого у сам пристрій серверу, наприклад WEB серверу. Для популярних мікроконтролерів є багато готових бібліотек, що дозволяють у короткі строки вбудувати у програмний код backend частину веб сайту чи інше програмне рішення. Наприклад, для популярних WiFi модулів ESP32 із вбудованими мікроконтролерами загального призначення широко використовуються такі синхронні та асинхронні сервери, як WebServer та ESPAsyncWebServer [3]. Так можна забезпечити доступ комп'ютерам або смартфонам до web сайту такого пристрою із локальної мережі і здійснювати локальний моніторинг або керування. При цьому глобальний доступ обмежується архітектурою сучасних мереж. В основі мережних протоколів передачі даних лежить IP адресація електронних пристроїв [1]. Пристрої локальної мережі мають внутрішню IP адресацію, яка невідома для глобальної мережі, а роутер, що поєднує локальну і глобальну мережу зазвичай має динамічну IP адресу, що видає йому провайдер. Навіть, якщо провайдер видає статичну IP адресу, за якою можна зайти до нього із мережі Internet, то для маршрутизації на web сторінку електронного пристрою необхідно виконати додаткові налаштування роутеру. Користувачі, що покупають такі пристрої не мають необхідної кваліфікації для цього, а використання сервісних спеціалістів коштує дорого і економічно необґрунтовано. Саме тому останні роки поширюється використання хмарних технологій і серверів, на яких розміщуються спеціальні додатки, що приймають інформацію із сукупності електронних пристроїв та передають її за запитом до клієнтських додатків на персональні комп'ютери, смартфони і т.д.

На початку 2000х років практично усі фірми виробники обладнання з дистанційним доступом закупали апаратні сервери, адміністрували їх та розташовували один або декілька програмних серверів з їх додатками [4]. Такі крупні компанії як Samsung, Xiaomi і зараз мають власні сервери, а менші компанії намагаються скоротити витрати на покупку обладнання, заробітню платню адміністраторів і віддають перевагу розташуванню серверів з додатками на сторонніх хмарних серверах та оплачують орендну платню за експлуатацію ресурсів сервера.

Таким чином на хмарних серверах повинні одночасно існувати десятки, сотні, мільйони незалежних додатків. Їх виконання забезпечується завдяки сучасній технології віртуалізації Hyper-V [5]. Спочатку на одному фізичному сервері створювали та запускали декілька віртуальних машин із

своїми операційними системами. Але кожна операційна система потребує багато ресурсів: пам'ять, обчислювальна потужність (ядра) процесора. Тому ця технологія мала високу вартість. Зараз використовують нові підходи до віртуалізації. Docker - це платформа для розробки, доставки та запуску програмного забезпечення відокремленими контейнерами [6]. Ця технологія дозволяє упаковувати програми та їх залежності в стандартизовані контейнери, які можуть бути запущені на будь-якому комп'ютері, що підтримує Docker, без будь-яких змін. Основними компонентами Docker є: Docker Engine - рішення для створення та управління контейнерами. Він включає в себе сервер, який запускає та управляє контейнерами, та набір інструментів для їх створення та керування; Docker Image - це шаблон або темплейт, який використовується для створення контейнерів. Він містить всі необхідні файли та налаштування для запуску програми або сервісу; Docker Container - це інстанція Docker Image, яка виконується та працює на операційній системі. Контейнер є ізольованим середовищем, в якому виконується програма або сервіс, і містить усі необхідні компоненти для його роботи; Docker Hub - це хмарна платформа для зберігання та обміну Docker Images. Основними переваги використання Docker є: портативність, ізоляція та легковагість (від декількох мегабайт до сотен мегабайт), швидкість розгортання.

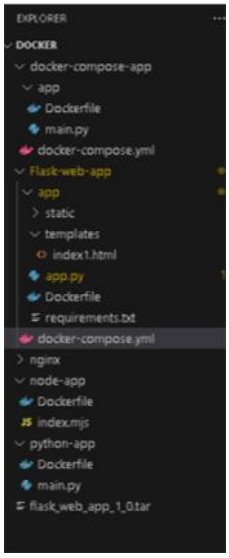


Рисунок 1 – Структура проекту для створення образу Docker

Для проведення дослідження ефективності платформи Docker у якості апаратної платформи був обраний модуль ESP32. До модуля ESP32 було підключено датчик температури DS18B20 та релейний модуль для керування системою нагріву приміщення. Вмикання та вимикання нагрівача здійснюється за відповідними температурними порогами, початкові значення яких задані у базовій прошивці модуля і можуть бути переналаштовані за допомогою web додатку. Програмне забезпечення було

розроблено мовою C++. Для обміну даними між пристроєм та web додатком використано бібліотеку HTTP клієнту.

Web додаток було реалізовано мовою Python із застосуванням мікрофреймверку Flask для розгортання самого додатку та контенту сайту (web сторінки, графічні файли, css файли). Для створення проекту web додатку використовувалось середовище VS Code 2023. У VS Code було інстальовано розширення Docker. Структура загального проекту наведена на рисунку 1. Папка Flask-web-app містить усі файли web додатку. Файл docker-compose.yaml містить опис процесу створення образу і поєднання порту web додатку у контейнері із зовнішнім портом. Файл Dockerfile описує процес створення контейнеру web додатку у середині образа і інсталяцію додаткових модулів (Python, Flask і т.д.) від яких залежить робота додатка. В подальшому робота додатка була протестована у сукупності із роботою модуля ESP32.

Висновки. В роботі були проаналізовані технічні аспекти проблеми дистанційного доступу до електронних пристроїв, а також шляхи їх вирішення. Аналіз сучасної технології віртуалізації Docker і її тестування з використанням одного із найпоширеніших мікроконтролерів ESP32 показала стабільність роботи із мінімумом використаних апаратних ресурсів сервера (розмір образу 58 Мбайт).

Список використаних джерел.

1. Sachin Kumar, Prayag Tiwari & Mikhail Zymbler Internet of Things is a revolutionary approach for future technology enhancement: a review Jornal of Big Data Vol. 6, 2019, pp.1-21

2. Сидни Фейт. TCP / IP. Архітектура. Протоколи. Реалізація. – К. вид-во Лори, 2014, 424 с.

3. Зубков О.В., Зубков А.О. Особливості реалізації web серверів на модулях ESP8266 та ESP32 у Arduino IDE AERT-2022, с.8-11

4. Rob Barrett, Eser Kandogan, Paul P. Maglio, Eben M. Haber, Leila Takayama Field studies of computer system administrators: Analysis of system management tools and practices roceedings of the 2004 ACM Conference on Computer Supported Cooperative Work, CSCW 2004, Chicago, Illinois, USA, November 6-10, 2004

5. Dandu, Sujitha, "Data Center Server Virtualization Solution Using Microsoft Hyper-V" (2017).Culminating Projects in Information Assurance. 23. https://repository.stcloudstate.edu/msia_etds/23?utm_source=repository.stcloudstate.edu%2Fmsia_etds%2F23&utm_medium=PDF&utm_campaign=PDFCoverPages

6. Minh Thanh Chung, Nguyen Quang-Hung, Manh-Thin Nguyen, Nam Thoai Using Docker in High Performance ComputingApplications 2016 IEEE Sixth International Conference on Communications and Electronics pp.52-57

ВПЛИВ ТАКТОВОЇ ЧАСТОТИ ОПЕРАТИВНОЇ ПАМ'ЯТІ НА ПРОДУКТИВНІСТЬ КОМП'ЮТЕРНИХ СИСТЕМ

асистент Желавський Д.Ю., викладач Бабич О.В., студент Грисенко А.О.
Харківський національний університет радіоелектроніки,
кафедра медіаінженерії та інформаційних радіоелектронних систем,
м. Харків, Україна;
Відокремлений структурний підрозділ «Полтавський політехнічний фаховий коледж Національного технічного університету «Харківський політехнічний інститут», м. Полтава, Україна
e-mail: denys.zhelavskyi@nure.ua

Abstract. With the launch of AMD Ryzen processors, as well as six and eight-core Intel Core, the situation has changed significantly. Now high bandwidth, low memory latency are among the most important characteristics of a PC. You can achieve best performance in two opposite ways: try to manually boost a cheap low-frequency RAM (this is always a gamble) or directly buy a selected high-frequency one and boost it even more.

Ключові слова: оперативна пам'ять, розгін, частота, напруга, таймінги.

Вступ. З появою процесорів AMD Ryzen, а також шести і восьмиядерних Intel Core ситуація істотно змінилася. Зараз висока пропускна здатність і низька затримка пам'яті є одними з найважливіших характеристик ПК. Ви можете досягти найкращої продуктивності двома протилежними способами: спробувати вручну збільшити дешеву низькочастотну оперативну пам'ять (це завжди ризиковано) або безпосередньо купити вибрану високочастотну і збільшити її ще більше.

Основна частина. Процес розгону процесора [1] полягає в тому, що потрібно просто знайти баланс між частотою і напругою живлення. Процес оверклокінгу пам'яті (ОЗП) трохи складніший, адже потрібно знайти точку рівноваги між трьома параметрами: частотою, напругою і таймінгами. Цих самих таймінгів, до речі, цілих п'ять, і це не враховуючи ще більше десятка субтаймінгів, які, однак, зазвичай не чіпають, залишаючи стандартними. Існує три способи розгону ОЗП [2]: автоматичний розгін за допомогою активації вбудованого в пам'ять профілю налаштувань XMP (DOCP); ручне підвищення частоти, хоча і з вимушеним підвищенням затримок; і ручне зниження таймінгів при незмінній частоті. Найпростішим, звичайно, є перший спосіб – авторозгін. Саме тому є сенс придбати високочастотну оперативну пам'ять AMD Radeon, і заощадити час, який був би витрачений на ручний підбір параметрів.

В наших тестах ми змінили напругу живлення з базових 1.2 до 1.35 В за допомогою DOCP в системних налаштуваннях BIOS (для розгону пам'яті DDR4 напруга до 1.4 В вважається нормальною), а таймінги

встановили на 16-18-18-36. Іншими словами, ми дещо зекономили, перетворивши пам'ять на швидшу, з 3333 МГц. Можливо, пам'ять з вищою частотою з заводу могла б розігнатися ще більше, наприклад, до 3466 МГц. Ця зміна параметру зазвичай є корисною для багатьох користувачів, оскільки зміна частоти оперативної пам'яті значно покращує продуктивність мультимедійних програм. Зміну пропускної здатності пам'яті до і після розгону ми можемо виміряти за допомогою програми AIDA64 (існує безкоштовна пробна версія). Також ми провели синтетичні тести з застосуванням програм CinebenchR23 та Ryzen Dram Calculator. Слід зазначити, що ми змінювали частоту оперативної пам'яті в двоканальному режимі [3], тобто це 2 модулі AMD Radeon 2666 MHz, а загальний обсяг пам'яті становить 16 Гб. Процесор, який ми використовували – AMD Ryzen 3600, відеокарта ASUS GTX 1060 3 Gb та материнська плата ASUS TUF B450. Двоканальний режим – найефективніший для домашніх настільних комп'ютерів і для деяких ноутбуків, оскільки дозволяє збільшити пропускну здатність ОЗП в 2 рази порівняно з одноканальним режимом.

Рисунок 1 – Зовнішній вигляд оперативної пам'яті AMD Radeon

Таблиця 1 – Співвідношення тактової частоти оперативної пам'яті та отриманої кількості балів у тестах програми CinebenchR23

Тактова частота, MHz	Singlecore, pts	Multicore, pts
2400	1075	5089
2666	1092	5222
2733	1094	5229
2800	1100	5331
2866	1087	5215
2933	1100	5353
3000	1093	5464
3066	1092	5348
3133	1099	5249
3200	1084	5183
3266	1090	5059
3333	1086	5089

Збільшення частоти оперативної пам'яті сприяє зростанню продуктивності в багатьох програмах, а оптимальні таймінги позитивно впливають на надійність системи і частково збільшують її продуктивність.

Також можна проводити тести в одноканальному режимі, але цей режим дещо знижує продуктивність.

Таблиця 2 – Співвідношення тактової частоти оперативної пам’яті та отриманих результатів у тестах програми AIDA64

Тактова частота, MHz	CPU PhotoWorxx, Mpx/s	Затримка пам'яті, ns	CPU Queen, pts
2400	18044	92,2	50179
2666	19145	87,5	50338
2733	19318	87,8	50257
2800	20022	85,8	50162
2866	20293	84,8	50300
2933	20728	83,2	50085
3000	21145	81,3	50364
3066	21149	82,9	50405
3133	21574	82,1	50388
3200	21989	81,2	50265
3266	22194	79,5	50178
3333	22305	80,8	50270

Таблиця 3 – Співвідношення тактової частоти оперативної пам’яті та отриманих результатів у тестах програми Ryzen Dram Calculator

Тактова частота, MHz	Random latency, ns	Time, s	Custom latency, ns	Read Speed, GB/s	Write Speed, GB/s
2400	89,1	182,59	92,0	31,5	18,6
2666	84,7	177,39	86,8	32,8	20,9
2733	86,5	180,59	89,2	32,7	21,5
2800	83,1	176,90	86,7	34,2	21,9
2866	81,5	170,01	86,7	35,1	21,9
2933	80,1	172,32	84,3	35,5	22,4
3000	79	163,61	81,3	36,5	22,7
3066	81	166,22	84,1	36,5	23,4
3133	79,5	167,55	82,8	37,2	24,7
3200	78,6	164,01	83,8	37,5	24,6
3266	77,4	160,44	80,6	39,1	25,4
3333	78,5	164,34	82,3	38	25,2

Висновки. Ми дослідили вплив різних налаштувань та змін частоти оперативної пам’яті на продуктивність системи. В процесі тестування ми отримали чимало даних, які уважно проаналізували та порівняли, а головна цінність результатів полягає в тому, що вони надають корисну інформацію та рекомендації стосовно оптимальних налаштувань параметрів частоти для покращення продуктивності комп’ютерних систем.

Список використаних джерел.

1. https://www.amd.com/en/newsroom/press-releases/2020-4-21-amd-expands-3rd-gen-amd-ryzen-desktop-processor-fa.html - інформаційний сайт;

2. https://www.itbox.ua/ua/blog/Rozgin-operativnoyi-pamyati-DDR3-DDR4-DDR5-Yak-ce-zrobiti-Plyusi-ta-minusi-rozgonu/ - інформаційний сайт;

3. https://www.moyo.ua/ua/news/chto-takoe-dvukhkanalnyy-rezhim-dual-mode-operativnoy-pamyati-gayd-v-3-razdelakh.html - інформаційний сайт.

ОСОБЛИВОСТІ ВИКОРИСТАННЯ СУЧАСНИХ ГРАФІЧНИХ ФОРМАТІВ

ст. викл. Колісник В.І., викладач Бабич О.В., студентка Анур'єва К.С.
Харківський національний університет радіоелектроніки,
кафедра медіаінженерії та інформаційних радіоелектронних систем,
м. Харків, Україна;
Відокремлений структурний підрозділ «Полтавський політехнічний фаховий коледж Національного технічного університету «Харківський політехнічний інститут», м. Полтава, Україна
e-mail: viktoriia.kolisnyk@nure.ua

Abstract. Editing raster graphics is now widely used, as it is popular in photography and copying technology. Moreover, such editors help both professional graphic designers and creative artists in their work. Therefore, exploring the capabilities of modern graphic formats is useful for them.

Ключові слова: сучасні мультимедіа, растрові графічні редактори, графічні формати, стиснення зображення.

Вступ. Растрові графічні редактори – це програми, які створюють зображення з сітки маленьких квадратів, які називаються пікселями. Сітку пікселів називають растром. Растрове формування зображення використовується сучасними сканерами та фотоапаратами, тому растрові графічні редактори дуже затребувані в наш час [1–3].

Основна частина. Растрові графічні редактори застосовуються в фотографії і при підготовці поліграфії, яка містить фотографії. Вони дозволяють робити фото ретуш: видаляти дефекти, змінювати фон фотографії, змінювати спектр і інтенсивність кольорів, змінювати загальний настрій зображення за допомогою спеціальних світлових ефектів. Також вони можуть бути корисними для розробників різного мультимедійного контенту при створенні текстових і фонових ефектів та для зменшення кількості кольорів зображень. Растрові графічні редактори використовують в своїй роботі не тільки професійні графічні дизайнери, але і творчі художники чи фотографи. Вони допомагають створювати графічні двовимірні та тривимірні об'єкти досить високої якості.

В наш час існує багато програм для редагування растрової графіки, та більшість з них є хоч і недорогими, але нестандартними. Є також дорогі професійні програми, які розроблені та використовуються відомими компаніями з розробки програмного забезпечення. Тому варто розглянути деякі з них з точки зору перспектив використання якісних загальнодоступних редакторів растрової графіки.

Растрові зображення зазвичай створюються за допомогою сканера або цифрової камери. Сканер дозволяє оцифрувати старі слайди, діапозитиви чи фотографії. Сучасна цифрова фотографія зберігає зображення в одному

з стандартних форматів растрових зображень: JPEG, GIF, PNG тощо. Розглянемо основні риси найпопулярніших растрових графічних форматів [4 – 6].

На рис. 1 наведено порівняльний аналіз найчастіше використовуваних графічних форматів та їх особливостей в контексті застосування, відображення та стиснення графічної інформації.

Рисунок 1 – Типи графічних форматів

Перш за все слід згадати формат BMP, який хоч і не використовується вже багато років, але підтримується абсолютно всіма графічними редакторами, які працюють під керуванням операційної системи Windows і не тільки. Колись він застосовувався зокрема для зберігання фонів робочого столу Windows. Цей формат використовує глибину кольору від 1 до 24 біт. Оскільки це просто двовимірний масив чисел, кожен з яких задає колір пікселя, такі файли дуже легко формувати й обробляти програмно. Ще одна перевага формату – дуже швидкий показ (відображення) зображень, головний недолік – великі обсяги файлів (формула 1).

Розмір BMP-файлу T можна оцінити за наступною формулою:

$$T = G \cdot V \cdot n, \quad (1)$$

де: G – розмір зображення по горизонталі; V – розмір зображення по вертикалі; n – глибина пікселів.

Формат TIFF (рис. 2) є одним з найпопулярніших форматів, особливо у галузі поліграфії та керування електронними документами.

Він підтримує усі кольорові моделі – від чорно-білої до RGB, CMYK, LAB та інших. Формат файлу TIFF, створений на IBM-сумісному комп'ютері сумісний з операційною системою Mac OS і більшістю UNIX/Linux платформ. Також він підтримується всіма основними

пакетами растрової та векторної графіки і програмами, що призначені для редагування тексту.

Рисунок 2 – Стандартна піктограма формату TIFF

Розглянемо деякі додаткові функції які надає формат TIFF:

–використання додаткових каналів (альфа каналів). Збереження зображення з альфа-каналами, для продовження редагування окремих частин зображення після того, як воно вперше розміщено на сторінці, і до кінцевого результату [5, 6].

–використання компресії. Це функція зменшення обсягу файлу до 50% від початкового обсягу за допомогою алгоритму стиснення LZW, що виконується без втрати інформації.

–попередній кольороподіл. Ця функція виконується в окремому файлі в колірній моделі CMYK. Вона спрощує подальшу процедуру розміщення файлу зображення на сторінці та друку документа. В цьому плані TIFF є зручнішим за інші формати. На сьогодні цей формат найчастіше використовується для імпорту растрової графіки у векторні програми при використанні у видавничих системах [5, 6].

Формат JPEG (рис. 3) зараз є одним з найпопулярніших графічних форматів, які використовуються в побутовій цифровій фотографії. Він реалізує алгоритм стиснення з втратами, тобто процес стиснення зображення призводить до часткової втрати інформації, що зберігається у файлі [5,6]. Тому в процесі застосування цієї процедури треба шукати компроміс між ступенем стиснення і якістю зображення, що зберігається. Чим більше стиснення, тим нижча якість, і навпаки.

Рисунок 3 – Порівняння використання формату TIFF та JPEG

Кодування даних за допомогою використовуваного в JPEG алгоритму виконується в декілька етапів:

1. Графічні дані перетворюються на кольоровий режим LAB.
2. Відкидається від 1/2 до 3/4 інформації про колір (залежно від реалізації алгоритму).
3. Аналізуються блоки розміром 8 х 8 пікселів. Кожному блоку створюється набір чисел. Перші кілька чисел описують колір блоку в загальному, а наступні цифри описують дрібніші деталі. Оскільки спектр деталей базується на людському візуальному сприйнятті, великі деталі є помітнішими.
4. Залежно від обраного рівня якості, частина чисел, що характеризують дрібні деталі, відкидається.
5. Використовується кодування за методом Хаффмана для ефективнішого стиснення кінцевих даних. Одночасно виконується послідовний перегляд проаналізованих наборів номерів для визначення частоти появи кожного числа. Тоді числа, які зустрічаються найчастіше, кодуються з використанням мінімально можливої кількості бітів. Розкодування даних відбувається в зворотному порядку.

Висновки. Отже, чим вищий рівень стиснення, тим більше даних втрачається й тим нижча якість зображення. Використовуючи формат JPEG, можна отримати файл від 1 до 500 разів менший, ніж в форматі BMP. Цей формат апаратно-незалежний, може бути використаний незалежно від операційної системи й підтримується практично будь-якими графічними програмами. Крім стандартного варіанту, існує ще два підтипи формату JPEG, орієнтованих на використання в Інтернеті.

Список використаних джерел.

1. Комп’ютерна графіка: конспект лекцій / Укладач: Скиба О.П. – Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя, 2019. – 88 с.
2. Комп'ютерна графіка: навчальний посібник: в 2-х кн. Кн. 1. / Укладачі: Тотосько О. В., Микитишин А. Г., Стухляк П. Д. Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя, 2017. 304 с.
3. Веселовська Г.В., Ходакова В.Є.: Компютерна графіка. Навч. пос. - К.: Кондор, 2015. - 584 с.
4. Програми для роботи з комп’ютерною графікою та формати графічних зображень. Конспект лекцій. https://financial.lnu.edu.ua/wp-content/uploads/2015/12/Lektsiia2-1.pdf
5. Типи графічних файлів: https://shorturl.at/hxHSX
6. Графічні формати: https://uk.wikipedia.org/wiki/Графічні_формати

УЧБОВА АВТОМАТИЗОВАНА СИСТЕМА РОЗРАХУНКУ СТАТИЧНИХ Н-ПАРАМЕТРІВ БІПОЛЯРНОГО ТРАНЗИСТОРУ З ВИКОРИСТАННЯМ МОДЕЛІ РЕАЛЬНОГО ТРАНЗИСТОРУ ТА ВБУДОВАНОГО МІКРОКОНТРОЛЕРНОГО ПРИСТРОЮ

к.ф.-м.н., доцент Цехмістро Р.І., викладач Кожем'якін М.В.,
студент Яценко В.С.
Харківський національний університет радіоелектроніки,
кафедра медіаінженерії та інформаційних радіоелектронних систем,
м. Харків, Україна;
Відокремлений структурний підрозділ «Полтавський політехнічний фаховий коледж Національного технічного університету «Харківський політехнічний інститут», м. Полтава, Україна
e-mail: roman.tsekhmistro@nure.ua

Abstract. The automated system is a computer program that can be used either independently or with a laboratory model with a microcontroller module installed for communication with a computer.

Aim-works: familiarize the student with the method of developing the static input and output characteristics of a bipolar transistor and the value of static H-parameters for their assistance. Schemes for varying the static characteristics of the transistor, a circuit with a lead base and a lead emitter, are used both autonomously and by extracting data from the microcontroller.

Ключові слова: транзистор, мікроконтролер, схема, h-параметри

Вступ. Комп'ютеризовані системи дослідження параметрів біполярних транзисторів та пристроїв на їх основі, успішно використовуються в навчальному процесі. Однак, враховуючі тематику відповідних навчальних дисциплін, данні системи найчастіше обмежуються створенням віртуального вольтметру та осцилографу. Це безумовно сприяє автоматизованій обробці результатів поряд з економією матеріальних та людських ресурсів. Однак подібні системи часто не дають можливості поспостерігати фізичну сутність процесів, які відбуваються в напівпровідникових приладах, робота яких описана реальним моделями.

Розроблена програма присвячена питанню розрахунку статичних h-параметрів транзисторів за допомогою побудованих статичних вхідних та вихідних залежностей. Вона дозволяє порівнювати вхідні та вихідні характеристики, зняті експериментально за схемою з загальною базою та емітером, з теоретичними залежностями, отриманими на основі реальної моделі з урахування ефекту Ерлі.

Основна частина. Запропонована система дозволяє використовувати як окремо від макету(розрахунки за формулами), так и експериментально в останньому випадку можливо будувати графіки як автоматично (передавати в ПК), так и вводити окремі значення.

У нього також входить модуль, що забезпечує графічне відображення вхідних та вихідних характеристик за схемою із загальною базою з консольним введенням даних від амперметру та вольтметру, що дає можливість виділити області насичення, активну область, область відсікання. передбачена можливість завдання кількості (до 100) значень показань значень струму та напруги, що вводяться.

Вказаний модуль передбачає також можливість розрахунку вхідної характеристики за співвідношенням:

$$I_e = I_0\left(1+\frac{U_{кб}}{U_{Ep}}\right)\left(e^{\frac{qU_{бе}}{кT}}-1\right), \quad (1)$$

де I_0 – зворотній струм p-n переходу; q=1,6·10^{-19} Кл; к=1,38·10^{-23} Дж/К; Т=300 К, U_{Ep} – напруга Ерлі.

Ця напруга, яка вводиться для опису явища «модуляції ширини бази», яка призводить до зміни її опору, має вид

$$U_{Ep} = \frac{q(Wb)^2 Nd}{2\varepsilon}, \quad (2)$$

де q – заряд електрону; wb – товщина бази транзистора; Nd – концентрація донорних домішок; Е– діелектрична проникність.

Значення напруги Ерлі зазвичай складає залежно від типу транзистора десятки вольт.

У програмі передбачено введення значень струму насичення $U_{бе}$, $U_{ке}$. На одних і тих же графіках є можливість відобразити експериментальну залежність $I_б=f(U_{бе})$ $U_{кб}$=const і аналогічні залежності отриманих теоретично. Указана залежність дозволяє визначити статичні параметри h_{11e} – вхідний опір ($h_{11e}=\Delta U_{бе}/\Delta I_e$) як за теоретичними так і експериментальними залежностями та спів поставляти їх.

Вихідна характеристика біполярного транзистора відповідно зі схемою загальна база описується залежністю $I_к=f(U_{кб})$ $I_е$=const:

$$I_к = \alpha\cdot I_e + \frac{U_{кб}}{r_к} + I_{e0}\cdot\alpha\cdot I_к = \alpha\cdot I_y + \frac{I_{e-}}{1-\alpha} + \frac{U_{кб}}{r_к}, \quad (3)$$

де α – коефіцієнт передавання; $I_{к0}$ – зворотній струм колектора; $U_к$ – напруга на колекторі; $r_к$ – опір колекторного переходу; $\alpha \le 1-\alpha$.

З рис. 1-2 видно, що вказаний модуль дозволяє проводити розрахунок зі співвідношення (2) для різних значень $U_{кб}$. При цьому вводиться $U_{еб}$ – максимальне, $U_{еб}$ – мінімальне, значення I_0, напруга Ерлі, значення коефіцієнту β. На рис.1 показана схема отримання значень току емітера та бази транзистора, яка вираховується з закону Ома через падіння напругі на вбудованому резистору скрізь модуль вбудованого мікроконтролеру.

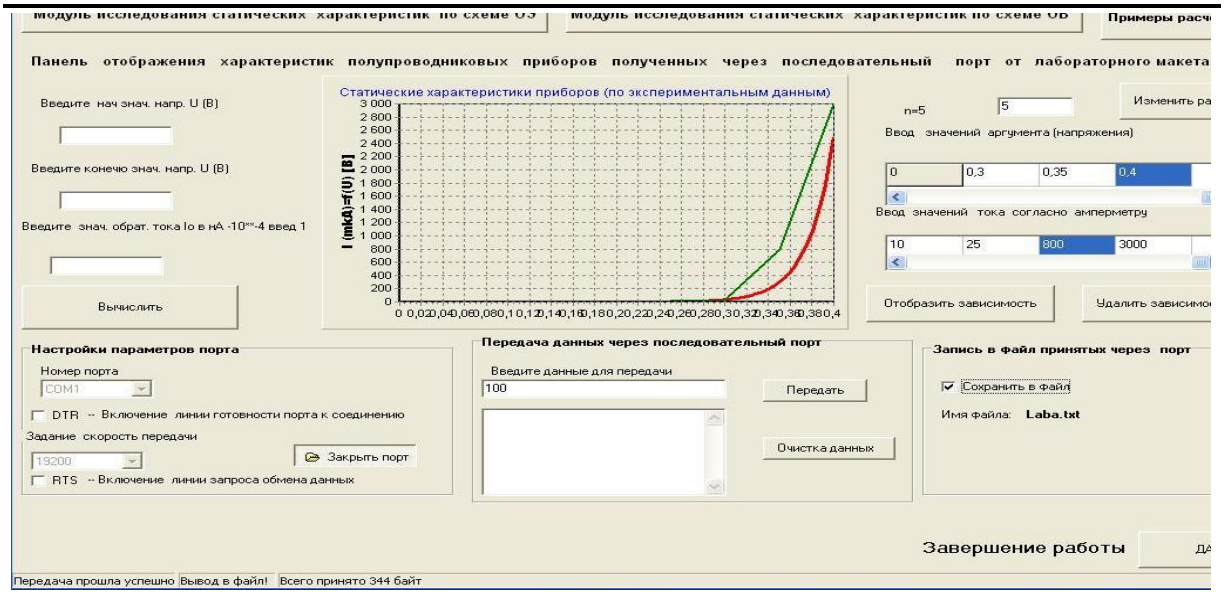


Рисунок 1

На рис. 2 наведені форми програми, яка дозволяє відображувати вхідні характеристики біполярного транзистора (співвідношення 1,3) при включення із загальним емітером. $I_Б = f(U_{ЕБ})$ при $U_{КЕ} = const$ наведено на верхньому графіку. Ліворуч наведено опції для введення вихідних даних для побудови залежності за співвідношенням (1): I_0; напруга Ерлі $U_{Ер}$; $U_{КЕ}$; $U_{ЕБ}$ – початкового та максимального значення.

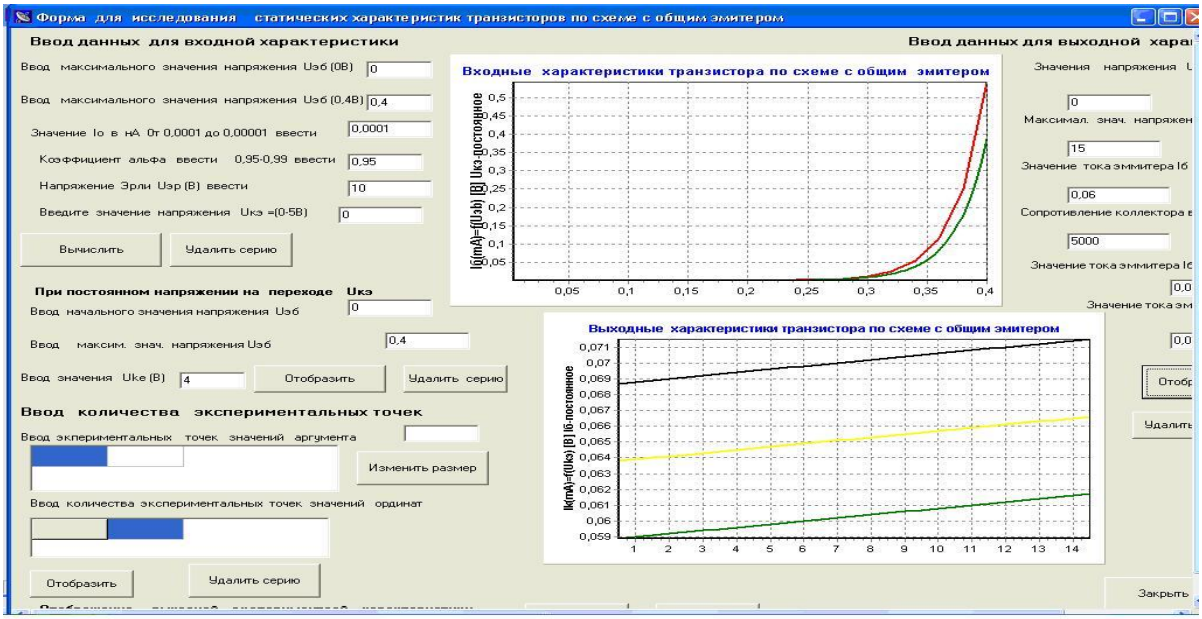


Рисунок 2

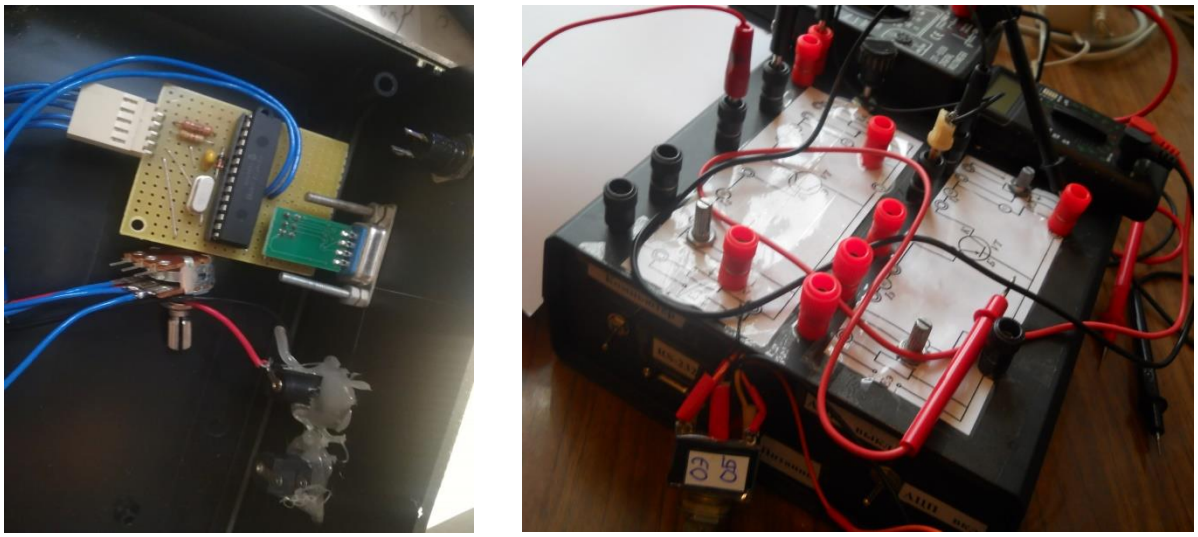


Рисунок 3

На рисунку 3 наведено загальний вигляд макету з вбудованим мікроконтролерним пристроєм на основі PIC16F73, який має вбудований інтерфейс UART (USART) для передавання даних у ПК.

Висновки. Тобто програмний продукт можливо використовувати самостійно (теоретичні розрахунки) так і з лабораторним макетом (експериментальні розрахунки з переданими у ПК). Новизна та відмінність розробки від існуючих складається у використання аналітичних розрахункових формул побудованих на основі реальних моделей роботи транзисторів. Самі параметри розраховуються із відомих формул за графіками ($h_{11E} = \frac{\Delta U_{БЕ}}{\Delta I_{Б}} = \frac{U_{Б2} - U_{Б1}}{I_{Б2} - I_{Б1}}$) [1, 2].

Список використаних джерел.

1. Зі С. Фізика напівпровідникових приладів. Т.1. – К.: Вища школа, 2 видання, 1984. – 453 с.

2. Росадо Л. Фізична електроніка та мікроелектроніка. – К.: Вища школа, 1991. – 351с.

ПРОГНОЗУВАННЯ РУХУ БІРЖЕВИХ КОТИРУВАНЬ

викладач Марченко С.М., студентка Тимофєєва К.О.
Відокремлений структурний підрозділ «Полтавський політехнічний фаховий коледж Національного технічного університету «Харківський політехнічний інститут», м. Полтава, Україна
e-mail: smarchenko876@gmail.com

Abstract. The work is devoted to the problem of forecasting the movement of quotations on the stock exchange. This is the most difficult problem of stock exchange data analysis. The success of many financial organizations and the economy in general depends on the correct analysis of stock market data. Despite the long path of its development, technical and fundamental analysis of stock exchange data did not reveal the main methods of forecasting. The reasons for the complexity of statistical evaluation of stock market quotations for forecasting are considered.

Ключові слова: технічний аналіз, фундаментальний аналіз, котирування цінних паперів, прогноз даних, нестаціонарність.

Вступ. Гра на біржі, судячи з стрімкого темпу зростання обороту торгівлі цінними паперами, приносить суттєві прибутки. Успішна гра на біржі супроводжується вирішенням цілого ряду завдань [1]. Інвестор має бути достатньо освіченим, щоб правильно оцінити ситуацію на біржі та в економіці загалом. Йому належить вибрати найбільш перспективні цінні папери для покупки. Тому найважливішою умовою успішної гри є застосування ефективного інструменту прогнозу. Жоден із існуючих методів фундаментального та технічного аналізу не може дати достатньо надійного прогнозу. У роботі розглядаються причини складності аналізу біржових даних.

Основна частина. Аналіз біржових даних можна умовно поділити на технічний аналіз (ТА) та фундаментальний аналіз. При аналізі біржових даних найчастіше використовують ТА. Вважають, що ціни на акції вже увібрали в себе всю інформацію. Варто тільки знайти спосіб їх прогнозування і ви будете впевнено почуватися на біржі. Наразі існують і використовуються понад 500 методів прогнозування біржових даних. На думку деяких аналітиків, їх розвиток призведе врешті-решт до створення такого методу ТА, який даватиме достовірні прогнози.

Фундаментальний аналіз також складається, в основному, із числових показників. Наприклад, дані фінансової звітності компанії, перспективи її продукції та послуг на ринку, всілякі фінансові показники компанії, різні фінансові коефіцієнти тощо. У фундаментальному аналізі розрахунки прогнозів виробляються з урахуванням або макроекономічних показників економіки загалом, або мікроекономічних показників галузі, фірми. Основний аналіз, що базується на досить добре розвинених економічних

теоріях, дозволяє не тільки ефективно управляти фінансовими справами фірми, а й коригувати стан її економіки. Теоретичний аналіз та багатий досвід, накопичений у фундаментальному аналізі, дає можливість враховувати численні фактори, що різною мірою впливають на прибутковість цінних паперів. Використовуючи ринкову модель, можна навіть так сформувати портфель акцій, що для обраної прибутковості портфеля ви отримаєте мінімально можливий ризик.

Знаючи середньостроковий або довгостроковий прогноз, ви отримаєте уявлення про загальний напрямок щоденної зміни котирувань. Численні поради, теорії, системи гри на біржі, рекомендації аналітиків зрештою впираються в одну невирішену проблему - прогноз біржі. Без вирішення цієї проблеми ви будете вічним спонсором біржі.

Деякі фактори легко розрахувати, деякі фактори з великими труднощами ми можемо оцінити чисельно. Для цього потрібно використовувати не лише числові, а й нечислові дані. До одних з таких числових показників варто віднести біржові індекси: S&P, DJ, Nasdaq та ін. До даних нечислової природи, можна віднести такі як фон новин, ситуація у світі, галузі, заяви відомих представників: галузі, ФРБ, політиків, економістів, гуру біржі і т.д. Проте є труднощі їх використання, особливо у прогнозах.

Відсутність ефективних методів прогнозування породжує цілу низку другорядних проблем, вирішення яких набагато простіше, і тому ними більше захоплюються багато аналітиків [2]. Якщо ви використовуєте ефективний метод прогнозування, у вас менше проблем виникає з ризиком інвестицій, психологією особистості та натовпу, тактики та стратегії гри на біржі. У вас зникає потреба мати широкий кругозір у сфері фундаментального та фінансового аналізу, вміння користуватися всіма методами ТА, оволодінням системою гри на біржі. Немає потреби у докладному вивченні різноманітної інформації, що впливає рух ринку.

Не варто думати, що десь існують достовірні способи прогнозування руху ринку, і хтось ними успішно користується. Звернемося до неупередженої думки відомого біржового гравця Дж. Сороса [3]. У своїх книгах він постійно наголошує на неефективності економічних наук у галузі аналізу, а особливо прогнозу руху ринку. Він показує, що немає хороших методів передбачення ні технічному аналізі, ні фундаментальному. Дуже складно прогнозувати фінансові ринки, аналізуючи політичну, економічну, фінансову ситуацію, що впливає світові фінансові ринки. Великий практик Дж. Сорос може собі дозволити зробити зауваження про те, що біржова гра це історія помилок і помилок, а не наукового прогнозу.

Помилки прогнозів обумовлені численними економічними чинниками, постійно змінюють вплив на біржу. Усе це дає можливість досі створити формалізовану математичну теорію руху біржі. Незважаючи на

те, що методи статистичного прогнозування успішно застосовуються в науці та техніці, їх використання в аналізі фінансових ринків є неефективним [4, 5]. Якщо складні математичні моделі не працюють у таких випадках, застосування простих методів ТА біржових даних можна виправдати.

Статистичний аналіз біржових даних [6, 7] не такий ефективний через існуючі проблеми, які ускладнюють його використання. До них відносяться: нестаціонарність ринкових даних, наявність у них трендів, високий рівень ринкового шуму, відсутність яскраво вираженої періодичної складової, труднощі експериментальної перевірки ефективності методів, обмеженість кореляції та довжини вибірок корельованих даних, відсутність ансамблю спостережень, використання для прогнозу лише історичних даних тощо. Тому застосування строгих методів математичного прогнозування подібних часових рядів, як видно, не приносить поки що багато користі. Інакше, інформаційні агентства вже давно надавали б більш точні прогнози поведінки ринку. Інвестори та гравці на біржі, користуючись цими методами, тільки б вигравали. Зараз інформаційні агентства пояснюють лише події на біржі в минулому. Звертають нашу увагу на показники економіки, що зіграли певну роль, а точніше кажучи, на які було б слід звертати увагу.

Висновки. Хоча є наукові теорії формування ефективного портфеля, успішні гравці більше довіряють своїй інтуїції. Стверджується, що прогнозування руху біржових котирувань існуючими методами є безперспективним. І від прогнозу спрямування руху біржі слід відмовитися. Проте дослідження причин складності обробки біржових даних це кроки наукового підходу до проблем біржі. Об'єднання ТА та фундаментального аналізу сприятиме правильному аналізу біржових даних. Слід зазначити також слабке використання під час прогнозу даних нечислової природи.

Список використаних джерел.

1. Бергер Ф. Что Вам надо знать об анализе акций / Пер. с нем. - М.: АОЗТ "Интерэксперт"; ЗАО "Финстатинформ", 1998 - 206 с.

2. Sharpe W. F., Alexander G. J., Bailey J. V. Investments. Пер. с англ. - М.:ИНФРА-М, 1998. - 1028с.

3. Soros G. The Alchemy of Finance, John Wiley &Sons, Inc., New York, 1988.

4. Box, G. E. P., and G. M. Jenkins, Time Series Analysis, Forecasting and Control, Revised Edition, Holden-Day, San Francisco, CA, 1976.

5. Марпл. - мл. С. Л. Цифровой спектральный анализ и его приложения: Пер. с англ. - М.: Мир, 1990. - 584с.

6. Дрейпер Н., Смит Г. Прикладной регрессионный анализ: Пер. с англ. - М.: Статистика, 1973. - 392с.

7. Montgomery D. C., Johnson L. A., Gardiner J. S. Forecasting and Time Series Analysis. McGraw-Hill, Inc., 1990.

МУЛЬТИМОДАЛЬНИЙ ПІДХІД ДО СПОСТЕРЕЖЕННЯ БПЛА

к.т.н., доц. Посошенко В.О., викладач Холопов В.В., студент Зубарєв В.О.
Харківський національний університет радіоелектроніки,
кафедра медіаінженерії та інформаційних радіоелектронних систем,
м. Харків, Україна;
Харківський радіотехнічний коледж, м. Харків, Україна
e-mail: vitalii.pososhenko@nure.ua, victor.kholopov1952@gmail.com

Abstract. The UAV model is considered as a source of multimodal signals of different physical nature. It is shown that such signals are the acoustic and optical radiation of the apparatus, as well as radar reflections from acoustic disturbances in the atmosphere, which arise as a result of its normal functioning. The possibility of a significant improvement in the quality characteristics of UAV detection with a synergistic combination of information on each channel of interaction with it in the case of compatible complex processing and interpretation of signals of different modalities is considered. Experimental samples of similar signals and their mathematical description are presented.

Ключові слова: БПЛА, мультимодальні сигнали, акустика, оптика, РЛС.

Вступ. На сьогоднішній день існують численні галузі застосування, які потребують об'єднання багатомодальних даних. Прикладами таких областей можуть бути біомедичні додатки (моніторинг інтенсивної терапії та медичних зображень), транспортні системи (розумний автомобіль та дорожні системи), мультимедійний аналіз (аудіовізуальна ідентифікація людини, багатомодальна взаємодія з роботом і багатомодальний відеопошук), дослідження поодиноких подій і складних багатофакторних явищ (наприклад, спалах наднової зірки або вивчення метеорних явищ у верхніх прошарках атмосфери Землі), виявлення та спостереження безпілотних літальних апаратів тощо.

Ключовим моментом у цій царині є поняття модальності джерел інформації. На даний момент під цим поняттям частіше за все розуміють канал інформаційної взаємодії системи спостереження з подією або явищем, які досліджуються та використовуються у практичній діяльності або людиною, або комплексом «людина-машина».

Це передбачає знаходження стохастичного функціоналу F, який оперує з ймовірнісними функціями f(D_k) від D_k кожної модальності (F(f(D_k), k=1,n) для вирішення конкретної практичної задачі: виявлення, отримання оцінок поточних Кожна модальність забезпечує надходження у систему аналізу первинних даних D_k, які надають певну кількість інформації I_k, k=1,n, де n – кількість каналів взаємодії (модальностей) системи спостереження.

Часто виникає потреба поєднання (бажано у реальному часі) окремих видів інформації I_k з наміром отримання такої сукупної інформації I_c, яка б перевищувала кожну з парціальних I_k. Подібні ефекти підвищення результативності спільної дії чинників у порівнянні з їх окремими діями називають синергетичними.

Таким чином, алгоритм поєднання багатомодальної інформації передбачає знаходження стохастичного функціоналу F, який оперує з ймовірнісними функціями f(D_k) від D_k кожної модальності (F(f(D_k), k=1,n) для вирішення конкретної практичної задачі: виявлення, отримання оцінок поточних або узагальнених параметрів об'єкту, його еволюції у просторі і часі тощо.

Основна частина. Проблема своєчасного виявлення БПЛА і організації ефективної протидії їх несанкціонованому застосуванню є безумовно актуальною. Для виявлення БПЛА найбільш ефективними вважаються такі методи і засоби, як: радіолокаційний, акустичний, оптичний та їх різновиди [1].

Основні модальності при спостереженні БПЛА є такими: Акустичні спостереження БПЛА, радіолокаційні спостереження БПЛА, оптичні спостереження БПЛА, інфрачервоні спостереження БПЛА.

Акустичні спостереження базуються на застосуванні акустичного методу, який базується на реєстрації акустичного випромінювання (АВ), яке утворює БПЛА під час свого руху в атмосфері Землі. Тому значні зусилля дослідників спрямовано на з'ясування структури і параметрів АВ, що надає важливу апріорну інформацію (I_{aa}) для розробки стохастичних алгоритмів виявлення БПЛА на фоні шумових завад. Основними джерелами АВ БПЛА є його двигуни та їх гвинти. В їх роботах доведено, що спектр АВ малорозмірного БПЛА містить гармонічні смугові компоненти у смузі частот до 500 Гц. Гармонічні компоненти є кратними частоті обертання гвинтів апарату. При цьому перша гармоніка має найбільшу амплітуду. Зі збільшенням номеру спектральних складових їх рівень монотонно спадає і поступово стає співставним з рівнем фонового шуму. Також важливу апріорну інформацію надають спектрограми БПЛА. Приклад такої спектрограми наведено на рис.1 [1].

Аналізуючи цю спектрограму, можна зробити висновок про те, що АВ БПЛА є за структурою широкосмуговим сигналом. Найбільш потужними є спектральні складові у смузі частот до 500 Гц. Максимальна амплітуда притаманна першій гармоніці. Наступні за номером гармонічні складові монотонно зменшуються до рівня шумових завад оточуючого середовища. Крім того, експериментальні діаграми спрямованості акустичного випромінювання БПЛА надають апріорну інформацію про напрямки переважного випромінювання енергії акустичних коливань у просторі. При цьому широко використовують як двомірні, так і трьохмірні діаграми спрямованості.

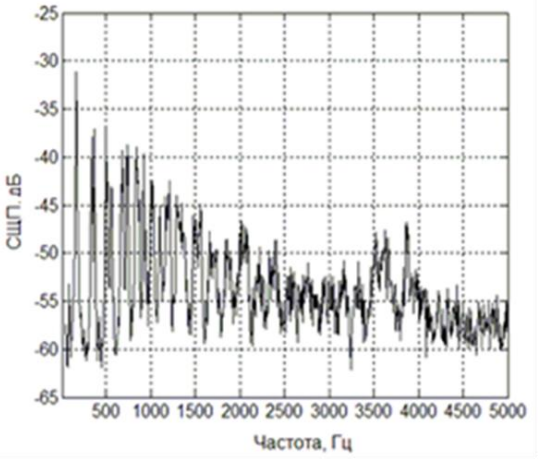


Рисунок 1 – Спектр акустичного випромінювання БПЛА «Phantom Dji» [1]

Активну радіолокацію БПЛА характеризують незалежність від погодних умов, значна дальність виявлення, просторовий дозвіл за дальністю та кутовими координатами, стійкість до перешкод, незалежність від часу доби і т.п. У свою чергу, існуючі технології виготовлення БПЛА дозволяють мінімально задіяти металеві компоненти у його конструкції , широко використовувати композитні матеріали та спеціальні покриття, що різко знижує ЕПР планера як радіолокаційної цілі. Тому при активній радіолокації БПЛА на перший план виходить аналіз сигналу, розсіяного не конструкцією планера, а пакетом акустичних хвиль, які виникають у процесі функціонування літального апарату.

Експериментально встановлено, що БПЛА випромінюють акустичні хвилі у діапазоні частот від сотень Герц до 15 кГц. Для отримання розсіяного радіосигналу від пакету акустичних коливань потрібно виконання умов Брегга:

$$\lambda_e = 2 \cdot \lambda_s \cdot \sin\theta,$$

де λ_e - довжина електромагнітної хвилі; λ_s - довжина хвилі акустичних сигналів; θ - кут між фронтом акустичної хвилі і напрямком розповсюдження зондуючих радіохвиль.

Відповідно, діапазон довжин хвиль розсіяних радіохвиль з інтенсивністю, достатньою для вирішення завдань їх виявлення та оцінювання, тягнеться від λ_e=6.8м (що відповідає частоті акустичного випромінювання f_s=100Гц, λ_s=3.4м) до λ_e=5.4см (що відповідає частоті акустичного сигналу f_s=15кГц, λ_s=2.7 см).

Оптична та інфрачервона модальності спостереження БПЛА багато в чому співпадають за фізичною сутністю процесів і апаратних засобів (вони розрізняються лише за смугою частот електромагнітних коливань, які використовуються для досліджень). Тобто інфрачервона модальність дуже близька до оптичної. Але є одна суттєва відмінність: оптичні спостереження БПЛА людина може вести безпосередньо, без застосування

будь-яких технічних засобів, а інфрачервоні дослідження БПЛА виконуються виключно за допомогою спеціальних датчиків інфрачервоного випромінювання, яке людське око не бачить. Ця обставина суттєво впливає на організацію процедур спостереження, а також на інтерпретацію отриманих даних. Приклади сформованих ІЧ зображень показані на рис. 2 [2].

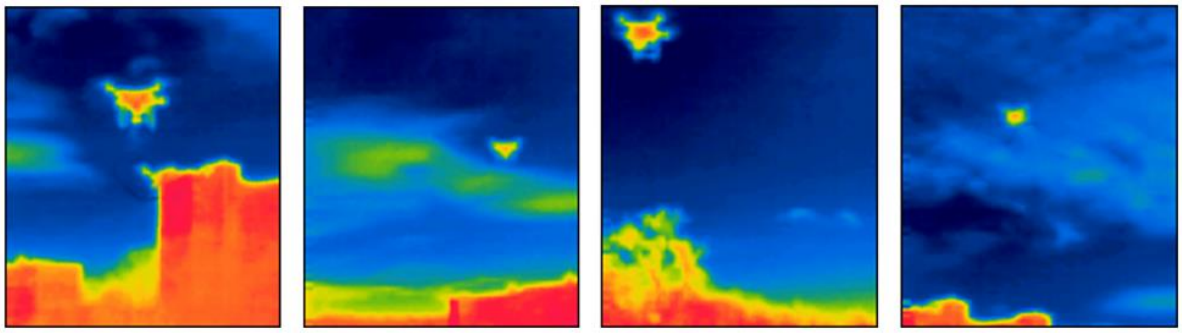


Рисунок 2 – Приклади сформованих ІЧ зображень

База даних зображень БПЛА у інфрачервоному діапазоні постійно поповнюються і досліджується [2].

Висновки. Таким чином, приклад БПЛА, як об’єкта дослідження (в окремому випадку – для спостереження) доводить, що для його вивчення можуть бути застосовані різні модальності (канали взаємодії). Кожна модальність має свої переваги і недоліки [1]. Тому виникла проблема поєднання інформації від джерел різної модальності з наміром найкращого використання їх сильних сторін і досягнення синергетичного ефекту, що суттєво покращить тактик-технічні характеристики пристроїв, призначених для спостереження БПЛА.

На першому етапі такого поєднання потрібно визначити взаємну кореляцію між різними модальностями та виявити статистичні алгоритми прийняття рішень в умовах дії шумів і нешумових завад також різної фізичної природи.

Подальший розвиток подібного мультимодального підходу до спостереження БПЛА буде базуватися на використанні нейронних мереж.

Список використаних джерел.

1. Карташов В.М., Посошенко В.О., Колісник В.І., Капуста А.І., Рибников М.В., Першин Є.В., Кізка В.О. Комплексування інформаційних каналів систем виявлення та спостереження безпілотних літальних апаратів з позицій теорії статистичних рішень // Радіотехніка: Всеукраїнський міжвідомчий наук.-техн. збірник. 2021.Вип. 207. С. 124-131.

2. Zubkov O.V., Sheiko S.O., Oleynikov V.M., Kartashov V.M., Babkin S.I. Investigation of Efficiency of Detection and Recognition of Drone Images from Video Stream of stationary video Camera // Telecommunications and Radio Engineering. New York. 2021. Vol. 80. №3. P23-37.

ПРИСТРІЙ ПІДВИЩЕННЯ ТА СТАБІЛІЗАЦІЇ НАПРУГИ POWER BANK

к.т.н., доц. Шаповалов С.В., викладач Романовська І.О.,
студент Озернюк Т.В.
Харківський національний університет радіоелектроніки,
кафедра медіаінженерії та інформаційних радіоелектронних систем,
м. Харків, Україна;
Харківський радіотехнічний коледж, м. Харків, Україна
e-mail: d_res@nure.ua

Abstract. The purpose of the development is to modify the voltage increase and stabilization module when using portable chargers for household use.

In the process of work, a solution was found to reduce the effect of temperature on the functionality of the module board and increase its efficiency during further use, as well as during the development of portable chargers for household use.

Ключові слова: Power bank, напруга, стабілізація, зарядні пристрої.

Вступ. Power bank (портативні зарядні пристрої) знайшли своє місце в сучасному світі у побуті та промисловості. Power bank застосовують для зберігання енергії та передачі її побутової техніці. В основі їх конструкції знаходяться накопичувач енергії і плата керування [1].

Основна частина. Основними вимогами до Power bank є високі коефіцієнти корисної дії (ККД) і стабілізації вихідної напруги, великий об'єм батареї, малі вихідні пульсації, захист від короткого замикання або перегріву, масо-габаритні характеристики та інші.

Серед Power bank існує два основних типи: промислові та побутові.

Промислові Power bank мають значну вагу та великі габаритні розміри. Застосовують їх у випадку відсутності електромережі для забезпечення роботи систем відеоспостереження, електроінструменту.

Побутові портативні зарядні пристрої (ПЗП) мають набагато меншу вагу, ціну та більш простішу конструкцію. Призначені вони в основному для зарядки мобільних телефонів, бездротових навушників, екшен-камер.

Конструкція побутових ПЗП (рис. 1) складається з батареї, плати керування і роз’ємів для підключення [2].

Під час проведення тесту модуля MT3608 [2] [3] було визначено залежність його вхідної напруги від вихідного навантаження плати. На лабораторному блоку живлення було виставлено 4.2V, тим самим імітуючи заряджений акумулятор ПЗП.

ККД плати починає падати при збільшенні вихідного струму. Вже при значені струму 1500 мА, цей показник знижається нижче 75%, що в свою чергу викликає нагрів модулю в цілому.

Рисунок 1 – Конструктивне оформлення побутового ПЗП

Рисунок 2 – Модуль підвищення та стабілізації напруги MT3608

Рисунок 3 – Макет тесту плати MT3608

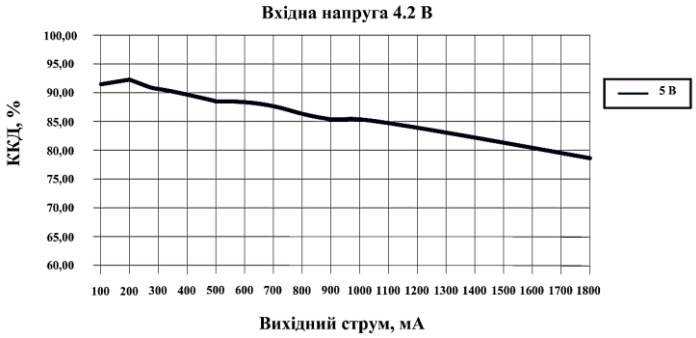


Рисунок 4 – Вихідний струм та ККД при напрузі 4.2V

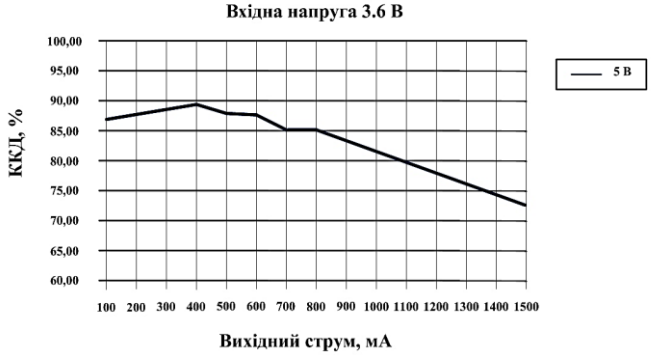


Рисунок 5 – Вихідний струм та ККД при напрузі 3.6V

Таблиця 1 – Температура елементів

Елемент	Температура, C°			
	Навантаження 1А		Навантаження 1.5А	
	3.6V	4.2V	3.6V	4.2V
Дросель 220	62	57	86	80
Діод SS34	77	71	89	85
Мікросхема MT3608	69	62	101	95

В конструкції існуючого модуля використана котушка індуктивності номіналом 22 мкГн, яка в подальшому, під час модернізації, була замінено на високочастотну котушку 4,7 мкГн. Встановлений танталовий конденсатор ємністю 220 мкФ та напругою 10V для згладжування пульсації на виході. Діод SS34 номіналом 3А був замінений на два діода SS54 більшого номіналу по 5А кожний для зменшення нагріву і за рахунок цього було збільшено ККД.

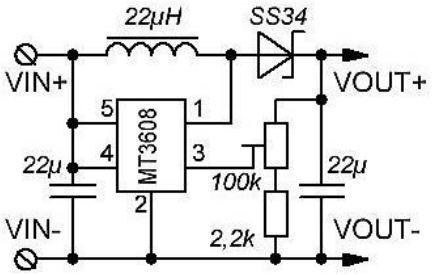


Рисунок 6 – Принципова схема існуючого модулю [2]

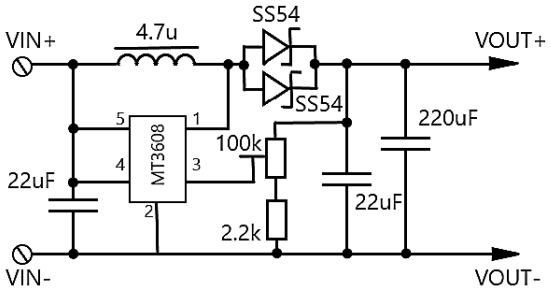


Рисунок 7 – Модернізована принципова схема модулю

Таблиця 2 – Температура елементів

Елемент	Температура, C°			
	Навантаження 1А		Навантаження 1.5А	
	3.6V	4.2V	3.6V	4.2V
Дросель 220	51	49	53	50
Діод SS34	69	65	75	69
Мікросхема MT3608	70	64	97	89

На рис. 8 та 9 синім кольором виділено результати виміру до модернізації, а червоним після модернізації. Можна замітити, що заміна компонентів плати, за рахунок чого було досягнуто зниження температури, змогли підвищити ККД модулю. Тобто, більше на 2% при вихідному струмі 1100 мА при 4.2V і до 6% при 3.6V.

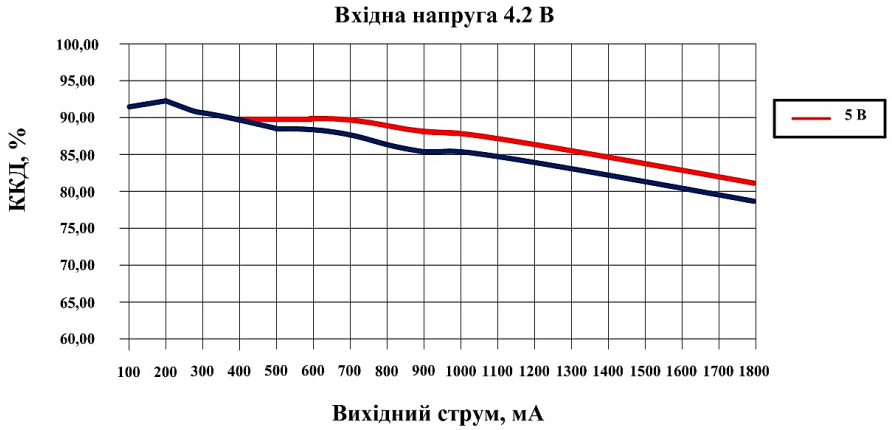


Рисунок 8 – Вихідний струм та ККД при напрузі 4.2V

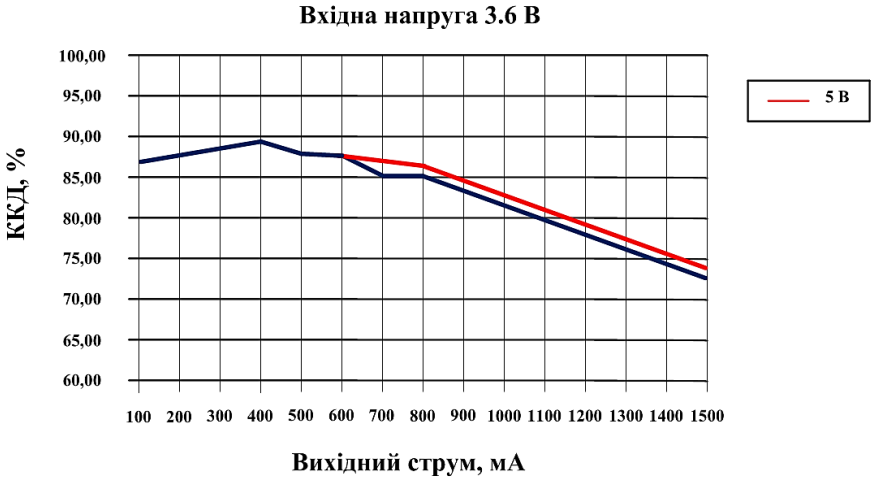


Рисунок 9 – Вихідний струм та ККД при напрузі 3.6V

Висновки. Збільшення ККД було досягнуто за рахунок заміни компонентів на існуючої платі модуля підвищення та стабілізації напруги MT3608, що у подальшому дозволило зменшити нагрів всього модуля під час його роботи, що позитивно вплинуло на його довговічність.

Список використаних джерел.

1.https://dostyp.com.ua/novini/printsipi-viboru-ta-poriadok-iekspluatatsiyi-powerbank/ - інформаційний сайт.

2.https://www.kirich.blog/stati/informaciya-dlya-nachinayuschih/136-para-step-up-konverterov-i-ih-nebolshoy-apgreyd-do-sepic.html - інформаційний сайт.

3.https://www.olimex.com/Products/Breadboarding/BB-PWR-3608/resources/ MT3608.pdf.

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ГАЛУЗІ FPGA

студент Вовсянікер М.Ю., асистент Білоцерківець О.Г.
Харківський національний університет радіоелектроніки,
кафедра мікропроцесорних технологій і систем, м. Харків, Україна
e-mail: mark.vovsianiker@nure.ua

Abstract. This article explores the utilization of Artificial Intelligence (AI) in the field of Field Programmable Gate Arrays (FPGAs). FPGAs are versatile hardware platforms that are programmable and can be tailored for specific applications. With the advancements of AI, integrating AI algorithms into FPGAs can significantly enhance their capabilities and accelerate various computing tasks. This article examines the potential benefits and challenges associated with using AI in FPGA systems. It also discusses the current trends, developments, and applications of AI in FPGA-based systems.

Ключові слова: AI, FPGA, глибоке навчання.

Вступ. Вимоги до апаратного забезпечення для програм штучного інтелекту та машинного навчання розвивалися експоненціально. Оскільки велика кількість обчислень обробляється системами на основі штучного інтелекту та глибокого навчання, існує потреба в більш потужній і надійній системі підтримки для їх виконання [1].

Основна частина. Саме тут з’являються FPGA, які значно прискорили розвиток ШІ та машинного навчання. Постачальники FPGA пропонують платформу для швидкої та ефективної обробки інформації з вихідних даних.

У той час як графічні процесори домінували на ринку протягом досить тривалого часу, а їх апаратне забезпечення агресивно позиціонувалося як найефективніша платформа, FPGA показали себе з точки зору високої продуктивності в програмах глибоких нейронних мереж (DNN), та продемонстрували кращі показники відносно енергоспоживання. FPGA значною мірою адаптовані для роботи з інтенсивним об’ємом даних, наприклад глибокого навчання.

FPGA не нові та існують уже деякий час. Головним відмінним фактором є те, що їх можна змінювати на відміну від інших чіпів . Це дозволяє вказати мову опису обладнання (HDL), яку, у свою чергу, можна налаштувати таким чином, щоб відповідати вимогам конкретних завдань або програм. FPGA також пропонує такі переваги, як використання OpenCL, що робить програмування швидшим і легшим. FPGA також може запропонувати економічно ефективний варіант для прототипів. FPGA набагато гнучкіші і, отже, є гарним вибором для додатків, орієнтованих на клієнта [2].

До переваг слід віднести велику гнучкість, що підходить для додатків ШІ, які швидко розвиваються та змінюються. Наприклад, удосконалення

нейронних мереж забезпечується зміною архітектури. FPGA показують краще співвідношення продуктивності та споживання енергії в порівнянні з графічними процесорами, як апаратної платформи для ШІ. При використанні ШІ та FPGA забезпечується висока точність розрахунків та стає доступним паралельна обробка інформації.

Основні недоліки при використанні FPGA та ШІ це складність програмування та витрата часу на реалізацію проєкту зазвичай більша ніж на аналогічних апаратних платформах.

Штучний інтелект можна використовувати в FPGA для реалізації різноманітних завдань AI. Застосування штучного інтелекту до FPGA може забезпечити високу продуктивність і низьке енергоспоживання, що робить цю комбінацію привабливою для багатьох завдань ШІ [3]. Деякі приклади використання штучного інтелекту в FPGA включають:

1. Прискорення обчислень нейронної мережі. FPGA можна використовувати для реалізації апаратних прискорювачів, які забезпечують більш швидке виконання операцій, пов'язаних з нейронними мережами, таких як згортка, об'єднання (очищення) тощо.
2. Обробка відеопотоків в реальному часі. FPGA можна використовувати для апаратної обробки великих обсягів відеоданих, що швидко призводить до результатів у реальному часі, таких як візуальне виявлення об'єктів або відеоаналітика.
3. Виконання складних алгоритмів ШІ. FPGA можна запрограмувати для запуску складних алгоритмів, таких як машинне навчання або глибоке навчання, що робить можливим розгортання рішень ШІ на апаратному рівні.

Висновки. Однак використання штучного інтелекту в FPGA вимагає розуміння архітектури FPGA, програмування та оптимізації логіки обладнання. Фахівці зі штучного інтелекту та FPGA повинні мати глибокі знання в обох сферах, щоб успішно впроваджувати такі рішення.

Список використаних джерел.

1. Architecture Apocalypse Dream Architecture for Deep Learning Inference and Compute - VERSAL AI Core, URL: https://www.xilinx.com/content/dam/xilinx/support/documents/white_papers/EW2020-Deep-Learning-Inference-AICore.pdf (дата звернення: 01.11.2023).
2. Features of the AI Engine Array Interface URL: https://docs.xilinx.com/r/en-US/am009-versal-ai-engine/Features-of-the-AI-Engine-Array-Interface (дата звернення: 01.11.2023).
3. Білоцерківець О. Г. Тенденції створення системи розумного будинку / О. Г. Білоцерківець, А. О. Зубков, О. В. Зубков // Радіоелектроніка і молодь у XXI столітті: матеріали 25-го : Міжнар. молодіж. форум, 20–22 квітня. 2021 р. – Харків : ХНУРЕ, 2021. – Т. 3. – С. 185–186.

ОГЛЯД ПРИСТРОЮ KRIA KV260 VISION AI ДЛЯ ІНТЕЛЕКТУАЛЬНОГО МАШИННОГО БАЧЕННЯ

студент Столовий І.В., асистент Білоцерківець О.Г.
Харківський національний університет радіоелектроніки,
кафедра мікропроцесорних технологій і систем, м. Харків, Україна
e-mail: ihor.stolovyi@nure.ua

Abstract. Deep Learning (DL) has revolutionized research and development. A couple of problems are that DL requires a lot of power and can be slow. Programmable gate arrays (FPGAs) are excellent candidates for implementing DL algorithms and solutions because they are configurable and offer low latency and low power consumption. Additionally, the versatile FPGA architecture allows users to design application-specific hardware instead of using general-purpose hardware in the processor. An example of these solutions is the Xilinx Kria KV260 Vision AI (KV260) FPGA board. This board contains numerous accelerated programs for performing DL using live camera feed.

Ключові слова: Kria KV260, FPGA, Vitis AI, машинне бачення.

Вступ. Стартовий набір Kria KV260 Vision AI від AMD Xilinx надає готове рішення для розробки розширених додатків для машинного зору, не вимагаючи складних знань про дизайн апаратного забезпечення. Цей початковий набір включає систему-на-модулі (або SOM) K26 із Zynq Ultra-Scale Plus MP-SoC, пам’ять, завантажувач і модуль безпеки.

Основна частина. Kria KV260 виробляється з підтримкою кількох камер, інтерфейсами Onsemi IAS і Raspberry Pi MIPI, вбудованим процесором сигналу зображення, а також виходами HDMI і Display Port. Завдяки численним параметрам підключення до мережі, можливостям розширення PMOD і зростаючій екосистемі прискорених програм розробники можуть запускати свої програми менш ніж за 1 годину [1].

Kria KV260 Vision AI ідеально підходить для розробки рішень для роздрібної аналітики, камер безпеки, розумних міст і машинного бачення, які потім можна розгортати у великій кількості на SOM AMD Xilinx Kria.

Xilinx Kria KV260 Vision — це система-на-модулі (SoM), розроблена для вбудованих програм бачення, оснащена Xilinx Zynq UltraScale+ MPSoC з чотирьохядерним процесором ARM Cortex-A53 і програмованою структурою FPGA, а також різноманітними інтерфейсами та периферійними пристроями для підключення камери та дисплея [2].

Kria KV260 призначений для використання в якості будівельного блоку для розробки периферійних пристроїв, які вимагають обробки в реальному часі та можливостей штучного інтелекту.

Плата також поставляється з підтримкою середовища розробки Vitis AI і ряду програмних і апаратних засобів для полегшення розробки додатків.

Розглянемо деякі характеристики та сильні сторони даного продукту. Описане вище рішення являється універсальним і гнучким. Kria KV260 досягає даних результатів завдяки поєднанні в собі чотирьохядерного процесора ARM Cortex-A53 і програмовану структуру FPGA, яку можна використовувати для реалізації спеціальних прискорювачів або апаратних інтерфейсів [3].

Наступна перевага на ринку даних пристроїв це висока продуктивність даної плати. Kria KV260 розроблено для забезпечення високопродуктивних обчислень і виведення з низькою затримкою, що робить плату придатною для вимогливих периферійних програм, які потребують обробки в реальному часі.

Плата містить багатий набір інтерфейсів. Kria KV260 поставляється з різноманітними інтерфейсами та периферійними пристроями, включаючи Gigabit Ethernet, USB, HDMI, MIPI CSI-2 тощо, що полегшує підключення камер, дисплеїв та інших периферійних пристроїв. Виробник зазначає, що даний продукт простий у використанні. Kria KV260 підтримується середовищем розробки Vitis AI, яке надає ряд програмних і апаратних інструментів для спрощення процесу розробки додатків.

Перейдемо до деяких недоліків, які слід зазначити, а саме це вартість. Kria KV260 є відносно дорогим рішенням порівняно з іншими платформами вбудованого бачення, що може бути перешкодою для деяких користувачів.

Наступним недоліком плати являється енергоспоживання. Kria KV260 має відносно високе енергоспоживання, що може викликати проблеми для периферійних пристроїв, що живляться від батареї.

Висновки. Аналізуючи плюси та мінуси даного апаратно-програмного рішення, то приходимо до висновку, що завдяки таким перевагам, як вища пропускна здатність, менші затримки та будучи гнучким і масштабованим для майбутніх потреб, Kria K26 SOM є гарним вибором для додатків на основі Vision AI для проектів в різних сферах використання машинного зору.

Список використаних джерел.

1. Xilinx White Paper, WP528, “Achieving Embedded Design Simplicity with Kria SOMs,” URL: https://www.xilinx.com/products/som/achieving-embedded-design-simplicity-with-kriasoms.html (дата звернення: 01.11.2023).

2. Xilinx User Guide, UG1089, Kria KV260 Vision AI Starter Kit User Guid. URL:https://www.xilinx.com/cgi-bin/rdoc?t=som-doc;v=latest;d=ug1089-kv260-starter-kit.pdf (дата звернення: 01.11.2023).

3. Білоцерківець, О. Г. Рішення PYNQ для розширення можливостей ПЛІС / О. Г. Білоцерківець, наук. керівник – Свид І. В // Радіоелектроніка та молодь у XXI столітті : тези доповідей 27-го Міжнародного молодіжного форуму, 10–12 травня 2023 р. – Харків : ХНУРЕ, 2023. – Т. 3. – С. 317-318.

ВИКОРИСТАННЯ ESP-EYE ДЛЯ ПОШУКУ РЕЧЕЙ З ЗАЛУЧЕННЯМ AI ТА ФУНКЦІЇ АКТИВАЦІЇ ГОЛОСОМ

асистент Білоцерківець О.Г., к.т.н., доц., Воргуль О.В.
Харківський національний університет радіоелектроніки,
кафедра мікропроцесорних технологій і систем, м. Харків, Україна
e-mail: oleksii.bilotserkivets@nure.ua

Abstract. The application of AI allows the ESP-EYE board to recognize objects and determine their placement in images, potentially allowing you to quickly and efficiently find the desired objects or things. In addition, with the voice activation function, ESP-EYE can respond to commands received through a summoned AI assistant or other voice interface. This system under investigation could find applications in a variety of areas, including home smart home, office automation, and other scenarios where object detection and voice activation can be useful.

Ключові слова: ESP-EYE, AI, машинне бачення, активація голосом.

Вступ. На сьогодні штучний інтелект (ШІ) та можливість голосового керування стають все більш популярними та знаходять практичне застосування в різних сферах людського життя. Дані технології можливо застосувати використовуючи спеціалізовані плати ESP-EYE, розроблені Espressif Systems, для пошуку речей за допомогою штучного інтелекту та голосової активації.

Основна частина. ESP-EYE – це спеціальна плата, розроблена командою інженерів Espressif Systems, яка поєднує в собі основні функції ESP32 (мікроконтролера) із вбудованою камерою та аудіосистемою. Ця розробка має великий потенціал для створення проектів з використанням систем штучного інтелекту, особливо в області розпізнавання об’єктів і голосу [1].

Плата ESP-EYE досить маленька, розміром лише 40 × 20 мм, але даний параметр не впливає на досить гарну продуктивність в своїй сфері. Окрім ESP32-D0WD та 3D-антени, плата містить 4 МБ флеш-пам’яті, 8 МБ PSRAM, 2-мегапіксельну камеру, мікрофон, інтерфейс USB-UART на основі CP2102, два світлодіоди (червоно-білий) і три кнопки (скидання, завантаження та функціональну). Хоч і не змонтований, але місце для роз’єму антени IPEX також присутнє. На платі також є монтажний отвір і кілька регуляторів напруги [2].

Крім того, що ESP-EYE пропонує практично всі чудові функції, які зазвичай є на платформах для розробників на основі ES32, як-от вбудований зв’язок Wi-Fi і Bluetooth, а також просте у використанні середовище розробки, ESP-EYE переносить AIoT на новий рівень. Об’єднавши всі типові периферійні пристрої, необхідні для AIoT, і розмістивши їх на одній платі. Це не тільки робить даний девайс

доступнішим і простішим у використанні для кінцевих користувачів, але також гарантує ідеальну сумісність кожної частини з самого початку, а це означає, що ви можете просто зосередитися на тому, що важливо для вас як розробника – фактично на розробці програмного забезпечення і системи, без необхідності возитися з апаратним забезпеченням [3].

ESP-EYE також підтримує голосову активацію, тож ви можете керувати системою за допомогою голосових команд. Завдяки вбудованому мікрофону та обробці голосу ESP-EYE може розпізнавати ключові фрази чи команди та виконувати певну дію. За допомогою цієї функції можна, наприклад, активувати пошук певних елементів – об’єктів, змінити режим роботи системи або видавати інші команди управління.

Одним із застосувань ESP-EYE є пошук об’єктів за допомогою штучного інтелекту. Наприклад, ви можете створити систему, яка розпізнає об’єкти або голосові команди, отримані камерою та мікрофоном ESP-EYE. Для цього вам потрібно навчити модель машинного навчання (наприклад, за допомогою нейронних мереж) розпізнавати ці об’єкти чи шаблоні голосові команди.

Якщо ESP-EYE отримує зображення від камери або голосову команду, то за допомогою штучного інтелекту, девайс може аналізувати отримані дані та виявляти речі, які відповідають заданим критеріям. Це можуть бути, наприклад, обличчя людей, машини, певні предмети тощо.

Висновки. Перевагою використання ESP-EYE для таких завдань є його компактність, вбудований мікроконтролер ESP32, який дозволяє обробляти вхідні дані та запускати алгоритми ШІ без додаткових зовнішніх ресурсів. Крім того, ESP-EYE підтримує різноманітні бібліотеки та фреймворки машинного навчання, що робить це рішення гнучким для виявлення об’єктів на основі ШІ. Використовуючи ESP-EYE для виявлення об’єктів на основі ШІ, можна реалізувати багато програм, включаючи системи відеоспостереження, ідентифікацію об’єктів, відстеження руху, контроль якості та багато іншого. Пристрій має значний потенціал для розширення можливостей інтелектуальних систем з комп’ютерним зором і штучним інтелектом.

Список використаних джерел.

1. ESP-EYE Getting Started Guide URL: https://github.com/espressif/esp-who/blob/master/docs/en/get-started/ESP-EYE_Getting_Started_Guide.md (дата звернення: 04.11.2023).

2. Documentation ESP-EYE, URL: https://www.espressif.com/en/products/devkits/esp-eye/resources (дата звернення: 05.11.2023).

3. Білоцерківець О. Г. Тенденції створення системи розумного будинку / О.Г. Білоцерківець, А.О. Зубков, О.В. Зубков // Радіоелектроніка і молодь у XXI столітті: матеріали 25-го : Міжнар. молодіж. форуму, 20–22 квітня. 2021 р. – Харків : ХНУРЕ, 2021. – Т. 3. – С. 185–186.

СУЧАСНІ ТЕНДЕНЦІЇ КІБЕРБЕЗПЕКИ БАНКІВСЬКИХ РАХУНКІВ ТА БАНКІВСЬКИХ БУДІВЕЛЬ

асистент Булага В.А., студент Передерій І.А.
Харківський національний університет радіоелектроніки,
комп'ютерної радіоінженерії та систем технічного захисту інформації,
м. Харків, Україна
e-mail: victoria.bulaga@nure.ua, illia.perederii@nure.ua

Abstract. This work is dedicated to the importance of financial security of the banking system of Ukraine and conducting a comprehensive assessment of the current situation. An analysis of the protection and insecurity of the current bank was carried out. The technical details of the bank's security system have been reviewed. Cybersecurity of banking and banking sectors is an important part of our economy. However, cyber-attacks are becoming increasingly sophisticated, and banks are at risk of losing their efforts to protect the data of their clients. By keeping up to date with the latest security technologies and best practices, banks can continue to provide their clients with safe and reliable banking services.

Ключові слова: банківська безпека, кібербезпека , брандмауери, шифрування.

Вступ. Сьогодні кожна людина має свою банківський рахунок у банку, їх безпека є дуже важливою економічним аспектом у розвитку України та взагалі будь-якого континенту. Безпека країни складається з безпеки її структурних і насамперед із безпеки її первинної ланки господарювання [1, 2]. Про це свідчить реакція впливу ринкової конкуренції на економіку країни в цілому та економіку окремого підприємства або банка. Для соціально орієнтованої економіки країни конкуренція є двигуном її розвитку та вдосконалення, і в інтересах держави захистити її всіма можливими засобами. Таким чином, банківська безпека з одного банку є складовою частиною системи національної безпеки, поряд з такими її елементами як технічна безпека, енергетична, військова, екологічна, інформаційна та інше. При цьому слід враховувати, що однією з найбільш небезпечних загроз для економіки України є порушення її фінансово-банківської системи. На сьогодні склалася така ситуація що крадії все більше і більше намагаються хакнути наші картки та забрати ваші гроші, тому мета цього реферату розповісти про те як банківська система захищає ваші збереження так, та що робити якщо ви загубили вашу карту, і як не втратити всі ваші гроші [3, 4].

Банківська система України сьогодні переживає важкі часи, реагуючи, як лакмус, на зміни як в економічному, так і соціально-політичному середовищі країни. Соціально-політична криза в Україні 2013-2014 рр. спричинила глибоку економічну кризу, яка найбільше вплинула на

банківську сферу. До систем безпеки банків завжди пред'являлися підвищені вимоги, і уявити собі банк без охоронної та тривожної сигналізації, системи контролю доступу та відеоспостереження неможливо. Щоб отримати дозвіл на відкриття офісу банку, додаткового офісу та відділення потрібно здати систему безпеки спеціальної комісії. Засоби забезпечення безпеки охоплюють організаційні заходи, інформаційне забезпечення, нормативно-методичні матеріали, роботу з персоналом, засоби фізичної захисту, засоби протидії тощо.

Система контролю доступу до банку. Основне призначення СКД у банку - запобігання проникненню небажаних осіб у приміщення, що охороняються банку. Мережева система контролю доступу до банку повинна працювати під управлінням центрального сервера системи у межах відділення. Бажано, щоб СКД усіх філій та додаткових офісів банку працювали в рамках єдиної системи з адмініструванням та контролем з центрального офісу.

Відео контроль у помешканні та прилеглій території банку. Ситуаційне відеоспостереження для банку – основний інструмент оперативного контролю служби безпеки. При оснащенні банку системами відеоспостереження сповідається принцип тотального контролю всієї території. Виняток становлять лише кабінети в офісній частині банку. Відеокамери контролюють: операційний зал, зону самообслуговування, банкомати та терміналі, касовий вузол і кабіни кас, комора і шляхи проходження грошових коштів, зону інкасації, внутрішній двір і периметр. Сучасні технології дозволяють отримувати зображення високої якості, що дуже важливо для проведення розслідувань та передачі матеріалів до правоохоронних органів. Дозвіл IP-камер і HD-SDI досягає FullHD і більше, а швидкість до 60 к/с. Від такої камери неможливо сховатися. Шкірна деталь того, що сталося буде зафіксована у найдрібніших подробицях.

Відеоспостереження у банку для контролю за обслуговуванням клієнтів та завдань маркетингу. Системи відео аналізу сьогодні пропонують широкий набір інструментів, що допомагають підвищити ефективність та контроль роботи банківського відділення: 1) підрахунок відвідувачів; 2) підрахунок довжини черги.

Програмні та апаратні засоби захисту інформації. Усі платіжні документи СЕП перед відправленням з банку обробляються апаратно-програмними засобами захисту інформації, що забезпечують виконання таких вимог з точки зору безпеки інформації: інформація, що передається, має бути закритою, тобто повідомлення може бути прочитане лише тим, кому воно адресоване; цілісність — випадкове чи навмисне пошкодження повідомлення на етапі його передачі буде виявлене під час його прийому; автентичність відправника (під час прийому повідомлення можна однозначно визначити, хто його відправив).

Низка допоміжних вимог, що дає змогу більш детально аналізувати можливі нестандартні ситуації: 1. Засобами захисту інформації ведеться шифрований арбітражний журнал, в якому зберігається протокол обробки інформації, а також вміст файлів, що обробляються; 2. У шифроване повідомлення включені поля дати та часу обробки.

Основними засобами захисту інформації в СЕП є апаратні засоби. Секретність ключів у них забезпечується технологічно: 1. Ключі зберігаються в спеціальній електронній картці, прочитати їх можна тільки за допомогою спеціального блоку, що виконує процес шифрування інформації. Прочитати ключі іншими засобами неможливо; 2. Електронна картка видається банку з попередньою прив'язкою її до конкретного блоку шифрування цього ж банку; втрачена чи викрадена картка не буде працювати в іншому шифро-блоці (наприклад, в апаратурі іншого банку); 3. У випадку крадіжки одночасно блоку і картки у конкретного банку передбачено режим виключення цієї апаратури зі списку користувачів СЕП; банк може продовжити роботу в СЕП після вирішення юридичних та фінансових питань, пов'язаних з втратою апаратури та отриманням нового комплексу. Найбільш слабким місцем з точки зору безпеки є ділянка підготовки платежів персоналом банку - учасника СЕП. Всі зареєстровані більш-менш успішні спроби НДС були з боку представників банків, що призводило до крадіжки коштів у власного банку, а не в держави чи в інших банках. В усіх цих випадках особи, які робили спроби НДС, мали легальний доступ до системи підготовки та захисту платіжної інформації, причому їх повноваження були перевищені (доступ до багатьох чи навіть до всіх банківських ресурсів системи).

З метою гарантування безпеки інформації на цій ділянці від учасників СЕП вимагається виконання низки організаційних вимог: 1. Допуск тільки довірених осіб до ключових операцій підготовки платіжних документів; 2. Виконання відповідальними особами банку постійного, реального та достатнього контролю за станом бухгалтерського балансу та кореспондентського рахунку банку. Всі повноваження щодо доступу до програмно-апаратних засобів банку недоцільно зосереджувати в особі одного співробітника банку: за кожну ділянку обробки платежів має відповідати окремо уповноважений (адміністратор локальної мережі, адміністратор електронної пошти, відповідальний за роботу АРМ-3 СЕП і т. ін.). Для гарантування безпеки інформації на рівні банків—учасників СЕП пропонується впровадження перехресного накладення електронного підпису на платіжні документи. Банкам пропонується використання програмних засобів, що реалізують цифровий підпис, реалізований на основі алгоритму RSA. Кожний учасник обміну електронними документами має два ключі: 1.Секретний, що повинен ретельно оберігатися від сторонніх осіб і бути відомим тільки його власнику;

2.Відкритий, що розповсюджений в системі і може бути відомим кожному учаснику системи.

Суть алгоритму RSA. 1. В основу електронного цифрового підпису покладено оброблене спеціальним секретним ключем відправника і відкритого ключа отримувача повідомлення.

2. Під час перевірки електронного цифрового підпису програмним комплексом отримувача формується прототип електронного підпису отриманого повідомлення.

3. Отриманий цифровий підпис дешифрується відкритим ключем відправника і секретним ключем отримувача повідомлення і вираховується прототип електронного цифрового підпису.

4. Отриманий прототип порівнюється з обрахованим прототипом електронного цифрового підпису. Збіг цих двох прототипів підпису (отриманого та обчисленого) показує, що повідомлення було підписане зазначеним відправником інформації та отримане у тому ж вигляді, в якому воно було підписане.

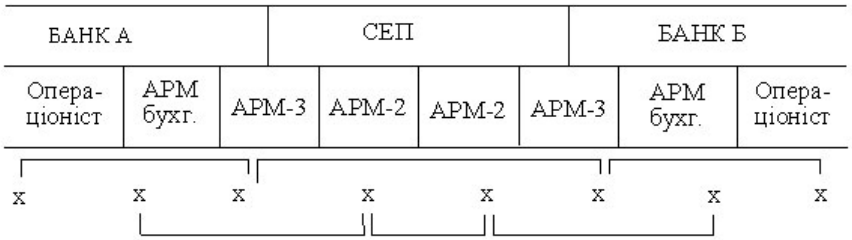


Рисунок 1 – Схема накладення електронного цифрового підпису в СЕП

Висновки. Кібербезпека банківських рахунків та банківських будівель є дуже важливою частиною нашої економіки . Вона є головним пріоритетом для банків, оскільки вони обробляють конфіденційну фінансову інформацію та транзакції. Залишаючись у курсі найновіших технологій безпеки та найкращих практик, банки можуть продовжувати забезпечувати своїм клієнтам безпечні та надійні банківські послуги.

Список використаних джерел.

1. Сердюк С. Л. Цифрова система для митного контролю ручного багажу в аеропортах та зонах підвищеної небезпеки / С. Л. Сердюк, В. А. Булага // Радіоелектроніка та молодь в XXI столітті : матеріали 26-го Міжнародного молодіжного форуму, 24-25 листопада 2022 р. – Харків : ХНУРЕ, 2022. – Т. 3. – С. 132–133.

2. V. Bulaga. Digital System for Customs Inspection of Baggage in High Security Areas // III International Scientific and Practical Conference Theoretical and Applied Aspects of Device Development on Microcontrollers and FPGAs (MC&FPGA), Kharkiv, Ukraine, 2021, pp. 43-46. DOI: 10.35598/mcfpga.2021.015

3. https://rating.zone/chem-obernetsia-dlia-ukrayny-rekordnyj-rost-tsen-na-syrevye-tovary/

4. https://osvita.ua/vnz/reports/bank/20375/

ПОРІВНЯЛЬНИЙ АНАЛІЗ БЕЗПЕКОВИХ ХАРАКТЕРИСТИК ОПЕРАЦІЙНИХ СИСТЕМ WINDOWS І LINUX

асистент Булага В.А., студент Посохова Г.Є.
Харківський національний університет радіоелектроніки,
комп'ютерної радіоінженерії та систем технічного захисту інформації,
м. Харків, Україна
e-mail: victoria.bulaga@nure.ua, hlib.posokhov@nure.ua

Abstract. It is dedicated to considering the comparative characteristics from the point of view of security of the two operating systems Windows and Linux. Windows and Linux are the two most popular operating systems for desktop and server computers. They have a number of similarities and differences in their architectures, features, licensing and popularity. One of the key questions that users and experts often raise is the question of which of these OSes is safer. In this essay, we will try to compare the security of Windows and Linux according to several criteria and give a conclusion about their advantages and disadvantages.

Ключові слова: конфіденційність, цілісність, доступність інформації.

Вступ. Операційна система (ОС) - це низькорівневе програмне забезпечення, яке керує апаратними та програмними ресурсами комп'ютера і забезпечує виконання основних функцій комп'ютера, таких як планування завдань, управління ресурсами, управління пам'яттю, управління периферійними пристроями, мережева взаємодія тощо. Безпека ОС - це здатність ОС захищати свої дані та ресурси від несанкціонованого доступу, зміни або знищення. Безпека ОС є актуальною темою для дослідження, оскільки вона впливає на конфіденційність, цілісність та доступність інформації та послуг, які надаються комп'ютерами [1, 2].

Основні загрози для операційних систем. Шкідливе програмне забезпечення (malware) є однією з найбільших загроз для операційних систем. Воно включає в себе різні типи вірусів, троянські програми, черв'яки, шпигунське програмне забезпечення і багато іншого. Шкідливе ПЗ може пошкодити систему, викрасти конфіденційну інформацію, таку як паролі та особисті дані, або наприклад, зашифрувати файли та вимагати викупу за їх розшифрування. Другою загрозою є вразливості (exploits). Це можуть бути слабкі місця в системі, які зловмисники можуть використовувати для отримання несанкціонованого доступу або виконання шкідливого коду [3-6].

Історичний нарис та особливості Windows. Windows - це ліцензійна операційна система компанії Microsoft із закритим вихідним кодом. Перша версія Windows, відома як Windows 1.0, з'явилася в 1985 році і базувалася на ядрі MS-DOS. Після стартового запуску системи компанія Microsoft почала розробляти нові версії Windows, включаючи перше велике

оновлення та Windows версії 3.0. У 1995 році з'явилася, мабуть, найпоширеніша версія - Windows 95. Вона працювала на 16-бітному ядрі DOS і 32-бітному користувацькому оточенні. Зараз актуальними версіями Windows є: для настільних ПК - Windows 11 (2021 р.); для серверів - Windows Server 2022. Попри величезну кількість нових функцій та можливостей для сучасних обчислень, архітектура ядра Windows практично не зазнала змін. Windows має ряд механізмів безпеки, які спрямовані на запобігання або зменшення ризиків вразливостей та загроз. Деякі з них є: антивірусне програмне забезпечення (antivirus software); брандмауер (firewall); контроль облікових записів користувача (User Account Control, UAC); бітлокер (BitLocker).

Історичний нарис та особливості Linux. Linux - це сімейство Unix-подібних операційних систем, що використовують ядро Linux, яке розробив Лінус Торвальдс. ОС, які використовують ядро Linux, називаються дистрибутивами Linux. Талісманом Linux є пінгвін Tux. Ядро Linux було написано в 1991 році (набагато пізніше, ніж була створена перша версія Windows) Лінусом Торвальдсом, який хотів створити вільне ядро ОС, яке зможе використати будь-хто. Сьогодні ядро Linux містить понад 23 мільйони рядків вихідного коду, яке поширюється (починаючи з 1992 року) під ліцензією вільного програмного забезпечення GNU General Public License. Linux є не однією ОС, а родиною ОС, які мають різні дистрибутиви. Дистрибутив Linux - це набір програмного забезпечення, який містить ядро Linux і додаткові компоненти, такі як графічний інтерфейс користувача (GUI), пакетний менеджер, утиліти командного рядка, офісні програми тощо. Деякі з найбільш відомих дистрибутивів Linux є: Ubuntu - один з найпопулярніших дистрибутивів Linux для настільних і серверних комп'ютерів; Debian - один з найстаріших і найвпливовіших дистрибутивів Linux. Він славиться своєю стабільністю, безпекою і великою кількістю пакетів програмного забезпечення; Fedora - дистрибутив Linux, який спонсорується компанією Red Hat. Він фокусується на інноваціях і включає останні версії програмного забезпечення.

CentOS - дистрибутив Linux, який є безкоштовною версією комерційного Red Hat Enterprise Linux. Він призначений для стабільної і надійної роботи на серверах; Mint - дистрибутив Linux, який базується на Ubuntu і має привабливий і функціональний інтерфейс. Він вважається одним з найлегших у використанні дистрибутивів для початківців.

Linux має ряд механізмів безпеки, які спрямовані на запобігання або зменшення ризиків вразливостей та загроз. В цілому вони схожі з механізмами безпеки інших ОС. Деякими з них є: антивірусне програмне забезпечення (antivirus software); брандмауер (firewall); SELinux (Security-Enhanced Linux)

Порівняння безпеки між Windows і Linux. Одним з найбільш важливих факторів, які впливають на безпеку ОС, є захист від шкідливого програмного забезпечення. Шкідливе ПЗ може заражати систему через інтернет, електронну пошту, USB-пристрої або інші канали. Шкідливе ПЗ може виконувати різні дії, такі як шпигунство, крадіжка даних, шифрування файлів, використання ресурсів системи для майнінгу криптовалют або DDoS-атак. Windows і Linux мають різний рівень захисту від шкідливого ПЗ. Загалом, Windows є більш вразливою ОС, ніж Linux, з таких причин: Windows має більшу частку ринку на настільних комп'ютерах, тому є більш привабливою цілю для хакерів і зловмисників; Windows має закритий вихідний код, тому її помилки і недоліки не завжди швидко виявляються і усуваються; Windows має слабку систему прав користувача, тому багато користувачів працюють під адміністраторським обліковим записом, який дає повний доступ до системи.; Windows має багато сумісностей з різними форматами файлів і протоколами мережевого обміну, тому її можна легко інфікувати через відкриття небезпечних документів або підключення до небезпечних мереж. Linux є більш безпечною ОС, ніж Windows, з таких причин: Linux має відкритий вихідний код, тому її помилки і недоліки швидко виявляються і усуваються спільнотою розробників і користувачів; Linux має сильну систему прав користувача, тому багато користувачів працюють під звичайним обліковим записом, який має обмежений доступ до системи; Linux має менше сумісностей з різними форматами файлів і протоколами мережевого обміну, тому її важче інфікувати через відкриття небезпечних документів або підключення до небезпечних мереж.

Система користувачів та доступ до ресурсів. Іншим важливим фактором, який впливає на безпеку ОС, є система користувачів та доступ до ресурсів. Система користувачів визначає, хто може використовувати систему і які дії вони можуть виконувати. Доступ до ресурсів визначає, хто може читати, писати або виконувати певні файли або каталоги. Windows і Linux мають різну систему користувачів та доступ до ресурсів. Загалом, Linux має більш сильну і гнучку систему користувачів та доступ до ресурсів, ніж Windows, Оновлення та патчі безпеки Ще одним важливим фактором, який впливає на безпеку ОС, є оновлення та патчі безпеки. Оновлення та патчі безпеки - це програми, які виправляють помилки або недоліки в код ОС або додатках, які можуть бути використані для атак на систему. Оновлення та патчі безпеки також можуть додавати нові функції або покращувати продуктивність системи. Windows і Linux мають різну систему оновлень та патчів безпеки. Загалом, Linux має більш швидку і прозору систему оновлень та патчів безпеки, ніж Windows.,з таких причин: Windows має закритий вихідний код, тому її оновлення та патчі безпеки залежать від компанії Microsoft; Linux має відкритий вихідний код, тому її

оновлення та патчі безпеки залежать від спільноти розробників і користувачів.

Висновки. Windows є більш простою і популярною ОС для настільних комп'ютерів, але є більш вразливою ОС, ніж Linux, через свій закритий код, слабку систему прав користувача і багато сумісностей з різними форматами файлів і протоколами мережевого обміну. Windows має вбудовані механізми безпеки, але вони не завжди ефективні або достатні для захисту системи. Windows також має повільну і неефективну систему оновлень та патчів безпеки, яка залежить від компанії Microsoft. Linux є більш складною і менш популярною ОС для настільних комп'ютерів, але є більш безпечною, через свій відкритий код, сильну систему прав користувача і менше сумісностей з різними форматами файлів і протоколами мережевого обміну. Linux також має вбудований брандмауер Iptables і модуль безпеки SELinux, які дозволяють контролювати мережевий трафік і доступ до системних ресурсів.

Список використаних джерел.

1. Сердюк С. Л. Цифрова система для митного контролю ручного багажу в аеропортах та зонах підвищеної небезпеки / С. Л. Сердюк, В. А. Булага // Радіоелектроніка та молодь в XXI столітті : матеріали 26-го Міжнародного молодіжного форуму, 24-25 листопада 2022 р. – Харків : ХНУРЕ, 2022. – Т. 3. – С. 132–133.

2. V. Bulaga. Digital System for Customs Inspection of Baggage in High Security Areas // III International Scientific and Practical Conference Theoretical and Applied Aspects of Device Development on Microcontrollers and FPGAs (MC&FPGA), Kharkiv, Ukraine, 2021, pp. 43-46. DOI: 10.35598/mcfpga.2021.015

3. Aldossary, S., Almhdood, F., Alhothail, B., Alshimer, M., Alotaibi, S., Alqahtani, R., Aldossary, T., Alshammari, L., Almuqbel, S., Albatli, L., & Nagy, N. (2023). Comparison between Windows and Linux operating system by analyzing the related security features. Journal Not Specified, 1(0). https://doi.org/10.13140/RG.2.2.33615.30886

4. Awan, M. T. (2022). Linux vs. Windows: A comparison of two widely used platforms. International Journal of Computer Science and Network Security, 22(1), 1-

5. Guru99. (n.d.). Linux vs Windows: Key difference between them. Retrieved October 30, 2022, from https://www.guru99.com/linux-differences.html

6. Linux Journal. (2020, June 19). Linux vs. Windows: What's the difference in 2022? Retrieved October 30, 2022, from https://www.linuxjournal.com/content/linux-vs-windows

АНАЛІЗ РІВНЯ БЕЗПЕКИ ВЕБ-СЕРВІСІВ

асистент Булага В.А., студент Кушнарьов А.О.
Харківський національний університет радіоелектроніки,
комп'ютерної радіоінженерії та систем технічного захисту інформації,
м. Харків, Україна
e-mail: victoria.bulaga@nure.ua, artem.kushnarov@nure.ua

Abstract. This work is devoted to the technical security of web services, which plays a key role in protecting information and ensuring the reliability of web services. It covers a wide range of technologies, methods and practices aimed at preventing unauthorized access, hacking, data leakage and other security threats that can occur in the online environment.

Ключові слова: аутентифікація, шифрування, контроль доступу, моніторинг.

Вступ. Технічне забезпечення безпеки веб-сервісів включає в себе розробку та застосування захисних механізмів, які забезпечують цілісність, конфіденційність та доступність даних, а також запобігають вразливостям та атакам з боку зловмисників [1-3]. Це охоплює такі аспекти, як аутентифікація користувачів, шифрування, контроль доступу, моніторинг і виявлення вторгнень, а також розробка безпечного програмного забезпечення [4, 5].

У сучасному світі, де технології інтернету займають центральне місце у багатьох аспектах життя, безпека веб-сервісів стала критично важливою. Зростаюча кількість користувачів, обмін конфіденційною інформацією, електронна комерція, онлайн-банкінг, доступ до особистих даних - все це робить безпеку веб-сервісів необхідною складовою для забезпечення довіри та захисту користувачів. Недостатня безпека веб-сервісів може призвести до серйозних наслідків, включаючи втрату конфіденційної інформації, порушення приватності, фінансові втрати, психологічну шкоду та пошкодження репутації. Нестача довіри в користувачів може призвести до втрати клієнтів та негативного впливу на ділову репутацію організації. Тому, забезпечення безпеки веб-сервісів є важливим завданням для розробників, підприємств і організацій, що працюють у цифровому просторі. Воно вимагає постійного вдосконалення, використання найсучасніших технологій та розуміння потенційних загроз, щоб забезпечити безпеку та надійність веб-сервісів для всіх користувачів.

Веб-атаки та їхні види. 1. Кросс-сайтовий скриптинг (XSS); 2.Впровадження SQL-запитів (SQL Injection); 3. DDoS-атаки (Distributed Denial of Service); інжиніринг. Які представлені на рис.1.

На додаток до вищезазначених загроз, існують інші потенційні загрози, що можуть вплинути на безпеку веб-сервісів. Деякі з них включають вразливості програмного забезпечення, використання слабких

алгоритмів шифрування, атаки на сесії користувачів, недостатні контролі доступу до системи, а також зловживання привілеїв та експлуатацію системних дефектів.

Засоби технічного забезпечення безпеки веб-сервісів. Засоби технічного забезпечення безпеки веб-сервісів включають різноманітні технології, методи та практики, що допомагають захистити веб-сервіси від загроз і забезпечити безпеку інформації.

Аутентифікація та авторизація. Аутентифікація - це процес перевірки ідентифікації користувача або системи. Це може включати використання паролів, біометричних даних, одноразових кодів тощо. Рекомендується використовувати сильні паролі та вимагати їх регулярну зміну.

Авторизація - це процес надання прав доступу до ресурсів або функцій після успішної аутентифікації. Вона гарантує, що користувачі мають лише необхідні привілеї і не можуть отримати несанкціонований доступ до конфіденційної інформації.

Використання протоколів HTTPS / SSL / TLS: Шифрування комунікації між веб-сервером і клієнтом, що запобігає перехопленню та зловживанню інформацією.

Рисунок 1 – Використання протоколів HTTPS / SSL / TLS

Розробка безпечного програмного забезпечення. Розробка безпечного програмного забезпечення є однією з найважливіших стратегій для забезпечення безпеки веб-сервісів. Для досягнення цієї мети, розробники повинні враховувати різні аспекти безпеки під час процесу розробки програмного забезпечення. Ось кілька детальних кроків, які можна вжити для розробки безпечного програмного забезпечення:

1. Використання безпечних програмних мов та фреймворків; 2. Перевірка безпеки коду; 3. Безпечна обробка даних; 4. Захист аутентифікації та авторизації; 5. Захист від вразливостей переповнення буфера; 6. Безпечна обробка помилок; 7. Регулярні оновлення та патчі.

Тестування на проникнення та перевірка на вразливості:

1) планування тестування; 2) Виявлення вразливостей; 3) аналіз результатів; 4) виправлення вразливостей; 5) перевірка усунення вразливостей; 6) звіт та документація.

Тестування на проникнення та перевірка на вразливості є постійним процесом, оскільки загрози безпеки постійно еволюціонують.

Контроль доступу та обмеження привілеїв користувачів є важливим

аспектом технічного забезпечення безпеки веб-сервісів. Ця стратегія включає в себе набір заходів, спрямованих на забезпечення тільки авторизованого доступу до ресурсів веб-сервісу та обмеження привілеїв користувачів. Контроль доступу та обмеження привілеїв користувачів є ключовим елементом технічного захисту веб-сервісів. Ці заходи допомагають запобігати несанкціонованому доступу, зламам та використанню недозволених функцій системи, забезпечуючи безпеку та конфіденційність веб-сервісу.

Системи моніторингу та реагування на інциденти. Системи моніторингу та реагування на інциденти є необхідною складовою технічного забезпечення безпеки веб-сервісів. Ця стратегія передбачає наявність інструментів та процесів, які надають можливість виявляти аномальну активність, потенційні загрози та реагувати на них вчасно. Системи моніторингу та реагування на інциденти допомагають виявляти, аналізувати та ефективно реагувати на загрози безпеки веб-сервісів. Вони грають важливу роль у забезпеченні безпеки та зменшенні можливих наслідків інцидентів. Правильна конфігурація та постійне поновлення цих систем є ключовими факторами для успішного захисту веб-сервісу від загроз безпеки.

Висновки. Технічне забезпечення безпеки веб-сервісів є надзвичайно важливим для забезпечення захисту від різноманітних загроз у сучасному світі. Застосування стратегій технічного захисту, таких як розробка безпечного програмного забезпечення, тестування на проникнення, контроль доступу та обмеження привілеїв користувачів, а також використання систем моніторингу та реагування на інциденти, допомагають зменшити ризик вразливостей та забезпечити безпеку веб-сервісу. Усі стратегії технічного забезпечення безпеки веб-сервісів повинні застосовуватися в комплексі та постійно оновлюватися, оскільки загрози безпеки постійно еволюціонують. Лише завдяки цілісному підходу та постійному вдосконаленню можна забезпечити надійний рівень безпеки веб-сервісу і захистити користувачів від потенційних загроз.

Список використаних джерел.

1. https://www.dnsstuff.com/sql-injection

2. http://dspace.onua.edu.ua/bitstream/handle

3.https://ela.kpi.ua/bitstream/123456789/22234/1/Zahist_web_servisiv_Laboratornyi_praktikum.pdf

4. Сердюк С. Л. Цифрова система для митного контролю ручного багажу в аеропортах та зонах підвищеної небезпеки / С. Л. Сердюк, В. А. Булага // Радіоелектроніка та молодь в XXI столітті : матеріали 26-го Міжнародного молодіжного форуму, 24-25 листопада 2022 р. – Харків : ХНУРЕ, 2022. – Т. 3. – С. 132–133.

5. V. Bulaga. Digital System for Customs Inspection of Baggage in High Security Areas // III International Scientific and Practical Conference Theoretical and Applied Aspects of Device Development on Microcontrollers and FPGAs (MC&FPGA), Kharkiv, Ukraine, 2021, pp. 43-46. DOI: 10.35598/mcfpga.2021.015

ПРОГРАМНІ ЗАСОБИ АНАЛІЗУ ЛОКАЛЬНИХ МЕРЕЖ ЩОДО УРАЗЛИВОСТЕЙ

асистент Булага В.А., студент Патлан Є.О.
Харківський національний університет радіоелектроніки,
комп'ютерної радіоінженерії та систем технічного захисту інформації,
м. Харків, Україна
e-mail: victoria.bulaga@nure.ua, yehor.patlan@nure.ua

Abstract. This work is devoted to the analysis of vulnerabilities of local networks through software tools. The goal is to investigate potential threats and identify weaknesses in network security. The researcher uses software tools to automate network scanning, identify vulnerabilities, and provide recommendations for improving security.

Ключові слова: локальна мережа, уразливості, аналіз.

Вступ. В сучасному інформаційному суспільстві локальні мережі (ЛМ) відіграють важливу роль у забезпеченні обміну даними, ресурсами та послугами між комп'ютерами та пристроями в межах певного фізичного простору [1-3], такого як офіс, школа, будинок, підприємство тощо [4, 5].

Загальне визначення локальних мереж та їх важливість:

- локальна мережа (ЛМ) - це комп'ютерна мережа, що об'єднує комп'ютери, сервери та інші пристрої в межах обмеженого фізичного простору, такого як офіс, школа або будинок;
- ЛМ відіграють важливу роль у сучасному світі, забезпечуючи ефективну комунікацію та обмін інформацією;
- уразливості в ЛМ можуть призвести до витоку конфіденційної інформації, несанкціонованого доступу до системи, атак зловмисників та інших негативних наслідків;
- в рамках даної роботи ми розглянемо програмні засоби, які призначені для аналізу уразливостей в локальних мережах.

Таким чином, метою даної роботи є дослідження програмних засобів аналізу локальних мереж щодо уразливостей та їх впливу на забезпечення безпеки ЛМ.

Основна частина. Локальна мережа зазвичай складається з набору комп'ютерів, які підключені до спільної мережевої інфраструктури, такої як комутатори або маршрутизатори. Комп'ютери в ЛМ можуть обмінюватись інформацією, виконувати спільні завдання, друкувати документи на спільному принтері та забезпечувати спільний доступ до ресурсів, таких як файли або бази даних. Один з основних принципів ЛМ - це локальність, тобто обмеженість фізичного простору.

Уразливість в контексті локальних мереж означає наявність слабкого місця або потенційної вразливості, яка може бути використана зловмисниками для несанкціонованого доступу, пошкодження або

викрадення даних, переривання послуг або інших зловмисницьких дій. Уразливості можуть виникати як через технічні недоліки в мережевому обладнанні та програмному забезпеченні, так і через людські помилки або необережне використання ресурсів.

Деякі загальні типи уразливостей, що можуть виявитися в локальних мережах, включають:

- недостатня аутентифікація та авторизація;
- незахищені мережеві протоколи;
- недостатня фізична безпека;
- недостатня оновлення та патчі;
- соціальна інженерія (люди можуть стати слабким ланцюжком у безпеці мережі, коли їхні дії або недії допомагають зловмисникам отримати несанкціонований доступ).

Наведемо огляд деяких таких програмних засобів.

1. Nessus: Nessus є одним з найпопулярніших програмних засобів для аналізу уразливостей.
2. OpenVAS: OpenVAS (Open Vulnerability Assessment System) - це відкрите програмне забезпечення для аналізу уразливостей в мережах.
3. Nmap: Nmap (Network Mapper) - це інструмент для сканування мереж і виявлення живих хостів, відкритих портів та розпізнавання операційних систем.
4. Wireshark: Wireshark - це популярний аналізатор мережевих пакетів, який дозволяє перехоплювати, аналізувати та відстежувати мережевий трафік.
5. Metasploit: Metasploit - це потужний фреймворк для тестування на проникнення, який включає в себе велику кількість експлойтів, модулів та інструментів для використання в різних типах атак.
6. Nikto: Nikto - це веб-сканер з відкритим вихідним кодом, спеціально розроблений для виявлення потенційних уразливостей на веб-серверах.
7. Aircrack-ng: Aircrack-ng - це набір інструментів для аналізу бездротових мереж, зокрема Wi-Fi.
8. Burp Suite: Burp Suite - це інтегроване середовище тестування вразливостей додатків, спеціально розроблене для виявлення уразливостей в веб-додатках.
9. Acunetix: Acunetix - це інструмент для автоматичного сканування веб-додатків з метою виявлення потенційних уразливостей.

Ці програмні засоби представляють лише частину широкого спектру інструментів, доступних для аналізу уразливостей в локальних мережах.

Висновки. У даній роботі було розглянуто тему "Програмні засоби аналізу локальних мереж щодо уразливостей. У процесі дослідження було встановлено, що локальна мережа є важливою складовою сучасної інформаційної інфраструктури. Вона забезпечує зв'язок між комп'ютерами та пристроями, що дозволяє обмінюватися даними та використовувати

спільні ресурси. Однак, разом з розвитком технологій, зростають і загрози безпеці локальних мереж. Уразливості локальних мереж можуть виникати з різних причин, включаючи помилки в конфігурації, недостатній рівень захисту, вразливість програмного забезпечення та недосконаліть протоколів мережі. Ці уразливості можуть призвести до несанкціонованого доступу, пошкодження даних та інших шкідливих наслідків. Застосування програмних засобів аналізу локальних мереж є важливим кроком у забезпеченні безпеки і захисту мережі.

Список використаних джерел.

1. Бурячок В. Л. Технології забезпечення безпеки мережевої інфраструктури. [Підручник] / В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. – К.: КУБГ, 2019. – 218 с.

2. N. Jovanovic. (березень 2006). TxtForum: script injection vulnerability. http://www.seclab.tuwien.ac.at/advisories/TUVSA-0603-004.txt

3. Вишня В. Б. Основи інформаційної безпеки : навч. посібник / В. Б. Вишня, О. С. Гавриш, Е. В. Рижков. Дніпро : Дніпроп. держ. ун-т внутріш. справ, 2020. 128 с.

4. Сердюк С. Л. Цифрова система для митного контролю ручного багажу в аеропортах та зонах підвищеної небезпеки / С. Л. Сердюк, В. А. Булага // Радіоелектроніка та молодь в XXI столітті : матеріали 26-го Міжнародного молодіжного форуму, 24-25 листопада 2022 р. – Харків : ХНУРЕ, 2022. – Т. 3. – С. 132–133.

5. V. Bulaga. Digital System for Customs Inspection of Baggage in High Security Areas // III International Scientific and Practical Conference Theoretical and Applied Aspects of Device Development on Microcontrollers and FPGAs (MC&FPGA), Kharkiv, Ukraine, 2021, pp. 43-46. DOI: 10.35598/mcfpga.2021.015

ОГЛЯД ІННОВАЦІЙНИХ РІШЕНЬ XILINX

студент Мачоніс Т.С., к.т.н., доц. Свид І.В.
Харківський національний університет радіоелектроніки,
кафедра мікропроцесорних технологій і систем, м. Харків, Україна
e-mail: tomas.machonis@nure.ua

Abstract. Xilinx develops flexible and adaptive platforms that enable rapid innovation in a variety of technologies from the cloud to the edge and intelligent end devices.

Ключові слова: Xilinx, FPGA, CPLD, ASIC, ISE, Vivado, AMD.

Вступ. Xilinx – американська компанія, найбільший виробник у світі напівпровідникових програмованих логічних пристроїв (FPGA, CPLD, ASIC), також займається: розробкою програмних модулів і бібліотек інтелектуальних ядер для кристалів; розробкою пакетів програмного забезпечення для програмування логічних пристроїв (ISE, Vivado, Vitis), призначених для роботи в середовищі операційних систем (ОС) Windows і Linux. Xilinx не має власних виробничих потужностей, а для виготовлення програмованих логічних пристроїв компанія співпрацює з різними виробниками інтегральних схем, такими як Samsung, TSMC, UMC тощо. 27 жовтня 2020 корпорація AMD оголосила про злиття з компанією Xilinx. 14 лютого 2022 р. AMD оголосила про завершення придбання Xilinx у рамках угоди з усіма акціями [1].

Основна частина. Xilinx заснована у 1984 році та винайшла польову програмовану вентильну матрицю, і була першою компанією з виробництва напівпровідників (рис. 1). У 1985 році започаткувала серійне виробництво програмованих користувачем вентильних матриць (FPGA). Впровадження у виробництво FPGA дало новий поштовх розвитку техніки, бо це дозволило розробнику електронної техніки реконфігурувати кристал на робочому місці [1].

Перелік основний інновацій та здобутків Xilinx представлено на рисунку 1:

1984 рік – World’s First FPGA;
1999 рік – First High End High Capacity FPGA;
2001 рік – First FPGA with Integrated SerDes and Processor;
2012 рік – First 3D FPGA and Zynq Dual HW Programmable SoC;
2017 рік – First Zynq ® MPSoC & RFSoC;
2018 рік – ALVEO ™ Data Center Accelerator Card;
2019 рік – VERSAL ® First Adaptive Compute Acceleration Platform;
2021 рік – ALVEO SN100 First Composable, Adaptable SmartNIC;
2021 рік – KRIA SOM Adaptive System on Module with First Embedded App Store.

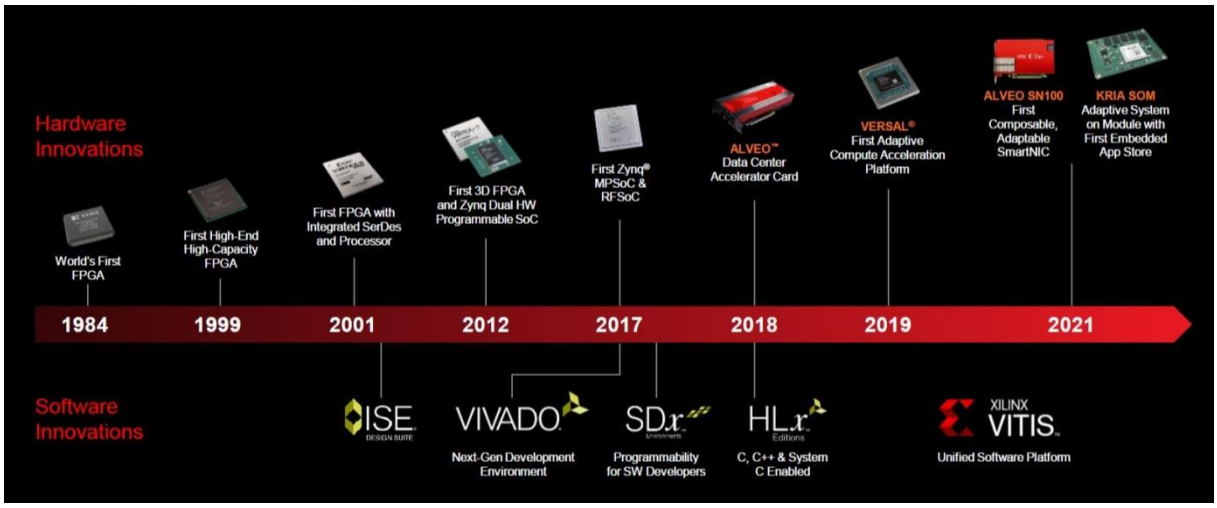


Рисунок 1 – Список інновацій Xilinx [1]

Xilinx розробила та вивела на ринок у 1984 році першу польову програмовану вентильну матрицю, тим самим вони породили нову галузь, яка дозволила створювати індивідуальні рішення для різних ринків. Через десять років, у 1994 році, Xilinx випустила Virtex ® FPGA, зробивши прорив в архітектурі та продуктивності їх оригінальної FPGA.

У 2012 році Xilinx представила перший 28-нм пристрій Zynq ®, повноцінну SoC з підтримкою прикладних процесорів і повною підсистемою кешу, контролера пам’яті, периферійних пристроїв, логіки FPGA, блоків DSP і блоків SerDes. Zynq SoC Xilinx створив нові можливості для роботи з перефірийними функціями.

Друге покоління Zynq SoC (гетерогенна MPSoC) з’явилося в 2017 році та додало нові механізми обробки з метою створення правильних апаратних механізмів для правильних завдань, оптимізації вимог до обробки складних систем. Платформу було розширено за допомогою високошвидкісних прямих радіочастотних перетворювачів даних для підтримки адаптивних радіоплатформ, розроблених відповідно до нових стандартів бездротових додатків.

У 2018 році Xilinx анонсувала карти прискорення центрів обробки даних Alveo™, які спростили розробку та розгортання високопродуктивного, адаптованого прискорення FPGA в центрі обробки даних.

На сьогодні, Versal є першою адаптивною платформою прискорення обчислень (ACAP). Versal ® ACAP була створена з нуля як гетерогенна, гнучка платформа, яка підтримує кілька доменно-спеціальних архітектур (DSAs) і обчислювальних структур, включаючи ядра процесора, програмовану логіку та масив AI інженерії. Перевагою ACAP є його функціональність, як багатоядерної SoC загального призначення, яка включає додаткові програмовані апаратні та програмні механізми для

оптимального співвідношення потужності та продуктивності.

З розвитком продуктів Xilinx змінила свої пропозиції від пристроїв до платформ. Почавши з програмованих логічних мікросхем у перші роки, Xilinx перейшла до вбудованих платформ для розробників SoC і стеків програмного забезпечення для розробників прикладного програмного забезпечення.

Сьогодні платформи Xilinx обслуговують розробників і науковців з обробки даних і пропонують численні можливості для проектування і широкий спектр методів розгортання проектів [2-7].

Висновки. Xilinx розробляє гнучкі й адаптивні платформи, які забезпечують швидке впровадження інновацій у різноманітних технологіях від хмари до периферії та інтелектуальних кінцевих пристроїв.

Об’єднання AMD і Xilinx створить ще сильнішу AMD [1]: Xilinx пропонує провідні технології в галузі FPGA, адаптивні SoC, механізми штучного інтелекту та досвід програмного забезпечення, що дозволяє AMD пропонувати найпотужніший портфель високопродуктивних і адаптивних обчислювальних рішень у галузі хмарних, периферійних та інтелектуальних пристроїв.

Список використаних джерел.

1. https://www.amd.com/en.html

2. В.В. Семенець, І.В. Свид, О.В. Зубков, О.В. Воргуль, Н.В. Бойко, В.С. Чумак. Методичні та технічні аспекти реалізації онлайн лабораторії з проектування пристроїв. // Збірник матеріалів ІІ форуму «Автоматизація, електроніка та робототехніка. Стратегії розвитку та інноваційні технології» до 90-річчя ХНУРЕ. – Харків, ХНУРЕ, 2020. – С. 45-48.

3. В.В. Семенець, І.В. Свид, О.В. Зубков, О.В. Воргуль. Методика розробки та впровадження освітньої компоненти щодо проектування пристроїв. // Збірник матеріалів ІІ форуму «Автоматизація, електроніка та робототехніка. Стратегії розвитку та інноваційні технології» до 90-річчя ХНУРЕ. – Харків, ХНУРЕ, 2020. – С. 40-44.

4. I. Svyd, O. Vorgul, V. Semenets, O. Zubkov, V. Chumak, N. Boiko. Special Features of the Educational Component “Design of Devices on Microcontrollers and FPGA”. // II International Scientific and Practical Conference Theoretical and Applied Aspects of Device Development on Microcontrollers and FPGAs, Kharkiv, Ukraine, 2020, pp. 55-57. doi: 10.35598/mcfpga.2020.017.

5. O. Vorgul, I. Svyd, V. Semenets, O. Zubkov. Enhancement of the Laboratory Workshop on FPGA: Opportunities and Prospects. // IV International Scientific and Practical Conference Theoretical and Applied Aspects of Device Development on Microcontrollers and FPGAs, Kharkiv, Ukraine, 2022, pp. 29-31, doi: 10.35598/mcfpga.2022.010.

6. I. Svyd, V. Semenets, O. Vorgul, I. Shevtsov. Aspects of STEM Education in the Design of Devices on Microcontrollers and FPGAs. // IV International Scientific and Practical Conference Theoretical and Applied Aspects of Device Development on Microcontrollers and FPGAs, Kharkiv, Ukraine, 2022, pp. 52-54, doi: 10.35598/mcfpga.2022.018.

7. В. Чумак, І. Свид. Створення модуля VHDL-опису при проектуванні цифрових систем на ПЛІС в Xilinx ISE Design Suite. // Перспективні напрямки сучасної електроніки, інформаційних і комп'ютерних систем (MEICS-2019). – Дніпро, Дніпровський національний університет імені Олеся Гончара, Кременчук: ПП Щербатих О. В., 2019. – С. 94-95.

КЕРУВАННЯ МІКРОКОНТРОЛЕРОМ ЗА ДОПОМОГОЮ МОВНОГО КАНАЛУ

студент Літовченко О.А., канд. техн. наук, доц. Воргуль О.В.
Харківський національний університет радіоелектроніки,
кафедра мікропроцесорних технологій і систем, м. Харків, Україна
e-mail: oleksii.litovchenko@nure.ua

Abstract. The possibility of building a small-sized system on a microcontroller with voice control is being considered. The required set of functions and the need for special hardware are analyzed.

Ключові слова: мікроконтролер, керування, мовний канал.

Вступ. Використовуючи сучасний 32 бітний мікроконтролер ми наближаємо майбутнє. Можна пофантазувати про пристрій, що керується голосом і голосом надає відповідь [1, 2]. Так, великі комп'ютери із помічником, що має підключення до глобальної мережі та розмовний модуль це вже буденність. А використовуючи мікроконтролер від STM можна принаймні уявити, яка буде складність проекту і, намагаючись реалізувати таке, наблизити майбутнє [3-7].

Основна частина. Власно кажучи, на перший погляд, для того, щоб реалізувати керування голосом у сучасних мікроконтролерів все вже присутнє [1]. Бо для сприйняття мови необхідні принаймні мікрофон та АЦП, щоб перетворити мову в електричний, а надалі в цифровий вигляд. І для генерації мови мікроконтролером є необхідність у ЦАП та звуковідтворююче обладнання – гучномовець (рис. 1).

Рисунок 1 – Голосове керування

Але така система буде лише цифровим оброблювачем мови. Та аж ніяк не системою із мовним керуванням. Для мовного керування необхідно ще присутність модуля аналізу мови та розпізнавання команд з потоку мови.

Здається, що простіше всього може бути реалізована підсистема відповіді мікроконтролера, тобто звуковідтворення. Відповіді можуть бути просто записані в пам'ять та відтворюватись в необхідний момент. Таку

підсистему можна довго і успішно вдосконалювати, додаючи їй нових корисних рис. Так, для зменшення обсягу пам'яті можна зберігати повідомлення у стиснутому вигляді, передбачивши кодек для швидкого або економного відтворення потоку даних що подається на ЦАП або ШІМ.

Щодо розпізнавання мови, як команди, то такий процес є знатно складнішим. І навіть на перший погляд здається неоптимальним підхід, у якому ми спробуємо відрізнити звуки з запису мови що отримано з мікрофону, а далі перетворювати набори звуків на слова та заходитись вчити мікроконтролер відрізняти команди.

Найпростішою системою може бути випадок обмеженої кількості команд. Такий підхід може виявитись хибним для вдосконалення, бо не є загальним. Якщо в майбутньому виявиться за необхідне додати декілька функцій, можливо, прийдеться переробляти всю систему в цілому.

З точки зору більш багатого за можливостями підходу, використання нейронних мереж дозволяє аналізувати голос, розпізнавати різні мови і з них виділяти команди, але сукупність необхідної потужності, доступу до Інтернету, часу та ціни може виявитись завеликими для малогабаритного пристрою, що є в центрі уваги цієї роботи.

Тому в спрощеному варіанті пристрій не зможе розуміти мову. Він зможе лише розрізняти команди. Цими командами для мікроконтролера можуть бути лише номер функції що необхідно виконати – відкрити двері або вимкнути світло.

По-перше, для розпізнавання декількох команд буде достатньо підтримки невеликої нейронної мережі, а такі можливості для STM вже реалізовано [2].

По-друге, це виклик підтвердити або спростувати, що може бути і інше рішення. Наприклад, можна спробувати побудувати систему у вигляді, наданому на рисунку 2.

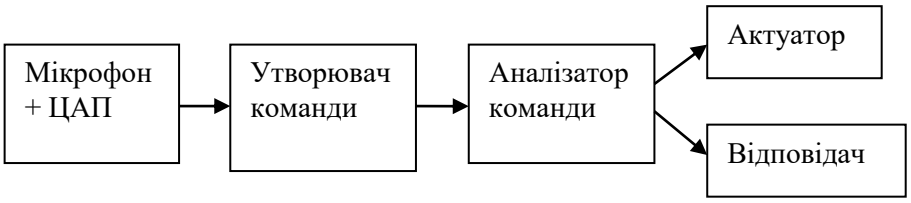


Рисунок 2 – Структурна схема системи з МК та голосовим керуванням

Блок "Утворювач команди" сприймає набір цифрових даних з мікрофону з мінімальною обробкою. Він повинен лише розрізнити команди одну від одної. Детальна розробка такого модуля є окремою темою, завершення якої і наблизить майбутнє.

Висновки. Керування голосом виглядає багатообіцяючим, якщо буде гнучким та не вимагатиме забагато ресурсів. Наразі є певні обмеження

щодо розпізнавання голосових команд, але технології розвиваються швидко, скоріш за все, найближчим часом будемо мати нові перспективні варіанти рішення даної задачі. Наявність голосового керування є перспективним напрямком для великих та малих систем. Роботу над цим напрямком буде продовжено.

Список використаних джерел.

1. STM32 F407 datasheet https://www.st.com/resource/en/datasheet/ stm32f405rg.pdf

2. Free tool for edge AI developers https://www.st.com/resource/ en/datasheet/ stm32f405rg.pdf

3. Програмування мікроконтролерів STM32 в середовищі STM32CubeIDE в прикладах і задачах: Навч. посіб. / О. В. Зубков, І. В. Свид, О. В. Воргуль, В. В. Семенець. Дніпро : ЛІРА ЛТД, 2022. 144 с.

4. O. Zubkov, I. Svyd, O. Vorgul. Study of the Effectiveness of Using Nextion Displays in Projects Based on STM32 Microcontrollers // V International Scientific and Practical Conference Theoretical and Applied Aspects of Device Development on Microcontrollers and FPGAs (MC&FPGA-2023), Kharkiv, Ukraine. pp. 6-9.

5. O. Vorgul, I. Svyd, O. Zubkov. Pseudo Random Value Generation in STM32 Cube // V International Scientific and Practical Conference Theoretical and Applied Aspects of Device Development on Microcontrollers and FPGAs (MC&FPGA-2023), Kharkiv, Ukraine. pp. 46-48.

6. O. Zubkov, I. Svyd, O. Vorgul. Features of the Implementation of an Over/Under Voltage Relay on STM 32 Microcontrollers. // IV International Scientific and Practical Conference Theoretical and Applied Aspects of Device Development on Microcontrollers and FPGAs (MC&FPGA-2022), Kharkiv, Ukraine, 2022, pp. 6-8, doi: 10.35598/mcfpga.2022.001

7. O. Zubkov, I. Svyd, O. Vorgul. Features of the Digital Filters Implementation on STM32 Microcontrollers. // III International Scientific and Practical Conference Theoretical and Applied Aspects of Device Development on Microcontrollers and FPGAs (MC&FPGA), Kharkiv, Ukraine, 2021, pp. 6-8, doi: 10.35598/mcfpga.2021.001.

ОГЛЯД АРХІТЕКТУРИ VERSAL ACAP

студент Скорбатюк М.В., к.т.н., доц. Свид І.В.
Харківський національний університет радіоелектроніки,
кафедра мікропроцесорних технологій і систем, м. Харків, Україна
e-mail: maksym.skorbatiuk@nure.ua

Abstract. Xilinx Versal ACAP is a powerful, adaptive platform that can be used for high-performance and adaptive computing solutions in the cloud, edge and smart device industries. In particular, Versal ACAP has found implementation in the following industries: 5G, data centers, smart factories; auxiliary electronic control system of the car and parking, machine learning, etc.

Ключові слова: Xilinx, ACAP, Versal, архітектура, AI, AMD.

Вступ. На сьогодні, Versal є першою адаптивною платформою прискорення обчислень (ACAP). Versal ® ACAP була створена з нуля як гетерогенна, гнучка платформа, яка підтримує кілька доменно-спеціальних архітектур (DSAs) і обчислювальних структур, включаючи ядра процесора, програмовану логіку та масив AI інженерії.

Основна частина. Перевагою ACAP є його функціональність, як багатоядерної SoC загального призначення, яка включає додаткові програмовані апаратні та програмні механізми для оптимального співвідношення потужності та продуктивності (рис. 1).

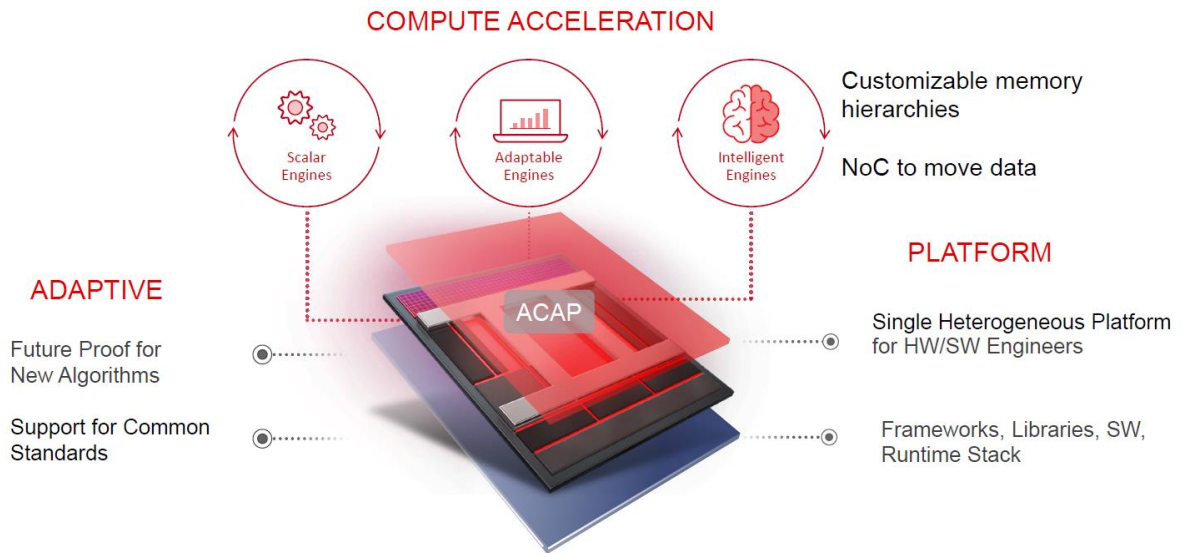


Рисунок 1 – Адаптивна платформа прискорення обчислень Versal [1]

Архітектура Versal включає (рис. 2) [1]:

1) адаптивні процесори: 2х щільність обчислень; масштабування напруги для продуктивності/ват;

2) скалярні процесори: керування платформою; вбудовані периферійні обчислення;

3) PCIe Gen5 і CCIX: 2x PCIe і DMA пропускна здатність; когерентність кешу;

4) пам'ять DDR4: 3200-DDR4, 4266-LPDDR4; 2x пропускна здатність/пін;

5) керування трансивера: широкий діапазон, 25G →112G; 58G у основних пристроях;

6) інтелектуальні процесори: ШІ-обчислення; різноманітні робочі навантаження DSP;

7) програмований NoC: гарантована пропускна здатність; дозволяє програмувати ПЗ;

8) процесори протоколів: ядра 400G/600G; оптимізована потужність;

9) програмований вхід/вихід: будь-який інтерфейс або датчик; включає MIPI 3,2 Гбіт/с.

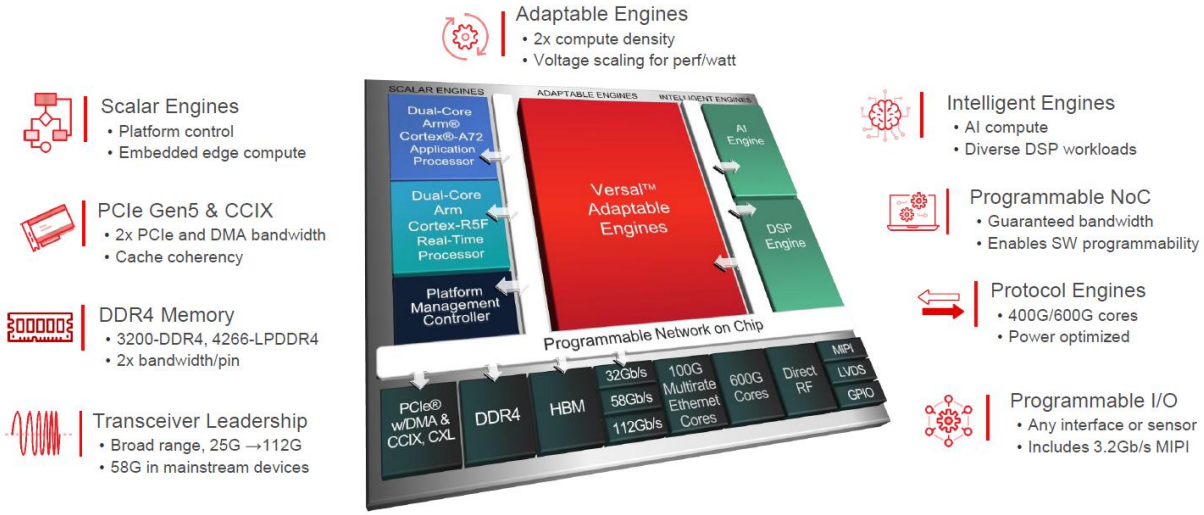


Рисунок 2 – Архітектура Versal [1]

Скалярні механізми для управління платформою дозволяють [1]:

- виконувати складні алгоритми та приймати рішення для автономних систем;
- забезпечувати обробку безпеки та резервування для критично важливих додатків;
- керувати всією платформою;
- використовувати всі можливості ACAP і відстежувати їх стан;
- надають розширення можливостей підтримки - процесор MicroBlaze ™ на основі PL.

Процесор програми [1]:

- двоядерний прикладний процесор Arm Cortex A72;
- швидкість до 1,7 ГГц - 2-кратна однопотокова продуктивність;
- архітектура ARMv8;
- піднімається за лічені секунди;

- підтримує Linux і bare-metal.

Процесор реального часу [1]:

- двоядерний процесор реального часу Arm Cortex R5F;
- функціональна безпека;
- розділений режим для продуктивності або блокування кроків для безпеки;
- низька затримка, детермінізм і контроль у реальному часі для будь-якої програми;
- підлягає сертифікації ASIL/SI.

Адаптивні механізми апаратного забезпечення - програмована логіка:

- паралельна обробка, агрегація даних і об’єднання датчиків;
- програмована ієрархія пам’яті для оптимізації ефективності обчислень.

Інтелектуальні механізми для різноманітних обчислень:

- ШІ всюди: дротовий зв'язок, автомобільний та споживчий ринки;

Процесори DSP: підтримка високоточного обчислення з плаваючою комою; розвантажте додаткові функції для прискорення;

Процесори ШІ: висока пропускна здатність, низька затримка, детермінований і енергоефективний; ідеально підходить для штучного інтелекту та розширеної обробки сигналів.

Програмований NoC, мостові механізми та жорсткий IP [1]:

- терабітний програмований NoC з високою пропускною здатністю: синхронізація критичних з’єднань; гарантований QoS (пропускна здатність проти затримки);
- полегшує розміщення IP та ядра: спрощує підключення IP і периферійних пристроїв; легко міняйте ядра на межах портів NoC;
- інфраструктура програмування: доступ до всіх ресурсів із відображенням пам’яті; вбудований арбітраж між процесорами та пам'яттю.

У Versal ACAP реалізовано адаптивну ієрархія пам'яті та наявна належна пам’ять для правильної роботи. Задля AI Engine посилені обчислення, пам'ять і з'єднання. Також реалізована адаптація апаратного забезпечення задля прискорення роботи всієї програми.

Опис основних характеристик сімейств Versal ACAP наведено у табл. 1 [1].

Розробка архітектури ACAP є найбільшим інженерним досягненням Xilinx з моменту винаходу FPGA.

Versal ACAP – це високоінтегрована багатоядерна гетерогенна обчислювальна платформа, яку можна змінювати як на апаратному, так і на програмному рівні, щоб динамічно адаптуватися до потреб широкого кола додатків і робочих навантажень у центрах обробки даних, автомобільній промисловості, бездротовому, дротовому та оборонному

ринках 5G. Пристрої Versal ACAP можуть забезпечити до 10 разів більшу продуктивність і енергоефективність для конкретних застосувань.

Таблиця 1 – Опис основних характеристик Versal ACAP

Resources & Capabilities	Prime Series	Premium Series	HBM Series	AI Edge Series	AI Core Series
Description	Signal processing and connectivity capabilities	High-end bandwidth series	Heterogeneous integration of HBM	Low Power AI for Real-Time Systems	Breakthrough AI Inference Throughput
LUT (K)	150-1,000	720-3,360	1,753-2,574	20-520	246-900
Distributed RAM (Mb)	4.6-31.2	22-103	54-79	0.6-15.9	7.5-27.5
Block RAM (Mb)	5.4-69.6	49-174	89-132	0.8-33.5	15.5-34
Ultra RAM (Mb)	43.6-190.4	453-2,549	366-541	6.8-129.9	58.8-130.2
Accelerator RAM (Mb)	0-32	-	-	0-32	0-32
DSP Engine	464-3,984	1,904-14,352	7,392-10,848	90-1,312	928-1,968
AI Engine	-	-	-	8-304	128-400
Serial Transceivers	8-48	48-168	88-128	0-44	8-44
Max. GT Bandwidth (Tb/s)	7.8	17.6	11.2	2.5	2.5
I/O	316-770	586-780	780	114-530	478-770
Memory Controllers	1-4	3-4	4	1-3	2-4
HBM (GB)	-	-	8-32	-	-

Архітектура Versal ACAP може бути запрограмована та оптимізована розробниками програмного забезпечення, науковцями з даних та розробниками апаратного забезпечення за допомогою багатьох інструментів, програмного забезпечення, бібліотек, IP, проміжного програмного забезпечення та фреймворків [1], які дозволяють динамічно налаштовувати прискорені обчислювальні рішення в обраній галузі [2, 3].

Висновки. Xilinx Versal ACAP є потужною адаптивною платформою, яка може використовуватися для високопродуктивних і адаптивних обчислювальних рішень у галузі хмарних, периферійних та інтелектуальних пристроїв. Зокрема, Versal ACAP знайшов впровадження у наступних галузях: 5G, центри обробки даних, розумні заводи; допоміжна електронна система керування автомобілем і паркуванням автомобілю, машинне навчання, тощо.

Список використаних джерел.

1. AMD Versal Adaptive SoC Design Process Documentation, https://docs.xilinx.com/p/ai-engine-development

2. В.В. Семенець, І.В. Свид, О.В. Зубков, О.В. Воргуль, Н.В. Бойко, В.С. Чумак. Методичні та технічні аспекти реалізації онлайн лабораторії з проектування пристроїв. // Збірник матеріалів II форуму «Автоматизація, електроніка та робототехніка. Стратегії розвитку та інноваційні технології» до 90-річчя ХНУРЕ. – Харків, ХНУРЕ, 2020. – С. 45-48.

3. В.В. Семенець, І.В. Свид, О.В. Зубков, О.В. Воргуль. Методика розробки та впровадження освітньої компоненти щодо проектування пристроїв. // Збірник матеріалів II форуму «Автоматизація, електроніка та робототехніка. Стратегії розвитку та інноваційні технології» до 90-річчя ХНУРЕ. – Харків, ХНУРЕ, 2020. – С. 40-44.

ДОСЛІДЖЕННЯ МОЖЛИВОСТІ ВИКОРИСТАННЯ АЛГОРИТМУ ПРЮІТ ДЛЯ ОБРОБКИ МЕДИЧНИХ ЗОБРАЖЕНЬ

студент Дерюга І.М., асистент Чумак В.С.
Харківський національний університет радіоелектроніки,
кафедра мікропроцесорних технологій і систем, м. Харків, Україна
e-mail: valeriia.chumak@nure.ua

Abstract. In the context of rapid advancements in medical technologies and the increasing utilization of digital technologies in the healthcare sector, addressing challenges in medical image processing becomes crucial. Computational methods for analyzing boundaries in images obtained from various scanning devices have garnered particular interest. This article explores the application of the Pruitt algorithm for detecting boundaries in medical images. The use of FPGA is proposed for implementing this algorithm to optimize productivity and real-time image processing speed. Experimental results underscore the importance of further research and refinement of medical image processing algorithms to achieve improved accuracy and efficiency in diagnostics.

Ключові слова: алгоритм Прюіт, FPGA, обробка медичних зображень.

Вступ. Останнім часом у медичній галузі робиться багато нових відкриттів, та вона розвивається швидкими темпами. Це є наслідком збільшення використання цифрових та комп’ютерних технологій у медицині.

Основна частина. Обчислювальні системи поки не здатні аналізувати інформацію у людський спосіб, натомість, вони можуть бути помічником для лікаря та допомагати прискорити діагностику різних захворювань. Однією з головних проблем медицини зараз є методи обробки зображень, які отримуються за допомогою різноманітного сканувального обладнання (томографи, рентген-апарати та ін.). За допомогою алгоритмів пошуку границь можна знаходити окремі об’єкти на медичних зображеннях, які не може розрізнити людське око. Варіантом такого алгоритму є оператор Прюіт. Він відносно невитратний з погляду кількості обчислень. [1], а тому гарно підходить для реалізації на компактних обчислювальних системах, таких як FPGA [2-5]. FPGA, у свою чергу, є гарним кандидатом для використання у галузі обробки медичних зображень з двох причин:

По-перше, FPGA мають паралельні обчислювальні можливості, що дозволяють виконувати багато операцій одночасно та підвищити швидкість розрахунків;

По-друге, FPGA мають високу обчислювальну потужність, що дозволяє ефективно виконувати складні операції. Ця висока

обчислювальна потужність дозволяє FPGA швидко обробляти зображення в реальному часі та забезпечувати високу продуктивність алгоритму.

При цьому, FPGA мають відносно невеликі розміри та енергоспоживання, що дозволяє виготовляти компактні пристрої, які можуть працювати від акумуляторних батарей [6]. Таким чином, завдяки паралельним обчисленням і високій обчислювальній потужності, FPGA є ідеальною платформою для реалізації алгоритму Прюіт, забезпечуючи швидку та ефективну обробку зображень.

Математичний апарат алгоритму Прюіт.

Алгоритм розраховує градієнт яскравості зображення у кожній точці, даючи напрямок найбільшого можливого збільшення від світлого до темного, а також швидкість зміни у цьому напрямку [7]. У результаті можна побачити, наскільки «грубо» чи «плавно» відбувається зміна зображення у цій точці, та, як наслідок, наскільки ймовірно, що саме ця частина зображення є границею. Також, алгоритм дає можливий варіант орієнтації цієї границі.

Математично у алгоритмі використовується два ядра, за допомогою яких виконується згортка зображення:

$$G_x = \begin{bmatrix} +1 & 0 & -1 \\ +1 & 0 & -1 \\ +1 & 0 & -1 \end{bmatrix} * A \wedge G_y = \begin{bmatrix} +1 & +1 & +1 \\ 0 & 0 & 0 \\ -1 & -1 & -1 \end{bmatrix} * A,$$

де G_x, G_y – два зображення, що мають у кожній точці апроксимовану горизонтальну та вертикальну похідні відповідно; A – зображення, що оброблюється.

Це дає можливість отримати апроксимовані похідні (оскільки точки зображення є дискретними) – для горизонтальних змін та для вертикальних.

Оскільки ці ядра можна розкласти як добутки усереднювального та диференціювального ядер, вони дозволяють обчислити градієнт зі згладжуванням. Координата x у цих розрахунках визначається як зростаюча «ліворуч», а координата y – як зростаюча «вгору» [7]. У кожній точці зображення, кінцеві наближення градієнта можуть бути поєднані для отримання величини градієнта:

$$G = \sqrt{G_x^2 + G_y^2}.$$

З цього можна отримати також напрямок градієнту:

$$\Theta = arctan2\left(G_y, G_x\right).$$

Експериментальна перевірка роботи алгоритму.

В 2014 році у статті [8] було описано використання різноманітних методів обробки медичних зображень з метою покращення їх інтерпретації людським оком, а також проведено експериментальне дослідження цих

методів. Результат обробки зображення алгоритмом Прюіт можна побачити нижче.

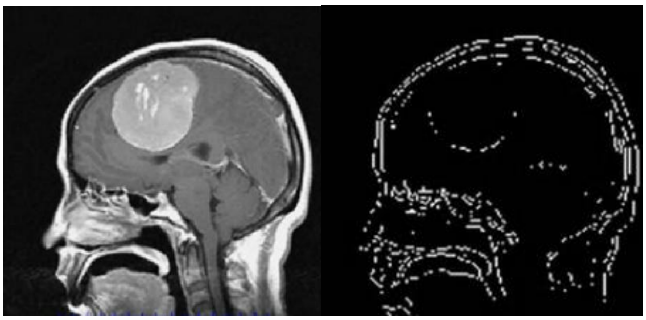


Рисунок 1 – Результат обробки зображення алгоритмом Прюіт [8]

Висновки. Фактично, можна побачити, що хоча алгоритм виділяє границі пухлини (біла маса), але ці границі є розірваними та слабкими. З цього можна зробити висновок, що цей алгоритм погано підходить для використання у обробці медичних зображень, та слід дослідити можливості використання інших алгоритмів.

Список використаних джерел.

1. Woods R. E., Gonzalez R. C. Digital Image Processing (3rd Edition). 3rd ed. Prentice Hall, 2007. 976 p.

2. Чумак В. С. Реализация структуры нейронных сетей на FPGA / Чумак В.С., Свид І.В. // Наука, технології, інновації: тенденції розвитку в Україні та світі: матеріали міжнародної студентської наукової конференції, 17 квітня, 2020 рік. – Харків, Україна: Молодіжна наукова ліга. –Т.2– С. 30-32.

3. Чумак, В. С., & Свид, І. В. (2019). Перспектива использования продукта FPGA в медицинских системах. X. У Міжнародна науково-практична конференція магістрантів та аспірантів «Теоретичні та практичні дослідження молодих науковців» (с. 288–289).

4. Oleg Zubkov, Iryna Svyd, Oleksandr Maltsev, Liliia Saikivska. In-circuit Signal Analysis in the Development of Digital Devices in Vivado 2018. First International Scientific and Practical Conference «Theoretical and Applied Aspects of Device Development on Microcontrollers and FPGAs» MC&FPGA2019, (p. 12-13) July 26-27, 2019. Kharkiv, Ukraine.

5. Луценко О. В. Використання FPGA для реалізації штучної нейронної мережі / О. В. Луценко, В. С. Чумак // Автоматизація, електроніка та робототехніка. Стратегії розвитку та інноваційні технології : матеріали IV форуму, 24–25 листопада 2022 р. – Харків : ХНУРЕ, 2022. – С. 26-27.

6. Computing Models for FPGA-Based Accelerators / M. C. Herbordt et al. Computing in Science & Engineering. 2008. Vol. 10, no. 6. P. 35–45. URL: https://doi.org/10.1109/mcse.2008.143 (date of access: 12.09.2023).

7. Prewitt J. M. Object Enhancement and Extraction. Picture Processing and Psychopictorics. New York-London, 1970. P. 75–148.

8. Zhao J., Zhang L., Yin M. Medical Image Segmentation Based on Wavelet Analysis and Gradient Vector Flow. Journal of Software Engineering and Applications. 2014. Vol. 07, no. 12. P. 1019–1030. URL: https://doi.org/10.4236/jsea.2014.712089 (date of access: 12.09.2023).

ІНТЕГРАЦІЯ НЕЙРОННИХ МЕРЕЖ У МЕДИЧНІ ПРИСТРОЇ НА ОСНОВІ STM32 ДЛЯ АВТОМАТИЧНОЇ ДІАГНОСТИКИ ТА МОНІТОРИНГУ ПАЦІЄНТІВ

асистент Чумак В.С.
Харківський національний університет радіоелектроніки,
кафедра мікропроцесорних технологій і систем, м. Харків, Україна
e-mail: valeriia.chumak@nure.ua

Abstract. This article discusses the technical aspects of integrating neural networks into medical devices based on STM32 microcontrollers. The focus is on the selection and optimization of communication interfaces, the development of software for interacting with neural networks, and the implementation of machine learning algorithms. Technical analysis includes memory management, code optimization, and the use of development tools. Overcoming challenges associated with limited resources ensures the creation of intelligent medical devices with increased diagnostic accuracy and efficiency.

Ключові слова: догляд персоналізований, STM32, нейронна мережа.

Вступ. Зі зростанням ступеня інтеграції мікросхем якісно змінюється межа складності систем, які можуть бути реалізовані на їхній основі [1, 2]. В сучасній медичній практиці впровадження технологій нейронних мереж у мікроконтролери STM32 відкриває нові перспективи для автоматичної діагностики та моніторингу пацієнтів. Ця інтеграція є симбіозом передових методів і технічних рішень для покращення точності та ефективності медичних пристроїв.

Основна частина. Нейронні мережі відіграють ключову роль в автоматизації діагностики та моніторингу захворювань. Їхній здатність аналізувати складні дані дозволяє ефективно обробляти медичну інформацію, виявляти патології та надавати точні прогнози. Прикладами успішного використання нейронних мереж у медицині є системи розпізнавання зображень, аналізу біомедичних даних і навіть підтримка в процесі прийняття рішень в хірургії.

Проте інтеграція нейронних мереж з мікроконтролерами STM32 ставить технічні виклики:

- вибір відповідних інтерфейсів зв'язку між мікроконтролером та нейронними мережами. Наприклад, SPI, I2C або UART можуть використовуватися залежно від вимог системи. Особливості вибору інтерфейсу можуть залежати від обсягу передаваємих даних, швидкості обміну та обмежень енергоспоживання. Розробники також повинні враховувати фізичні характеристики медичних пристроїв, такі як розміри та електромагнітна сумісність.

- розробка спеціалізованих драйверів і алгоритмів, які забезпечують взаємодію між STM32 та нейронними мережами. Це може включати в себе

адаптацію бібліотек машинного навчання для роботи з обмеженими ресурсами мікроконтролера, оптимізацію продуктивності та використання апаратних прискорювачів, що може значно підвищити ефективність виконання алгоритмів нейронних мереж. Керування пам'яттю включає в себе оптимізацію завантаження та зберігання моделей, а також ефективне управління буферами даних.

- адаптація алгоритмів машинного навчання до обмежених ресурсів мікроконтролера. Одним із методів є квантування, яке дозволяє зменшити розмір моделі, зберігаючи при цьому її функціональність. Оптимізація коду. При використанні бібліотек машинного навчання важливо враховувати, які частини коду можуть бути оптимізовані для конкретної апаратної архітектури STM32. Даний етап включає в себе вибір відповідних оптимізацій компілятора та структур даних.

- для полегшення інтеграції нейронних мереж з STM32 існує низка інструментів розробки, таких як STM32CubeMX [3], який надає графічний інтерфейс для налаштування периферійних пристроїв і генерації коду для проекту. Для розробки програмного забезпечення для нейронних мереж можна використовувати фреймворки, такі як TensorFlow Lite Micro або CMSIS-NN.

Висновки. Інтеграція нейронних мереж в STM32 в медичні пристрої відкриває унікальні можливості для персоналізованого підходу до догляду за пацієнтами. Алгоритми машинного навчання, вбудовані в мікроконтролери STM32, дозволяють обробляти та інтерпретувати дані з більшою точністю, зменшуючи ризик помилкових спрацювань і забезпечуючи довіру до результатів. Однак, незважаючи на потенційні переваги, існують технічні труднощі, які вимагають додаткових досліджень та інновацій. Це включає розробку більш ефективних алгоритмів оптимізації ресурсів, а також роботу над зниженням енергоспоживання при збереженні високої продуктивності.

Список використаних джерел.

1. Чумак, В. С., & Свид, І. В. (2019). Перспектива использования продукта FPGA в медицинских системах. Х. У Міжнародна науково-практична конференція магістрантів та аспірантів «Теоретичні та практичні дослідження молодих науковців» (с. 288–289).

2. Чумак В. С. Реализация структуры нейронных сетей на FPGA / Чумак В.С., Свид І.В. // Наука, технології, інновації: тенденції розвитку в Україні та світі: матеріали міжнародної студентської наукової конференції, 17 квітня, 2020 рік. – Харків, Україна: Молодіжна наукова ліга. –Т.2– С. 30-32.

3. I. Svyd, O. Vorgul, V. Semenets, O. Zubkov, V. Chumak, N. Boiko. Special Features of the Educational Component “Design of Devices on Microcontrollers and FPGA”. // II International Scientific and Practical Conference Theoretical and Applied Aspects of Device Development on Microcontrollers and FPGAs (MC&FPGA), Kharkiv, Ukraine, 2020, pp. 55-57. doi: 10.35598/mcfpga.2020.017.

ВИКОРИСТАННЯ НЕЙРОННИХ МЕРЕЖ В АДАПТИВНИХ СИСТЕМАХ ОНЛАЙН-МЕДИЧНОЇ ОСВІТИ НА БАЗІ МІКРОКОНТРОЛЕРІВ STM32 В УМОВАХ ВОЄННИХ КРИЗ

асистент Чумак В.С.
Харківський національний університет радіоелектроніки,
кафедра мікропроцесорних технологій і систем, м. Харків, Україна
e-mail: valeriia.chumak@nure.ua

Abstract. Adaptive online medical education systems that integrate neural networks and STM32 microcontrollers offer innovative solutions for effective learning in times of war crises. STM32 microcontrollers, with their powerful hardware architecture, ensure fast data processing and efficient interaction with peripheral devices, crucial for creating responsive adaptive systems.

The application of reinforcement learning methods allows for personalized learning tailored to each student's individual needs, while neural networks analyze student performance data, optimizing educational programs. The proposed system combines advanced neural network technologies with high-performance STM32 microcontrollers, providing a personalized and adaptive approach to education in the context of military crises.

Ключові слова: адаптивні системи, STM32, онлайн-медична освіта.

Вступ. Адаптивні системи, що базуються на синтезі нейронних мереж і мікроконтролерах STM32, надають сучасні рішення для онлайн-медичної освіти в умовах воєнних криз. З інтеграцією мікросхем різного рівня стає очевидним, що межа складності систем, які можуть бути реалізовані на їх основі, якісно змінюється [1, 2]. Мікроконтролери STM32, завдяки своїй видатній апаратній архітектурі, забезпечують швидку обробку даних та ефективне взаємодію з периферійними пристроями, що є критичним для створення реактивних адаптивних систем.

Основна частина. Застосування методів навчання з підсиленням дозволяє адаптувати навчання до потреб кожного студента, враховуючи його індивідуальні особливості та стиль навчання. Нейронні мережі можуть аналізувати дані про успішність студента і автоматично коригувати навчальну програму для максимізації ефективності навчання.

Пропонується розробити систему, яка представляє інноваційне рішення для забезпечення якісної та доступної медичної освіти в умовах воєнних криз. Вона об'єднує передові технології нейронних мереж і високоефективні мікроконтролери STM32, забезпечуючи персоналізований та адаптивний підхід до навчання. Основні характеристики проекту:

Апаратна платформа: використання мікроконтролерів STM32 з ARM Cortex-M ядрами забезпечує високу продуктивність і низьке енергоспоживання. Модульність вибору ядра дозволяє адаптувати систему

під конкретні вимоги проекту.

Інтеграція нейронних мереж: програмування з використанням CMSIS-NN та оптимізованих алгоритмів забезпечує ефективну інтеграцію нейронних мереж, що дозволяє системі адаптуватися до індивідуальних потреб студентів і забезпечувати персоналізований освітній досвід.

Периферійні пристрої та інтерфейси: можливості мікроконтролерів STM32 у сфері портів GPIO, SPI, I2C та USART [3] забезпечують гнучкість у інтеграції з різними пристроями, включаючи сенсори та комунікаційне обладнання. Забезпечення доступності в умовах кризи: система розроблена з урахуванням можливих обмежень ресурсів в умовах воєнних криз. Режими низького споживання енергії мікроконтролерів STM32 та ефективне використання енергії гарантують стабільну роботу системи за мінімальних витрат.

Інтеграція в онлайн-платформу: розроблена система може бути легко інтегрована в існуючі онлайн-платформи для освіти, забезпечуючи плавний перехід та мінімізацію необхідності внесення змін в інфраструктуру.

Тип системи: Адаптивна система онлайн-медичної освіти на основі нейронних мереж і мікроконтролерів STM32 може бути представлена як веб-платформою, так і мобільним додатком.

Обидві ці опції дозволяють системі бути гнучкою і легко інтегрованою в різні освітні контексти. Тип системи може бути обраний залежно від конкретних потреб і вподобань користувача.

Висновки. Інтеграція нейронних мереж в адаптивні системи онлайн-медичної освіти на базі мікроконтролерів STM32 відкриває нові перспективи для ефективної та доступної освіти в умовах воєнних криз. Технічна оптимізація і практичний досвід дозволяють з впевненістю говорити про застосовність цих технологій в реальних умовах, що робить даний напрямок перспективним і багатообіцяючим для майбутніх досліджень і розробок.

Список використаних джерел.

1. Чумак, В. С., & Свид, І. В. (2019). Перспектива использования продукта FPGA в медицинских системах. Х. У Міжнародна науково-практична конференція магістрантів та аспірантів «Теоретичні та практичні дослідження молодих науковців» (с. 288–289).

2. Чумак В. С. Реализация структуры нейронных сетей на FPGA / Чумак В.С., Свид І.В. // Наука, технології, інновації: тенденції розвитку в Україні та світі: матеріали міжнародної студентської наукової конференції, 17 квітня, 2020 рік. – Харків, Україна: Молодіжна наукова ліга. – Т.2– С. 30-32.

3. I. Svyd, O. Vorgul, V. Semenets, O. Zubkov, V. Chumak, N. Boiko. Special Features of the Educational Component “Design of Devices on Microcontrollers and FPGA”. // II International Scientific and Practical Conference Theoretical and Applied Aspects of Device Development on Microcontrollers and FPGAs (MC&FPGA), Kharkiv, Ukraine, 2020, pp. 55-57. doi: 10.35598/mcfpga.2020.017

СУЧАСНІ ТЕНДЕНЦІЇ ВПРОВАДЖЕННЯ SMART-ЛАБОРАТОРІЙ ДЛЯ IIOT

старший викладач Галкін П.В., студент Шаповал І.Р.
Харківський національний університет радіоелектроніки, кафедра проектування та експлуатації електронних апаратів, м. Харків, Україна
e-mail: galkinletter@ukr.net, illia.shapoval@nure.ua

Abstract. The In the era of technological innovations, smart laboratories, a component of the Industrial Internet of Things (IIoT), play a crucial role in automating and optimizing industrial processes. These labs, driven by intelligent systems, enable real-time data analysis and decision-making. They enhance the work environment and integrate with IIoT for improved efficiency. Characterized by high automation and flexibility, smart laboratories are central to managing production flows effectively. Their implementation aligns with Industry 4.0 and Industry 5.0 concepts, contributing to the evolution of highly automated and competitive industrial environments. Addressing technical aspects and cybersecurity is vital for the seamless and secure operation of these innovative systems. The focus on individualization of production and collaboration between humans and technology distinguishes Industry 5.0, emphasizing a human-centric approach in the evolving industrial landscape.

Ключові слова: Smart Laboratories, IIoT (Industrial Internet of Things), Automation, Industry 4.0, Industry 5.0.

Вступ. В епоху постійних технологічних інновацій [1], промисловий інтернет речей (IIoT) та концепція "розумних" технологій стають необхідною складовою для досягнення оптимальної продуктивності та ефективності в промисловості. Однією із важливих складових цього розвитку є впровадження сучасних "розумних лабораторій" або smart-лабораторій [2], які використовують передові технології для автоматизації та оптимізації промислових процесів. Smart-лабораторії сприяють покращенню робочого середовища, забезпечуючи розумне використання даних та забезпечуючи інтеграцію з IIoT [3]. Ці лабораторії базуються на інтелектуальних системах [4], що дозволяють автоматизовано збирати, аналізувати та використовувати інформацію для прийняття рішень в реальному часі. Вони стають центром для впровадження передових технологій, таких як штучний інтелект, аналітика даних, інтернет речей [5, 6] та машинне навчання.

Цей напрямок визначається високою автоматизацією, гнучкістю та віддаленим доступом до даних, що дозволяє забезпечити необхідну швидкість реакції на зміни в виробничих процесах. Smart-лабораторії стають ключовим елементом ефективного управління виробничими потоками та дозволяють підприємствам вдосконалювати якість продукції, зменшувати витрати та збільшувати конкурентоспроможність на ринку. У

цьому контексті важливо розглядати не лише технічні аспекти впровадження smart-лабораторій, але і питання кібербезпеки [7], стандартизації та регулювання, щоб забезпечити безперебійну та безпечну роботу цих інноваційних систем в промислових умовах. Впровадження smart-лабораторій і їхній зв'язок з концепціями Industry 4.0 та Industry 5.0 [8] сприяють еволюції виробництва та промисловості, роблячи їх ще більш автоматизованими [9], ефективними [9] та гнучкими [10].

Основна частина. Впровадження Smart-лабораторій для IIoT є актуальною та передовою тенденцією в сучасній промисловості. Ці лабораторії, засновані на концепції IIoT, використовують передові технології, такі як сенсори, з'єднані мережі та аналітика даних, для оптимізації виробничих процесів. Smart-лабораторії дозволяють збирати та аналізувати великі обсяги даних в реальному часі, сприяючи прийняттю обґрунтованих рішень на підставі точних та зрозумілих даних. Вони допомагають виробникам підвищити ефективність виробничих процесів, скоротити витрати, а також запроваджувати нові рішення у сфері якості та інновацій. Основні складові Smart-лабораторій включають в себе автоматизацію, віддалений моніторинг та керування, інтеграцію з великими хмарними платформами та використання штучного інтелекту для прогнозування та оптимізації процесів. Така ініціатива дозволяє підприємствам адаптуватися до вимог сучасного виробництва, забезпечуючи підвищену продуктивність та конкурентоспроможність в епоху Індустрії 4.0.

Складові Smart-лабораторії для IIoT. Smart-лабораторії для IIoT можуть включати різноманітні компоненти та технології для забезпечення ефективності та інновацій в виробничих процесах. Ключові складові такої лабораторії:

1. Сенсори та IoT-пристрої:

- розміщені на обладнанні сенсори для збору даних про стан устаткування та виробничих параметрів;
- IoT-пристрої для передачі зібраних даних до центральної системи.

2. Мережева інфраструктура:

- використання високошвидкісної мережі для забезпечення передачі даних між сенсорами, пристроями та центральною системою;
- застосування промислових мережевих стандартів для забезпечення стабільності та безпеки передачі даних.

3. Хмарні системи та аналітика даних:

- інтеграція з хмарними обчисленнями для зберігання та обробки великих обсягів даних;
- використання аналітики даних для отримання інсайтів та прийняття рішень.

4. Віддалений моніторинг та керування:

- системи для віддаленого моніторингу виробничих ліній та

обладнання;

- можливості дистанційного керування та управління процесами з використанням мобільних пристроїв.

5. Інтернет Речей (IoT) та Інтеграція з ERP-системами:

- використання технологій IoT для зв'язку та обміну даними між пристроями;

- інтеграція з системами управління ресурсами підприємства (ERP) для оптимізації виробничих процесів.

6. Штучний інтелект та машинне навчання:

- застосування алгоритмів штучного інтелекту для аналізу та прогнозування даних;

- використання машинного навчання для оптимізації процесів та виявлення аномалій.

7. Безпека та кіберзахист:

- застосування заходів для забезпечення безпеки мережі та захисту важливих виробничих даних;

- використання технологій кіберзахисту для уникнення атак та забезпечення цілісності систем.

8. Апаратне та програмне забезпечення:

- оптимізація обладнання та використання спеціалізованого програмного забезпечення для забезпечення сумісності та ефективності роботи Smart-лабораторії.

Кожний із 8 пунктів є складовою елементів концепції Industry 4.0, а також концепції Industry 5.0[8].

Відмінності Smart-лабораторій для Industry 4.0 та Industry 5.0. Smart-лабораторії для Industry 4.0 та Industry 5.0 відрізняються за своїм підходом, фокусом та інтеграцією передових технологій в виробничих процесах.

Підхід Industry 4.0 ставить акцент на автоматизацію виробничих процесів за допомогою IoT, машинного навчання та аналізу даних. Такий підхід зосереджений на оптимізації виробничих ланцюгів та впровадженні принципів "розумної фабрики". Також такий підхід зводиться до використання технологій комунікацій та обміну даними між різними системами в реальному часі, а також забезпечення цифрового зв'язку між обладнанням та комп'ютерними системами. Крім вище вказаного концепт Industry 4.0 зосереджений на аналізі великих обсягів даних для покращення прийняття рішень та застосування аналітики для прогнозування умов та виявлення аномалій у виробництві.

Підхід Industry 5.0 ставить акцент на співпрацю людей та автоматизованого обладнання в одній ефективній системі із залучення робітників до виробничих процесів і використання їхнього інтелекту та креативності. Також концепт допускає взаємодію між людьми та роботами в режимі реального часу, де обидві сторони використовують свої сильні

сторони, а фокус на роботі пліч о пліч, де люди та роботи доповнюють одне одного.

Отже, підхід Industry 4.0 зорієнтований на цифрову трансформацію та автоматизацію, тоді як Industry 5.0 ставить людський фактор у центрі та прагне до співпраці між людьми та технологіями для досягнення найкращих результатів.

Висновки. У сучасному світі промисловості визначається постійна трансформація, і дві ключові концепції, Industry 4.0 та Industry 5.0, впроваджують інноваційні та перспективні підходи до оптимізації виробничих процесів. Smart-лабораторії будуть виступати ключовою ділянкою для реалізації концепцій Industry 4.0 та Industry 5.0.

Список використаних джерел.

1. Маркевич К. Smart-інфраструктура у сталому розвитку міст: світовий досвід та перспективи України – Київ: Центр Разумкова. – ydavnytstvo" Zapovit", 2021.

2. Nugent C. D. et al. Experiences in the development of a smart lab //International Journal of Biomedical Engineering and Technology. – 2009. – Т. 2. – №. 4. – С. 319-331.

3. Langmann R. et al. Workshop: The TATU Lab & smart education //2016 13th International Conference on Remote Engineering and Virtual Instrumentation (REV). – IEEE, 2016. – С. 400-402.

4. Galkin P., Umiarov R., Grigorieva O. Design embedded system testbench based on FPGA and microcontrollers for TATU smart lab as education component of industry 4.0 //2019 IEEE 2nd Ukraine Conference on Electrical and Computer Engineering (UKRCON). – IEEE, 2019. – С. 628-633.

5. Ivan Buhrym, Oleksandr Vynokurov, Pavlo Galkin. Approaches to Designing a Wireless Sensor Network Node // First International Scientific and Practical Conference «Theoretical and Applied Aspects of Device Development on Microcontrollers and FPGAs» MC&FPGA-2019, Kharkiv, Ukraine, July 26-27, 2019. – Kharkiv: NURE, MC&FPGA, 2019. – P. 21-24. DOI: 10.35598/mcfpga.2019.007

6. Poongothai M., Subramanian P. M., Rajeswari A. Design and implementation of IoT based smart laboratory //2018 5th International Conference on Industrial Engineering and Applications (ICIEA). – IEEE, 2018. – С. 169-173.

7. Pennekamp J. et al. Security considerations for collaborations in an industrial IoT-based lab of labs //2019 IEEE Global Conference on Internet of Things (GCIoT). – IEEE, 2019. – С. 1-7.

8. Галкін П. В. Розробка лабораторного комплексу по вивченню вбудованих систем управління і промислової автоматизації // Матеріали 21-го Міжнародного молодіжного форуму "Радіоелектроніка та молодь у XXI столітті", 25-27 квітня 2017 р. [Текст] : [збірник] / П.В. Галкін // Т. 2 : Конференція "Автоматизовані системи та комп'ютеризовані технології радіоелектронного приладобудування".- Т. 2.- Харків: ХНУРЕ.- С.94-95.

9. S. Khriji, D. El Houssaini, R. Barioul, T. Rehman and O. Kanoun, "Smart-Lab: Design and Implementation of an IoT-based Laboratory Platform," 2020 IEEE 6th World Forum on Internet of Things (WF-IoT), New Orleans, LA, USA, 2020, pp. 1-5, doi: 10.1109/WF-IoT48130.2020.9221143.

10. Langmann R., Coppenrath M. A Cloud-Based Blended Learning Lab for PLC Education //Smart Industry & Smart Education: Proceedings of the 15th International Conference on Remote Engineering and Virtual Instrumentation 15. – Springer International Publishing, 2019. – С. 3-13.

РОЗРОБКА TESTBENCH НА БАЗІ ВБУДОВАНИХ СИСТЕМ ДЛЯ ДОСЛІДЖЕННЯ КОНЦЕПЦІЇ ІНДУСТРІЇ 5.0

старший викладач Галкін П.В., студент Кудря Т.К.
Харківський національний університет радіоелектроніки, кафедра проектування та експлуатації електронних апаратів, м. Харків, Україна
e-mail: galkinletter@ukr.net, tymur.kudria@nure.ua

Abstract. The rapid advancement of technology in recent years has necessitated the search for and implementation of new approaches to address industrial challenges. The emergence of the Industry 5.0 concept is aimed at not only enhancing but also revolutionizing production, placing a key emphasis on collaboration between humans and automation technologies. In this context, a pressing task arises – the development of a Testbench based on embedded systems for investigating the concept of Industry 5.0. Modern embedded systems have become crucial tools for studying and validating the functionality and efficiency of new production approaches within the framework of Industry 5.0. In this article, we will delve into the key aspects of developing a Testbench for embedded systems, shedding light on the vital interactions between technology and humans critical in Industry 5.0. We will explore the core principles, challenges, and prospects associated with implementing the Industry 5.0 concept in contemporary manufacturing settings.

Ключові слова: вбудовані системи, IIoT, IoT, Testbench, Industry 5.0.

Вступ. Швидкий розвиток технологій в останні роки привів до необхідності в пошуку та впровадженні нових підходів до вирішення завдань у промисловості. Поява концепції Індустрії 5.0 покликано не лише вдосконалити, а й революціонізувати виробництво, надаючи ключовий акцент на співпрацю між людиною та технологіями автоматизації. У цьому контексті виникає актуальна задача – розробка Testbench на базі вбудованих систем для дослідження концепції Індустрії 5.0 [1]. Сучасні вбудовані системи стають важливим інструментом для вивчення та перевірки функціональності та ефективності нових підходів до виробництва в умовах Індустрії 5.0 [2-3]. У цій статті ми детально розглянемо основні аспекти розробки Testbench пристроїв для вбудованих систем, що дозволить висвітлити важливі взаємодії між технологією та людиною, які стають критичними у Індустрії 5.0. Висвітлимо основні принципи, виклики та перспективи, які виникають у зв'язку з впровадженням концепції Індустрії 5.0 в сучасних виробничих умовах.

Основна частина. У змінному ландшафті промисловості сучасного світу концепція Індустрії 5.0 займає центральне місце, прагнучи не лише трансформувати, але й змінити підхід до виробництва. В умовах стрімкого розвитку вбудованих систем, розробка Testbench [4-5] на їх основі стає ключовою ланкою для проведення наукових досліджень та вивчення

взаємодії між технологією та концепцією Індустрії 5.0. Використання бездротових сенсорних мереж (WSN) може бути важливим елементом в розробці Testbench на базі вбудованих систем для дослідження концепції Індустрії 5.0. Існує кілька можливих сценаріїв [4-6], які відображають, як WSN може збагатити такий підхід.

Бездротові сенсори можуть встановлюватися на обладнанні [4] для моніторингу різноманітних параметрів [6], таких як температура, вологість, вібрація тощо. Зібрані дані використовуються для аналізу працездатності обладнання та виявлення потенційних проблем наприклад за допомогою штучного інтелекту, побудованого на базі нейронних мереж [7]. Бездротові сенсори створюють можливість для взаємодії між різними вбудованими системами. Це особливо корисно при тестуванні взаємодії різних компонентів, що використовуються в системах Industry 5.0 [8]. Вбудовані бездротові сенсори можуть служити для вимірювання взаємодії людини з технологією в виробничому середовищі. Це може включати в себе оцінку фізичних зусиль, часу реакції та інших параметрів, що дозволяють краще розуміти, як людський фактор впливає на результативність систем Industry 5.0. Бездротові сенсори дозволяють автоматизовано збирати та передавати дані на центральну систему аналізу, спрощуючи процеси моніторингу та полегшуючи прийняття рішень. За допомогою WSN можна легко розгортати масштабовані системи моніторингу [8-10], які охоплюють велику територію виробничого приміщення чи навіть кілька об'єктів, дозволяючи отримати повний обсяг інформації. Використання бездротових сенсорних мереж розширює можливості тестового середовища [8], забезпечуючи зручність, мобільність та високу гнучкість у вивченні та впровадженні концепції Індустрії 5.0.

Сценарії розробки тестових макетів. Створення тестових макетів на базі мікроконтролерів для дослідження концепції Industry 5.0 може включати різноманітні сценарії та аспекти виробництва. До основних компонентів таких систем можна віднести:

- макет для взаємодії людина-машина (HMI);
- модель автоматизованого виробництва;
- модель IIoT-з'єднання;
- система контролю якості на основі вбудованих систем.

Такі тестові макети можуть служити інструментами для вивчення різних аспектів концепції Industry 5.0 та впровадження відповідних технологій у виробничі умови.

Розробка IIoT-з'єднання на базі WSN Розробка IIoT-з'єднання на базі бездротових сенсорних мереж (WSN) включає в себе використання різних компонентів для забезпечення ефективного моніторингу та обробки даних у промислових умовах. Спеціалізовані сенсори для вимірювання різних параметрів, таких як температура, вологість, тиск, вібрація, рівень рідини тощо. Такі сенсори забезпечують збір великого обсягу даних з

виробничого середовища. Існують різні модулі на основі SoC CC2530, по суті, це плата, на якій розміщено сам CC2530, зовнішній кварцовий резонатор, кілька пасивних компонентів, антенний роз'єм (або вбудована антена) і виходи для підключення до інших пристроїв. Типовий вузол бездротової сенсорної мережі може бути побудований за допомогою мікросхеми CC2530. Цей трансивер може бути готовий до прототипу на платі-модулі PCB, рис. 1.

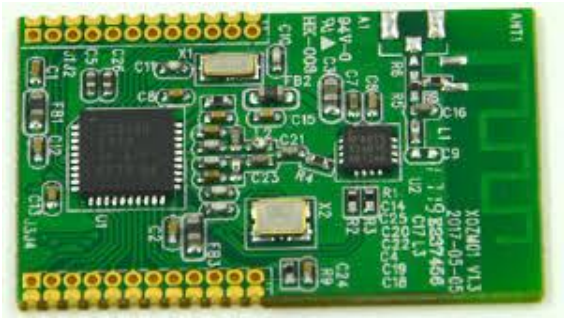


Рисунок 1 – Модуль трансивер CC2530

Розроблений тестовий стенд на основі CC2530, показаний на рис. 2.

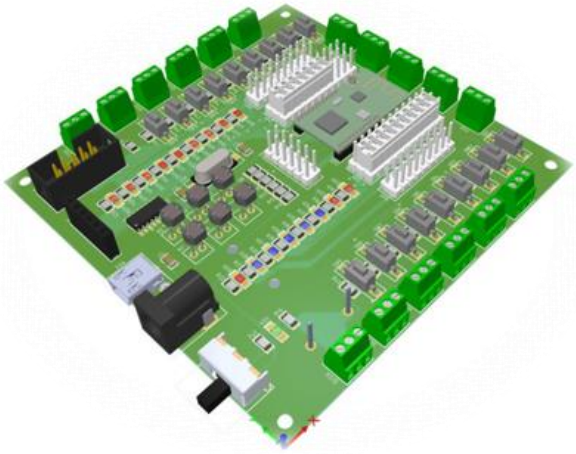


Рисунок 2 – Приклад розробленого тестового макету для IIoT-з'єднання на базі WSN

Також слід врахувати, що модулі для бездротового передавання даних від сенсорів до центрального вузла. Це може бути здійснено, наприклад, за допомогою Bluetooth, Zigbee, Wi-Fi або інших протоколів. В нашому випадку це технологія Zigbee на базі CC2530. Такий модуль через перефірійні мережі можу бути вбудований в промислове рішення, як в роботі [4]. З'єднання модуля, такого як CC2530, з промисловим програмованим логічним контролером (ПЛК), може бути виконане за допомогою бездротових комунікаційних технологій, таких як Zigbee або Bluetooth, або за допомогою стандартних інтерфейсів, таких як UART (Universal Asynchronous Receiver-Transmitter) чи SPI (Serial Peripheral Interface). Важливо враховувати вимоги конкретного промислового

середовища та вибрати технології та інтерфейси, які найкраще відповідають таким потребам. Інтегрування бездротового з'єднання з загальною системою виробництва чи автоматизації, забезпечить взаємодію з іншими компонентами системи Індустрії 5.0.

Висновки. За останні десятиріччя взаємодія між технологічними інноваціями та промисловістю дедалі посилилася. З метою вдосконалення виробництва та оптимізації витрат, важливим кроком є впровадження концепції IIoT на основі бездротових сенсорних мереж. Розробка IIoT-з'єднання на базі бездротових сенсорних мереж є перспективним напрямком для покращення промислового виробництва. Отримані результати вказують на значущий потенціал цього підходу для досягнення інтелектуалізації та оптимізації виробничих умов.

Список використаних джерел.

1. Xu X. et al. Industry 4.0 and Industry 5.0—Inception, conception and perception //Journal of Manufacturing Systems. – 2021. – Т. 61. – С. 530-535.

2. Leng J. et al. Industry 5.0: Prospect and retrospect //Journal of Manufacturing Systems. – 2022. – Т. 65. – С. 279-295.

3. Akundi A. et al. State of Industry 5.0—Analysis and identification of current research trends //Applied System Innovation. – 2022. – Т. 5. – №. 1. – С. 27.

4. Langmann R. et al. Workshop: The TATU Lab & smart education //2016 13th International Conference on Remote Engineering and Virtual Instrumentation (REV). – IEEE, 2016. – С. 400-402.

5. Galkin P., Umiarov R., Grigorieva O. Design embedded system testbench based on FPGA and microcontrollers for TATU smart lab as education component of industry 4.0 //2019 IEEE 2nd Ukraine Conference on Electrical and Computer Engineering (UKRCON). – IEEE, 2019. – С. 628-633.

6. Ivan Buhrym, Oleksandr Vynokurov, Pavlo Galkin. Approaches to Designing a Wireless Sensor Network Node // First International Scientific and Practical Conference «Theoretical and Applied Aspects of Device Development on Microcontrollers and FPGAs» MC&FPGA-2019, Kharkiv, Ukraine, July 26-27, 2019. – Kharkiv: NURE, MC&FPGA, 2019. – P. 21-24. DOI: 10.35598/mcfpga.2019.007

7. Holikov, M., & Galkin, P. (2018). Analysis of possibilities to use neural network for remote control of electronic devices. Technology Audit And Production Reserves, 6(2(44)), 42-49. doi:http://dx.doi.org/10.15587/2312-8372.2018.149539

8. Pennekamp J. et al. Security considerations for collaborations in an industrial IoT-based lab of labs //2019 IEEE Global Conference on Internet of Things (GCIoT). – IEEE, 2019. – С. 1-7.

8. Галкін П. В. Розробка лабораторного комплексу по вивченню вбудованих систем управління і промислової автоматизації // Матеріали 21-го Міжнародного молодіжного форуму "Радіоелектроніка та молодь у XXI столітті", 25-27 квітня 2017 р. [Текст] : [збірник] / П.В. Галкін // Т. 2 : Конференція "Автоматизовані системи та комп'ютеризовані технології радіоелектронного приладобудування".- Т. 2.- Харків: ХНУРЕ.- С.94-95.

9. Skobelev P. O., Borovik S. Y. On the way from Industry 4.0 to Industry 5.0: From digital manufacturing to digital society //Industry 4.0. – 2017. – Т. 2. – №. 6. – С. 307-311.

10. Galkin P. Design Testbench for Wireless Sensor Network Based on CC2530 Transceiver //2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T). – IEEE, 2019. – С. 1-6.

АЛФАВІТНИЙ ПОКАЖЧИК

А

Анур'єва К.С. 80

Б

Бабич О.В. 80, 77
Беззабарний Д.І. 66
Білоцерківець О.Г. 99, 101, 103
Булага В.А. 105, 109, 113, 116

В

Васильєв Ю.С. 24
Васильченко Є.Р 59
Вирвихвост О.В. 49
Вовсянікер М.Ю. 99
Воргуль О.В. 66, 103, 122

Г

Галкін П.В. 136, 140
Головатенко С.В. 63
Горбенко Є.О. 20, 24
Грисенко А.О. 77

Д

Дерюга І.М. 129

З

Забрянська М.О. 69
Зелінська А.О. 69
Зубарєв В.О. 91
Зубков О.В. 8, 73

Ж

Желавський Д.Ю. 77

І

Іванов Л.С. 55
Іванова О.О. 47

К

Карнаушенко В.П. 20, 24
Кирпота Ф.В. 28
Кожем'якін М.В. 84
Колісник В.І. 80
Костін Д.О. 12
Кудря Т.К. 140
Куркурін І.П. 16
Кушнарьов А.О. 113

Л

Літовченко О.А. 122
Лузан М.С. 53

М

Марченко С.М. 88
Мачоніс Т.С. 119
Мірошніченко С.Ю. 43

Н

Натарова В.С. 40
Новоселов С.П. 4

О

Обод І.І. 63
Олійник В.В. 73

П

Павлій С.С. 73
Патлан Є.О. 116
Передерій І.А. 105
Поддубняк І.А. 36
Посохова Г.Є. 109
Посошенко В.О. 91
Пятайкіна М.І. 20, 24

С

Свид І.В. 63, 119, 125
Сердюк С.Л. 47
Сичова О.В. 8
Скорбатюк М.В. 125
Сотник С.В. 28, 32, 59
Столовий І.В. 101

Т

Тимофєєва К.О. 88
Толкунов І.О. 16, 55

Х

Халімонов Я.І. 32
Холопов В.В. 91

Ц

Цехмістро Р.І. 84
Цимбал О.М. 36

Ч

Чала О.О. 40
Чумак В.С. 129, 132, 134

Ш

Шаповал І.Р. 136
Шафроненко Є.О. 69

Я

Яковенко О.С. 8
Янушкевич Д.А. 43, 49, 53, 55
Яценко В.С. 84

ЗМІСТ

Новоселов С.П., Сичова О.В. *Розроблення віртуальної лабораторної роботи з дослідження основ роботи АЦП* 4

Зубков О.В., Яковенко О.С. *Реалізація цифрових фільтрів на мікроконтролерах STM32 з використанням кільцевих буферів* 8

Костін Д.О. *Роботизована система для економічного автоматизованого нанесення паяльної маски та захисного покриття на підкладках з текстоліту* 12

Толкунов І.О., Куркурін І.П. *Застосування роботизованої техніки, оснащеної вогнепальною зброєю, для знищення вибухонебезпечних предметів* 16

Пятайкіна М.І., Горбенко Є.О., Карнаушенко В.П. *QSPICE – поповнення в ряду симуляторів* 20

Пятайкіна М.І., Горбенко Є.О., Васильєв Ю.С., Карнаушенко В.П. *Виклики п'ятої індустріальної революції* 24

Сотник С.В., Кирпота Ф.В. *Огляд базових елементів автоматизованої системи контролю навколишнього середовища портативної ділянки зеленого побуту* 28

Сотник С.В., Халімонов Я.І. *Аналіз систем автоматизації визначення умов у житлових та робочих приміщеннях з використанням комп'ютерно-інтегрованих рішень* 32

Поддубняк І.А., Цимбал О.М. *Аналіз комп'ютерного зору в сучасних симуляторах роботів* 36

Натарова В.С., Чала О.О. *Сучасні тенденції мікропроцесорної техніки* 40

Янушевич Д.А., Мірошніченко С.Ю. *Розроблення автоматизованої системи управління для знешкодження вибухонебезпечних предметів* .. 43

Іванова О.О., Сердюк С.Л. *Порівняльний аналіз антен Коха та Гільберта для прийому сигналів на частоті 2100 МГц* 47

Вирвихвост О.В., Янушкевич Д.А. *Апаратний модуль робототехнічного комплексу для пошуку вибухонебезпечних предметів* 49

Лузан М.С., Янушкевич Д.А. *Моделювання робототехнічної системи для дистанційного знешкодження вибухонебезпечних предметів* 53

Янушкевич Д.А., Іванов Л.С., Толкунов І.О. *Креативні підходи управління якістю у сфері гуманітарного розмінування із застосуванням робототехнічних систем* 55

Sotnik S.V., Vasylchenko Y.R. *Analysis of design process of automated fire protection system* 59

Головатенко С.В., Обод І.І., Свид І.В. *Аналіз системи селекції рухомих цілей в РЛС* 63

Воргуль О.В., Беззабарний Д.І. *Огляд програмного забезпечення для виконання проектів на ПЛІС* 66

Шафроненко Є.О., Зелінська А.О., Забрянська М.О. *Огляд візуальних мов програмування* 69

Зубков О.В., Олійник В.В., Павлій С.С. *Аналіз технологій віддаленого доступу до пристроїв на мікроконтролерах* 73

Желавський Д.Ю., Бабич О.В., Грисенко А.О. *Вплив тактової частоти оперативної пам'яті на продуктивність комп'ютерних систем* 77

Колісник В.І., Бабич О.В., Анур'єва К.С. *Особливості використання сучасних графічних форматів* 80

Цехмістро Р.І., Кожем'якін М.В., Яценко В.С. *Учбова автоматизована система розрахунку статичних h-параметрів біполярного транзистору з використанням моделі реального транзистору та вбудованого мікроконтролерного пристрою* 84

Марченко С.М., Тимофєєва К.О. *Прогнозування руху біржевих котирувань* 88

Посошенко В.О., Холопов В.В., Зубарєв В.О. *Мультимодальний підхід до спостереження БПЛА* 91

Шаповалов С.В., Романовська І.О., Озернюк Т.В. *Пристрій підвищення та стабілізації напруги Power Bank* 95

Вовсянікер М.Ю., Білоцерківець О.Г. *Використання штучного інтелекту в галузі FPGA* 99

Столовий І.В., Білоцерківець О.Г. *Огляд пристрою KRIA KV260 VISION AI для інтелектуального машинного бачення* 101

Білоцерківець О.Г., Воргуль О.В. *Використання ESP-EYE для пошуку речей з залученням AI та функції активації голосом* 103

Булага В.А., Передерій І.А. *Сучасні тенденції кібербезпеки банківських рахунків та банківських будівель* 105

Булага В.А., Посохова Г.Є. *Порівняльний аналіз безпекових характеристик операційних систем Windows і Linux* 109

Булага В.А., Кушнарьов А.О. *Аналіз рівня безпеки веб-сервісів* 113

Булага В.А., Патлан Є.О. *Програмні засоби аналізу локальних мереж щодо уразливостей* 116

Мачоніс Т.С., Свид І.В. *Огляд інноваційних рішень Xilinx* 119

Літовченко О.А., Воргуль О.В. *Керування мікроконтролером за допомогою мовного каналу* 122

Скорбатюк М.В., Свид І.В. *Огляд архітектури Versal ACAP* 125

Дерюга І.М., Чумак В.С. *Дослідження можливості використання алгоритму Прюіт для обробки медичних зображень* 129

Чумак В.С. *Інтеграція нейронних мереж у медичні пристрої на основі STM32 для автоматичної діагностики та моніторингу пацієнтів* 132

Чумак В.С. *Використання нейронних мереж в адаптивних системах онлайн-медичної освіти на базі мікроконтролерів STM32 в умовах воєнних криз* 134

Галкін П.В., Шаповал І.Р. *Сучасні тенденції впровадження SMART-лабораторій для IIOT* 136

Галкін П.В., Кудря Т.К. *Розробка TESTBENCH на базі вбудованих систем для дослідження концепції Індустрії 5.0* 140

МАТЕРІАЛИ

V ФОРУМУ
«Автоматизація, електроніка та робототехніка.
Стратегії розвитку та інноваційні технології»
AERT-2023

Відповідальний за випуск: Свид І.В.

Комп’ютерна верстка Свид І.В.

Матеріали збірника публікуються в авторському варіанті
без редагування

ХНУРЕ 61166, Харків, просп. Науки, 14

Тел. +38 (057) 755 0220, e-mail: iryna.svyd@nure.ua

Свідоцтво суб’єкта видавничої справи ХНУРЕ : Серія ДК № 7529 від 03.12.2021 р.