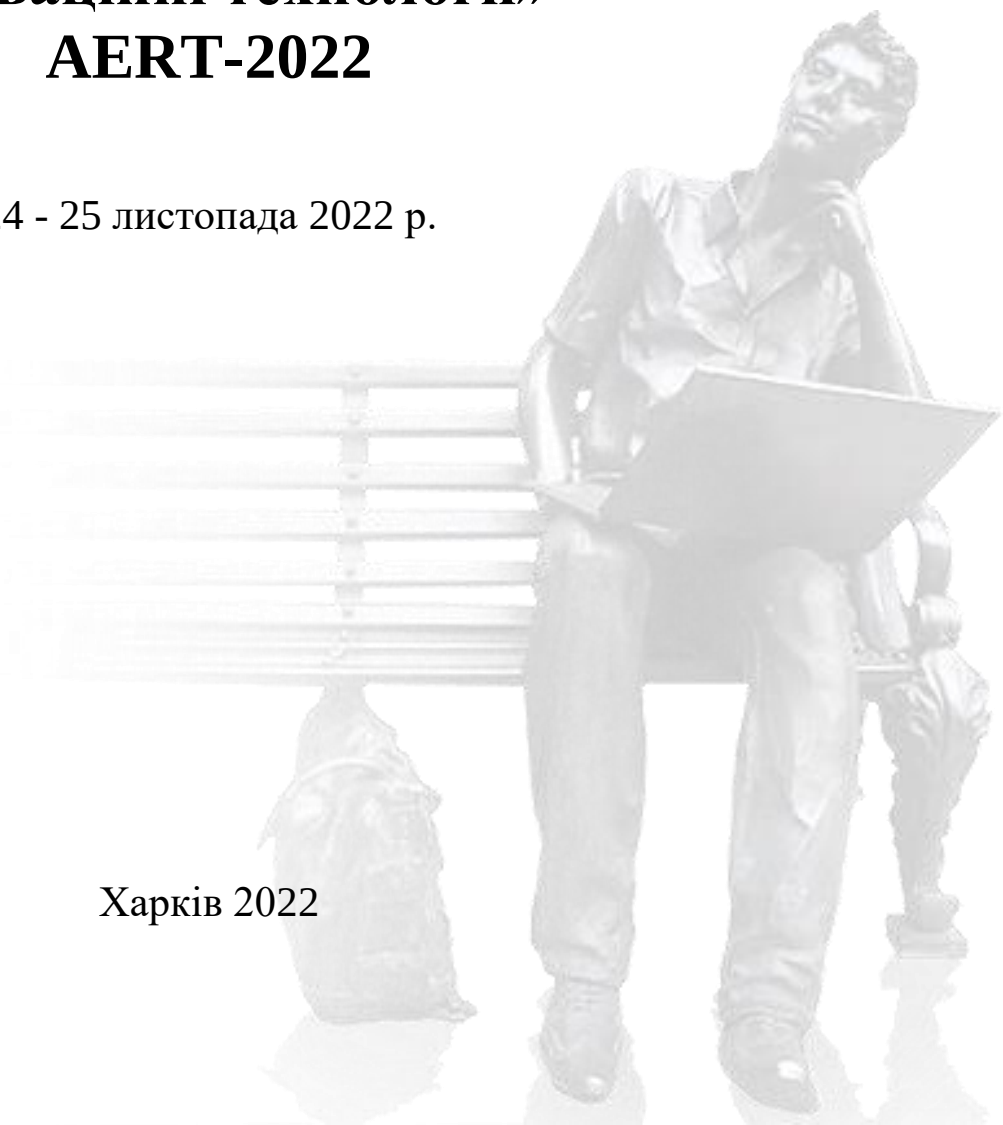
Харківський національний університет радіоелектроніки

МАТЕРІАЛИ
IV ФОРУМУ
«Автоматизація, електроніка та робототехніка. Стратегії розвитку та інноваційні технології»
AERT-2022

24 - 25 листопада 2022 р.



Харків 2022

Збірник матеріалів IV форуму «Автоматизація, електроніка та робототехніка. Стратегії розвитку та інноваційні технології» AERT-2022. – Харків, ХНУРЕ, 2022. – 178 стр.

В збірник включені матеріали IV форуму «Автоматизація, електроніка та робототехніка. Стратегії розвитку та інноваційні технології» AERT-2022.

IV форум «Автоматизація, електроніка та робототехніка. Стратегії розвитку та інноваційні технології» AERT-2022 проведено кафедрами:

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

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

© Харківський
національний університет
радіоелектроніки (ХНУРЕ), 2022

КОМІТЕТ ФОРУМУ

Голова комітету форуму:

Рубан І.В.	д.т.н., проф., в.о. ректора ХНУРЕ, перший проректор ХНУРЕ, м. Харків, Україна.

Програмний комітет форуму:

Семенець В.В.	д.т.н., проф., проф. каф. БМІ ХНУРЕ, м. Харків, Україна.
Свид І.В.	к.т.н., доц., зав. каф. МТС ХНУРЕ, м. Харків, Україна.
Новоселов С.П.	к.т.н., доц., проф. каф. КІТАМ ХНУРЕ, м. Харків, Україна.
Обод І.І.	к.т.н., проф., проф. каф. МТС 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., старший викладач каф. КІТАМ ХНУРЕ, м. Харків, Україна.

Секретаріат комітету форуму:

Теслюк С.І.	старший викладач каф. КІТАМ 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.

АВТОМАТИЗАЦІЯ КОНТРОЛЮ ВИКОНАННЯ МОНТАЖНИХ ОПЕРАЦІЙ

професор, к.т.н., Новоселов С.П., студент Пащенко Є.В.
Харківський національний університет радіоелектроніки,
кафедра КІТАМ, м. Харків, Україна
e-mail: sergiy.novoselov@nure.ua, yevhenii.pashchenko@nure.ua

Abstract. This paper presents the developed scheme of the automated system for monitoring the execution of assembly operations. The basis of the proposed scheme is a technical vision system for detecting defects after assembly operations. The technical vision system is integrated into the technological sequence of operations on the conveyor of the assembly shop. The proposed scheme of the automated system for monitoring the execution of assembly operations allows you to perform current control at the stage of the operation to quickly eliminate defects. In this scheme, the automated system monitors the actions of a worker who performs manual assembly operations for installing components on the chassis of the device.

Вступ. Впровадження автоматизованих систем контролю якості продукції, що виробляється виробничим підприємством, є досить актуальною задачею. Для цього застосовуються різні додаткові програмні й апаратні засоби. Наприклад, дуже популярною наразі є використання системи комп'ютерного зору для виконання задач контролю монтажних операцій.

Під якістю виробництва розуміють ступінь відповідності виготовленого виробу заданим розмірам, формі, механічним, фізичним та іншим характеристикам, які з призначення цього вироби. Точність виконання операції відрізняється від точності всього процесу. Застосування операцій контролю на кожній стадії виробництва підвищує якість виробництва та знижує розхід матеріалів і тим самим дозволяє знизити вартість кінцевої продукції.

Якість кінцевого виробу багато в чому залежить від правильного виконання операції встановлення компонентів на друковані плати або шасі [1]. Організація контролю при виробництві електронних засобів переслідує дві мети: вилучення браку і попередження його. Особливо актуальним і відповідальним є контроль в автоматизованому виробництві, в якому вся сукупність технологій і технічних засобів, пов'язаних інформаційними потоками, складає систему автоматизованого контролю (САК).

В автоматизованому виробництві САК має забезпечувати не тільки отримання заданої якості продукції, але і безвідмовний хід виробничого процесу. У комплекс задач контролю автоматизованих виробництв входять також контроль за забезпеченням безперебійних потоків виробів,

інструментів, пристосувань і вимірювальних пристроїв, перевірка стану інформаційних зв'язків усередині комплексу і між технологічними комплексами, транспортних систем, систем керування виробничим процесом.

Основна частина. Об'єктом дослідження в даній роботі є система контролю якості виконання монтажних операцій. Предмет дослідження – методи визначення правильності розташування компонентів на монтажній основі з використанням системи комп'ютерного зору.

Враховуючи проведений аналіз предметної області розроблено схему роботи автоматизованої системи контролю виконання монтажних операцій (рис. 1).

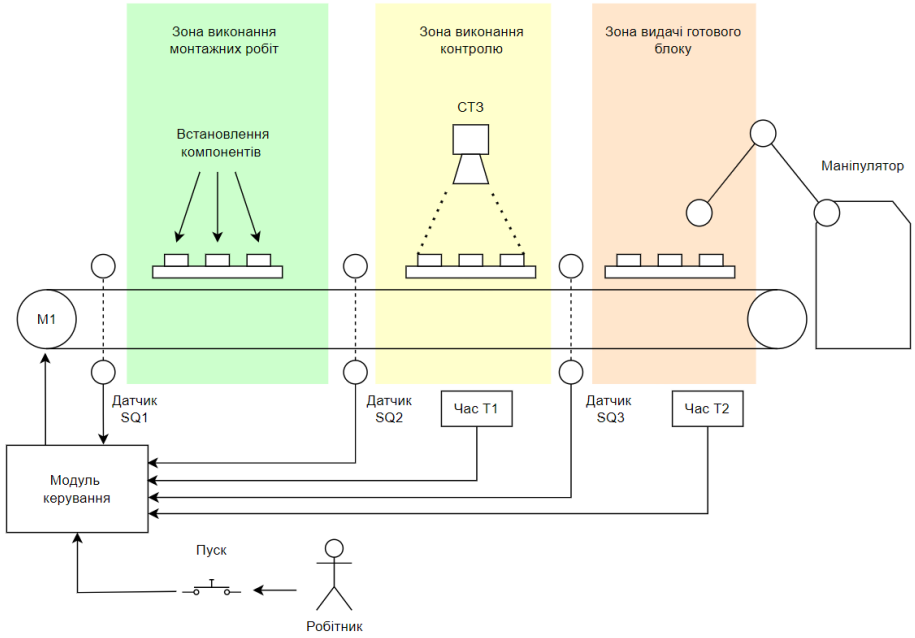


Рисунок 1 – Схема роботи автоматизованої системи контролю виконання монтажних операцій

Основою запропонованої схеми є система технічного зору для виявлення дефектів після монтажних операцій. Система технічного зору інтегрована в технологічну послідовність операцій на конвеєрі збирального цеху [2]. В даній схемі автоматизована система контролює дії робітника, що виконує ручні монтажні операції з встановлення компонентів на шасі приладу.

Робітник виконує необхідні операції та після їх завершення запускає конвеєр із спеціальним лотком для переміщення шасі до зон контролю. Для цього він кладе шасі в напрямні та має змогу натиснути на кнопку «Завершення операції».

У вихідному положенні механізму кінцевий датчик SQ1 знаходиться в стані включено. Це той випадок, коли лоток із шасі приладу знаходиться в зоні виконання монтажних операцій (рис 1, зелена зона).

Цикл роботи починається після надходження команди "Пуск" від працівника після завершення монтажної операції. Механізм переміщується в положення, що фіксується кінцевим вимикачем SQ2 – це зона виконання контролю. В даному стані система знаходиться протягом часу Δt_1 (рис 1, жовта зона).

У випадку, коли помилок в монтажу не знайдено, лоток переміщується в положення, що фіксується кінцевим вимикачем SQ3. В даному положенні шасі стоїть протягом часу Δt_2 (рис 1, червона зона).

Після видалення шасі з лотка за допомогою маніпулятора, механізм повертається в вихідне положення. Для повторення циклу необхідно знов подати команду "Пуск".

Якщо система технічного зору знаходить помилку в монтажу, шасі переміщується в першочергове положення. Якщо команда від працівника буде надходить безперервно, то після відпрацьовування одного циклу автоматично починається наступний.

Приймемо наступні позначення вхідних і вихідних сигналів, а також сигналів таймерів, які необхідно розглядати як вхідні сигнали для графа переходів.

Вхідні сигнали:

– a – команда "Пуск";

– b, c, d – сигнали кінцевих вимикачів SQ1, SQ2, SQ3 відповідно;

– t_1, t_2 – сигнали таймерів, що дають затримки Δt_1 і Δt_2.

Вихідні сигнали:

– f_1 – команда на переміщення механізму з вихідного положення;

– f_2 – команда на повернення механізму в вихідне положення.

Синтез релейної схеми для керування автоматизованою системою починаємо з визначення кількості станів, в яких може перебувати схема автоматичного керування. Таких станів шість:

– 1 – вихідне положення;

– 2 – переміщення з вихідного положення;

– 3 – стоянка протягом часу Δt_1;

– 4 – подальше переміщення;

– 5 – стоянки протягом часу Δt_2;

– 6 – повернення в вихідне положення.

Застосувавши процедуру, що описана в [3], визначення умов вмикання і скидання тригерів:

$$S_{P_1} = ap_2\overline{p_3}; \quad (1)$$

$$R_{P_1} = a\overline{p_2}p_3 + \overline{p_2}\,\overline{p_3}; \quad (2)$$

$$S_{P_2} = c\overline{p_1}p_3; \quad (3)$$

$$R_{P_2} = bp_1p_3; \quad (4)$$

$$S_{P_3} = a\overline{p_1}\,\overline{p_2} + t_2p_1p_3; \quad (5)$$

$$R_{P_3} = t_1\overline{p}_1 p_3 + \overline{a}p_1\overline{p}_2. \quad (6)$$

Формули для вихідних сигналів f_1 і f_2 записуються як комбінаційні функції вихідних сигналів тригерів P_1, P_2 , P_3. Дійсно, функція f_1 =1 в станах 2 і 4, тобто в станах, яким відповідають такі комбінації значень вихідних сигналів тригерів: $p_1 = 0$, $p_2 = 0$, $p_3 = 1$ і $p_1 = 0$, $p_2 = 1$, $p_3 = 0$. Тому

$$f_1 = \overline{p}_1\overline{p}_2 p_3 + \overline{p}_1 p_2\overline{p}_3. \quad (7)$$

Аналогічно, функція $f_2 = 1$ в стані 6 ($p_1\, p_2\, p_3 = 111$), тобто

$$f_2 = p_1 p_2 p_3. \quad (8)$$

Таймер T_1 вмикається в стані 3 ($p_1\, p_2\, p_3 = 011$), а таймер T_2 – в стані 5 ($p_1\, p_2\, p_3 = 110$), тому

$$T_1 = \overline{p}_1 p_2 p_3. \quad (9)$$

$$T_2 = p_1 p_2\overline{p}_3. \quad (10)$$

Висновки. Таким чином, в даній роботі розроблено схему роботи автоматизованої системи контролю виконання монтажних операцій. Основою запропонованої схеми є система технічного зору для виявлення дефектів після монтажних операцій. Система технічного зору інтегрована в технологічну послідовність операцій на конвеєрі збирального цеху.

Виконано синтез математичної моделі запропонованої автоматизованої системи, за якою можна побудувати релейно-контактну схему для промислового контролеру.

Запропонована схема автоматизованої системи контролю виконання монтажних операцій дозволяє вже на етапі виконання операції виконувати поточний контроль для швидкого усунення дефектів. Таким чином, знижується час на виправлення помилок і зменшується кількість бракованих виробів на виробництві.

Список використаних джерел.

1. Пушкар, М.С. Проектування систем автоматизації [Текст]: навч. посібник / М.С. Пушкар, С.М. Проценко – Д.: Національний гірничий університет, 2013. – 268 с.

2. Пащенко Є.В. Побудова SIFT дескрипторів і завдання зіставлення зображень для автоматизованої системи розпізнавання деталей на виробництві [Текст] // 25-й Міжнародний молодіжний форум «Радіоелектроніка та молодь у XXI столітті». Зб. матеріалів форуму. Т. 2. – Харків: ХНУРЕ. 2021 – 19-20 с.

3. Grout I. Digital Systems Design with FPGAs and CPLDs. Amsterdam: Elseveit, 2008. 784 p.

ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ WEB СЕРВЕРІВ НА МОДУЛЯХ ESP8266 ТА ESP32 У ARDUINO IDE

доцент, к.т.н. Зубков О.В., студент Зубков А.О.
Харківський національний університет радіоелектроніки,
кафедра МТС, м. Харків, Україна
e-mail: oleh.zubkov@nure.ua, artem.zubkov@nure.ua

Abstract. The shortcomings of the Web servers implementation based on ESP8266 and ESP32 modules are considered. The choice of file system for storing Web site content is substantiated. The advantages and disadvantages of using the AsyncWebServer and WebServer libraries to implement Web servers in the Arduino IDE in the ESP8266 and ESP32 modules are determined. Measurements of the loading web pages with content speed for different modifications of modules and using different libraries of Web servers were performed. Practical recommendations are given to the principles of updating information on a Web page to achieve maximum performance. The disadvantages of using the ArduinoJSON library on dual-core processors are revealed.

Вступ. Останні роки характеризуються значним ростом ринку IoT речей та систем автоматизації. Сучасна промисловість може дозволити вкладати великі кошти у створення систем автоматизації на брендовому обладнанні таких виробників, як Siemens, ABB, GE Fanuc і т.д. Однак однією з головних вимог до систем автоматизації приватного житла, малого бізнесу є невелика ціна таких систем. Саме тому все більше проектів реалізується на сучасних WiFi модулях ESP8266 та ESP32 [1, 2]. Обидва модулі мають чіпи з підтримкою сучасних стандартів WiFi і можуть конфігуруватися, як точка доступу або клієнт WiFi мережі на базі роутера, вони мають цифрові лінії для підключення різних датчиків та сухих контактів, багато сучасних інтерфейсів для взаємодії з будь-якою периферією. Однак першій модуль має одноядерний процесор із тактовою частотою 80МГц, а другий двохядерний із частотою 160-240МГц, більшу розрядність аналого-цифрового перетворювача, цифро-аналоговий перетворювач. Для початкового конфігурування модуля, що є складовою частиною автоматизованої системи, або керування за його допомогою цією системою необхідно реалізовувати Web сервер на базі такого модуля. Багато розробників електронної апаратури вважають, що з реалізацією серверу багато складнощей, він повільно працює і відмовляються від використання ESP8266 і ESP32 та використовують більш дорогі рішення. Тому, метою цього дослідження було знаходження рішень, що відповідають сучасним вимогам з розробки Web серверів та забезпечують високу швидкість роботи серверу на процесорах з малою тактовою частотою.

Основна частина. Розробка програмного забезпечення Web серверів складається з двох частин: backend (програмне забезпечення, що запускається на сервері – у нашому випадку у ESP8266 чи ESP32) та frontend (web сторінка, що передається користувачу за його запитом та відображується браузером) [3, 4]. Цю розробку виконують різні спеціалісти-розробники, які, навіть, можуть працювати окремо та незалежно, обговорюючи лише структуру сайту. Тобто контент сайту (web сторінки, графічні файли, css файли) повинен розроблятись і зберігатись окремо від головної керуючої програми серверу. Це скорочує розробку та дозволяє оновлювати будь-яку складову сайту незалежно від інших складових. Але у більшості прикладів проектів для ESP8266 та ESP32 у код backend складової вбудовується код web сторінки для збільшення швидкості роботи сайту і це є помилковим рішенням. Для вирішення цієї проблеми необхідно розділяти загальну пам'ять модулів ESP8266 та ESP32 на дві частини: 1) для зберігання керуючої програми; 2) для складових frontend частини із реалізацією файлової системи. Найбільш популярними файловими системами є SPIFFS, litleFS, FatFS. Хоча файлову систему SPIFFS позиціонують, як спеціально розроблену для використання в ESP8266 та ESP32, але її супровід з боку розробників припинений ще у 2019 році. Експериментальна перевірка показала, що у модулях ESP8266 така система реалізується без проблем, а у останніх версіях модулів ESP32 виникають проблеми із записом файлів у створений розділ SPIFFS. На відміну від SPIFFS файлова система FatFS однаково добре реалізується та функціонує у всіх сучасних модифікаціях ESP8266 та ESP32, що підтверджує експериментальна перевірка. Завантаження файлів у створену файлову систему може відбуватись з використанням спеціалізованих додаткових інструментів (наприклад, ESP32 Sketch Data Uploader у Arduino IDE) або за допомогою вбудованого у серверну програму Ftp серверу.

Найчастіше для розробки програмного забезпечення для ESP8266 та ESP32 використовується середовище Arduino IDE у сукупності із бібліотеками реалізації серверів AsyncWebServer та WebServer. Обидва сервери дозволяють за запитом клієнту відкрити необхідний .html, .css і т.д. файли сайту, що зберігаються у розділі із файловими системами SPIFFS, litleFS, FatFS. Перевагами AsyncWebServer є: обробка запитів клієнтів за подією та можливість заповнювати шаблони html сторінок поточними даними перед відправкою клієнту. Це дає можливість створювати програми великого об’єму у головному нескінченому циклу не затримуючи обробку запитів клієнтів. Але головним недоліком є необхідність пропису реакції на запит завантаження будь-якого файла на рівні керуючої серверної програми. Тобто при зміні контенту web сайту необхідно вносити зміни і в серверну частину для додавання завантаження нових сторінок, графічних файлів і т.д. При використанні бібліотеки WebServer є можливість потокового завантаження будь-якого файлу з

файлової системи. Тобто можна створити універсальну функцію потокового зчитування будь-якого файлу контенту web сайту і при додаванні нових файлів чи вилученні існуючих немає потреби вносити зміни у існуючий код серверної частини програмного забезпечення. Головним недоліком бібліотеки WebServer є необхідність створювати нескінчений цикл і у ньому перевіряти – чи не надійшли нові запити від користувачів на завантаження чи оновлення web сторінок або їх контенту. Це призводить к обмеженню об'єму, а відповідно і часу виконання, програми, що розташовується у нескінченому циклу разом із частиною коду перевірки нових запитів від клієнтів. Тобто використання бібліотеки WebServer відповідає сучасним вимогам до розробки backend та frontend частин сайту, але для модулів ESP8266 його використання ефективне лише у випадку невеликого часу (декілька мілісекунд) виконання програми, що розташована у нескінченому циклі. Для модулів ESP32 таких обмежень не існує, бо тут використовується двохядерний процесор, у якому одне з ядер можна задіяти для обробки запитів клієнтів, а інше для реалізації головного керуючого алгоритму. Для експериментальної перевірки ефективності роботи бібліотек AsyncWebServer та WebServer було створено серверну та клієнтську частини сайту із завантаженням не тільки html сторінок, але й з додатковими файлами css, js і завантаженням двох графічних зображень у форматі jpg. При використанні AsyncWebServer та ESP32 час первинного завантаження сторінки був 0,9с, а при використанні WebServer 0,4с. При використанні модулів ESP8266 час збільшився у 1,8 рази.

При розробці frontend частини сайту також слід приділяти значну увагу вимогам до розробки web сторінок. Після першого завантаження сторінки оновлення зображень на сторінці, а також показань датчиків, стану системи можна реалізувати із оновленням всієї сторінки цілком, або лише окремих її елементів. Оновлення усієї сторінки спрощує розробку, але кожне перезавантаження сторінки потребує часу, що відповідає часу початкового завантаження сторінки. Реалізація оновлення стану лише деяких елементів web сторінки потребує написання додаткових скриптів на сторінці і відповідних функцій передавання серверною частиною короткого пакету інформації, але значно зменшує час оновлення, значення котрого не перевищує 0,1с у практичних прикладах. Також при написанні коду html сторінки можна значно скоротити час завантаження зображень, коли, наприклад, декілька зображень відповідають одному елементу сторінки та відображають різні стани цього елементу. Якщо при першому завантаженні сторінки завантажувати графічні зображення, що містять одночасно графічний вигляд усіх станів деякого елементу системи, а потім показувати на сторінці лише частину цього зображення, що відповідає поточному стану елементу сторінки, то немає необхідності знов зчитувати це зображення з серверу, а достатньо користуватись зображенням, що вже

є. Для реалізації такого підходу достатньо прописати клас для елементу сторінки та у java скрипті забезпечити зміну зображення. При передаванні даних для оновлення елементів web сторінки від сервера до клієнта дуже популярною є бібліотека ArduinoJSON. Але, як показали практичні досліди, у випадку використання двохядерних процесорів і одночасного доступу із підпрограм різних ядер до загальної структури JSON, виникають помилки запису і цю бібліотеку не слід використовувати.

Останнім важливим елементом реалізації сайту є вибір між реалізацією синхронних чи асинхронних запитів до серверу. У стандартних сайтах, що не керують автоматизованими системами, використовують асинхронні запити, тобто користувач, наприклад, натиснувши кнопку, не очікує результату а може далі щось робити на сторінці. Такий підхід є невірним для багатьох систем автоматизації, бо лише після виконання однієї команди у автоматизованій системі можна виконувати наступну і користувач повинен очікувати завершення виконання його попередньої команди. Синхронні запити дозволяють вирішити ці запити.

Висновки. Реалізація сучасних web серверів на модулях ESP8266 та ESP32 в середовищі Arduino IDE повинна реалізовуватись з розміщенням контенту сайту у розділі з файловою системою FatFS, що дозволяє реалізувати роздільний підхід до розробки backend та frontend частин програмного забезпечення. Виходячи з цієї умов також слід використовувати бібліотек WebServer для завантаження контенту сайту клієнту. Лише при значному часі виконання головної програми у ESP8266 слід використовувати бібліотеку AsyncWebServer. При оновленні інформації на сторінці у клієнта слід активно використовувати JS, оновлюючи лише стан елементів сторінки.

Список використаних джерел.

1. Yogendra Singh Parihar Internet of Things and Nodemcu A review of use of Nodemcu ESP8266 in IoT products. ETIR, 2019, Vol.6, Issue 6, pp. 1085-1088.

2. T. Sandeep Rao, Pawan Pranay, Sriman Narayana, Yamunadhar Reddy, Sunil, Pawandeep Kaur ESP32 Based Implementation of Water Quality and Quantity Regulating System. Proceedings of the 3rd International Conference on Integrated Intelligent Computing Communication & Security, Vol. 4, pp. 122-129.

3. Dlnya Abdulahad Aziz Webserver Based Smart Monitoring System Using ESP8266 Node MCU Module International. Journal Of Scientific & Engineering Research, 2018, Volume 9, Issue 6, pp. 801-807.

4. P. Machesoa, S. Chisale, C. Dakab, N. Dzupirec, J. Mlathodand, D. Mukanyirigira Design of Standalone Asynchronous ESP32 Web-Server for Temperature and Humidity Monitoring. 7th International Conference on Advanced Computing and Communication Systems, 2021, pp. 76-79.

ВИКОРИСТАННЯ ВІРТУАЛЬНИХ ЛАБОРАТОРНИХ МАКЕТІВ ДЛЯ НАЛАГОДЖЕННЯ ТЕХНОЛОГІЧНИХ ПРОГРАМ ПЛК

професор, к.т.н., Новоселов С.П., доцент, к.т.н., Сичова О.В.
Харківський національний університет радіоелектроніки,
кафедра КІТАМ, м. Харків, Україна
e-mail: sergiy.novoselov@nure.ua, oksana.sychova@nure.ua

Abstract. This work considers the possibility of using digital duplicates of automation devices in a laboratory workshop. Also shown is one of the possible implementations of a universal software platform for creating virtual devices using the example of a dosing device. The possibility of applying the method of synthesis of a relay-contact circuit based on RS-triggers is demonstrated.

Вступ. На етапі підготовки фахівців, в процесі навчання, коли досвіду роботи з програмованими логічними контролерами (ПЛК) ще недостатньо, лабораторні макети відіграють найважливішу роль – розвивають навички в інженерів передбачувати можливі наслідки від помилки в програмі. Для цього створюються макети реальних пристроїв, верстатів або навіть цілих автоматизованих виробничих ділянок.

Перевага лабораторних макетів – це можливість наочно побачити результати роботи програми для ПЛК в дії на прикладі реального обладнання. В останні роки навчання переважно відбувається онлайн з використанням дистанційних технологій. В таких умовах використовувати реальні лабораторні макети виявляється практично неможливо. Тому створення віртуальних цифрових двійників пристроїв автоматизації є актуальною задачею, вирішення якої значно підвищить рівень підготовки фахівців у відповідній галузі. Концепція віртуальних макетів передбачає можливість як найповніше імітувати поведінку реальних пристроїв. Це стосується і анімації переміщення рухомих частин приладу, і способів підключення до самого макету. В даній роботі подано одну з можливих реалізацій універсальної програмної платформи на прикладі дозуючого пристрою.

Основна частина.

В основу платформи була закладена можливість взаємодії з віртуальним пристроєм через декілька комунікаційних протоколів: Serial Protocol, Modbus TCP/IP, Inter-Process Communication. В процесі навчання основам програмування ПЛК, а також основам застосування електропневмоавтоматичних приводів для автоматизації технологічних процесів використовується програмний засіб LDmicro [1]. Цей проєкт динамічно розвивається, має відкритий вихідний код та перетворює звичайний мікроконтролер в «промисловий» контролер, що програмується за допомогою технологічної мови LD. Наявність відкритого коду дало можливість зробити необхідні зміни в роботі програми та додати таку

функцію, як обмін даними між зовсім незалежними програмами через іменовані канали (Named Pipes) за допомогою технології IPC (Inter-Process Communication) [2].

Створена універсальна платформа складається з трьох рівнів: комунікаційного, обробки даних, візуалізації. Загальний комунікаційний рівень використовується для взаємодії зі сторонніми програмними середовищами розробки технологічних програм, або навіть з апаратними засобами. Рівень накопичення та обробки даних використовується для обміну інформацією між нижнім і верхнім рівнями. На даному рівні виконується інтерпретація змінних, що використовуються у технологічній програмі та масивами даних, з якими працюють графічні компоненти. Візуалізація процесу відбувається на верхньому рівні. Він створюється засобами програмування мовою C# та його зовнішній вигляд залежить від принципу дії того макету, дія якого симулюється і може бути реалізована як 3D або 2D-анімація. За допомогою вбудованого редактора властивостей призначаються змінні та закріпляються за відповідними графічними компонентами. В подальшому, отриманні дані візуалізуються, а динамічні компоненти, наприклад, кнопки, генерують потік інформації, яка впливає на хід роботи технологічної програми. Таким чином відбувається емуляція роботи реального пристрою.

Розглянемо приклад вирішення задачі автоматизації дозуючого пристрою з наступними умовами. У вихідному положенні ємність порожня і всі крани перекриті. Кнопка «Пуск» запускає роботу пристрою на один цикл. З надходженням сигналу a кнопки «Пуск», спрацьовує датчик першого крану K_1 і у дозуючий пристрій наливається рідина 1 поки не спрацює датчик d_1 – датчик потрібного об’єму рідини 1 (рис. 1, а). Після спрацьовування датчика, K_1 закривається і відкривається K_3, через який рідина 1 зливається у ємність. Після спрацьовування датчика d_0, який показує, що дозуючий пристрій порожній, відкривається кран K_2, що наповнює пристрій рідиною 2 до рівня d_2. Після цього рідина 2 також зливається у ємність. Якщо кнопка «Пуск» натиснена, то цикл повторюється спочатку, якщо ні, то повертаємося у початкове положення.

Таким чином, станів, в яких перебуває система, буде шість:

– 1 – початковий ($K_1 = 0$, $K_2 = 0$, $K_3 = 0$);

– 2 – наливається рідина 1, $K_1 = 1$;

– 3 – виливається рідина 1, $K_3 = 1$;

– 4 – наливається рідина 2, $K_2 = 1$;

– 5 – виливається рідина 2, $K_3 = 1$;

– 6 – повернення у початковий стан ($K_1 = 0$, $K_2 = 0$, $K_3 = 0$).

Графоперехід за умовою задачі подано на рис. 1, б. Запишемо рівняння які визначають умови вмикання тригерів [3]:

$$S_{P_1} = d_2\overline{p_2}p_3; \quad (1)$$

$$S_{P_2} = a\overline{p_1}\,\overline{p_3} + \overline{d_0}p_1p_3; \quad (2)$$

$$S_{P_3} = d_1\overline{p_1}p_2; \quad (3)$$

Умови скидання тригерів:

$$R_{P_1} = ap_2\,\overline{p_3} + \overline{p_2}\,\overline{p_3}; \quad (4)$$

$$R_{P_2} = \overline{a}\,p_1\,\overline{p_3} + \overline{d_0}\,\overline{p_1}\,p_3; \quad (5)$$

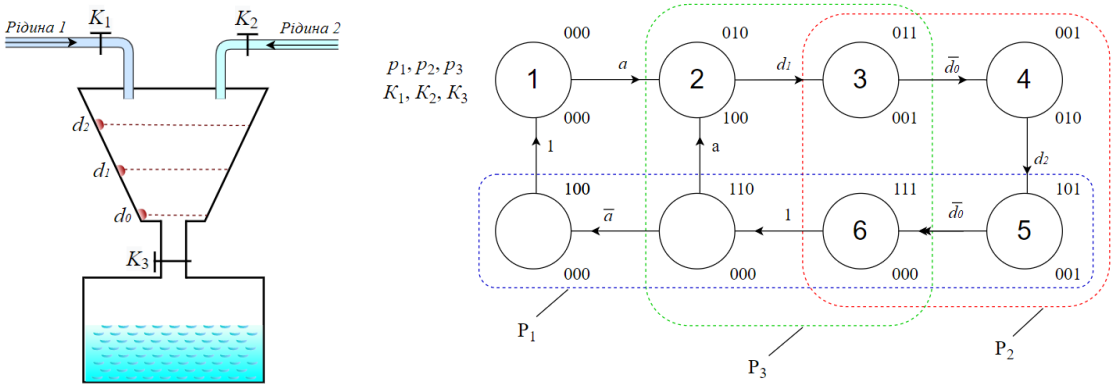
$$R_{P_3} = p_1p_2; \quad (6)$$

Формули для вихідних змінних:

$$K_1 = \overline{p_1}\,p_2\,\overline{p_3}; \quad (7)$$

$$K_2 = \overline{p_1}\,\overline{p_2}\,p_3; \quad (8)$$

$$K_3 = \overline{p_1}\,p_2\,p_3 + p_1\,\overline{p_2}\,p_3; \quad (9)$$



а) б)

Рисунок 1 – Дозуючий пристрій (а) і граф переходів (б)

Віртуальний макет дозуючого пристрою (рис. 2) дозволяє провести експериментальні дослідження. Кнопки *XSP_key1* та *XSP_key2* макету вмикають перший та другий крани *YSPK_1* та *YSPK_2* відповідно. Червона кнопка *XSP_key3* зливає рідину до резервуару, відкриваючи кран *YSPK_3*. Датчики *XSP_sns1*, *XSP_sns2* та *XSP_sns3* призначені для регулювання потрібного рівня рідини у ємності дозуючого пристрою.

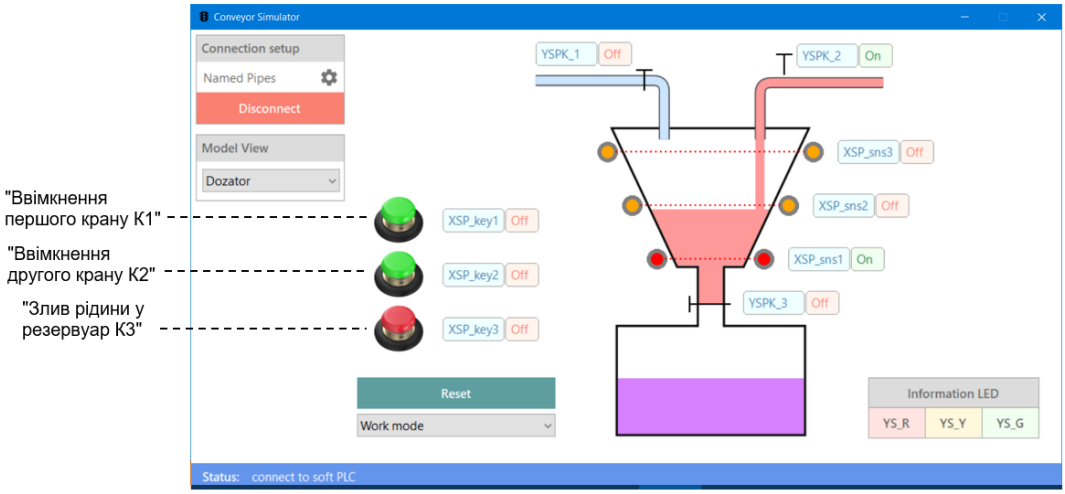


Рисунок 2 – Віртуальний макет дозуючого пристрою

Проміжні стани P_1, P_2 та P_3 реалізовані внутрішніми контактами реле *Rp1*, *Rp2* та *Rp3* (рис. 3).

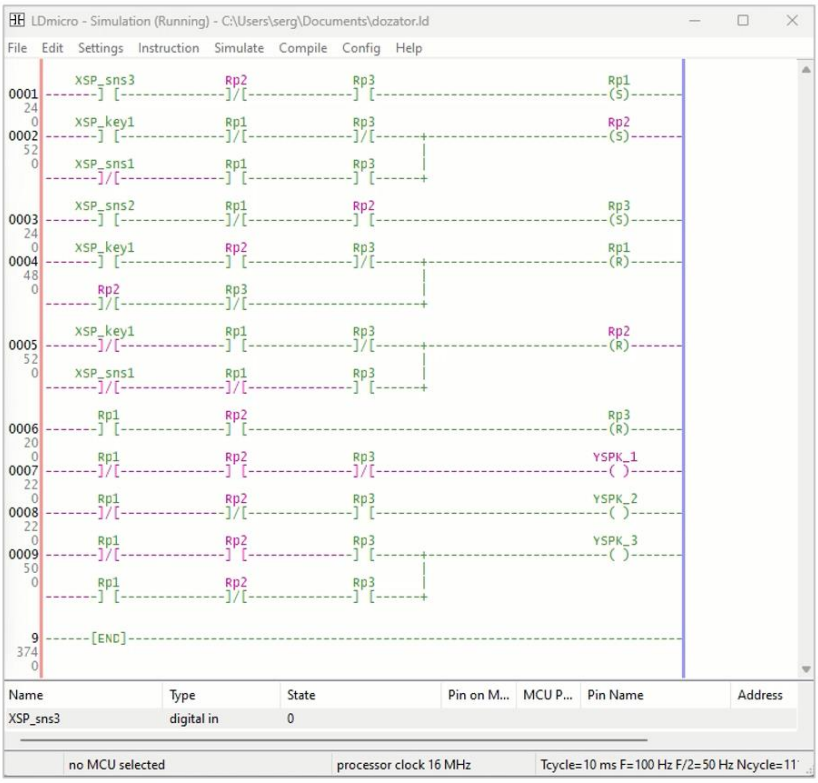


Рисунок 3 – Східчаста діаграма, що реалізує роботу дозуючого пристрою

Висновки. Таким чином, застосування віртуальних приладів в процесі дистанційного навчання дозволяє візуалізувати роботу розробленої програми і виявити помилки на стадії налагодження. Розглянутий приклад вирішення задачі автоматизації дозуючого пристрою наочно продемонстрував можливість застосування методики синтезу релейно-контактної схеми на основі RS-тригерів.

Список використаних джерел.

1. Електропневмоавтоматичні приводи в автоматизованих системах керування : навч. посіб. / І. Ш. Невлюдов, Л. О. Кривопляс-Володіна, С. П. Новоселов, О. В. Сичова ; М-во освіти і науки України, Харків. нац. ун-т радіоелектроніки. – Харків : ХНУРЕ, 2021. – 292 с. – ISBN 978-966-659-332-3 ; DOI: 10.30837/978-966-659-332-3.

2. Невлюдов І. Ш. Технологія програмування промислових контролерів в інтегрованому середовищі CODESYS : навч. посіб. / І. Ш. Невлюдов, С. П. Новоселов, О. В. Сичова ; М-во освіти і науки України, Харків. нац. ун-т радіоелектроніки. – Харків : ХНУРЕ, 2019. – 264 с. : іл. – DOI: 10.30837/978-966-659-265-4. ISBN 978-966-659-265-4.

3. Grout I. Digital Systems Design with FPGAs and CPLDs. Amsterdam: Elseveit, 2008. 784 p.

АВТОМАТИЗАЦІЯ ПРОКЛАДЕННЯ ШЛЯХУ В ПРОСТОРІ НА ОСНОВІ ДАНИХ З СЕНСОРІВ МОБІЛЬНИХ РОБОТІВ

професор, к.т.н., Новоселов С.П., ст. викл. Теслюк С.І.
Харківський національний університет радіоелектроніки,
кафедра КІТАМ, м. Харків, Україна
e-mail: sergiy.novoselov@nure.ua, serhii.tesliuk@nure.ua

Abstract. This work presents a detailed method of building a room map using the sensors of a mobile robot. The task of navigating mobile robots in space using SLAM technology and a cloud server has been solved. Information is provided about a proprietary software tool for creating a terrain map based on data from a cloud storage. The proposed results can be applied in practice to solve the problem of navigating a mobile robot in an environment with uncertain obstacles.

Вступ. На сьогоднішній день існує два методи побудови карти приміщення: за допомогою камери та за допомогою лазерного далекоміра. Автономна навігація на заздалегідь відомій карті – один із можливих сценаріїв застосування роботів, який має великий інтерес з боку дослідників у галузі робототехніки. Для функціонування робота в даному режимі необхідно заздалегідь побудувати карту місцевості, де передбачається навігація [1].

На даний час все більше популярності набуває колективне застосування мобільних роботів для виконання спільних завдань. В даному випадку зазвичай використовуються хмарні технології для організації спільного доступу до бази знань та даних.

Актуальністю застосування хмарних обчислень можуть бути завдання спільної роботи роботів. Наприклад, обмін даними при створенні загальної карти, або кооперативне планування для виконання спільного завдання, може бути легше досягнуто на базі централізованої архітектури, що має потужні обчислювальні можливості.

Основна частина.

Основною ідеєю хмарної робототехніки є те, що, як правило, робот взаємодіє з навколишнім середовищем за допомогою своїх датчиків та виконавчих пристроїв. Фактично, це означає, що дані, отримані від датчиків повинні бути оброблені та використані для прийняття рішень (як зворотний зв'язок) щодо наступної дії робота. Для завдань, які потребують роботи в режимі реального часу, обробка може бути переміщена в хмару. Це знижує необхідну обчислювальну потужність робота, що може покращити тривалість його мобільної роботи (без підзарядки), а також дозволяє знизити вартість робота.

Хмарний сервер призначений для збирання інформації з сенсорів робототехнічного обладнання та використання її для побудови карти робочого простору переміщення мобільного роботу [2].

Основна вимога до серверу, що розроблюється – це:

– збирання даних з сенсорів;

– накопичення отриманої інформації у вбудованій системі керування базами даних;

– відображення актуальних даних у графічному або текстовому вигляді;

– автоматичне оновлення інформації;

– організація доступу до сервера через виділений інтерфейс;

– відображення графічної інформації карти приміщення на будь-якому пристрою, що має доступ до мережі та графічний дисплей.

На рисунку 1 наведено архітектуру взаємодії сервера з сенсорами мобільного робота, що розроблюється [2].

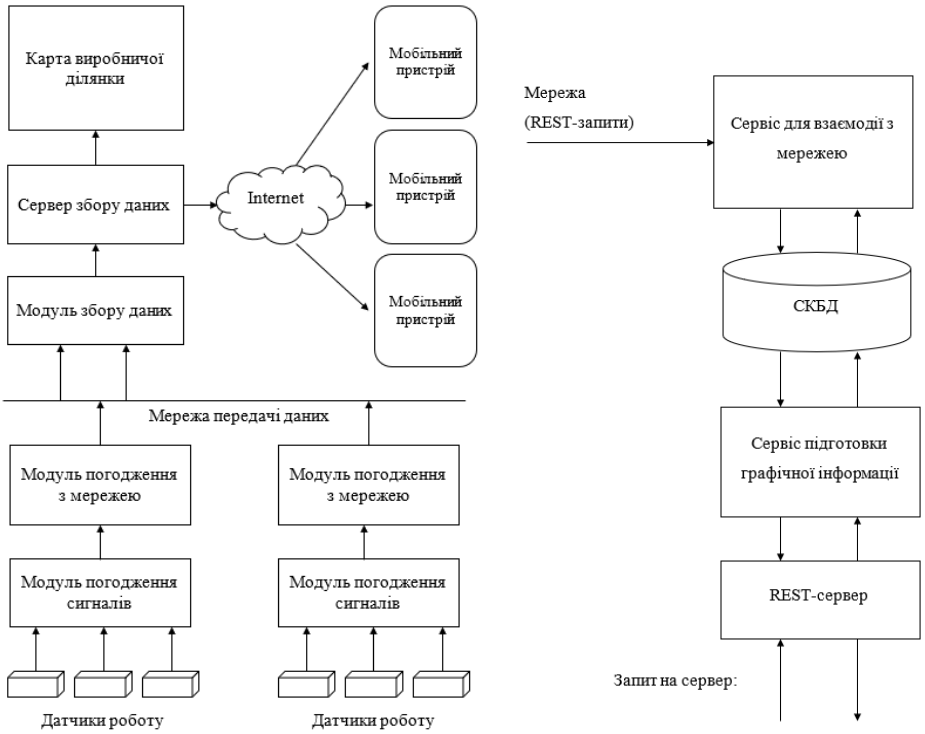


Рисунок 1 – Архітектура взаємодії сервера з сенсорами мобільногоробота

Інформація з датчиків, що розміщаються на мобільному шасі потрапляє на модуль погодження для накопичення та підготовки для передавання на сервер. Далі вже підготовлені дані потрапляють на модуль погодження з мережею для передачі вже оцифрованих даних до хмарного сервера.

Оцифровані дані можуть бути використані будь-яким мобільним пристроєм, в тому числі вони також потрапляють на модуль збирання даних, який підключено до серверу, що розробляється.

Для рішення поставленої задачі сервер збору даних повинен мати наступні програмні модулі:

– систему керування базами даних;

– REST-сервер;

– сервіс підготовки графічної інформації;

– сервіс для взаємодії з мережею за допомогою REST-технології.

Для перевірки запропонованого алгоритму роботи з хмарним сховищем розроблена програма, що виконує наступні функції:

– відображення списку зареєстрованих на сервері мобільних пристроїв;

– відображення плану приміщенні;

– формування карти місцевості на основі даних із хмарного сховища;

– накопичення інформації про навколишнє оточення мобільної платформи для побудови карти місцевості.

Головне вікно програми показано на рисунку 2. Інтерфейс складається зі списку мобільних роботів, що зареєстровано на сервері (ліва область програми), та робочої зони, що дає змогу оператору виконувати дослідження пов'язані з побудовою карти приміщення на основі даних з датчиків (права область програми).

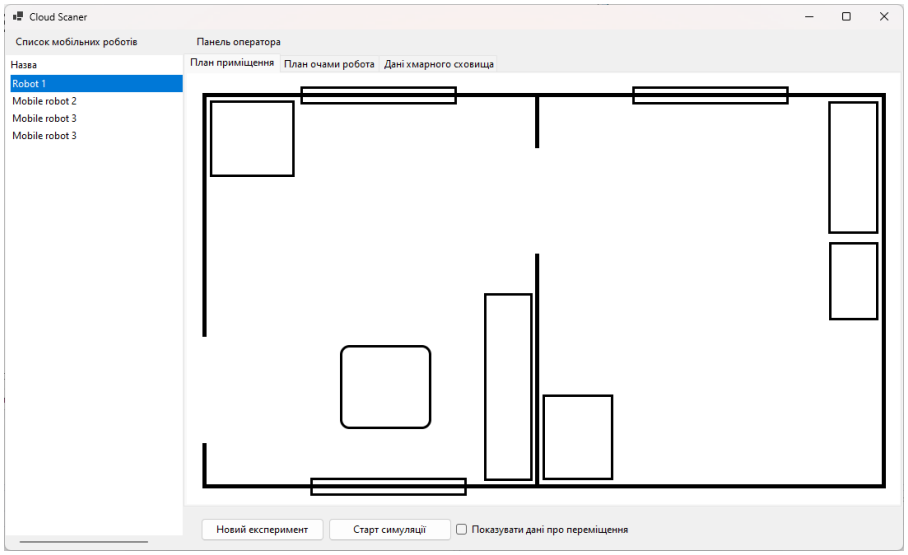


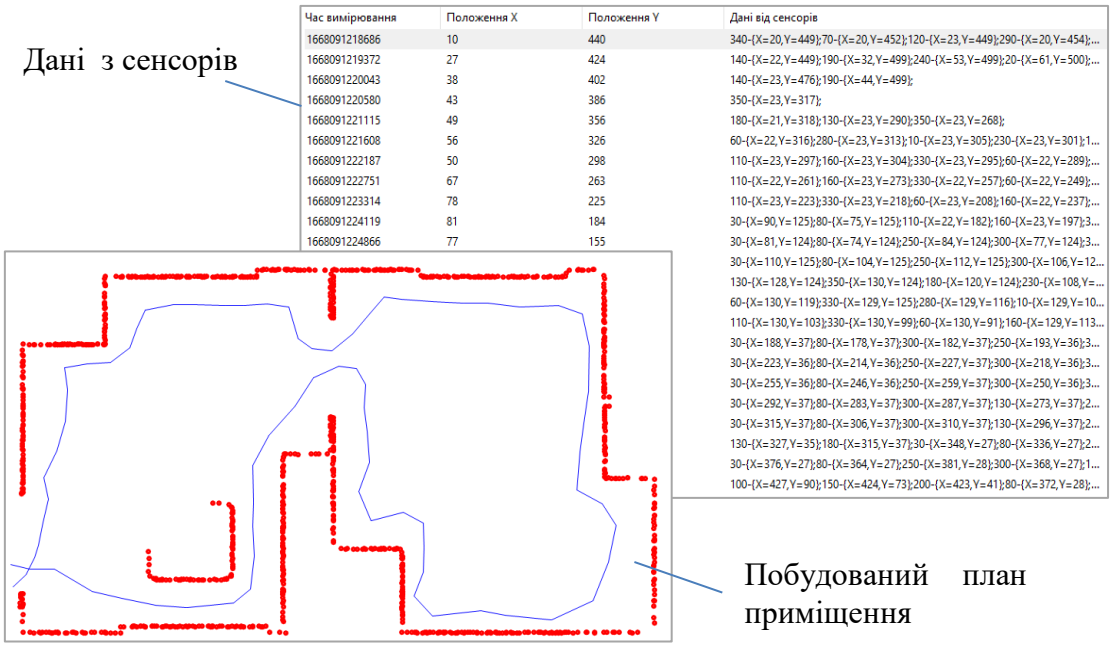
Рисунок 2 – Інтерфейс програми

Для мобільного робота, який потрапив в незнайоме приміщення його план буде повністю невизначеним. На першому етапі необхідно дослідити оточення за допомогою вбудованих сенсорів.

В програмі реалізовано симуляцію процесу сканування простору. В даному режимі запускаються послідовні хвилі пошуку та визначення координат розміщення перешкод в зоні дії датчику.

Після завершення етапу дослідження приміщення та збирання всіх даних про перешкоди в зоні дії сенсорів роботу ми отримуємо хмару точок, що описуються робочій простір.

Приклад даних, що отримані з сенсорів робота та побудованого плану приміщення показані на рисунку 3.



Час вимірювання	Положення X	Положення Y	Дані від сенсорів
1668091218686	10	440	340-{X=20,Y=449};70-{X=20,Y=452};120-{X=23,Y=449};290-{X=20,Y=454};...
1668091219372	27	424	140-{X=22,Y=449};190-{X=32,Y=499};240-{X=53,Y=499};20-{X=61,Y=500};...
1668091220043	38	402	140-{X=23,Y=476};190-{X=44,Y=499};
1668091220580	43	386	350-{X=23,Y=317};
1668091221115	49	356	180-{X=21,Y=318};130-{X=23,Y=290};350-{X=23,Y=268};
1668091221608	56	326	60-{X=22,Y=316};280-{X=23,Y=313};10-{X=23,Y=305};230-{X=23,Y=301};1...
1668091222187	50	298	110-{X=23,Y=297};160-{X=23,Y=304};330-{X=23,Y=295};60-{X=22,Y=289};...
1668091222751	67	263	110-{X=22,Y=261};160-{X=23,Y=273};330-{X=22,Y=257};60-{X=22,Y=249};...
1668091223314	78	225	110-{X=23,Y=223};330-{X=23,Y=218};60-{X=23,Y=208};160-{X=22,Y=237};...
1668091224119	81	184	30-{X=90,Y=125};80-{X=75,Y=125};110-{X=22,Y=182};160-{X=23,Y=197};3...
1668091224866	77	155	30-{X=81,Y=124};80-{X=74,Y=124};250-{X=84,Y=124};300-{X=77,Y=124};3...
			30-{X=110,Y=125};80-{X=104,Y=125};250-{X=112,Y=125};300-{X=106,Y=12...
			130-{X=128,Y=124};350-{X=130,Y=124};180-{X=120,Y=124};230-{X=108,Y=...
			60-{X=130,Y=119};330-{X=129,Y=125};280-{X=129,Y=116};10-{X=129,Y=10...
			110-{X=130,Y=103};330-{X=130,Y=99};60-{X=130,Y=91};160-{X=129,Y=113...
			30-{X=188,Y=37};80-{X=178,Y=37};300-{X=182,Y=37};250-{X=193,Y=36};3...
			30-{X=223,Y=36};80-{X=214,Y=36};250-{X=227,Y=37};300-{X=218,Y=36};3...
			30-{X=255,Y=36};80-{X=246,Y=36};250-{X=259,Y=37};300-{X=250,Y=36};3...
			30-{X=292,Y=37};80-{X=283,Y=37};300-{X=287,Y=37};130-{X=273,Y=37};2...
			30-{X=315,Y=37};80-{X=306,Y=37};300-{X=310,Y=37};130-{X=296,Y=37};2...
			130-{X=327,Y=35};180-{X=315,Y=37};30-{X=348,Y=27};80-{X=336,Y=27};2...
			30-{X=376,Y=27};80-{X=364,Y=27};250-{X=381,Y=28};300-{X=368,Y=27};1...
			100-{X=427,Y=90};150-{X=424,Y=73};200-{X=423,Y=41};80-{X=372,Y=28};...

Рисунок 3 – Приклад даних, що отримані з сенсорів робота та побудованого плану приміщення

В розробленій програмі також передбачена можливість зберігання всіх точок траєкторії переміщення мобільного робота. Далі, в процесі дослідження, можливо побачити в динаміці рух робота вздовж приміщення з урахуванням всіх точок в яких відбувалось сканування. З наведених прикладів можна бачити реальну картину руху мобільної платформи, передачу даних на хмарний сервер та візуалізацію отриманих даних в панелі оператору.

Висновки. Наведений приклад побудованої карти приміщення за допомогою сенсорів мобільного робота може застосовуватись на практиці для рішення задачі навігації мобільного роботу в середовище з невизначеними перешкодами. Виконана розробка структурної схеми хмарного сховища даних для побудови карти місцевості. Розроблена структура серверу збору даних та запропоновано алгоритм роботи мобільної платформи при взаємодії із хмарним сервером.

Список використаних джерел.

1. Nevludov I. Production workspace obstacle avoidance mobile robot trajectory modeling. I. Nevludov, S. Novoselov, O. Sychova, S. Tesliuk. Computer and information systems and technologies. 2021. pp. 61-62.

2. I. Nevliudov, Sh. Omarov, S. Tesliuk, S. Novoselov, O.Sychova, Robot group interaction technology using a cloud server // IV International conference on natural science and technologies, 24-26 August 2022, Antalya, Turkey, P.164.

РОЗРОБКА ПРИНЦИПОВОЇ СХЕМИ БЛОКА ЖИВЛЕННЯ МОБІЛЬНОГО РОБОТА-ГРАФОПОБУДОВНИК

Вадурін К.О., к.т.н., доцент Кухаренко Д.В.
Кременчуцький національний університет імені Михайла Остроградського,
кафедра КІЕ, м. Кременчук, Україна
e-mail: kir3337@gmail.com

Abstract. In this paper, we describe the main components of the developed circuit of the internal power supply of a mobile robotic plotter. The tasks of the developed scheme are as follows: providing recharging of batteries using 5V USB Type-C power supplies or from a computer; providing a connection of the input USB connector with the information lines of the leading microcontroller; formation of supply voltages necessary for the operation of the digital part, drive, sensors and cartridge. The developed circuit scheme of the internal power supply corresponds to a part of the previously created block scheme of a mobile robotic plotter, and in the future we plan to create circuit scheme of a sensor block and a microcontroller block.

Актуальність роботи. Наразі спостерігається зростання популярності ручних та портативних мобільних принтерів для роботи з твердими носіями, але можливості таких пристроїв до автоматичного друку обмежені розмірами їх корпусів. Тому актуальною задачею є розробка робота-графопобудовника з бездротовим інтерфейсом, який може робити відтиски на папері та рівних горизонтальних поверхнях будь-якого розміру.

Матеріал і результати досліджень. У попередніх публікаціях висвітлено досвід роботи з графопобудовниками [1, 2], процес вибору оптимального привода та розробки структурної схеми мобільного робота-графопобудовника. У даній роботі розглянемо основні частини принципової схеми блока живлення (БЖ) робота-графопобудовника.

Вбудований блок живлення має роз’єм XS101 для під’єднання шлейфу до входу USB Type-C. Що забезпечує можливість як під’єднання пристрою до мережі через зовнішній БЖ для зарядки, так і для підключення до персонального комп’ютера (ПК) для передачі зображення.

Підзаряджання блока акумуляторів здійснюється схемою з мікросхемою DA102 LTC4054, яка фактично є контролером зарядки акумуляторів. Світлодіод HL101 є індикатором заряджання, поки акумулятори заряджаються через роз’єм XS102 він світиться, коли заряд завершується HL101 вимикається. Роз’єм XS103 дозволяє розімкнути контури формування 9 В та 16 В для забезпечення енергозбереження. Діод VD101 знижує напругу на конденсаторі C105 до 3,3 В, для подальшого її перетворення на напруги 5 В, 9 В та 16 В.

Формування напруги 5 В здійснюється мікросхемою DA104 MC34063 з напруги 3,3 В (від C105). Введення мікросхеми DA104 до принципової схеми здійснено з обвісом рекомендованим у її Datasheet.

Формування напруг 9 В та 16 В здійснюється мікросхемами DA101 та DA103 відповідно. DA101 та DA103 представлені мікросхемами LM2731, що включені за схемами пропонованими у їх Datasheet.

Підключення внутрішнього БЖ до блока МК здійснюється з використанням роз'єму XS104. Який крім передачі сформованих напруг 3,3 В, 5 В, 9 В, 16 В передбачає передачу сигнальних провідників USB (D – та D +).

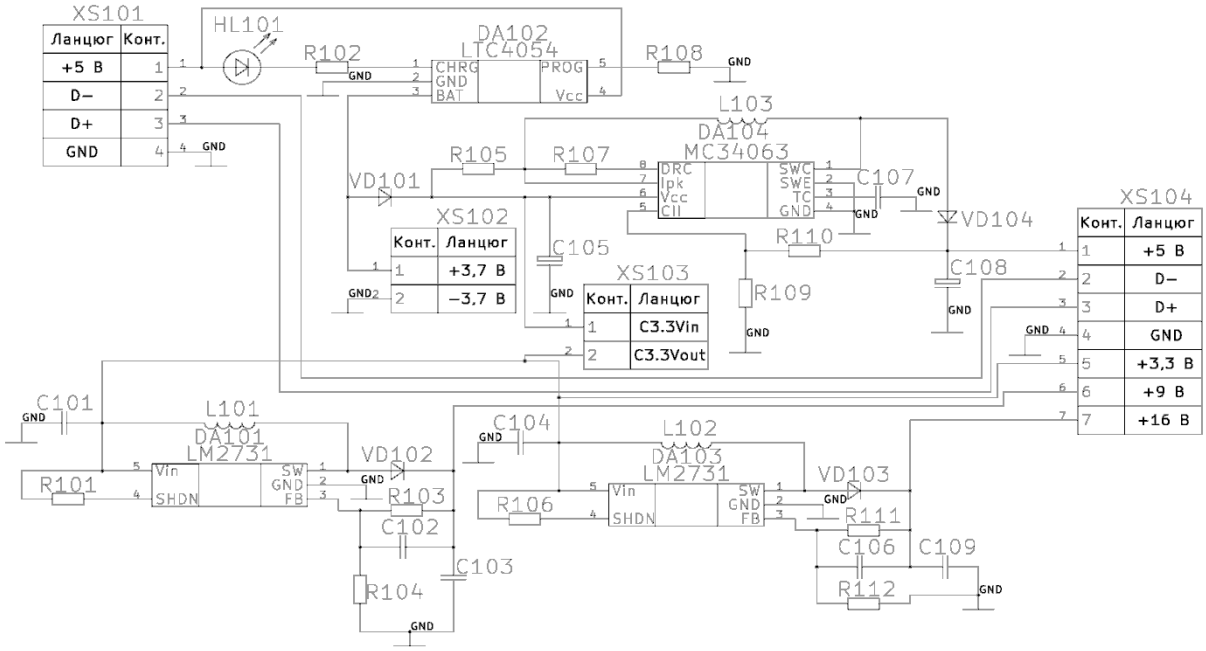


Рисунок 1 – Принципова схема БЖ мобільного робота-графопобудовника

Принципова схема внутрішнього БЖ робота-графопобудовника виконана засобами KiCad з максимальними наближеннями до ДСТУ та ЄСКД наведена на рисунку 1.

Висновки. У результаті роботи розроблено принципову схему для виконання нею наступних завдань: забезпечення підзарядки акумуляторів за допомогою блоків живлення 5В USB Type-C або від комп'ютера; забезпечення з'єднання вхідного USB-роз'єму з інформаційними лініями ведучого мікроконтролера; формування напруг живлення, необхідних для роботи цифрової частини, приводу, датчиків і картриджа.

Список використаних джерел.

1. Вадурін, К. О., Мєшков, М. Ю. (2021). Розробка методології застосування прийомів креслення у медичних системах. Радіоелектроніка та молодь у XXI столітті, Т. 1., 125–126.

2. Вадурін, К. О. (2021). Розробка методології виведення інформації з медичних систем застосовуючи прийоми креслення. Авіація, промисловість, суспільство, Ч. 1., 70–73.

РОЗРОБКА ПРИНЦИПОВОЇ СХЕМИ БЛОКА ДАТЧИКІВ ЛІНІЙ РОБОТА-ГРАФОПОБУДОВНИКА

Вадурін К.О., к.т.н., доцент Кухаренко Д.В.
Кременчуцький національний університет імені Михайла Остроградського,
кафедра КІЕ, м. Кременчук, Україна
e-mail: kir3337@gmail.com.

Abstract. In this paper, we present a description of the circuit scheme of the block of line sensors. The use of two such blocks placed on the same line will allow us to quickly obtain information about the placement of the device on the surface on which printing is carried out. Also, guided by data from such blocks, we will be able to: determine the boundaries of the print fields; boundaries of lines of printed data during inline movement; the position of the lines when moving along the contour of the image. In the future, we plan to develop a circuit scheme of a microcontroller unit that can work with several line sensor units.

Актуальність роботи. У зв'язку зі зростанням популярності мобільних принтерів, але їх обмеженістю в областях друку розмірами корпусів, актуальною є розробка пристрою з безрамковим корпусом для друку на твердих носіях з рівною поверхнею. У ролі такого пристрою розроблюється універсальний мобільний робот-графопобудовник з бездротовим інтерфейсом.

Матеріал і результати досліджень. У попередніх роботах описано: розробку графопобудовника медичних зображень [1, 2]; різні приводи та обрано двоколісний диференціальний привід, як основу для реалізації мобільного робота графопобудовника [3]; розробку структурної схеми мобільного графопобудовника; основні ланцюги принципової схеми внутрішнього блока живлення графопобудовника.

У даній роботі розглянемо розроблену принципову схему блока датчиків ліній робота-графопобудовника.

У пристрої передбачено використання двох блоків датчиків ліній виконаних за однією принциповою схемою. Принципова схема побудована на збірках 5 оптопар TCRT5000L включених за Datasheet.

TCRT5000L – світловідбиваючий сенсор, який зазвичай застосовується у складі датчиків «чорне-біле». Даний датчик випромінює інфрачервоний сигнал, а потім вловлює відображення цього сигналу від поверхні. Залежно від типу та кольору поверхні змінюється інтенсивність відбитого сигналу. За цією інтенсивністю можна приблизно судити про відтінки кольору поверхні, також він може використовуватися як альтернатива датчику Холла в енкодері для визначення швидкості обертання. Датчик складається з світлодіода, що випромінює світло в інфрачервоному діапазоні та фототранзистора.

Принципова схема блока датчиків ліній робота-графопобудовника виконана засобами KiCad з максимальними наближеннями до ДСТУ та ЄСКД наведена на рисунку 1.

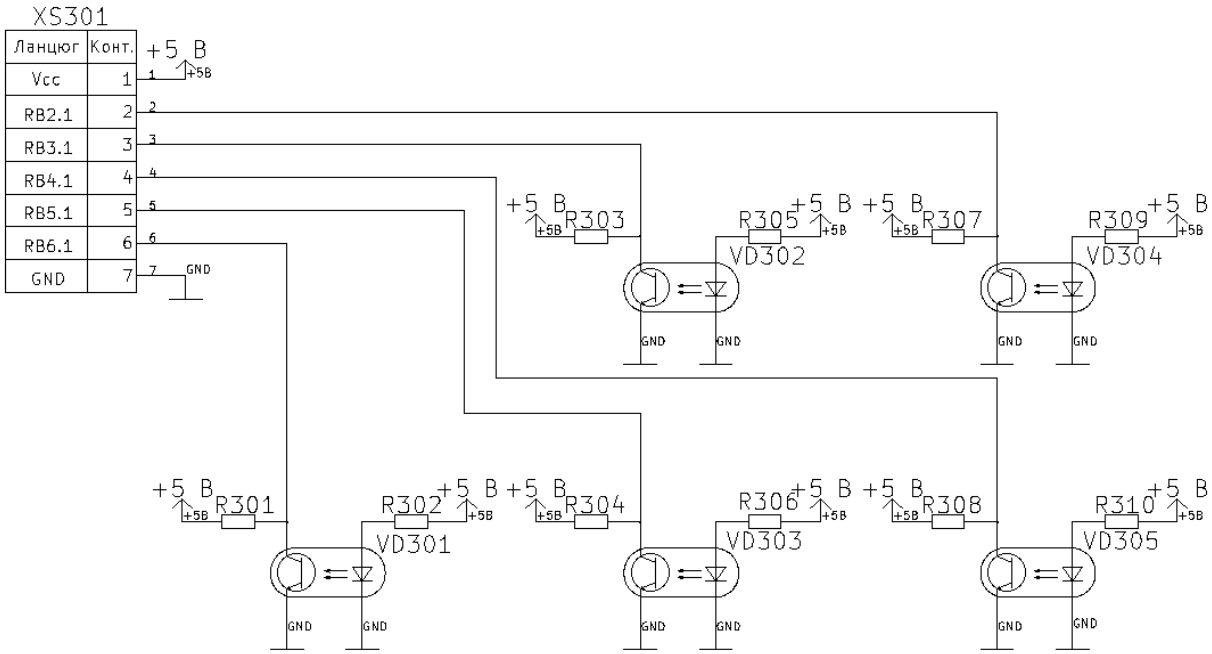


Рисунок 1 – Принципова схема блока датчиків ліній мобільного робота-графопобудовника

Висновки. У результаті виконання роботи здійснено опис принципової схеми розробленого блока датчиків ліній. Використання двох таких блоків, розміщених на одній лінії, дозволить оперативно отримувати інформацію про розміщення пристрою на поверхні, на якій здійснюється друк. Також, орієнтуючись за даними з таких блоків, можливо здійснювати наступні операції: визначати межі полів друку; виявляти межі ліній надрукованих даних при рядковому русі; встановлювати положення корпусу апарату за лініями, під час руху за контуром зображення. Надалі запланована розробка принципової схему мікроконтролерного блока, який зможе працювати із кількома блоками датчиків ліній.

Список використаних джерел.

1. Вадурін, К. О., Мєшков, М. Ю. (2021). Розробка методології застосування прийомів креслення у медичних системах. Радіоелектроніка та молодь у XXI столітті, Т. 1., 125–126.

2. Вадурін, К. О. (2021). Розробка методології виведення інформації з медичних систем застосовуючи прийоми креслення. Авіація, промисловість, суспільство, Ч. 1., 70–73. ISBN 978-966-610-244-1

3. Кухаренко, Д. В., Вадурін, К. О. (2021). Робот-графопобудовник медичних зображень. Виробництво & Мехатронні Системи 2021, 113–116.

РЕЄСТРАЦІЯ ЕЛЕКТРОМІОГРАФІЧНИХ БІОПОТЕНЦІАЛІВ НА БАЗІ МІКРОКОНТРОЛЕРНОЇ СИСТЕМИ

Малахова О.Ю., асистент Чумак В.С.
Харківський національний університет радіоелектроніки,
кафедра МТС, м. Харків, Україна
e-mail: olena.malakhova@nure.ua

Abstract. This paper considers the theoretical aspects of using a microcontroller system for recording electromyographic potentials. Characterizing the biopotentials obtained during the myographic study. The functional value of the microcontroller in the registration of electromyographic biopotential, the main technical characteristics that should be considered when choosing a microcontroller. Areas and prospects for the use of microcontrollers in the registration of biological activity of muscles are considered.

Електроміограма – графічний запис зміни біопотенціалів, що виникають у м’язах під час спостереження. ЕМГ є досить ефективним методом дослідження, оскільки дозволяє реєструвати різні функціональні стани м'язів, представляючи різну картину при рухових порушеннях, обумовлених ураженням центральної, периферичної нервової систем та м'язового апарату [1].

М’язова активність є сумарною різницею біоелектричних потенціалів всіх м'язових волокон, розташованих у проекції нашкірного електрода, а отримані при цьому сигнали мають наступні характеристики [2]:

− частота сигналу. У діагностичній практиці виділяють основні чотири типи поверхневої ЕМГ: I тип − інтерференційна крива, що становить високочастотну поліморфну активність, яка виникає при довільному скороченні м’язу або при напруженні м’язів; II тип − рідкісна електрична активність (6−50 Гц); III тип − підсилення частих коливань у спокої, групування їх у ритмічні розряди, поява спалахів ритмічних і неритмічних коливань на фоні ЕМГ довільного м’язового скорочення; IV тип − відсутність біопотенціалів, електричне мовчання.

− амплітуда сигналу: відповідно, I тип приймає значення в межах від 1000мкВ до 2000мкВ; II тип – від 50мкВ до 150мкВ; III тип – від 60мкВ до 90мкВ; у IV типу показник відсутній.

− тривалість: для I типу значення варіюються в межах 6мс - 10мс; для II типу – до 10мс; III тип – від 80мс до 100мс у IV типу показник відсутній.

− амплітуда низькочастотної завади;

− частоти завадоутворюючого сигналу.

Проблема виділення необхідного сигналу полягає саме у його відділенні від шумів у режимі реального часу, а також зіставлення одержуваних сигналів з відповідними скороченнями м'язів.

Схема вимірювання сигналу може містити біографічний модуль, блок мікроконтролера, блок передачі інформації на персональний комп'ютер (ПК).

Мікроконтролер є спеціалізованим пристроєм, виконаним у вигляді мікросхеми, що включає мікропроцесор, та як будь-який цифровий пристрій: ОЗУ та флеш-пам’ять, порти вводу-виводу і блоки зі спеціальними функціями (у МК-лічильники, компаратори, АЦП та ін.) [3, 4].

Сигнали від вимірювальних каналів направлені саме на мікроконтроллер, який забезпечує АЦ-перетворення, автокорекцію та передачу даних для обробки результатів на ПК. Враховуючи варіативність отримуваних під час визначення ЕМГ-біопотенціалів, слід враховувати і технічні аспекти мікроконтролера, до яких відносяться: продуктивність; розрядність; наявність визначених пристроїв (ЦАП, АЦП); тактова частота і частота дискретизації АЦП; інтерфейси; вартість.

Таким чином, метод реєстрації ЕМГ- біопотенціалів з використанням мікроконтролерної системи надає можливість отримувати інформацію про статику руху мускулатур навіть у механізмі здійснення активних дій. Такі прилади знаходять своє застосування в області реабілітації та розробки сучасних протезних пристроїв [5].

Список використаних джерел.

1. Чумак, В. С., Носова, Т. В., & Жемчужкіна, Т. В. (2019). Оценка возможностей распознавания мимических движений при помощи анализа характеристик лицевой электромиограммы. Збірник тез доповідей II Всеукраїнської науково-практичної конференції молодих учених, курсантів та студентів «Авіація, промисловість, суспільство» (с. 273–275).

2. Чумак, В. С., Чугуй, Є. А., Носова, Т. В., & Жемчужкіна, Т. В. (2019). Анализ электромиографического сигнала для контроля усталости мышц в режиме реального времени. Матеріали 23 Міжнародного молодіжного форуму «Радіоелектроніка та молодь у XXI столітті» (с. 243–244).

3. Кулик, А. Я., Нікольський, О. І., Ревенок, В. І., & Кулик, Я. А. (2020). Схемотехніка електронної медичної апаратури.

4. 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).

5. Чумак, В. С., Аврунін, О. Г., Чугуй, Є. А., & Свид, І. В. (2021). Аналіз принципів побудови телемедичних комплексів широкого призначення. АСУ та прилади автоматики, 177, 80–85.

ВИКОРИСТАННЯ FPGA ДЛЯ РЕАЛІЗАЦІЇ ШТУЧНОЇ НЕЙРОННОЇ МЕРЕЖІ

Луценко А.В., асистент Чумак В.С.
Харківський національний університет радіоелектроніки,
кафедра МТС, м. Харків, Україна
e-mail: anastasiia.lutsenko@nure.ua

Abstract. Advances in technology have greatly expanded the logical capabilities of FPGAs and, in turn, made them viable alternatives to large and complex implementations. Therefore, there is a prospect of implementing an artificial neural network on the FPGA. In the field of artificial intelligence and machine learning, an artificial neuron is a computing element that is a mathematical model of a biological neuron that is used as a basic element to build artificial neural networks.

Штучний нейрон (рис.1) має кілька входів (аналогів синапсів біологічного нейрона) та єдиний вихід (аналог аксона). Кожен вхід має деяку вагу, на яку множиться значення, що надійшло даним входом. У тілі (комірці) нейрона відбувається підсумовування зважених входів, а отримана сума перетворюється за допомогою активаційної функції нейрона, зазвичай, нелінійної.

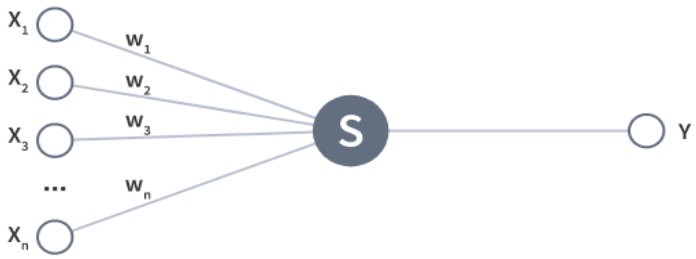


Рисунок 1 - Модель штучного нейрону

Зі зростанням ступеня інтеграції мікросхем якісно змінюється межа складності систем, які можуть бути реалізовані на їх основі. Для реалізації розпаралелюваних моделей нейронних мереж можливо використовувати програмовані логічні інтегральні схеми (ПЛІС) [1, 2]. На даний момент одним зі світових лідерів у розробці та продажу програмованої користувачем вентильної матриці (FPGA) є Xilinx. Компанія Xilinx виробляє кілька серій FPGA, таких як Spartan, Artix, Kintex, Virtex, які мають високошвидкісну смугу пропускання, велике кількість логічних елементів, низьке енергоспоживання та високу продуктивність за відносно низькою ціною [3-5].

Обчислювальні системи, засновані на штучних нейронних мережах, мають ряд якостей: навченість; здатність до узагальнення; асоціативне,

розподілене зберігання даних; адаптація до зміни довкілля; потенційно висока продуктивність; стійкість до відмов апаратної реалізації.

Існують два способи реалізації штучних нейронних мереж - апаратна та програмна. Програмна реалізація, поступаючись апаратною за швидкістю роботи та автономності, має низку очевидних переваг, пов'язаних з простотою використання та впровадження в інформаційно-керуючу систему. Проте спеціалізовані апаратні засоби пропонують помітні переваги у певних ситуаціях. До основних переваг апаратної реалізації ІНС можна віднести швидкість, надійність, безпеку та додаткові режими експлуатації.

Що стосується апаратної реалізації нейронних мереж на FPGA, то вона вигідно відрізняється від реалізації на спеціальних DSP-процесорах (оскільки вони випускаються серійно) та від реалізації на ASIC-мікросхемах (оскільки вони не підлягають переконфігуруванню). Реалізація на FPGA найточніше передає паралельну архітектуру нейронів і надає можливість гнучкого реконфігурування всієї нейронної мережі та її складових – штучних нейронів. Крім того, конфігурацію заснованих на FPGA нейронних мереж легко змінити.

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, & Свид, І. В. (2020). Реализация структуры нейронных сетей на FPGA. У Наука, технології, інновації: тенденції розвитку в Україні та світі : матеріали міжнародної студентської наукової конференції (с. 30–32).

3. Чумак, В.С, & Свид, І. В. (2019). Створення модуля VHDL-опису при проектуванні цифрових систем на ПЛІС в Xilinx ISE Design Suite. У Перспективні напрямки сучасної електроніки, інформаційних і комп'ютерних систем (MEICS-2019): тези доповідей IV Всеукраїнської науково-практичної конференції (с. 94–95).

4. Iryna Svyd, Oleksandr Vorgul, Valerii Semenets, Oleg Zubkov, Valeriia Chumak, Natalia 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

5. Чумак, В.С, & Свид, І. В. (2019). Современные тенденции подготовки технических специалистов. У Сучасна освіта – доступність, якість, визнання: збірник наукових праць XI Міжнародної науково-методичної конференції (с. 245– 247).

СИСТЕМА ГЛИБИННОГО ЗОНДУВАННЯ НА БАЗІ МІКРОКОНТРОЛЕРА СЕРІЇ STM32

Кавецький В.С., асистент Чумак В.С.
Харківський національний університет радіоелектроніки,
кафедра МТС, м. Харків, Україна
e-mail: viacheslav.kavetskyi@nure.ua

Abstract. This paper is about microcontroller-based signal processing systems. It considers the processing of an acoustic signal using a single microcontroller. The purpose of signal processing is to extract the necessary useful data from the signal and convert it for use. This paper investigates the processing of underwater acoustic signals for navigation by controlling the distance between the seabed and the device. The proposed system is a compact, portable, economical depth sounding system, energy efficient and occupies less space. The proposed method has an improved filtering technique that produces a less noisy signal and has more computing power, which provides an accurate, fast, cost-effective, and portable solution.

Обробка сигналів задіяна в кожній системі глибинного зондування, що використовується в підводних апаратах. Ця область також поширюється на судна та рибопошукові пристрої. Для безперебійної навігації необхідно постійно відстежувати та контролювати відстань між морським дном та корпусом апарату. Основна відмінність пристроїв, які задіяні у різних системах глибинного зондування полягає у методології обробки акустичного сигналу. Посилаючий імпульс може бути згенерований або кристалічним генератором або будь-яким іншим цифровим пристроєм. Потім імпульс проходить через підсилювач потужності для посилення сигналу, щоб його можна було подати на перетворювач.

Під час передачі сигналу першим кроком є генерація імпульсів, які передаватимуться під водою. Переважно генерувати синусоїдальну хвилю, оскільки моделювання синусоїди в акустичних умовах простіше, ніж трикутної або квадратної хвилі. Синусоїдальна хвиля потрібної частоти може бути згенерована декількома способами. Кристалічні генератори та інтегральні схеми використовуються для отримання синусоїдальної хвилі потрібної частоти. Після посилення сигнал потребує фільтрації для видалення зашумленого вмісту. Використовуються фільтри змінного стану, які мають більше переваг, ніж інші фільтри.

Відфільтрований аналоговий сигнал перетворюється на цифровий сигнал для розрахунку значення глибини морського дна щодо приладу. Зі зростанням ступеня інтеграції мікросхем якісно змінюється межа складності систем, які можуть бути реалізовані на їх основі. Таким чином, для вибірки та обробки пропонується використовувати один

мікроконтролер, а не окремі мікроконтролери для кожного процесу. Вибіркова та обчислювальна потужність ARM-мікроконтролера STM32F429 дуже висока в порівнянні з раніше використовуваними моделями. Цей мікроконтролер має частоту дискретизації 2,4M вибірок на секунду, що приблизно вп'ятеро вище, ніж у Arduino. Крім того, він містить 3-12-розрядний АЦП для обробки аналогових сигналів і 164 вхідних і вихідних пінів, що більш ніж достатньо для заміни всіх інших мікроконтролерів у системі глибинного зондування та виконання всіх пов'язаних з цим операцій. Крім того, є порт Ethernet, за допомогою якого можна віддалено контролювати глибину та координати в реальному часі через захищений інтернет-протокол. На додаток до всіх перерахованих вище функцій є інтерфейс камери, за допомогою якого можна підключити камеру для спостереження за підводними об'єктами і навколишнім середовищем.

Вагомою перевагою також є можливість реалізації нейронних мереж. Штучні нейронні мережі досить складні у реалізації. Для їх практичного застосування дуже важливі інструменти, що полегшують та прискорюють процес створення прикладних додатків з їх використанням. Компанія STMicroelectronics пропонує широкий набір програмних інструментів, що значно полегшують процес створення програм на базі штучних нейромереж. У сукупності з апаратними засобами налагодження це дозволяє значно скоротити цикл розробки пристроїв і в найкоротші терміни отримати конкурентоспроможний продукт.

В результаті отримуємо систему глибинного зондування з використанням одного мікроконтролера з покращеною частотою дискретизації 2,4M вибірок на секунду. Отримана система є енергоефективною, займає менше місця, компактною, портативною та економічною системою глибинного зондування.

Список використаних джерел.

1. Дж. У, Х. (1961). Основы гидролокации. Ленинград: Судпромгиз.

2. Istepanian R. S. H., Woodward B. (1997). Microcontroller-based underwater acoustic ECG telemetry system. IEEE transactions on information technology in biomedicine. Vol. 1, no. 2. (P. 150–154).

3. 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).

4. Ziomek L., Blount R. (1987) Underwater acoustic model-based signal processing. IEEE Transactions on Acoustics, Speech, and Signal Processing. Vol. 35, no. 12. (P. 1670–1683).

АНАЛІЗ ДЕРМАТОСКОПІЧНОГО ЗОБРАЖЕННЯ ПІД ЧАС УФ-ВІДЕОДЕРМАТОСКОПІЇ

Ісаєва О.А., асистент Чумак В.С.
Харківський національний університет радіоелектроніки,
кафедра МТС, м. Харків, Україна
e-mail: olha.isaieva@nure.ua

Abstract. Today, video dermatoscopy is one of the most important methods of examination for skin tumors. The method allows using special optical devices of video dermatoscopes to visually assess the condition of the skin and to examine tumors at a magnification of tens to hundreds of times with different depth of field. The color and shape of the tumor can determine its nature and the risk of recurrence.

Для поліпшення якісних характеристик зображень було розроблено численні універсальні та спеціалізовані програмні засоби.

Тому, метою роботи є аналіз методу обробки дерматоскопічних зображень для УФ-відеодерматоскопії [1].

Для проведення дослідження нам знадобилися такі пристрої, як апарат SKINSCOPE, за допомогою якого ми проводили дослідження. Камера Sony DSC QX-100. Камера встановлена до окуляру дерматоскопу в афокальній проекції. За допомогою цієї камери ми могли побачити збільшене чітке зображення, яке моментально передавалося в мобільну програму Imaging Edge Mobile (рис. 1) [2].

Після передачі дерматоскопічного зображення на електронний носій необхідно використати програму для обробки зображення задля знаходження патологій шкірного покриву. Використовуючи програму Delphi 10.3 та необхідні функції даної програми, отримаємо сегментоване зображення (рис. 2) [1].

Рисунок 1 – Установка для дослідження шкірного покриву

Рисунок 2 – Дерматоскопічні зображення

Розглянемо дерматоскопічне зображення, отримане методом ультрафіолетової дерматоскопії. Щоб з’ясувати патології, які присутні на

зображенні, подивимося на співвідношення кольору і патології.

Отже, якщо у нас є коралові плями, це означає, що шкіра жирна. Коли ми бачимо білі плями, то це суха шкіра. Деякі темні поля на шкірі означають пігментацію. Проаналізуємо стан шкіри пацієнта.У носогубній області спостерігається зневоднення шкіри, що означає, що пацієнт не має належного догляду за шкірою або не зволожує шкіру. Порівнюючи вихідне зображення та сегментоване, можна побачити, що на обробленому зображенні проблемні ділянки на обличчі помітні краще, ніж на оригіналі.

Висновки. У задачах автоматизованої обробки зображень та аналізу люмінесцентної відеодерматоскопії значну роль завжди відіграє апріорна інформація про досліджуваному зображенні. Обробка зображення відіграє значну роль при встановленні правильного догляду за шкірним покривом. Сьогодні важко представити область діяльності, у якій можна обійтися без комп'ютерної обробки зображень. При комп'ютерній обробці зображень вирішується широке коло завдань, таких як поліпшення якості зображень, вимірювання параметрів зображення або стиск зображень. Пропонується використовувати дану обробку зображень у телемедичних системах автоматизованного контролю [1-5].

Список використаних джерел.

1. Исаева О. А. Оценка изображений, полученных с помощью УФ-дерматоскопии / О. А. Исаева, О. Г. Аврунин // Матеріали XXIV Міжнародного молодіжного форуму «Радіоелектроніка та молодь у XXI столітті», Том 1. Харків, ХНУРЕ, 2020 .- С. 129-130.

2. Исаева О. А. Возможности диагностики заболеваний кожи с применением телемедицинских технологий / О. А. Исаева, А. А. Трубицин // XIX Міжнародна науково-технічна конференція «Фізичні процеси та поля технічних і біологічних об’єктів»: матеріали конференції. – Кременчук: КрНУ, 6-8 листопада 2020 р. – С. 56-57.

3. V. Semenets, V. Chumak, I. Svyd, O. Zubkov, O. Vorgul, N.a Boiko. Designing the Structure of a General-Purpose Telemedicine Complex. // III International Scientific and Practical Conference Theoretical and Applied Aspects of Device Development on Microcontrollers and FPGAs (MC&FPGA), Kharkiv, Ukraine, 2021, pp. 47-48, doi: 10.35598/mcfpga.2021.016.

4. Аналіз принципів побудови телемедичних комплексів широкого призначення / В. С. Чумак, О. Г. Аврунін, Є. А. Чугуй, І. В. Свид // АСУ та прилади автоматики. 2021. № 177. С. 80-85.

5. V. Semenets, V. Chumak, I. Svyd, O. Zubkov, O. Vorgul, N. Boiko. Features of the Design of a Telemedicine Complex of a Wide Profile Based on FPGA. // III International Scientific and Practical Conference Theoretical and Applied Aspects of Device Development on Microcontrollers and FPGAs (MC&FPGA), Kharkiv, Ukraine, 2021, pp. 41-42, doi: 10.35598/mcfpga.2021.014.

ВИКОРИСТАННЯ КРИСТАЛІВ В ТЕХНОЛОГІЯХ ОПТИЧНОГО ЗВ'ЯЗКУ

Пугач К. О., асистент Чумак В.С.
Харківський національний університет радіоелектроніки,
кафедра МТС, м. Харків, Україна
e-mail: kateryna.puhach@nure.ua

Abstract. This article looks at issues and concerns engineers face when interfacing microcontrollers and fiber optics. This includes the rudimentary tasks of setting up and controlling laser emitter power levels and sensitivity thresholds for receivers, as well as tracking performance in real time.

З'єднання на основі міді служить вже протягом тривалого часу і продовжуватиме використовуватися в галузях, де воно ефективне з точки зору продуктивності та вартості. Однак для більш високої швидкості та/або передачі сигналів на великі відстані більш ефективним є використання інших транспортних механізмів.

Ми можемо розділити зв'язок кристала з волоконною оптикою на дві основні категорії. З одного боку розташовані високоякісні мережеві процесори. Вони реалізують і декодують протоколи з кількох потоків даних на дуже високих швидкостях. З іншого боку розташовані менш спеціалізовані процесори, які керують, або розташовані в безпосередній близькості від модульних або дискретних передавачів, або приймачів. Дискретні детектори, випромінювачі, лазери, волоконні роз'єми та кабельні зборки дозволяють розмістити всі волоконно-оптичні елементи на платах.

Основні вбудовані процесори, безумовно, можуть зберігати та отримувати дані калібрування для рівнів потужності передачі, зміщення прийому та теплової компенсації. Їх можна налаштувати послідовно під час увімкнення живлення та скинути як частину процесу ініціалізації. Однак, відстеження продуктивності та динамічне налаштування параметрів зв'язку для багатьох каналів відбувається в режимі реального часу може негативно позначитися на центральному хост-процесорі, якщо потрібно багато оптоволоконних каналів.

Основним підходом в цьому випадку є розробка власного модуля або модульного схемного блоку, який можна реалізувати, як і будь-яку іншу частину, і відтворити як функцію копіювання та вставки в нових проектах. У цьому випадку невеликі процесори в кожному модулі можуть відстежувати та контролювати продуктивність зв'язків у режимі реального часу. Обробка даних у таких системах, як правило, вимагає інтенсивного вирішення завдань ЦОС та великої кількості каналів [1, 2]. Тому, пропонується використовувати FPGA Xilinx, які мають високошвидкісну смугу пропускання, велику кількість логічних елементів, низьке енергоспоживання і високу продуктивність за низькою ціною [1-5].

Використовувати десяток невеликих процесорів чи лише один буде залежати від того, скільки посилань знадобиться. Одне посилання може не займати занадто багато часу на обробку хоста та ресурсів від вбудованого контролера, але 1000 посилань може забирати достатньо ресурсів. Маленькі, дешеві й у великій кількості попередньо запрограмовані виділені процесори в упакованій або навіть кристалізованій формі будуть дешевшими, ніж більшість інших компонентів у модульній оптоволоконній конструкції.

Ще однією перевагою цього підходу є можливість живити модульні трансивери зовнішніми високоточними годинниками. Це дозволяє контролювати перекос і синхронізувати передачу даних через кілька каналів.

Такі модулі зможуть зберігати параметри, а також виконувати діагностику. Ці спеціалізовані процесори також зможуть діяти як перетворювачі послідовних сигналів у паралельні та паралельні у послідовні, коли для оптоволоконних з'єднань не потрібна висока швидкість.

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. Особливості реалізації вузла швидкого перетворення фур'є на пліс архітектури FPGA / В. С. Чумак, І. В. Свид // Радиоэлектроника и молодежь в XXI веке: материалы 25-го Междунар. молодеж. форума, 20–22 апр. 2021 г. – Харьков: ХНУРЭ, 2021. – Т. 3. – С. 187–188.

3. Чумак В. С. Поточне обчислення двійкового логарифму для ПЛІС Artix-7 та синтезатора Vivado / В. С. Чумак, І. В. Свид, Н. В. Бойко // III форум «Автоматизація, електроніка та робототехніка. Стратегії розвитку та інноваційні технології» AERT-2021. – Харків, ХНУРЕ, 2021. – С. 54-55.

4. O. Zubkov, I. Svyd, O. Maltsev, L. 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&FPGA-2019, Kharkiv, Ukraine, July 26-27, 2019. – Kharkiv: 2019. – P. 12-13. doi: 10.35598/mcfpga.2019.003.

5. 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.

ПІДКЛЮЧЕННЯ МІКРОКОНТРОЛЕРА ДО ЛОКАЛЬНОЇ МЕРЕЖІ ЗА ДОПОМОГОЮ МОДУЛЯ НА МІКРОСХЕМІ ENC28J60

Славгородський Я.В., ассистент Чумак В.С.
Харківський національний університет радіоелектроніки,
кафедра МТС, м. Харків, Україна
e-mail: yaroslav.slavhorodskyi@nure.ua

Abstract. Often, microcontrollers need access to the Internet, a local network. This can be useful, for example, for building a smart home, telemedicine systems [1, 2], creating weather stations, installing a simple web server, and much more. All this can be provided by the ENC28J60 Ethernet module. The ENC28J60 Mini Ethernet Module is a compact version of the ENC28J60 Ethernet Module. The board is designed to connect devices based on Arduino, AVR, PIC, ARM, etc. to an Ethernet network.

Мікросхема ENC28J60, це готове мережеве рішення, в якому присутній і фізичний і канальний рівень. Обмін даними з контролером ця мікросхема здійснює за допомогою шини SPI. Фізичний рівень у неї організований за стандартом 10BASE-T. Тобто максимальна швидкість передачі даних – 10 мегабіт на секунду.

ENC28J60 підтримує стандартний механізм взаємодії із зовнішнім контролером – через читання та запис значень у регістри, що відповідають за ту чи іншу функцію. Всі регістри поділяються на три основні групи: керуючі регістри, регістри для роботи з буфером Ethernet, регістри PHY.

Крім адресів регістрів існують і банки, тобто порядок адресації регістрів сегментований, а починаючи з адреси 1Bh(EIE) звернення до регістрів від банків не залежить, вони мапяться на всі банки. Якщо у нас активний банк 0, то при записі регістру з адресою 0x00 ми змінимо значення регістру ERDPTL, якщо банк 1 - то EHT0. Наприкінці кожного з банків є п'ять однакових регістрів, які є загальними, тобто, який би банк не був активним, ці адреси (0x1B - 0x1F) будуть належати тим самим регістрам EIE, EIR, ESTAT, ECON2, ECON1.Основне призначення регістрів можна дізнатися за їх початковими буквами в абревіатурі: E – Ethernet, MA – MAC, MII – MI.

ENC28J60 має буфер розміром 8 КБ. Частина цього буфера зазвичай виділяється для прийому пакетів, іншу можна використовувати як завгодно. Наприклад, для даних, що відправляються. Адреса першого непрочитаного пакета зберігатиметься в регістрах ERXRDPT. Забравши пакет, мікроконтролер записує адресу наступного пакета в ERXRDPT. Після цього місце, яке займав пакет, вважається вільним і ENC28J60 може використовувати його для прийому нових пакетів.

Робота з ENC28J60 побудована на наступному форматі - контролер відправляє команду завдовжки один байт, за якою слідують дані. Залежно

від типу команди за нею слідує або передача даних ENC28J60, або читання даних з неї ж.

Всього цих команд 7 штук: Read Control Register(RCR),Read Buffer Memory(RBM),Write Control Register(WCR),Write Buffer Memory(WBM),Bit Field Set(BFS),Bit Field Clear(BFC),System Command(Soft Reset)(SC). Байт команди складається з коду OpCode (3 біти) та 5 бітів, які або відповідають за адресу регістру, або мають фіксоване значення для деяких команд.

Само собою, щоб займатися програмуванням передачі даних через мережу, необхідні знання мережевих рівнів, моделі OSI і всього, що пов'язане з мережею. Мережева модель поділяється на кілька рівнів. Основні з них такі: прикладний рівень, рівень уявлення, сеансовий рівень, транспортний рівень, мережевий рівень, каналальний рівень, фізичний рівень.

При передачі даних із програми в мережевий дріт ми проходимо шлях зверху вниз по списку який написано вище. Спочатку дані об'єднуємо в якісь зручні послідовності або масиви, зрозумілі для прикладного рівня сторони, що приймається, потім шифруємо або ще перетворюємо іншим способом для захисту від несанкціонованого використання [2], потім обгортаємо в певний протокол, який допоможе підтримати з'єднання і не втратити його (сеансовий рівень), потім причіплюємо ще заголовок спереду, який забезпечить передачу певному порту від іншого певного порту, потім ще обгортаємо в протокол, який забезпечить доставку до певного пристрою, що має мережеву адресу (IP), потім ще обгортаємо протокол, який несе в собі фізичні адреси пристроїв MAC (канальний рівень), а останній рівень вже забезпечить безпосередню доставку всіх цих кілька разів обгорнутих пакетів (фізичний рівень), до якого належать трансформатори, дроти, концентратори, повторювачі сигналу та медіаконвертори.

Список використаних джерел.

1. Аналіз принципів побудови телемедичних комплексів широкого призначення / В. С. Чумак, О. Г. Аврунін, Є. А.Чугуй, І. В. Свид // АСУ та прилади автоматики. 2021. № 177. С. 80-85.

2. V. Semenets, V. Chumak, I. Svyd, O. Zubkov, O. Vorgul, N.a Boiko. Designing the Structure of a General-Purpose Telemedicine Complex. // III International Scientific and Practical Conference Theoretical and Applied Aspects of Device Development on Microcontrollers and FPGAs (MC&FPGA), Kharkiv, Ukraine, 2021, pp. 47-48, doi: 10.35598/mcfpga.2021.016.

3. Воргуль О. В. Поліпшений захист мікроконтролера від читання / О. В. Воргуль, О. Г. Білоцерківець // III форум «Автоматизація, електроніка та робототехніка. Стратегії розвитку та інноваційні технології» AERT-2021. – Харків, ХНУРЕ, 2021. – С. 34-35.

ПЕРЕВАГИ ВИКОРИСТАННЯ AVR МІКРОКОНРОЛЕРІВ

Факас О. В., асистент Чумак В.С.
Харківський національний університет радіоелектроніки,
кафедра МТС, м. Харків, Україна
e-mail: olena.fakas@nure.ua

Abstract. Microcontrollers are used almost everywhere. Almost every device of the 21st century runs on a microcontroller: measuring instruments, tools, household appliances, watches, toys, music boxes and postcards, and much more. AVR series microcontrollers are some of the fastest microcontrollers in the world. This series is represented by a very wide variety of models, ranging from small 8-pin devices to microcircuits in 40-pin packages. The command system is unified as much as possible, therefore, having written a program for one model, you can transfer it to another model with minimal.

Зі зростанням ступеня інтеграції мікросхем якісно змінюється межа складності систем, які можуть бути реалізовані на їхній основі [1, 2]. Різниця між мікропроцесором та мікроконтролером полягає в наявності вбудованих у мікросхему процесора приладів «пуск-завершення», таймерів та інших віддалених конструкцій. Застосування в нинішньому контролері досить сильного обчислювального апарату з великими здібностями, побудованого на моносхемі, натомість єдиного комплекту, суттєво зменшує масштаби, споживання та ціну створених на його основі приладів.

Найпоширенішим на сьогоднішній день є мікроконтролер AVR. До складу цього пристрою входять високошвидкісний RISC-мікропроцесор, 2 види витратної енергії пам'яті (Flash-кеш і кеш відомостей EEPROM), експлуатаційна кеш за типом RAM, порти вводу/виводу і різноманітні віддалені пов'язані структури [3].

Абсолютно всі мікроконтролери цього виду мають властивість самостійного кодування, здатність змінювати складові своєї пам'яті драйвера без сторонньої допомоги. Ця риса дає можливість формувати дуже пластичні концепції, та його спосіб діяльності змінюється особисто мікроконтролером у зв'язку з тієї чи іншої картиною, обумовленої заходами ззовні чи зсередини. Всім мікроконтролерам AVR властива багатоярусна техніка запобіжного заходу.

Розробник може використовувати аналоговий сигнал, подавши його на вхід мікроконтролера і маніпулювати з даними про його значення. Цю роботу виконує аналогово-цифровий перетворювач (АЦП). Ця функція дозволяє спілкуватися з мікроконтролером, а також сприймати різні параметри навколишнього світу за допомогою датчиків.

Переваги даного виду мікроконтролера:

- вартість. На даний момент найдешевший мікроконтролер – це Atmel AVR ATtiny11 на 6 МГц за 0,54 долара;

- швидкість. Більшість AVR здатні працювати на частоті 20 МГц (навіть ATtiny25/45/85 та ATmega48), але вони фактично працюють зі швидкістю близько 20 MIPS;

- підтримуються GNU Compiler Collection (GCC) ;

- Flash-ПЗУ програм, що програмується в системі, 10 000 циклів перезапису;

- EEPROM даних (100 000 циклів) - вона не "забуває" при вимк. живлення;

- синхронний або асинхронний UART (у mega64 та mega128 їх по 2);

- мікроспоживання (менше 100 мкА в активному режимі на частоті 32 кГц);

- JTAG-інтерфейс для підключення емулятора (МК з об'ємом ПЗУ від 16 кбайт) та ін.

Існує безліч застосувань мікроконтролера AVR: вони використовуються в домашній автоматизації, сенсорних екранах, автомобілях, телемедичних системах широкого призначення [4] та обороні. Для повсякденного та безпечного життя в своєму ж будинку або в квартирі та на роботі в офісі, на заводах, в магазинах та в різних торговий центрах використовують різні пожежні сигналізації, що мають в своїй конструкції мікроконтролер AVR. Для даної задачі використовуються різні сімейства цього мікроконтролера. Наприклад, ATMEGA8 має в своїй конструкції датчик пожежі. Цей датчик може бути будь-якого типу, однак в більшості використовується інфрачервоний датчик пожежі. Хоча в ІЧ-датчиків пожежі є деякі недоліки, в основному пов'язані з неточністю, це найдешевший і найпростіший спосіб виявлення спалаху.

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. Белов А. В. – «Самоучитель разработчика устройств на микроконтроллерах AVR».

4. Аналіз принципів побудови телемедичних комплексів широкого призначення / В. С. Чумак, О. Г. Аврунін, Є. А.Чугуй, І. В. Свид // АСУ та прилади автоматики. 2021. № 177. С. 80-85.

ОСОБЛИВОСТІ ПЕРСПЕКТИВ ВИКОРИСТАННЯ БЕЗБАТАРЕЙНИХ ДЖЕРЕЛ ДОДАТКОВОГО ЖИВЛЕННЯ ДЛЯ МІКРОПРОЦЕСОРНИХ ПРИСТРОЇВ ІЗ ІНТЕГРОВАНИМИ GSM/GPS/GPRS МОДУЛЯМИ

к.ф.-м.н., доц. Цехмістро Р. І., к.т.н., доц. Шаповалов С. В.,
аспірант Першин Є. В.
Харківський національний університет радіоелектроніки,
кафедра МІРЕС, м. Харків, Україна
e-mail: roman.tsekhmistro@nure.ua, serhii.shapovalov@nure.ua,
yevhenii.pershyn@nure.ua

Abstract. The given work is devoted to a comparative analysis of devices that provide power to microprocessor devices without the use of a traditional autonomous battery source. A detailed description of the converter of mechanical energy into electrical with the possibility of accumulating the converted energy is given. Built-in inexpensive GSM/GPS/GPRS modules used by civilians with an estimate of power consumption and a method for obtaining energy by piezoelectric transformation of mechanical energy are described.

Вступ. Успіх сучасних технологій дозволив створити мікропроцесорні модулі для отримання даних про місце розташування об’єкта та засоби передачі отриманих даних. Один із таких модулів є SIM808, показаний на рисунку 1. Це процесор для мобільного зв’язку, інтегрований з модулем місцезнаходження, роз’ємом для SIM-карти, стабілізатором живлення та інтерфейсом для зв’язку з ПК. Аналогом вбудованого модуля SIM808 є модуль SIM800C. SIM800C створено компанією SIMCom Wireless Solutions, модуль має габарити 17,6x15,7 мм та корпус LCC з контактами по периметру, що дає можливість як ручної, так і автоматизованої установки.

Рисунок 1 – Зовнішній вигляд вбудованого модуля SIM808

Основні технічні параметри модуля:

- частотні діапазони стандарту GSM: 850/900/1800/1900 МГц;
- керування через AT команди;
- діапазон напруги живлення: 3,4 В ~ 4,4 В;
- чутливість GPS: -165 дБм;
- холодний старт: 30 с;
- точність: <2,5 м;
- канали приймача: 22 для відстеження та 66 для захвату;
- грубий код/код придбання: GPS L1;
- чутливість відстеження: -165 дБм;
- час холодного запуску: 30 с;
- час гарячого старту: 1 с;
- час теплого старту: 28 с;
- точність горизонтального положення: <2,5 м;
- споживана потужність при зборі даних: 42 мА;
- споживана потужність при безперервному відстеженні: 24 мА;
- частота оновлення: 5 Гц;
- габаритні розміри модуля: 27х37 мм.

Огляд енергетичних параметрів даного малогабаритного модуля SIM808C (інтегрований модуль GSM зв'язку з модулем GPS позиціонування) вказує на гостру необхідність стабілізованого джерела живлення з акумуляторним живленням (18500 мА і більше). Цей факт зумовлений тим, що в окремих випадках задля забезпечення GSM зв’язку, тобто для відправлення повідомлень та здійснення дзвінків, необхідне споживання струму становить до 2 А. При використанні модуля GPS позиціонування для отримання стійкого сигналу із супутника при знаходженні модуля в приміщенні час отримання сигналу із супутника може становити кілька хвилин. Це пов’язано з тим, що при тривалому відключенні модуля (тиждень та більше) рівень заряду батареї, розташованої на платі (рисунок 2), вимагає підзарядки. Тип і конструкція антени також впливає на час виявлення супутникового сигналу.

Рисунок 2 – Зовнішній вигляд модуля GPS позиціонування NEO-6M

Основна частина. Все вищезазначене підштовхує на необхідність пошуку резервних джерел живлення мікропроцесорних пристроїв, що використовують зазначені модулі зв'язку та геолокації. Найбільш реальним резервним джерелом живлення, що не вимагає обслуговування в плані підзарядки, є пристрої, здатні перетворювати енергію механічного та теплового походження в електричну та накопичувати останню.

Більшість мікропроцесорних пристроїв із зазначеними модулями є невід'ємною частиною пристроїв автоматики та механіки [1]. Дано опис принципів перетворення, які за родом своєї діяльності вже використовують механізми готових пристроїв, що дозволяють проводити перетворення енергії без істотних змін їх конструкції, маси, об'єму, габаритів та ін. Це необхідно для дотримання параметрів ціна та якість.

Наприклад, перетворюючий пристрій являє собою електромагнітний індукційний генератор лінійного типу, виконаний з можливістю перетворення в електричний сигнал частини енергії, пов'язаної з прискоренням, що діє на корпус виробу в результаті виконання робочого циклу. При цьому перетворюючий пристрій містить котушку (індуктивність) і вантаж (невід'ємна частина основного механізму), що являє собою постійний магніт, розташований вільно в корпусі. В цьому випадку перетворюючий пристрій виконано з можливістю використання енергії, що отримується вантажем. У результаті прискорення процесорний блок, який входить до складу основного виробу, може бути виконаний з можливістю додаткового живлення від виробленого електричного сигналу.

Великі можливості мають також перетворювачі сонячної енергії на електричну, особливо в розвитку МЕМС технологій. Останні здатні зробити такі пристрої економічно рентабельними.

В ряді способів для приведення в дію перетворювача, що перетворює електричну енергію збуджуючого струму в механічну енергію хвилі напруги в тілі, використовується змінний струм, частота хвиль при цьому знаходиться між 20 кГц і 50 МГц. За допомогою відповідних контурів можна отримувати безперервний ряд хвиль або імпульси, що складаються з коротких серій хвиль високої частоти, що повторюються регулярно з низькою частотою. Для цього використовуються перетворювачі, принцип дії яких ґрунтується на магнітострикційному або п'єзоелектричному ефектах. Матеріалами для п'єзоелектричних перетворювачів, крім кристалів кварцу, є штучні фероелектричні кристали (зокрема, титанат барію у вигляді полікристалічної кераміки), що мають у порівнянні з природними кристалами більшу чутливість і менший опір.

Однак, температура Кюрі штучних кристалів порівняно низька (при нагріванні вище за цю температуру п'єзоелектричні властивості пропадають). Матеріалами для магнітострикційних перетворювачів служать феромагнітні елементи та сплави. Максимальні деформації в обох випадках визначаються механічними властивостями матеріалу тіла. Для

збудження слабких імпульсів напруги використовують іскровий спосіб, запропонований Кауфманом і Ревером [2-4]. Перевага цього способу полягає в тому, що іскра діє як точкове джерело, тоді як п’єзоелектричний перетворювач завдяки дифракції дає складну хвильову картину.

Однією з важливих особливостей сучасних технологічних проблем є пряме перетворення теплової енергії на електричну. Застосування для цієї мети сегнетоелектриків ще не набуло широкого поширення, але може бути перспективним [2-4]. Принцип дії сегнетоелектричних перетворювачів ґрунтується на зміні діелектричної проникності сегнетоелектриків при зміні температури. Нехай при температурі t_1 ємність сегнетоелектричного конденсатора дорівнює C_1, а за температури t_2 вона зменшиться і стане рівною C_2. Тоді, якщо зарядити конденсатор при температурі t_1 від джерела з напругою V_0, потім відключити від цього джерела і змінити температури до t_2, його ємність зменшиться, а напруга на обкладках зросте. Електрична енергія також збільшиться на величину. Перетворювач працюватиме в режимі періодичного нагрівання та охолодження.

Висновки. Представлені міркування дають чітке уявлення про необхідність наявності резервного джерела живлення для вбудованих мікропроцесорних модулів на основі механізмів, які забезпечують працездатність основних пристроїв. Перевагою їх може бути більша автономність і менші витрати часу на обслуговування.

Найбільш перспективними, на наш погляд, є пристрої, засновані на використанні явища електромагнітної індукції, ефекту п’єзоперетворення, а також їх можливого поєднання. Цікавими також є перспективи використання піроелектричних та сегнетоелектричних перетворювачів.

Список використаних джерел.

1. Murad Omarov, Vladimir Kartashov, Roman Tsekhmistro. Features of the use of microprocessors in the systems of ovojectors in their adaptation to the conditions of the former CIS. / I 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. 33-34. DOI: 10.35598/mcfpga.2019.012.

2. Пироэлектрические преобразователи / В. К. Новик [и др.]. – Москва: Советское радио, 1979. – 176 с.

3. Диэлектрики. Основные свойства и применения в электронике / И. С. Рез, Ю. М. Поплавко. – Москва: Радио и связь, 1989. – 288 с.

4. Пироэлектрический эффект и его практические применения / В. Ф. Косоротов [и др.]; под. общ. ред. Л. С. Кременчугского. – Киев: Наукова думка, 1989. – 224 с.

РЕКТЕНА З ТРИФАЗНОЮ СХЕМОЮ ВИПРЯМЛЕННЯ ДЛЯ IoT ДОДАТКІВ

аспірант Алєксєєв В.О.
Харківський національний університет радіоелектроніки,
кафедра КРіСТЗІ, м. Харків, Україна
e-mail: vasyl.alieksieiev@nure.ua

Abstract. The given paper presents research of the energetic characteristics of three-phase rectenna's element which receives and transforms custom electromagnetic fields to the direct current. Rectenna's element is formed from a system of three emitters, symmetrical vibrators which are interchanged. Input filters were connected to internal terminals of vibrators the first, second and third single-phase rectifier circuits respectively. Obtained simulation results of the three-phase rectenna's element showed the advantage of its energy characteristics in comparison with single-phase rectification schemes.

Вступ. В останні кілька років активно провадяться дослідження технології збору та перетворення енергії електромагнітного поля (ЕМП) в навколишньому середовищі (рис. 1) в корисну енергію постійного струму за допомогою ректен [1, 2]. Ця енергія може використовуватися безпосередньо або накопичуватися і зберігатися для подальшого використання, що дозволяє реалізувати альтернативні джерела енергії для тих місць, де немає енергетичних систем, або виникають труднощі енергоживлення різного характеру. Актуальність вирішення завдань збору енергії пов'язана з тим, що більшість електронних пристроїв IoT, наприклад, таких як датчики в промислових, комерційних і медичних додатках (наприклад, моніторингу забруднення повітря, лісових пожеж, контролю стану різних механізмів, устаткування та будівельних споруд і т.п.), безпроводові пристрої та інші схеми з низьким енергоспоживанням, живляться від батарей. Однак, навіть дуже якісні батареї мають обмежений термін використання. Заміна батарей стає

Рисунок 1 – Енергопостачання малопотужних пристроїв за рахунок видобування енергії з навколишнього ЕМП

"дорогим задоволенням", коли у віддалених місцях знаходяться сотні датчиків. Крім цього виникають нагальні екологічні проблеми, пов'язані з утилізацією відпрацьованих батарей. Застосування ж технологій збору електромагнітної енергії, що створюється радіоелектронними системами різного класу та призначення, практично не потребує технічного обслуговування цього устаткування, є економічно ефективним і привабливим з точки зору екологічної безпеки.

На рис. 2 наведена архітектура вузла IoT з безпровідним живленням. Для реалізації перетворення енергії ЕМП в постійний струм в світі широкого поширення набули ректени [3], які в загальному випадку будуються за відомою класичною схемою, наведеною на рис. 3.

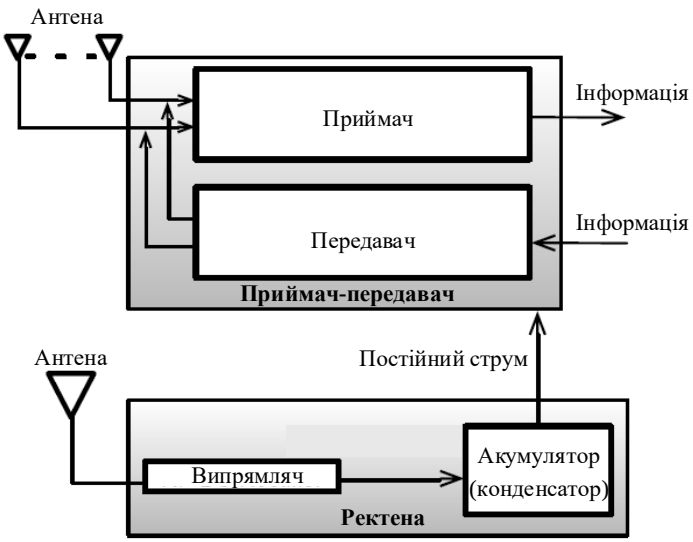


Рисунок 2 – Архітектура вузла IoT з безпровідним живленням

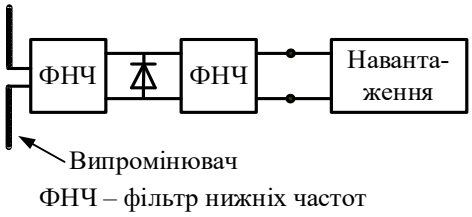


Рисунок 3 – Структурна схема ректени

На відміну від систем БПЕ сфокусованим мікрохвильовим променем [3], в яких ректени працюють на фіксованій частоті і на апертурі яких формуються оптимальні амплітудно-фазові розподіли при проектуванні ректен для збору енергії з навколишнього ЕМП, у зв'язку з іншими умовами їх функціонування, необхідно вирішувати ряд нових завдань, пов'язаних з розробкою та удосконаленням математичних моделей широкосмугових, багаточастотних ректен, які опромінюються малопотужними ЕМП із довільною поляризацією. Вирішення цих задач, безумовно, є актуальним, а успішне їх розв'язання дозволить приступити до розробки різних електронних пристроїв IoT з безпровідним живленням. В даній роботі вирішена одна із зазначених вище задач, яка пов’язана з дослідженням енергетичних характеристик багатофазної ректени, що перетворює ЕМП довільної поляризації у постійний струм.

Основна частина. Ректенний елемент з багатофазною схемою випрямлення являє собою M ідентичних ректенних елементів з однофазними схемами випрямлення, що працюють на загальне

навантаження й збуджувані друг відносно друга з певним фазовим зсувом (рис. 4). Збуджуються однофазні ректенні елементи рівноамплітудно із частотою ω_0 та фазовим зсувом $\Delta\varphi = 2\pi/M$, тобто розглядається так називана симетрична багатофазна система випрямлення [4].

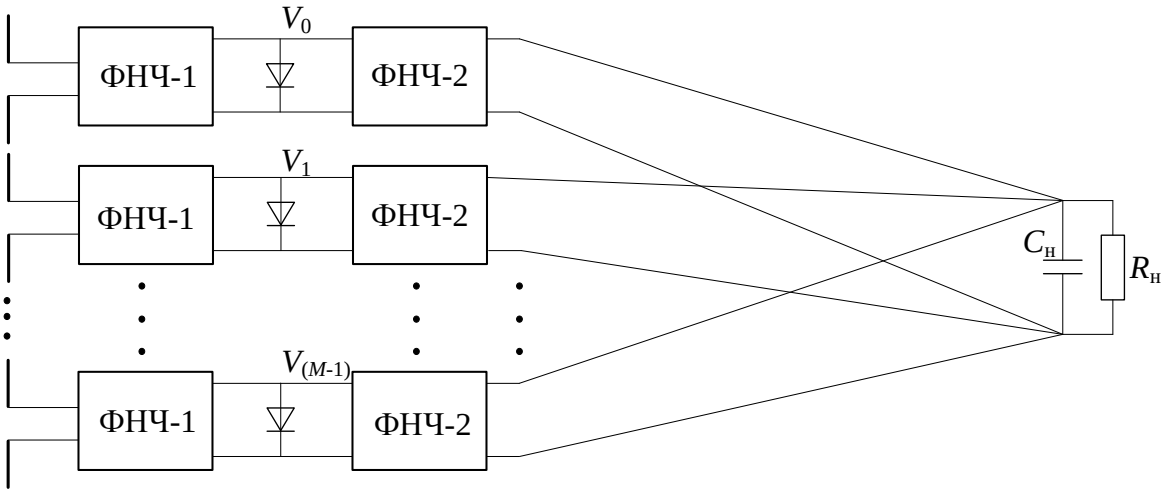


Рисунок 4 – Структурна схема багатофазного ректенного елемента

Наведемо результати дослідження трифазного ректенного елемента з використанням в якості системи випромінювання трьох пересічних симетричних вібраторів до вхідних клем яких (клеми $1-1'$, $2-2'$, $3-3'$ рис. 5) підключені вхідні фільтри, відповідно, першої, другої і третьої однофазних випрямних схем (рис. 3). Вібратори розташовані на висоті $\lambda_0/4$ над ідеально провідним екраном. Якщо параметри вхідних у схему однофазних ректенних елементів ідентичні, а збудливою є електромагнітна хвиля кругової поляризації, то даний ректенний елемент буде симетричним трифазним ректенним елементом.

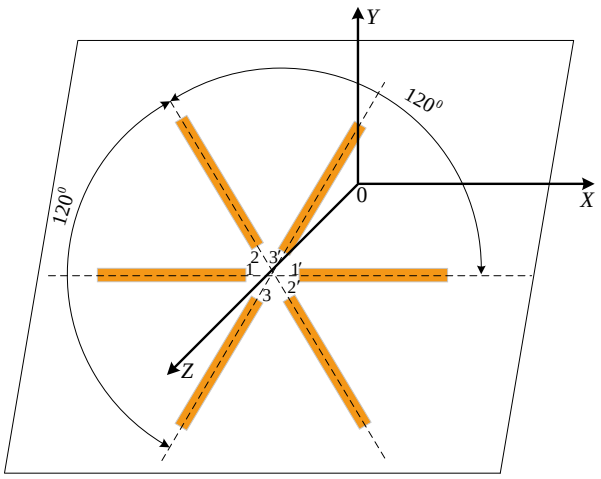
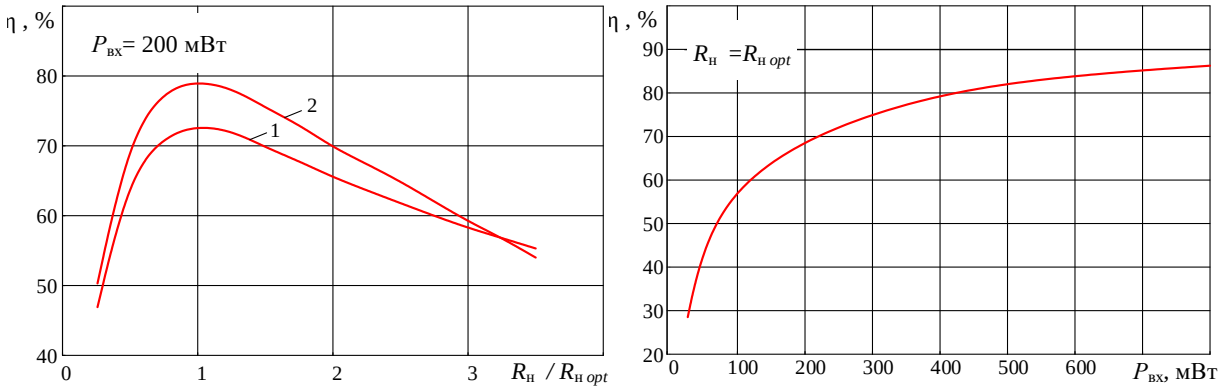


Рисунок 5 – Випромінювальна структура трифазного ректенного елемента

Результати розрахунку енергетичних характеристик трифазного ректенного елемента наведені на рис. 6. На рис. 6,а показана залежність коефіцієнта корисної дії від опору навантаження, що розрахована при $P_{вх} = 200$ мВт. При такому рівні вхідної потужності амплітуда напруги основної частоти, що прикладена до діодів трифазної схеми буде такою же, як й амплітуда напруги основної частоти, що прикладена до діода однофазного однопівперіодного ректенного елемента, який працює при

рівні вхідної потужності $P_{вх} = 100$ мВт. Це дозволяє дати порівняльну оцінку даних схем побудови ректенних елементів з погляду вимог до параметрів застосовуваних в них випрямних діодів.



а б

Рисунок 6 – Залежність ККД трифазного елемента ректени від опору навантаження та рівня вхідної потужності

Висновки. Порівняння кривих для трифазного ректенного елемента (рис. 6,а) з аналогічними кривими для однофазного ректенного елемента [3] показує, що трифазний та однофазний елементи ректен при будь-якому опорі навантаження мають різні значення ККД для ректенних елементів без вхідних фільтрів (рис. 6,а, крива 1) і якщо вхідні ФНЧ – фільтри з ідеальними характеристиками (рис. 6,а крива 2). Аналогічним чином поводиться й залежність коефіцієнта корисної дії від рівня вхідної потужності (див. рис. 6,б). З порівняння результатів моделювання з результатами [3], видно, що трифазний елемент ректени може прийняти потужність у два рази більшу, ніж однофазний ректенний елемент при однакових вимогах до таких параметрів застосовуваних в них випрямних діодів.

Список використаних джерел.

1. Husnain H., Sherazi R., Zorbas D., O'Flynn B. A comprehensive survey on RF energy harvesting: applications and performance determinants / Sensors 2022. N 22(8). p. 1–36.

2. Chen Y-S., Chiu C-W. Maximum achievable power conversion efficiency obtained through an optimized rectenna structure for RF energy harvesting / Transactions on Antennas and propagation. 2017. Vol. 65. Issue 5. p. 2305–2317.

3. Крупноапертурные антенны-выпрямители систем беспроводной передачи энергии микроволновым лучом / В.М. Шокало, А.И. Лучанинов, А.М. Рыбалко, Д.В. Грецких. – Харьков: Коллегиум, 2006. – 308 с.

4. Борисов П.А., Томасов В.С. Расчет и моделирование выпрямителей. – СПб: СПб ГУ ИТМО, 2009 – 169 с.

ТЕХНОЛОГІЇ СТВОРЕННЯ РОБОТОТЕХНІЧНИХ КОМПЛЕКСІВ ДЛЯ ГУМАНІТАРНОГО РОЗМІНУВАННЯ

студент Вирвихвост О. В., доцент, к.т.н., Янушкевич Д. А.
Харківський національний університет радіоелектроніки,
кафедра КІТАМ, м. Харків, Україна
e-mail: oleh.vyrvykhvost@nure.ua, dmytro.ianushkevych@nure.ua

Abstract. The object of research is military robotic complexes (MRC) used in the system of humanitarian demining. This work is aimed at studying the requirements for MRC. The research is based on the application of a functional approach to the construction of MRC models used in the system of humanitarian demining. It is established that a typical sample MRC can be presented as a set of functionally related elements: base media, mobile platform, specialized equipment, as well as information reception and processing systems, action planning, control systems, automatic pattern recognition, situation analysis, artificial intelligence and training.

Вступ. Всі воєнні конфлікти супроводжуються широким застосуванням протиборчими сторонами протипіхотних мін та вибухонебезпечних предметів (ВНП). Однією з проблем, з якою країни у всіх регіонах, де велись бойові дії або існують воєнні конфлікти, які були породжені війнами, міжнародними та міжнаціональними визвольними рухами (Україна, Ірак, Сирія, Афганістан, колишня Югославія тощо), стикаються з проблемами гуманітарного розмінування [1].

Від початку війни піротехнічними підрозділами Державної служби з надзвичайних ситуацій (ДСНС) станом на 15.09.2022 р. в Україні було обстежено територію площею понад 68 тисяч гектарів та було виявлено, вилучено та знешкодили понад 180 тисяч вибухонебезпечних предметів здебільшого боєприпасів ствольної та реактивної артилерії (калібрів 122 мм, 125 мм, 152 мм), мінометних мін (82 та 120 мм), гранатометних пострілів (ПГ-7, ВОГ-17, ВОГ-25), протитанкових мін (ТМ-62, ПТМ-3), протипіхотних мін (ОЗМ-72, МОН-50, ПМН-2, ПФМ-1, ПОМ-2), саморобних вибухових пристроїв.

Для здійснення розмінування характерним є зростання уваги усіх країн світу до проблем створення та застосування робототехнічних комплексів та систем військового, спеціального та подвійного призначення (РКВП) для здійснення гуманітарного розмінування [2].

Це обумовлюється намаганням усіх передових країн світу до збереження людського життя, в контексті якого використання РКВП дозволяє досягти позитивних результатів щодо ефективності та якості розмінування з мінімальними людськими втратами. Крім того, ця тенденція пояснюється стрімким розвитком новітніх технологій в інформаційній сфері, тобто «роботизація» різноманітних напрямів

діяльності людини, зокрема, військової сфери, що відповідає змісту сучасних концепцій постіндустріального суспільства на базі концепції Industry 4.0.

Основна частина. Гуманітарне розмінування – комплекс заходів, які проводяться з метою ліквідації небезпек, пов'язаних із вибухонебезпечними предметами (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 [3].

Гуманітарне розмінування у першу чергу 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 наземних мін.

Роботи по створенню РКВП проводяться в різних країнах світу. Так, США визнало, що застосування РКВП – один з найперспективніших напрямів розвитку військової справи. США можна вважати лідером не тільки розробок, а й практичного використання роботів, хоч багато зусиль нині здійснюють також Японія, Китай, Великобританія, Ізраїль, Туреччина тощо [4].

Викладені проблеми, мають бути вирішені за рахунок створення РКВП. Можна виділити основні характеристики РКВП, до яких належать:

– автономність (управління роботом здійснюється автономно або оператором дистанційно);

– адаптивність – наявність експертної системи, реагування на ситуаційні зміни;

– обробка та розпізнавання мовних і зорових образів;

– створення мовних інтерфейсів;

– мобільність та вогнева міць;

– навігація.

Сьогодні робота над РКВП 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.

Створення РКВП потребує опрацювання системного застосування 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 [4, 5]:

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 [4].

До основних можуть бути віднесені технології систем прийняття та обробки сенсорної інформації, оцінки ситуації та планування дій, систем дистанційного управління, автоматичного розпізнавання образів, аналізу ситуацій та динамічних сцен, штучного інтелекту та навчання, людино-машинного інтерфейсу, інтелектуальних систем керування [4]. До допоміжних можна віднести технології живлення, системи геоінформаційного та глобального позиціонування тощо.

Одним із основних результатів розробки РКВП є виявлення та ідентифікація ВНП у ґрунті. Для ідентифікація ВНП у ґрунті ВНП пропонується метод, принцип дії якого базується на опромінюванні поверхні ґрунту джерелом НВЧ-енергії і вимірюванні температури поверхні ґрунту за допомогою оптико-електронний пристрою для візуалізації температурного поля та вимірювання температури ґрунту (тепловізора). Внаслідок нагріву шару ґрунту та вимірюванні його температури проводиться подальший аналіз, який дає можливість зробити висновок про тип та форму ВНП, та таким чином ідентифікувати його.

Суть реалізації методу базується набором відомих технічних та апаратних засобів, які відповідають комплексу вимог до поставленої мети. Оцінка таких вимог приводить до наступних параметрів апаратури:

– частота НВЧ-променів, що нагрівають ґрунт;

– потужність НВЧ-променів;

– температурна чутливість тепловізора;

– габаритні характеристики.

Висновки. Таким чином встановлено, що застосування РКВП для проведення робіт з гуманітарного розмінування на даний час є дуже актуальним завданням.

Пошук та ідентифікація ВНП для гуманітарного розмінування є комплексним завданням. У зв'язку з цим, для проведення гуманітарного розмінування РКВП повинні бути оснащені відповідними маніпуляторами та детекторами (сенсорами, датчиками), засобами прийняття рішень та застосовуватись на етапах розвідки, пошуку, локації, маркування, ідентифікації, знешкодження, знищення (утилізації) ВНП [5]. 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 [4].

Одним із перспективних напрямків ідентифікації ВНП пропонується метод, принцип дії якого базується на опроміненні ґрунту джерелом НВЧ-енергії і вимірюванні температури поверхні ґрунту за допомогою тепловізора.

Список використаних джерел.

1. Invisible death: anti-personnel mines continue to claim thousands of lives [Електронний ресурс] / M. Tarhan // Агенство Анадолу. – 2021. – Режим доступу: https://bit.ly/352MG61. – Назва з екрана.

2. Наземні бойові роботи: лідери та Україна [Електронний ресурс] – Режим доступу: https://lb.ua/news/2021/11/17/498795_nazemni_boyovi_roboti_ lideri.html.

3. Гуманітарне розмінування [Електронний ресурс] – Режим доступу: https://uos.ua/uslugi/gumanitarnoe-razminirovanie. – Назва з екрана.

4. 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.

5. Янушкевич Д. А., Іванов Л. С. Сучасні тенденції застосування роботизованих систем для гуманітарного розмінування [Електронний ресурс] / Д. А. Янушкевич, Л. С. Іванов // Збірник матеріалів III форуму «Автоматизація, електроніка та робототехніка. Стратегії розвитку та інноваційні технології» AERT-2021. – Режим доступу: https://mts.nure.ua/conferences -ua/forum/aert-2021.

СУЧАСНІ ПІДХОДИ ДО СИСТЕМИ УПРАВЛІННЯ ЯКІСТЮ ПІДПРИЄМСТВА НА ПРИНЦИПАХ КОНЦЕПЦІЇ QUALITY 4.0

доцент, к.т.н., Янушкевич Д. А., доцент, к.т.н., Іванов Л. С.
Харківський національний університет радіоелектроніки,
кафедра КІТАМ, м. Харків, Україна
e-mail: dmytro.ianushkevych@nure.ua, leonid.ivanov@nure.ua

Abstract. The quality management system (QMS) of modern production is in constant development. Under the influence of digital technologies, there is a transition from the use of traditional QMS according to the standards of the ISO 9000 series to quality management based on the principles of the Quality 4.0 concept, which is applied within the framework of the fourth industrial revolution (Industry 4.0).

Industry 4.0 is a concept that allows to reduce production costs due to technical support and digitalization, and also makes enterprises more reliable, productive and competitive. In addition to the improvement of production technology in hardware and software, it also led to the creation of a new concept Quality 4.0, which significantly improves approaches to QMS at the enterprise. However, for the successful implementation of new approaches to enterprise quality management, it is necessary to develop key principles for the implementation of this system.

Вступ. Одним із перспективних напрямів розвитку управління якістю є розвиток систем управління якістю (СУЯ) на базі платформи четвертої промислової революції (Industry 4.0) [1]. Industry 4.0 – поняття, що означає розвиток і злиття автоматизованого виробництва, обміну даних і виробничих технологій в єдину саморегульовану систему, з незначним або взагалі відсутнім втручанням людини у виробничий процес [2].

Термін був визначений як «збірне поняття для технологій та концепцій організації ланцюга створення додаткової вартості» з використанням кіберфізичних систем, Інтернету речей (IoT) тощо. Industry 4.0 – це фаза промислової революції, яка характеризується злиттям технологій, що розмиває межі між фізичною, цифровою та біологічною сферами та дає змогу збирати та аналізувати дані з різних пристроїв, забезпечуючи більш швидкі, ефективні та більш гнучкі процеси виробництва продукції вищої якості за зниженими цінами.

До ключових технологій Industry 4.0 відносяться: штучний інтелект, Інтернет речей (IoT), роботизація та колаборизація, розумний завод (Smart Factory), безпілотні транспортні засоби, технології симуляції, які доповнені реальністю, хмарні технології, біоінженерія та нові матеріали, аналіз великих баз даних, безмежний доступ до Інтернету та розвиток інформаційних технологій, які ще недавно здавалися фантастикою, стають

реальністю. Це все здійснюється нової концепції управління якістю Quality 4.0

Основна частина. Система управління якістю підприємством знаходиться в постійному розвитку. Під впливом цифрових технологій та впровадження стандартів серії ISO 9001:2015, ведення паперового документообігу системи управління якістю (СУЯ) стає недостатнім для забезпечення постійного покращення системи. Відбувається перехід від застосування традиційної концепції управління якістю до концепції Quality 4.0. В рамках СУЯ сучасного підприємства ставляться завдання щодо впровадження таких інструментів, як електронний документообіг, програмне моделювання бізнес-процесів, застосування електронних документів, програмне забезпечення, інформаційні технології (IT), застосування аналітики та штучного інтелекту, обробка та аналіз великих баз даних (Big data), впровадження ключових показників ефективності (KPI).

Термін Quality 4.0 вперше був використаний аналітичною компанією LNS Research у 2017 р. і мав на увазі сукупність новітніх практик та інструментів управління якістю, що застосовуються в рамках четвертої промислової революції Industry 4.0. У сучасному світі настав етап Industry 4.0, який передбачає впровадження цифровізації, об'єднання людей, технологій, обладнання та даних у єдиному віртуальному просторі. Відповідно, змінюються і підходи до управління якістю [3].

Основними рисами концепції Quality 4.0 є:

– стратегічне планування якості;

– застосування цифрових технологій;

– виділення ключових показників та критеріїв при оцінці бізнес-процесів;

– щоденне використання;

– автоматизація бізнес-процесів;

– прозорість системи управління.

Концепція Quality 4.0 впливає не тільки на те, що відбувається на виробництві, а й охоплює весь життєвий цикл продукції – від маркетингових досліджень та проведення науково-дослідних та дослідно-конструкторських робіт до закупівель, виробництва, логістики та продажу, сервісного обслуговування, адміністрування та управління, утилізації продукції тощо Принципи концепції більш деталізовані порівняно з принципами ISO:9001:2015 і розроблені виходячи з сучасних тенденцій Industry 4.0. Основні складові концепції Quality 4.0 наведені на рис. 1.

До основних складових концепції Quality 4.0 належать:

1. Дані (data). Прийняття рішень на основі даних – це основа управління якістю. LNS розглядає 5 аспектів даних: обсяг, який передбачає автоматизацію способіи їх обробки; різноманітність, яка поділяє дані на структуровані, неструктуровані та частково структуровані; швидкість,

показник, що відображає частоту оновлення даних; достовірність даних; прозорість, що передбачає простий доступ до даних, незалежно від того, де вони створені та де застосовуються.

Рисунок 1 – Основні складові концепції Quality 4.0

2.Аналітика (analytics), яка отримує інформацію для прийняття рішень з бази даних. Аналітика ділиться на 4 категорії: описова (Що сталося?); діагностична (Чому сталося?); передбачувана (Що може статися?); приписувана (Що треба робити?).

3. Взаємодія (connectivity), яка визначає взаємодію між інформаційними технологіями для бізнесу (IT) та операційними технологіями (OT – operational technology).

4. Співпраця (collaboration), яка здійснюється через електронні повідомлення (e-mail), системи автоматизації робочих процесів (workflows) та портали. В останні роки сюди додаються й соціальні мережі (Social media), що особливо актуально для оперативного зв'язку користувачів та виробників продукції.

5. Розробка додатків (app development). Додатки – це механізм, через який забезпечується виконання процесів, збирання та створення даних, візуалізація аналітики та організація взаємодії.

6. Масштабованість (scalability, яка передбачає здатність підтримувати роботу з обсягом даних, користувачами, пристроями та аналітикою на глобальному рівні.

7. Системи управління (management systems). EQMS – це концентратор всієї діяльності організації у сфері управління якістю, що забезпечує масштабоване рішення для автоматизації робочих процесів (workflows), для зв'язку процесів якості між собою, покращення якості даних, централізованої аналітики, відповідність вимогам, організацію взаємодії в одній системі. Це саме концентратор (хаб), так як якість розглядається на всіх стадіях процесу проектування та виробництва виробу і цим треба керувати.

8. Відповідність вимогам (compliance). Продукція повинна відповідати вимогам нормативних документів, вимогам замовника та внутрішнім вимогам.

9. Культура (culture). При розгляді культури якості можна виділити 4 ключові елементи: участь у процессах; відповідальність; довіра; розширення повноважень.

10. Лідерство (leadership). Для переходу до Industry 4.0 завдання якості повинні бути тісно пов'язані з іншими функціями, а отже, їм треба приділяти більше уваги з боку керівництва. Керівники служби якості повинні пов'язувати свої завдання із загальними завданнями підприємства та просувати це на рівень керівництва.

11. Компетенції (competency), які дозволяють виконати роботу більш ефективноза рахунок підвищення кваліфікації персоналу та можливості обміну досвідом між співробітниками. Для цього використовуються системи управління навчаннями (Learning Management Systems), завдання яких входить планування навчання, сертифікація співробітників, створення центрів компетенції для обміну досвідом тощо. За статистикою LNS Research 35 % компаній вже використовують автоматизацію навчання на основі спеціалізованого програмного забезпечення.

Висновки. Таким чином, концепція Quality 4.0 не замінює традиційні методи управління якістю, що розвиваються в рамках СУЯ підприємств, а будується та вдосконалюється на їх основі. Основними етапами реалізації принципів концепції Quality 4.0 є:

1. Перехід на електронний документообіг та автоматизація управління.

2. Автоматизація бізнес-процесів та застосування технологій Quality 4.0 під час роботи із зацікавленими сторонами.

3. Проведення збору, обробки та аналізу даних у рамках контролю СУЯ та застосування ризик-орієнтованого мислення при впровадженні Quality 4.0.

4. Розробка рішень щодо постійного поліпшення системи.

Список використаних джерел.

1. Янушкевич Д. А. Іванов Л. С. Автоматизація процесу управління якістю підприємства / Якість, стандартизація та метрологічне забезпечення: [матеріали міжнародної науково-практичної конференції, Харків - 25-26 січня 2022 року]. - Українська інженерно-педагогічна академія. – Харків: УІПА, 2022. – С. 56-57.

2. Klaus Schwab The Fourth Industrial Revolution. – New York : Crown Publishing Group, 2017. – 192 p.

3. Dan Jacob What is Quality 4.0? [Еектронний ресурс] – Режим доступу: https://blog.lnsresearch.com/quality40.

МОДЕЛЮВАННЯ ПРОЦЕСУ ГУМАНІТАРНОГО РОЗМІНУВАННЯ ІЗ ЗАСТОСУВАННЯМ РОБОТОТЕХНІЧНИХ КОМПЛЕКСІВ

студент Бондаренко А. О., доцент, к.т.н., Янушкевич Д. А.
Харківський національний університет радіоелектроніки,
кафедра КІТАМ, м. Харків, Україна
e-mail: anton.bondarenko@nure.ua, dmytro.ianushkevych@nure.ua

Abstract. The aim of the work is to model the process of humanitarian demining with the use of military robotic systems. One of the problems facing countries in all regions of the world, where hostilities have taken place or where military conflicts exist, is facing the problem of finding and identifying explosive devices. The search for and identification of anti-personnel mines and explosive devices is characterized by increasing attention to the problems of creating military robotic systems. The characteristics of military robotic complexes used in the process of humanitarian demining should be determined by complex modeling, which can be described using a semi-Markov model of its operation.

Вступ. Всі воєнні конфлікти супроводжуються широким застосуванням протиборчими сторонами протипіхотних мін та вибухонебезпечних предметів (ВНП). Однією з проблем, з якою країни у всіх регіонах світу, де велись бойові дії або існують воєнні конфлікти стикаються з проблемами пошуку та ідентифікації ВНП. Для здійснення пошуку та ідентифікації ВНП характерним є зростання уваги до проблем створення робототехнічних комплексів та систем військового, спеціального та подвійного призначення (РКВП). Це обумовлюється намаганням усіх передових країн світу до збереження людського життя, в контексті якого використання РКВП дозволяє досягти позитивних результатів.

Основна частина. Гуманітарне розмінування – комплекс заходів, які проводяться з метою ліквідації небезпек, пов’язаних із вибухонебезпечними предметами (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/

Головними завданнями у проблемі гуманітарного розмінування є пошук та ідентифікація ВНП. В ідеальному варіанті бажано виявляти ВНП на безпечній відстані (70 - 100 метрів від розміщення людей), а розвідку мінних полів бажано вести у будь-який час доби і у будь-яких метеорологічних умовах. Також до актуальних завдань відноситься ідентифікація ВНП на тлі численних перешкод від неоднорідностей навколишнього середовища і різних посторонніх предметів (гільзи та

осколки від снарядів, зброї, металобрухт тощо). Ці вимоги можна забезпечити, якщо у системі гуманітарного розмінування застосовувати роботизовано комплекси.

Характеристики РКВП, які застосовуються у процесі гуманітарного розмінування повинні визначатись шляхом комплексного моделювання. Для моделювання процесу розмінування існує нагальна потреба розробки комплексної моделі цього процесу, як функціонування РКВП у процесі гуманітарного розмінування, складові якого наведені на рис. 1 [1].

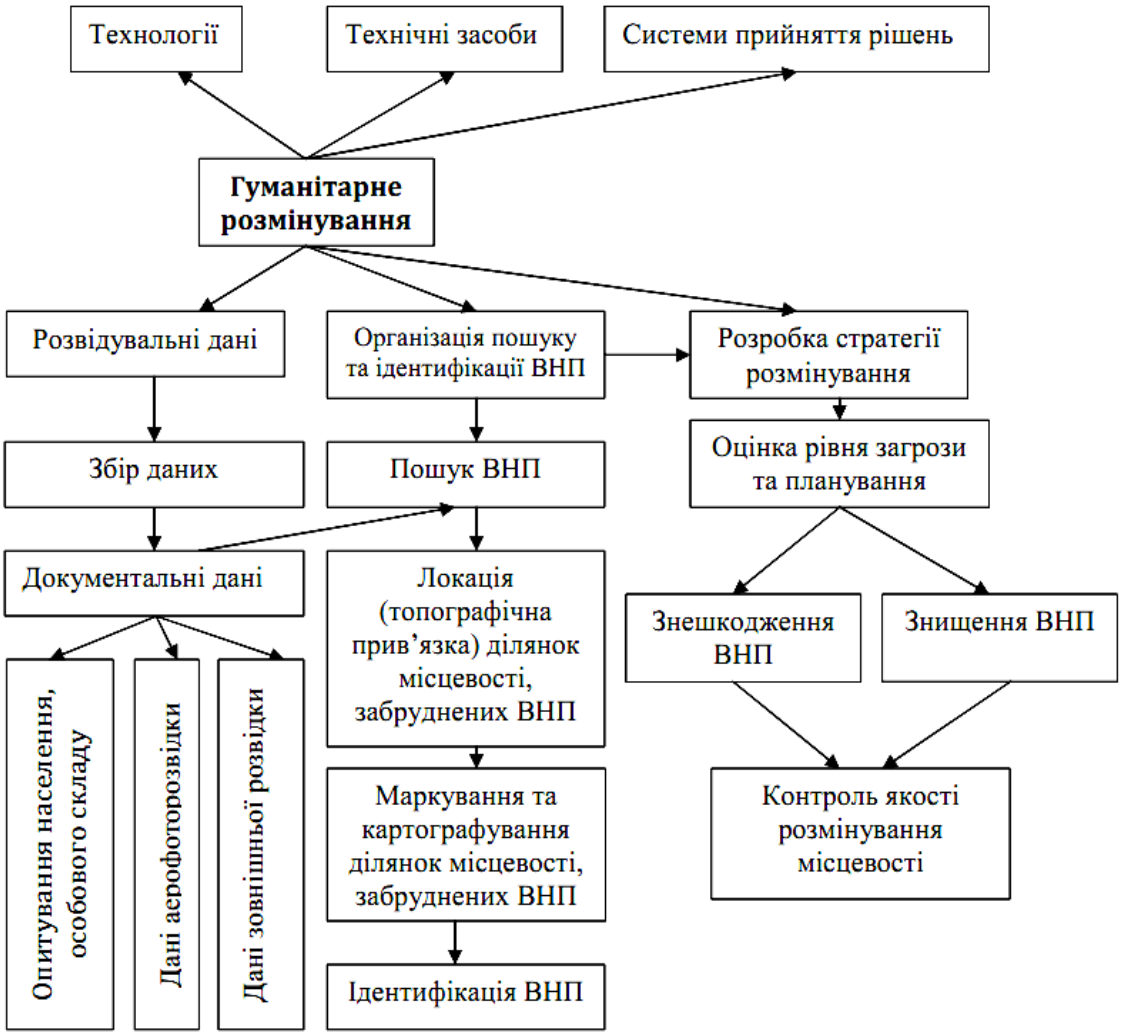


Рисунок 1 – Складові процесу гуманітарного розмінування

Виявлення ВНП означає їх пошук та ідентифікацію у відповідності з їх демаскуючими ознаками. Демаскуючі ознаки ВНП зумовлені низкою чинників. До них можна віднести:

– наявність вибухової речовини;

– наявність локально розташованої маси металу (навіть в так званих «неметалічних» югославських мінах є до 0,1 г алюмінію та металева пружина для спрацювання детонатора);

– характерна форма мін та ВНП;

– неоднорідності середовища, де розміщений ВНП (порушення поверхні ґрунту, дорожнього покриття, стіни будівлі, порушення кольору рослинності або снігового покриву тощо).

Додаткові демаскуючі фактори, які можуть бути не завжди:

– наявність провідної лінії управління міною;

– наявність годинникового механізму або електронного таймера;

– наявність сейсмічного, магнітного або оптичного датчика цілі;

– наявність антени для радіоприймальних пристроїв ВНП.

Отже, міна може виявлятися, в основному за рахунок трьох факторів:

– наявності зосередженої маси вибухової речовини;

– характерна конструкція міни (форми, матеріалу корпусу тощо);

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

Виявлення ВНП здійснюється за двома напрямками:

– пошук окремих мін (характерні відстані тут від декількох сантиметрів до декількох метрів);

– розвідка мінних полів (характерні дальності від десятків метрів до декількох кілометрів).

У загальному підході постановка задачі щодо комплексного моделювання процессу розмінування з використанням РКВП може бути розглянуто, як процес його функціонування.

Такий процес описується за допомогою деякої фізичної системи S, яка може перебувати в одному з наступних станів:

S_1 – РКВП розгорнуто, підготовлено для розмінування та почато пошук ВНП;

S_2 – РКВП здійснює маркування місцевості, яку перевірено на наявність ВНП;

S_3 – РКВП виявив невідомий предмет;

S_4 – РКВП ідентифікував невідомий предмет, як ВНП;

S_5 – РКВП вилучив ВНП із середовища, що його укриває;

S_6 – РКВП транспортує ВНП у разі можливості до місця знищення;

S_7 – РКВП знешкоджує ВНП;

S_8 – РКВП знищив ВНП;

S_9 – РКВП здійснив контроль якості розмінування місцевості або знищення ВНП;

S_{10} – РКВП втратив спроможність виконувати завдання згідно з бойовим призначенням.

Орієнтований граф переходів системи $S = \{S_1, S_2, ..., S_{10}\}$ з одного стану в інший під час розмінування наведено на рис. 2 та ґрунтується на представленні у вигляді напівмарковських процесів [2].

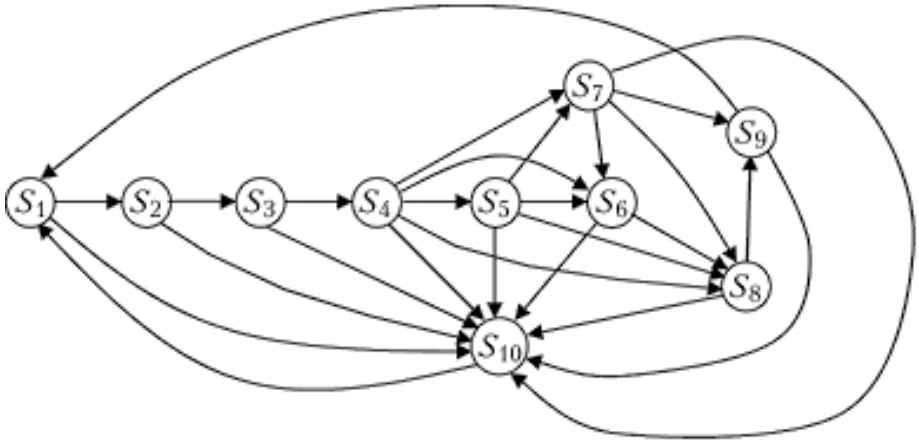


Рисунок 2 – Граф станів процесу гуманітарного розмінування

Висновки. Таким чином застосування РКВП для проведення робіт з гуманітарного розмінування дає можливість зберегти життя людей при його здійсненні та на даний час є дуже актуальним завданням.

Пошук та ідентифікація ВНП для гуманітарного розмінування є комплексним завданням. У зв'язку з цим, для проведення гуманітарного розмінування РКВП повинні бути оснащені відповідними маніпуляторами та детекторами, засобами прийняття рішень та застосовуватись на етапах розвідки, пошуку, локації, маркування, ідентифікації, знешкодження, знищення (утилізації) ВНП. Підвищити ефективність проведення робіт з гуманітарного розмінування можливо за рахунок моделювання його процедури та ґрунтується на представленні у вигляді напівмарковських процесів.

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. Шишанов М. О., Коцюруба В. І., Гусляков О. М. Комплексне моделювання процесу розмінування з використанням засобів інженерного озброєння / М. О. Шишанов, В. І. Коцюруба, О. М. Гусляков // Озброєння та військова техніка, 4 (2014). – .С. 42-44.

СИСТЕМА ЛОКАЦІЇ ТА КАРТОГРАФУВАННЯ ТЕРИТОРІЙ, ЗАБРУДНЕНИХ ВИБУХОНЕБЕЗПЕЧНИМИ ПРЕДМЕТАМИ

студент Чикота В. Ю., доцент, к.т.н., Янушкевич Д. А
Харківський національний університет радіоелектроніки,
кафедра КІТАМ, м. Харків, Україна
e-mail: vitalii.chykota@nure.ua, dmytro.ianushkevych@nure.ua

Abstract. Humanitarian demining is the activities carried out to eliminate the dangers associated with explosive objects (EO), including non-technical and technical survey of territories contaminated by EO, their mapping, marking, search, identification, decontamination, evaluation of demining quality, etc. One of the main tasks in the task of humanitarian demining is the location (topographic reference) of areas of terrain contaminated by EO, which includes marking and mapping of areas of terrain contaminated by GNV on the database of aerial photography, external intelligence, etc. The report examines the problematic issues of location and mapping of territories contaminated by EO.

Вступ. Гуманітарне розмінування – це заходи, які проводяться з метою ліквідації небезпек, пов’язаних із вибухонебезпечними предметами (ВНП), включаючи нетехнічне та технічне обстеження територій, забруднених ВНП, картографування, маркування, пошук, ідентифікація, знешкодження, здійснення оцінювання якості розмінування тощо. Одним із основних завдань у задачі гуманітарного розмінування є локація (топографічна прив’язка) ділянок місцевості, забруднених ВНП, яка включає маркування та картографування ділянок місцевості, забруднених ВНП на базі даних аерофоторозвідки, зовнішньої розвідки тощо.

У доповіді розглядаються проблемні питання локації та картографування територій, забруднених ВНП із застосуванням моделей географічних інформаційних систем.

Основна частина. Створення роботизованих комплексів військового призначення (РКВП) потребує створення ядра найважливіших технологій, які необхідні для створення всієї номенклатури перспективних РКВП. При цьому типовий зразок РКВП може бути представлений у вигляді сукупності функціонально пов’язаних елементів. Склад спеціалізованого обладнання встановлюється, виходячи з функціонального призначення РКВП і може включати:

– засоби розвідки та озброєння;
– навігаційні пристрої;
– спеціальне технологічне обладнання;
– засоби телекомунікації;
– спеціалізовані обчислювачі та контролери із програмно-алгоритмічним забезпеченням;

– засоби радіоелектронної боротьби (РЕБ);

– геоінформаційні та точного глобального позиціонування тощо.

Як показали дослідження, система гуманітарного розмінування має містити такі підсистеми:

– нетехнічне та технічне обстеження територій, забруднених ВНП;

– пошук, ідентифікацію та знешкодження ВНП;

– картографування та маркування територій, забруднених ВНП;

– здійснення оцінювання якості розмінування тощо.

Одними із основних проблем пошуку у ВНП у системі гуманітарного розмінування є локація (топографічна прив’язка) ділянок місцевості, забруднених ВНП, яка включає маркування та картографування ділянок місцевості, забруднених ВНП на базі даних аерофоторозвідки, зовнішньої розвідки тощо.

При цьому широко застосовуються цифрові моделі рельєфу (ЦМР) місцевості при актуалізації картографічних матеріалів рельєфу, забруднених ВНП, ректифікації супутників знімків, геоморфологічному і кліматичному аналізі тощо.

Традиційна технологія картографування ділянок місцевості, забруднених ВНП є трудомістким технологічним процесом і характеризується великими трудовитратами, що значно збільшує терміни і вартість виконання робіт зі створення карт територій, забруднених ВНП.

Сучасна картографія широко використовує результати розвитку інформатики, кібернетики, обчислювальних пристроїв і вдосконалюється разом з ними. Саме на стику традиційної картографії, інформаційних технологій, комп'ютерної графіки виникла автоматизована картографія.

Цифрова (автоматизована картографія) почала розвиватися в напрямку перетворення образно-знакової (аналогової) інформації карт в цифрову форму.

Автоматизована картографія розглядається в двох аспектах:

1. Технічна картографія акцентує увагу на методиці створення картографічного зображення з використанням технічних засобів та програмного забезпечення. При цьому необхідно знати призначення карти, специфіку картографуванню території, способи подальшого використання карти, прийоми роботи з нею.

2. Для географічної картографії більш значущі процеси отримання інформації з карти, досліджень по картах, тоді як технічні прийоми створення картографічного зображення і організації пошуку інформації не є пріоритетними. У свою чергу, процеси автоматизації в географічній картографії лежать в області інтересів геоінформаційного картографування - галузі картографії, що займається автоматизованим складанням і використанням карт як моделей географічних інформаційних систем (ГІС) на основі ГІС-технологій і баз географічних та картографічних даних і знань с

Географічні інформаційні системи – це:

– інформаційна система, що може забезпечити введення, маніпулювання й аналіз географічно визначених даних для підтримки прийняття рішень;

– реалізоване за допомогою автоматизованих засобів сховище системи знань, а також програмного забезпечення, що моделює функції пошуку, введення, моделювання;

– набір засобів для збору, збереження, пошуку, трансформації і відображення даних;

– інформаційна система, призначена для роботи з просторовими, чи географічними, координатами;

– апаратно-програмний людино-машинний комплекс, що забезпечує збір, обробку, відображення і поширення просторово-координованих даних і знань про територію для ефективного використання при рішенні наукових і прикладних завдань, пов'язаних з аналізом, моделюванням, прогнозуванням і керуванням процесів картографування відповідно до поставлених завдань;

– сукупність апаратних, програмних засобів і процедур, призначених для забезпечення введення, керування, обробки, аналізу, моделювання і відображення просторово-координованих даних;

– системи автоматизованого збору, систематизації, переробки і представлення (видачі) геоінформації з умовою одержання знань про досліджувані просторові системи;

– сукупність апаратно-програмних засобів і алгоритмічних процедур, призначених для збору, введення, зберігання, математико-картографічного моделювання і образного представлення геопросторової інформації;

– інформаційна система, що забезпечує збір, зберігання, обробку, доступ, відображення і поширення просторово-координованих (просторових) даних.

Програмні засоби ГІС призначені для роботи з просторовими даними, представляють в різноманітний сегмент програмного забезпечення, у якому можна виділити:

– векторизатори растрових зображень;

– пакети обробки даних розвідок;

– програмні засоби обробки даних дистанційного зондування;

– пакети просторового аналізу і моделювання;

– довідково-картографічні системи;

– ГІС-в'юери (пакети з обмеженою можливістю редагування даних, призначені для візуалізації і виконання запитів до баз даних, у тому числі і графічних, підготовлених у середовищі інструментальних ГІС);

– інструментальні ГІС (ГІС-пакети).

Програмні засоби ГІС є сукупністю інтегрованих програмних модулів, які забезпечують реалізацію всіх основних функцій ГІС. У загальному випадку виділяють шість базових модулів, що реалізовують функції:

– введення і верифікації даних;

– зберігання і маніпулювання даними, перетворення систем координат і трансформації картографічних проекцій;

– аналізу і моделювання;

– виведення і подання даних;

– взаємодії з користувачем.

Реалізація зазначених вище функцій вимагає розробки спеціалізованого програмного забезпечення.

Висновки. У даній роботі був проведений аналіз складових системи гуманітарного розмінування та проблем картографування ділянок місцевості, забруднених ВНП. Було встановлено, що при цьому широко застосовуються цифрові моделі рельєфу для актуалізації картографічних даних, про території, які забруднені ВНП

Традиційна технологія картографування ділянок місцевості, забруднених ВНП є трудомістким технологічним процесом і характеризується великими трудовитратами, що значно збільшує терміни і вартість виконання робіт зі створення карт. Процеси автоматизації у галузі картографії лежать в області інтересів геоінформаційного картографування, що займається автоматизованим складанням і використанням карт на основі ГІС-технологій баз даних процеси автоматизації в географічній картографії лежать в області інтересів геоінформаційного картографування – галузі картографії, що займається автоматизованим складанням і використанням карт на основі ГІС-технологій, програмних засобів ГІС та баз даних і знань.

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. Rul N., Velikodsky Yu. I., Zatcerkovnyi V.I. The algorithm of automatic vectorization of contours for constructing digital elevation models / N. Rul, Yu. Velikodsky V. Zatcerkovnyi // Conference ProceedingsConference Proceedings, 17th International Conference on Geoinformatics - Theoretical and Applied Aspects, May 2018 . – 2018. . – P. 1 – 5.

ТЕХНОЛОГІЇ ВИЯВЛЕННЯ ТА КЛАСИФІКАЦІЇ ВИБУХОНЕБЕЗПЕЧНИХ ПРЕДМЕТІВ

студент Шафоростов Д. Д., доцент, к.т.н., Янушкевич Д. А.
Харківський національний університет радіоелектроніки,
кафедра КІТАМ, м. Харків, Україна
e-mail: danylo.shaforostov@nure.ua, dmytro.ianushkevych@nure.ua

Abstract. The use of robotic complexes in the system of humanitarian demining is due to the efforts of all countries to save human lives, both in combat operations and in the process of humanitarian demining of territories contaminated with explosive objects (EO). The main tasks in the task of humanitarian demining are the search and identification of explosive objects by their unmasking features. Explosive ordnance detection solutions using robotic complexes with a suitable modular structure and properly adapted to the local conditions of hazardous unstructured areas can significantly increase personnel safety, as well as work efficiency, productivity and flexibility. In this sense, modern technologies for detecting and classifying EOs, the architecture of building robotic complexes and manipulators with which they are equipped to perform the assigned tasks are an actual direction of research.

Вступ. Застосування робототехнічних комплексів у системі гуманітарного розмінування обумовлено зусиллями всіх країн щодо збереження людських життів, як у бойових діях, так і в процесі гуманітарного розмінування територій, забруднених вибухонебезпечними предметами (ВНП). Основними завданнями в задачі гуманітарного розмінування є пошук та ідентифікація вибухонебезпечних предметів за їх демаскуючими ознаками.

Рішення щодо пошуку вибухонебезпечних предметів за допомогою робототехнічних комплексів 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, сучасні технології виявлення та класифікації ВНП, архітектура побудови робототототехнічних комплексів та маніпуляторів, якими вони оснащені для виконання поставлених завдань є актуальним напрямом досліджень.

Основна частина. Гуманітарне розмінування – комплекс заходів, які проводяться з метою ліквідації небезпек, пов’язаних із вибухонебезпечними предметами (ВНП), включаючи нетехнічне та технічне обстеження територій, виявлення, знешкодження та знищення ВНП, їх маркування та повинна виконувати такі завдання:

– пошук, ідентифікацію та знешкодження ВНП;
– картографування та маркування територій, забруднених ВНП;
– здійснення оцінювання якості гуманітарного розмінування.

Головними завданнями у проблемі гуманітарного розмінування є пошук та ідентифікація ВНП. Виявлення мін та ВНП означає їх пошук та ідентифікацію у відповідності з їх демаскуючими ознаками [1]. Демаскуючі ознаки ВНП зумовлені низкою чинників. До них можна віднести:

– наявність вибухової речовини;

– наявність локально розташованої маси металу (навіть в так званих «неметалічних» югославських мінах є до 0,1 г алюмінію та металева пружина для спрацювання детонатора);

– характерна форма мін та ВНП;

– неоднорідності середовища, де розміщений ВНП (порушення поверхні ґрунту, дорожнього покриття, стіни будівлі, порушення кольору рослинності або снігового покриву тощо).

Додаткові демаскуючі фактори ВНП: наявність провідної лінії управління міною; наявність годинникового механізму або електронного таймера; наявність сейсмічного, магнітного або оптичного датчика цілі тощо.

ВНП можуть бти виявлені, в основному за рахунок трьох факторів:

– наявності зосередженої маси вибухової речовини;

– характерна конструкція міни (форми, матеріалу корпусу тощо);

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

У табл. 1 наведені найбільш важливі демаскуючі ознаки ВНП, що реалізуються при їх пошуку. Їх основними фізичними характеристиками є: щільність, твердість, електрична провідність, діелектрична і магнітна проникності, коефіцієнти відбиття і випромінювання у видимому (0,4...0,76 мкм) і інфрачервоному (0,76...1000 мкм) діапазонах електромагнітних хвиль.

Сучасний стан методів виявлення ВНП характеризується різноманіттям. Аналіз стану методів виявлення ВНП показує, що кожен з них має певні обмеження. Звичайно, при цьому необхідно враховувати як апріорну інформацію про об'єкт пошуку (розміри, матеріали тощо), так і властивості оточуючого середовища [1].

В даний час найбільше застосування знайшли такі методи: електромагнітні (індукційний, радіохвильовий, магнітометричний, нелінійний), ядерно-фізичні, теплофізичний і механічний (механічного зондування). Саме вони дозволяють створити технічні засоби пошуку ВНП, які можуть бути придатними для гуманітарного розмінування. Традиційна система виявлення та ідентифікації мін та ВНП наведені у табл. 2. Систему можна розділити на 2 типи [1]:

– система типу А, призначена для виявлення та ідентифікації вибухонебезпечних предметів у середовищах, що покривають, що використовують енергію систем пошуку;

– системи типу П, що використовують енергію об'єкта пошуку.

Таблиця 1 – Демаскуючі ознаки вибухонебезпечних предметів

Вид контрасту між об'єктом і оточуючим середовищем	**Тип об’єкта пошуку**			
	ППМ	**ПТМ**	**ВНП з електронними компонентами**	**ВНП з кабельними лініями управління**
Відмінність електропровідності	+ (може бути дуже малою)	+	+	+
Відмінність магнітної проникливості	±	±	+	+
Відмінність діелектричної проникності	+	+	+	+
Відмінність теплофізичних характеристик	±	±	±	±
Відмінність оптичних характеристик	±	±	±	±
Відмінність механічних характеристик	+	+	+	+
Наявність парів вибухової речовини (ВР)	±	±	±	±
Наявність нелінійних електромагнітних властивостей	±	±	+	±

Примітка: + – контраст є; ± – контраст є не завжди.

Таблиця 2 –. Методи виявлення ВНП

«А»	«П»
1. Механічний 2. Оптичний 3. Теплолокаційний 4. Електромагнітний 5. Параметричний	1. Газоаналітичний 2. Ядерно-фізичний 3. Біофізичний 4. Акустичний

Проблеми, які виникають при застосування цих методів – це питання безпеки і зниження часових та матеріальних витрат на розмінування. Інші вимоги: кліматичні, ефективність роботи в темний час доби, стійкість до механічних впливів, електромагнітна сумісність тощо.

«Глибинність» найбільш практично значимих безконтактних методів пошуку та ідентифікації ВНП, які знаходяться у ґрунті наведено у табл. 3.

Таблиця 3 – Глибинність» безконтактних методів пошуку ВНП

Глибина пошуку	**Методи пошуку ВНП**	**Тип ВНП**
Поверхня ґрунту	Електромагнітний, оптичний, газоаналітичний, механічний, теплофізичний, біологічний	Всі типи ВНП
до 0,1 м	радіохвильовий	Всі типи ВНП
	індукційний	Металеві ВНП
до 1 м	короткоімпульсна радіолокація	Всі типи ВНП
	магнітометричний	Феромагнітні ВНП

Для підвищення ефективності виявлення ВНП доцільно комплексування різних пошукових методів в одному технічному засобі. Один з нових перспективних методів виявлення мін – це параметричний. Він заснований на реєстрації взаємодії збудливого (силового) і зондуючого (інформаційного) фізичних полів, на об'єктах пошуку штучного походження (мінах). Поєднання цих полів може бути різним.

Відповідно до цього РКВП повинні бути обладнані маніпуляторами з відповідним апаратним та програмним забезпеченням та які повинні виконувати завдання з пошуку та ідентифікації ВНП.

Висновки. Таким чином застосування РКВП для проведення робіт з гуманітарного розмінування дає можливість зберегти життя людей при його здійсненні та на даний час є дуже актуальним завданням.

Для підвищення ефективності виявлення ВНП за допомогою РКВП доцільно комплексування різних пошукових методів в одному технічному засобі.

Відповідно до цього РКВП повинні бути обладнані маніпуляторами з відповідним апаратним та програмним забезпеченням та які повинні виконувати завдання з пошуку та ідентифікації ВНП.

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

КОНЦЕПЦІЯ ІНТЕЛЕКТУАЛЬНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ АНАЛІЗУ ТА ОБРОБКИ АНТРОПОМЕТРИЧНИХ ДАНИХ

доцент, к.т.н., Рудніченко М. Д., студентка Бондаренко А. С.
Національний університет «Одеська політехніка»,
інститут комп'ютерних систем, кафедра ІТ, м. Одеса, Україна
e-mail: nickolay.rud@gmail.com, bondarenko.8865190@stud.op.edu.ua

Abstract. This work is devoted to modern developments in the field of designing devices on microcontrollers and programmable logic integrated circuits. The current endeavor examines the possibilities of using the ArduinoUno hardware and software platform, and the RobotDyn APC220 radio communication module, from the outlook of being sufficiently universal and practical tools for creating subsequent hardware and software tools. The main objective of this study is the formation of a new concept in modern technologies that can simultaneously facilitate and improve life at the household level. This implementation will be easily integrable, therefore, the positive effect of this technology development will be established.

Вступ. У поточний час розвитку високотехнологічних галузей від рівня підприємств повного циклу до систем, які інтегруються в побутові сфери життя, можна швидко вирішувати сьогоденні проблеми користувачів. Однією з таких проблем є складність та велика тривалість процесу підбору товарів за індивідуальними антропометричними даними особистості. Актуальність даного дослідження полягає у створенні нової концепції для розвитку технологічного сектору у вирішенні побутових проблем на базі використання програмно-апаратних засобів та алгоритмів. Даний проект поєднує у собі програмно-інженерну та інтелектуальну орієнтації.

Основна частина. Сучасні підходи до інтелектуального аналізу даних (ІАД) націлені в першу чергу на поетапне виявлення та визначення закономірностей з наявних баз фактів, що знаходяться в них у не чітко вираженому вигляді, особливо це актуально у разі аналізу стану здоров'я людини. ІАД найбільш ефективний у тих випадках, коли процес його імплементації виробляється шляхом інтеграції систем, що не імітують, а агрегують можливості аналізу великих наборів даних експертами. ІАД на практиці включає ряд наукових напрямів, таких як Data Mining (видобуток даних) і Knowledge discovery (виявлення знань) [1]. Актуальні завдання ІАД у контексті розглядаємої проблематики: пошук візуальних, функціональних, логічних та інших прихованих закономірностей у накопиченій антропометричній інформації, розпізнавання та класифікація образів різних зображень аналізу стану органів людини, побудова моделей та правил, що реалізують формалізацію виявлених аномалій та здатні до побудові прогнозів розвитку можливих станів (або їх змін) у часі із

заданим рівнем точності.

Основна концепція проекту полягає у створенні особливого простору в магазинах, де наявна функція підбору предмету одягу та інформаційних засобів технічного аналізу та оцінки параметрів людини для видачі подальших рекомендацій. Дана функція призначена для розпізнавання та оцінки фізіологічних даних й вимірів тіла конкретної людини.

Після аналізу отриманих даних, користувач отримує повну інформацію щодо критеріїв пошуку конкретного товару, який задовольнятиме його за фізичними вимірами. Головний підхід отримання правильних вхідних даних, які будуть більшою частиною задовольняти критерії запиту - це розгляд людини зі сторони індивідуально-типологічної діагностики [2].

Тобто отримання повної характеристики фізичного статусу особистості із сукупності властивостей, які притаманні конкретному типу з усіх сучасних конституцій організмів. При використанні даного аспекту є можливість охарактеризування особи без отримання додаткової інформації про показники метаболізму та інші [3]. Схема оцінювання людини полягає в техніці виміру антропометричних даних такі як: вимір росту, ваги та обхват грудної клітини, талії, стегон [4]. За допомогою об'ємної структурованої бази метаданих можна досягти чіткий результат в ідентифікації, пошуку, оцінки вхідних даних. Модульну схему даної ІС можна представити у вигляді схеми, зображеної на рисунку 1.

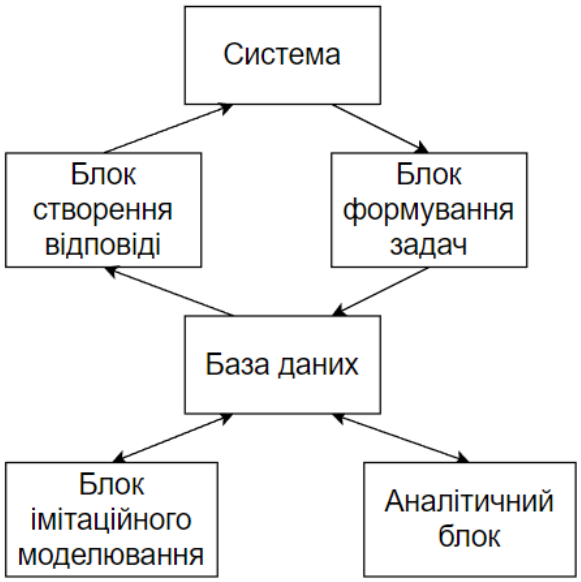


Рисунок 1 – Модульна схема інформаційної системи

Архітектура системи має містити наступні компоненти:

– користувальницький інтерфейс з викликом прикладних функцій сервера;

– виконання функцій, формування запитів до системи керування

базами даних для збереження та структурування даних;

– обробка та аналіз агрегованих даних шляхом використання моделей штучних нейронних мереж [5] для виявлення закономірностей та рішення завдання класифікації.

У якості апаратного забезпечення для збору даних пропонується використання платформи Arduino, модулів отримання зображень з відеокамери OV7670 та передачі даних RobotDyn APC220.

Найкращим методом збереження інформації є інтегрована база даних, яка витрачатиме менше часу для опрацювання складних логічних запитів. Вирішенням проблеми розпізнання фізичних параметрів особи є нейронна мережа, яка має здібності до самонавчання [6]. Збільшуючи об'єм опрацьованих відомостей, система буде удосконалювати результати вихідних даних та адаптувати їх.

Перевагою даного проекту є вирішення проблеми користувача з пошуком і підбором предмету одягу, що у той самий час сприятиме створенню нової концепції сучасного розвитку технологій у побутовій сфері діяльності людини. Така система може бути вільно інтегрована в повсякденне життя користувачів і легко удосконалена з розвитком технологічних систем.

Висновки. Проведене дослідження концепції даної системи показало її актуальність, адаптивність, гнучкість та перспективність у реалізації для вирішення прикладних практичних завдань з аналізу даних та в рамках створення системи підтримки прийняття рішень для зменшення часових витрат для підбору необхідних товарів.

Список використаних джерел.

1. Щербина А.Д. Порівняльний аналіз існуючих напрямів у інтелектуальному аналізі даних / А.Д. Щербина, Д.С. Шибаєв, М.Д. Рудніченко, Н.О. Шибаєва // Project, Program, Portfolio Management. The Third International Scientific-practical Conference, Odesa,ONPU 07–08 Dec 2018. – С.88-90

2. Алексіна Л.А. Інтегративно-антропологічні підходи у медицині / Л.А. Алексіна, Н.А. Корнетов // Організаційна конференція відділення біомедичної та біосоціальної антропології MAIA. – 2018. – С.7-10.

3. Богомолець А.А. Введення в вчення про конституції та діатези / А.А. Богомолець. – М.: Біомедгіз, 1926. – 178 с.

4. Вакуленко А. Біометричні методи ідентифікації особистості: обґрунтований вибір та впровадження / А. Вакуленко, А. Юхін. – О.:Наука, 2007. – 224 с.

5. Галушкін А.І. Теорія нейронних мереж / А.І. Галушкін. – К.:ІПРЖР, 2000. – 416 с.

6. Горбань А. Н. Навчання нейронних мереж / А.Н. Горбань. – К.:ParaGraph, 1990. – 160 с.

СУЧАСНІ МЕТОДИ НАДАННЯ ПЕРСОНАЛІЗОВАНИХ РЕКОМЕНДАЦІЙ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

студентка Мещан К.А., проф. Міщеряков Ю.В.
Харківський національний університет радіоелектроніки,
кафедра СТ, м. Харків, Україна
e-mail: kateryna.meshchan@nure.ua, iurii.mishcheriakov@nure.ua

Abstract. With the growing popularity of online stores, their assortment is also growing. Therefore, as a rule, problems arise that negatively affect both stores and customers. There is a large assortment here, but there are problems with it. A customer who saw in front of him a large number of products and their parameters may not immediately understand which of them he needs. However, unlike a regular store, there is no salesperson-consultant here. For this reason, new features have been introduced to increase the convenience of using online stores and increase profits. In particular, various personalized recommendations.

Вступ. Зі зростанням популярності інтернет-магазинів зростає і їх асортимент. Тому, як правило, виникають проблеми, які негативно позначаються як на магазинах, так і на клієнтах. Покупець, який побачив перед собою велику кількість товарів та їх параметрів, може не одразу зрозуміти, який із них йому потрібен. Однак, на відміну від звичайного магазину, тут продавець-консультант відсутній. З цієї причини для збільшення зручності користування інтернет-магазинами та підвищення прибутку було запроваджено нові функції. Зокрема різні персоналізовані рекомендації.

Основна частина. Під персоналізаціє слід розуміти спосіб як правильно підібрати потрібний тип послуги та продукту, а також вміст для потрібних користувачів. Завдяки цьому це допомагає покращити залучення користувачів – будь-яка взаємодія людей з продуктом, веб-сайтом, програмою тощо.

У систем рекомендацій використовуються системи фільтрації інформації надання індивідуальних рекомендацій. Такі системи, також відомі як механізми рекомендацій, надають індивідуальні рекомендації в режимі реального часу. Системи рекомендацій використовують алгоритми та методи машинного навчання для надання найбільш релевантних пропозицій користувачам, вивчаючи дані (наприклад, минулу поведінку) з метою прогнозування поточних інтересів.

Персоналізовані системи можуть надавати такі рекомендації, як: рекомендації на основі продуктів (наприклад, Amazon, Booking.com); рекомендації на основі вмісту (наприклад, Netflix, Spotify, TikTok, Instagram).

Є три основні підходи до створення системи рекомендацій, які засновані на методах і функціях для прогнозування того, яким елементам

віддадуть перевагу користувачі:

– фільтрація на основі вмісту (content-based filtering), яка генерує прогнози аналізуючи атрибути елементів та знаходячи схожість між ними;

– спільна фільтрація (collaborative filtering), яка генерує прогнози аналізуючи поведінку користувачів та порівнюючи їх зі схожими смаками;

– гібридна фільтрація (hybrid filtering), яка поєднує дві або більше моделей.

Модель фільтрації на основі вмісту надає рекомендації, використовуючи конкретні атрибути елементів для пошуку подібності. Дані, які вони використовують для створення профілів даних, створюються на основі описової інформації і можуть містити характеристики елементів або користувачів. Створені профілі використовуються для рекомендацій предметів, подібних до тих, які користувач любив/слухав/купував/дивився у минулому.

Найбільш поширена модель, спільна фільтрація, дає відповідні рекомендації на основі взаємодії різних користувачів з цільовими елементами. Вони збирають інформацію про минулу поведінку користувачів, а потім викопують її, щоб вирішити, які елементи відображати іншим активним користувачам з таким смаком. Ідея системи полягає в тому, щоб передбачити, як людина відреагує на предмети, з якими вона ще не стикалася.

Гібридна фільтрація призначена для усунення проблем та обмежень чистої моделі системи рекомендації. Гібридна модель використовує кілька методів рекомендацій разом для отримання більш високої точності та меншої кількості недоліків кожної окремої рекомендації. Зазвичай це спільна фільтрація, яка поєднується з іншими методами для вирішення проблеми холодного запуску. Але не виключно, бо підходи можуть поєднуватись різними шляхами.

Висновки. Таким чином, мета створення персоналізованих систем є допомога користувачам підібрати релевантний товар. Такі системи видають різні рекомендації для різних користувачів. Персоналізовані системи розділені на три великі групи: фільтрація на основі вмісту, спільна фільтрація та гібридна фільтрація. Для надання рекомендацій системи можуть використовувати конкретні атрибути елементів для пошуку подібності (колір, технічні характеристики) та взаємодію різних користувачів з цільовими елементами (перегляд товару, придбання).

Список використаних джерел.

1. Greg Linden, Brent Smith and Jeremy York Amazon.com recommendations: Item-to-Item Collaborative Filtering // Industry Report, IEEE INTERNET COMPUTING, 2003.

2. Николенко С. Рекомендательные системы: user-based и item-based [Електронний ресурс] / Сергей Николенко. – 2012. – Режим доступу до ресурсу: https://habr.com/ru/company/surfingbird/blog/139518/.

3. Recommender Systems: Behind the Scenes of Machine Learning-Based Personalization [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://www.altexsoft.com/blog/recommender-system-personalization.

УНІФІКОВАНИЙ ПОРТАТИВНИЙ ЗАРЯДНИЙ ПРИСТРІЙ НА ОСНОВІ СОНЯЧНИХ ЕЛЕМЕНТІВ

викладач Бенько Т.Г., студент Юрків В.Л.
Прикарпатський національний університет імені Василя Стефаника,
кафедра комп'ютерної інженерії і електроніки,
м. Івано-Франківськ, Україна
e-mail: taras.benko@pnu.edu.ua, urkivvladislav@gmail.com

Abstract. A portable battery or power bank is a very important accessory that allows you to charge most gadgets. It is needed everywhere in civilian life (travels, hikes, trips) and during combat operations. It is not for nothing that volunteers are constantly asking to purchase power banks for the front for military personnel. The uniqueness of this device lies in the ability to adjust the current and voltage, which makes it possible to use it in a much wider range. Thanks to the protected housing, this charger can work under extreme conditions.

Вступ. Ми живемо в сучасному світі, де не обійтися без різного роду гаджетів. Для того, щоб вони функціонували, потрібно їх підключати до джерела живлення. Чудовою альтернативою джерела живлення є уніфікований зарядний пристрій із великим вмістом функцій. А саме: безпровідна зарядка, можливість заряджати від сонячного світла, два USB порти по 5 Вольт, інтегрований і дискретний ліхтарик. А також присутня функція регулювання напруги від 5 до 28 Вольт на вихід.

Уніфікований портативний зарядний пристрій із сонячною панеллю на 5 акумуляторів ємністю 11000мА, та сонячною батареєю, який здатний заряджати одночасно два пристрої з силою струму в 1А та 2А. Пристрій здатен регулювати напругу в діапазоні від 1 до 24В, та силу струму від 0,1 до 2А. Це дає можливість живити більшість електронних гаджетів таких як телефони, ноутбуки,планшети, раціі, певні види квадрокоптерів. Пристрій також має інтегрований ліхтарик. При натисканні на кнопку пристрій покаже свій рівень заряду на світлодіодах. При подвійному натисканні на кнопку – увімкнеться ліхтарик, наступне подвійне натискання вимкне ліхтарик. Особливістю даного девайсу є також конструкція корпусу. Основа корпусу виготовлена з гнучких пластичних мас які з внутрішнього боку захищені алюмінієвими пластинами що дозволяє захистити від механічних пошкоджень, а з зовнішнього покриті рідкою резиною що дає можливість працювати в складних кліматичних умовах.

Основна частина.Основою зарядного пристрою є модуль контролю заряду та розряду батарей, регульований модуль джерела живлення та модуль безпровідної зарядки.

В основі даного пристрою лежить плата контролю заряду та розряду батарей зображена на рисунку 1.

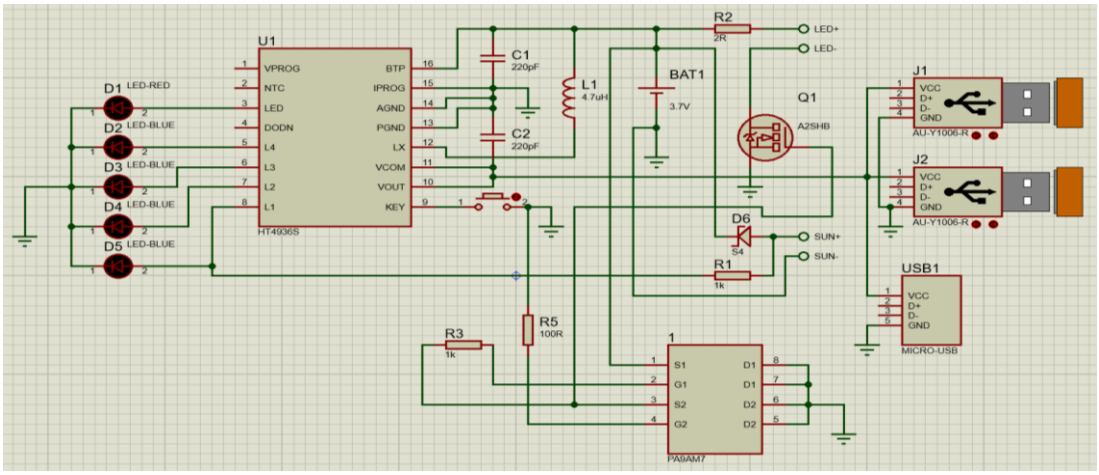


Рисунок 1 – Загальна схема пристрою плата контролю заряду та розряду батарей

Опис схеми. Плата містить 4 світлодіоди, які призначені для індикації ємності батарей. На платі є вхідний порт Micro-USB розрахований на 5В і 1,5А, та два USB виходи один розрахований на напругу 5В і силу струму 2А, а другий на напругу 5В і силу струму 1А. До даної плати підключається сонячна панель до виводів SUN+ і SUN-. Сонячна панель розрахована на напругу 4,5-5,5В. Для цієї плати підходять Li-ion батареї номіналом 3.7В. Також плата містить як інтегрований ліхтарик позначений D1 так і дескретний, який підключається до виводів LED+ і LED-. Щоб увімкнути інтегрований ліхтарик потрібно утримувати кнопку протягом три секунди. Щоб вимкнути ліхтарик потрібно утримати кнопку на три секунди і ліхтарик погасне. Дискретний ліхтарик розрахований на напругу 4В. На платі присутні виводи BAT+ і BAT- які підключаються до батарей.

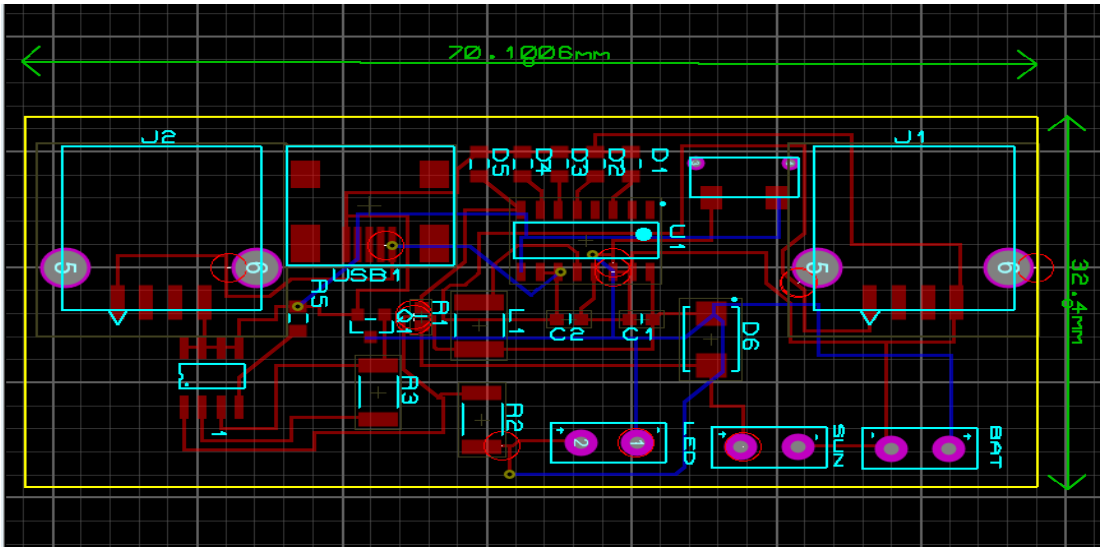


Рисунок 2 – Топологія плати контролю заряду та розряду батарей

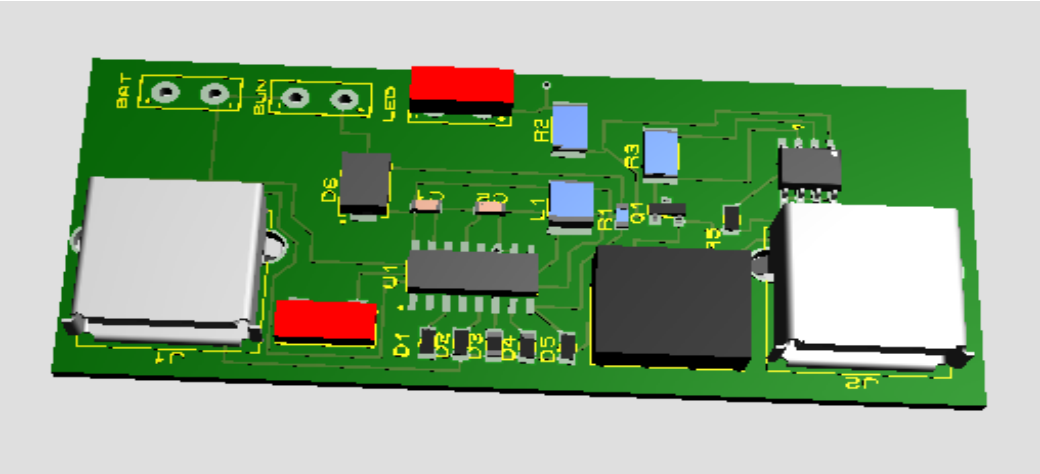


Рисунок 3 – 3-д модель плати контролю заряду та розряду батарей

Для живлення використовується модуль MT3608 (рис.4). Цей модуль призначений для зміни значення вихідної напруги. Розміри модуля досить малі, тому його можна інтегрувати у портативний пристрій. До модуля на вхід потрібно подати вхідну напругу від 2 до 24В. Підключати даний модуль потрібно безпосередньо до батарей на виводи BAT+ і BAT- плати контролю заряду і розряду. І на виході даного модуля отримуємо напругу від 5В до 28В і максимальну силу струму 2А. Для того щоб підлаштовувати напругу, потрібно крутити потенціометром R1.

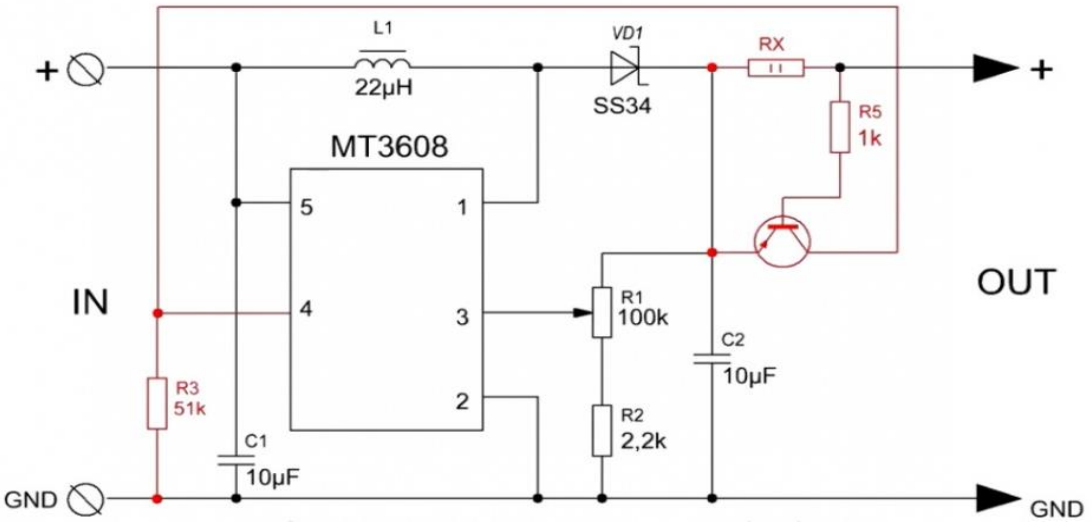


Рисунок 4 – Схема модуля джерела живлення MT3608

Даний модуль можна інтегрувати в портативний зарядний пристрій. Цей модуль живиться напругою 5В і силою струму 2А. Тобто потужність безпровідної зарядки складає 5 Ват. На модуль безпровідної зарядки потрібно припаяти два провідники де подається на нього живлення, а

гніздо Micro-USB можна випаяти воно не потрібне. Інші кінці провідників необхідно припаяти на плату контролю заряду і розряду батарей, а іменно до доріжок вихідного USB порта 5 Вольт і 2 Ампера.

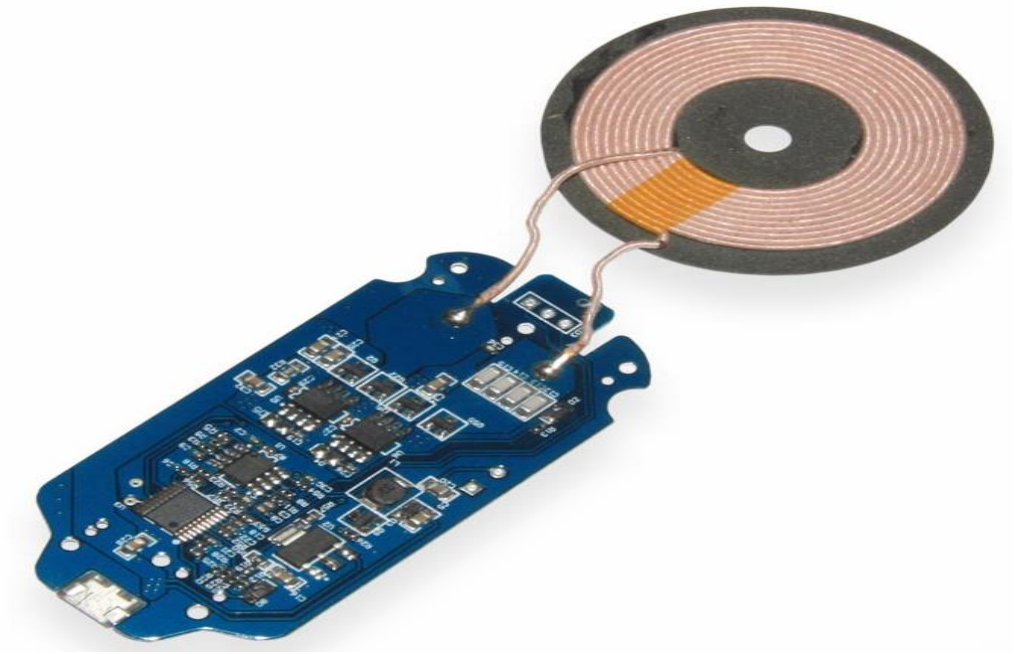


Рисунок 5 – Модуль безпровідної зарядки

Висновки. Гідність пристроїв з вбудованим акумулятором - можливість накопичувати енергію у вбудованому акумуляторі в будь-який світлий час доби, а витрачати тоді, коли буде потрібно, навіть вночі. Кожне з сонячних зарядних пристроїв можна використовувати з перехідниками, тому практично будь-який гаджет може бути заряджений далеко від цивілізації. Так, завдяки своїй універсальності, мобільності, захищеності та здатності працювати у складних фізичних та кліматичних усмовах даний зарядний пристрій стане невідмінним атрибутом військовослужбовців.

Список використаних джерел.

1. Основи схемотехніки електронних систем: Підручник /В.І.Бойко, А.М.Гуржій, В.І.Жуйков та ін. – К.: Вища шк., 2004.

2. Будніцев М. С. Електротехніка, електроніка та мікропроцесорна техніка. – Львів: Афіша, 2001 – 424 с.

3. Матвієнко М. П. Пристрої цифрової електроніки. – К.: Вид. Ліра-К, 2015 - 392 с.

ГОЛОВНІ ТЕНДЕНЦІЇ У ВИРОБНИЦТВІ ЕЛЕКТРОНІКИ

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

Abstract. The factory of the future will be heavily automated and emphasize sustainability, but the technologies and trends shaping electronics manufacturing aim to augment human innovation rather than replace it. Products and factories themselves will be environmentally friendly and will emphasize both cyber and physical security. Industry 4.0, or digitization, is the foundation of most manufacturing advancements. Factories are getting smarter – the IoT/IIoT enable sensors, applications, and associated networking equipment to work together to collect, monitor and analyze data from industrial operations. This data, in turn, provides information that can be used to enhance the manufacturing process.

Вступ. Фабрика майбутнього не є холодним темним приміщенням, де роботи безупинно збирають продукти розроблені штучним інтелектом. Так, процеси будуть значною мірою автоматизовані та забезпечувати стабільність, але технології та тенденції, що формують виробництво електроніки, спрямовані на посилення людських інновацій, а не на їх заміну.

Фактично, багато технологій, які покращують виробничі операції – доповнена/віртуальна реальність (AR/VR), IoT і промисловий IoT (IIoT), штучний інтелект (AI) – роблять фабрики безпечнішими для працівників, одночасно знижуючи витрати. Самі продукти та фабрики будуть екологічно чистими та будуть засновані як на кібербезпеці, так і на фізичній безпеці.

Індустрія 4.0, або цифровізація індустрії, є основою більшості виробничих досягнень. Заводи стають розумнішими – IoT/IIoT дозволяє сенсорам, програмам і пов’язаному мережевому обладнанню працювати разом, щоб збирати, контролювати й аналізувати дані виробничих операцій. Ці дані, у свою чергу, надають інформацію, яку можна використовувати для покращення виробничого процесу.

Основна частина. На початку цього року Microsoft і виробник споживчих товарів Procter&Gamble оголосили про спільне цифрове співробітництво. Цифрова виробнича система Microsoft буде надавати команді P&G доступ до даних у режимі реального часу та моделей штучного інтелекту, які допоможуть оптимізувати та спростити виробництво. Проект включає гібридну хмарну обчислювальну

платформу, яка дозволить бездоганно інтегрувати технології штучного інтелекту, машинного навчання та IIoT в існуючу інфраструктуру.

Обидві компанії також планують запровадити цифрових близнюків, які можуть допомогти в усьому: від розробки продукту до навчання співробітників. Цифрові близнюки дозволяють компаніям проводити віртуальні експерименти у своїх виробничих середовищах, не викликаючи збоїв. Подібним чином цифрові близнюки можуть віртуально конфігурувати фабрику та моделювати, як працівники взаємодіють із машинами. Співробітники можуть тренуватися в цьому віртуальному середовищі, щоб вони були повністю вправними з першого дня. Підвищення ефективності та продуктивності є основними цілями Індустрії 4.0.

AR/VR забезпечує рівень зв'язку між людиною та машиною, який поєднує творче з практичним. Інженери використовують VR і AR для вдосконалення та оптимізації дизайну на ранній стадії. Концепції та параметри можна швидко переглядати, коригувати та змінювати. Цифрові моделі також можна віртуально тестувати, аналізувати та симулювати. Результатом є швидкі ітераційні цикли проектування.

VR і AR також роблять можливим анімаційне моделювання, щоб розробники могли бачити, як продукти будуть використовуватися з часом, і враховували такі фактори, як ергономіка, доступ, зовнішній вигляд і відчуття. Двовимірні креслення або 3D-моделі не можуть передати такий самий досвід, як реалістична симуляція, тому виробники також використовують ці інструменти під час взаємодії з клієнтами. Зрештою, віртуальна реальність і доповнена реальність сприяють спілкуванню та підтримці під час розробки продукту. Результатом є зниження технічного ризику, з більшою ймовірністю компоненти та продукти будуть відповідати призначенню.

Впровадження штучного інтелекту у виробничий контекст означає використання даних для прийняття дієвих рішень швидше й точніше, ніж людина. Це передова технологія, що лежить в основі прогнозованого технічного обслуговування, яка передбачає, як машина поводитиметься під майбутнім корисним навантаженням і коли, чому і як це потрібно буде виправити на основі минулого досвіду. Ці системи значною мірою залежать від сенсорів, які надають дані про електричний струм, вібрацію, температуру та різноманітні показники, які можуть впливати на продуктивність виробництва. Минулі рішення для прогнозованого технічного обслуговування попереджали людей про проблеми з конкретними машинами; тепер вони визначають, який компонент викликав сповіщення.

Прогнозне технічне обслуговування скорочує час простою заводу та пов'язані з ним витрати, а ШІ відіграє важливу роль у якості, скороченні браку та прогнозуванні запасів чи попиту. Використання показників для

прогнозування поведінки за специфікаціями продукту може мінімізувати брак і максимізувати якість продукту. Прогнозування, коли машина чи процес більше не відповідатимуть заданим специфікаціям, або відхилятимуться дають змогу виробникам завчасно робити все необхідне для повернення їх до специфікацій.

Завдяки повному розумінню роботи заводу та даних, що стоять за виробництвом, виробники можуть спрогнозувати попит і рух критичних деталей, що призведе до значної економії запасів.

Аналіз даних також робить дистанційну допомогу більш ефективною. Деякі технічні спеціалісти використовують розумні окуляри, які записують аудіо- та відеозаписи поведінки машини та транслюють їх агенту служби підтримки. Сторона-одержувач може запропонувати допомогу в різних формах, включаючи надсилання відповідних документів або креслень клієнту.

Виробничі підприємства стають все більш пов’язаними. Вони оснащені інтелектуальними машинами, які збирають дані та представляють важливі тенденції. Деякі об’єкти оснащені роботами, які працюють разом з людьми, щоб підвищити продуктивність. Виробники також можуть мати автоматизовані системи, які дозволяють швидко замовляти товари перш ніж вони будуть закінчуватися.

Дослідження, опубліковані в 2020 році, показало, що виробники знаходяться під дедалі більшою загрозою від атак, які використовують зашифровані канали для обходу застарілих засобів контролю безпеки. Зокрема, виробничий сектор зіткнувся з мільярдом таких загроз, що становить великий відсоток всіх таких атак.

Практика, яка називається нульовою довірою , може бути застосована до виробництва, тобто сторони ніколи не дають автоматичного схвалення будь-якій організації, яка намагається отримати доступ до об’єкта чи мережі, незалежно від того, чи є ця особа працівником чи найнадійнішим постачальником виробника. Цей підхід сегментує дані так, що доступ до них мають лише відповідні сторони. Наприклад, якщо працівник виробничого цеху початкового рівня намагався отримати ресурси, які використовуються лише відділом бухгалтерії, ця дія викликала б сповіщення та залишала вміст заблокованим, доки хтось не перегляне запит на доступ і схвалить або відхилить його.

Зберігання матеріалів у закритому вигляді зменшує ймовірність масового витоку даних, що ставить під загрозу інформацію клієнтів. Хакер може отримати доступ до одного сегменту даних або окремого ресурсу. Однак їм доведеться успішно проникнути в безліч інших даних, перш ніж завдати шкоди, пов’язаної з витоком даних, коли компанії не використовують стратегію нульової довіри.

Висновки. Сталий розвиток зараз є пріоритетом для виробництва та охоплює кілька вимірів. Перший – це циклічна економіка, яка вимірює

вплив компанії на клімат і навколишнє середовище. Крім того, це стійке постачання: довгострокова життєздатність постачальників, наявні запаси та надійна логістика. Багато компаній, що займаються виробництвом електроніки, розробляють продукти більше на основі наявності компонентів, ніж на ціні чи продуктивності. Але визначення стійкості у високотехнологічному виробництві є складним завданням, оскільки воно варіюється від зусиль і ресурсів, таких як видобуток рідкоземельних матеріалів, транспортування, експлуатація та управління життєвим циклом, до екологічних систем, виробництва електроенергії та трудових ресурсів.

Список використаних джерел.

1. Shiyong Wang, Jiafu Wan, Di Li and Chunhua Zhang Implementing Smart Factory of Industrie 4.0: An Outlook / International Journal of Distributed Sensor Networks, pp. 1-10, 2015.

2. Emmanuel Nowakowski, Martin Häusler, Ruth Breu Analysis of Enterprise Architecture Tool Support for Industry 4.0 Transformation Planning / 22nd International Enterprise Distributed Object Computing Workshop, pp. 184-191, 2018.

3. Tiago M. Fernández-Caramés1, Paula Fraga-L0amasi A Review on Human-Centered IoT-Connected Smart Labels for the Industry 4.0, pp. 1-19, 2018.

4. Kanghoon Choi and Sang-Hwa Chung Enhanced time-slotted channel hopping scheduling with a quick setup time for the industrial Internet of Things networks / International Journal of Distributed Sensor Networks, vol. 13(6), pp. 1- 14, 2017.

5. Y.-K. Chen Challenges and Opportunities of Internet of Things / 17th Asia and South Pacific Design Automation Conference, pp. 383–388, 2012.

6. M. U.Farooq, M. Waseem, A. Khairi, and S. Mazhar A Critical Analysis on the Security Concerns of Internet of Things (IoT) / International Journal of Computer Applications, vol. 111, no. 7, pp. 1–6, 2015.

7. Wang, Y., Zhang, M. and Zuo, Y., 2016, June. Potential applications of IoT-based product lifecycle energy management. / 11th Conference on Industrial Electronics and Applications, pp. 1999-2002, 2016.

8. Nguyen Bach Long, Hak-Hui Choi and Dong-Seong Kim Energy-Aware Routing Scheme in Industrial Wireless Sensor Networks for Internet of Things Systems / 21st International Conference on Emerging Technologies and Factory Automation, pp. 1-8, 2016.

9. Kirk Bloede, Greg Mischou, Amar Senan, Adam Tilow, The industrial internet of things, making factory smart for the next industrial revolution / Woodside Capital Partners, pp. 1-126, 2017.

10. Nikkam S.M.G. and Pawar V.R. Water parameter analysis for industrial application using IoT. / 2nd International Conference on Applied and Theoretical Computing and Communication Technology, pp. 703-707, 2016.

11. Panayiotis Kolios, Georgios Ellinas, Christos Panayiotou, and Marios Polycarpou Energy Efficient Event-Based Networking for the Internet of Things / 3rd World Forum on Internet of Things (WF-IoT), pp. 1-6, 2016.

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ТРАНСПОРТНИХ ДОДАТКАХ

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

Abstract. Specifically, one of the most exciting value propositions of future EVs is the number of different connectivity technologies they will feature. This connectivity, called vehicle-to-everything (V2X), features technologies like vehicle-to-grid (V2G) and vehicle-to-network (V2N), which are already in use. It also features emerging technologies like vehicle-to-vehicle (V2V) that will shape the future of how EVs work.

The given work discusses the present and the future of EV connectivity and how it will shape the industry moving forward.

Вступ. Досягти справжнього широкого впровадження електромобілів можливо за впровадження величезних зусиль у галузі досліджень і розробок. Хоча значна частина цих розробок спрямована на збільшення запасу ходу, електромобілі майбутнього отримають набагато більше функцій, ніж просто інноваційні технології живлення.

Основна частина. Однією з найбільш цінних пропозицій для електромобілів є кількість різних технологій комунікації, які вони матимуть. Ці комунікації, які мають назву «автомобиль-все» (V2X), включають такі технології, як підключення транспортного засобу до промислової мережі (V2G) і підключення до глобальної мережі (V2N), які вже використовуються. Вони також містять такі нові технології, як, наприклад авто – авто (V2V), які формуватимуть майбутнє роботи електромобілів.

Підключення V2G. Однією з форм зв’язку транспортних засобів, яка нещодавно з’явилася на серійних електромобілях, є підключення V2G (рис.1). Підключення V2G означає здатність електромобіля забезпечувати потік електроенергії як від мережі до автомобіля, так і від автомобіля до мережі. Концепція полягає в тому, що батареї електромобілів, які є відносно великими, можуть виступати не просто джерелом енергії для автомобіля. Вони також можуть зберігати енергію для використання в мережі та вдома (V2H).

З апаратної точки зору підключення V2G базується на технології силової електроніки, що називається двонаправленою зарядкою. Двонаправлений інвертор в електромобілі потребує поєднання сучасної схемотехніки, компонентів та схеми керування, яка може забезпечити

перетворення між змінним струмом мережі та постійним струмом акумулятора.

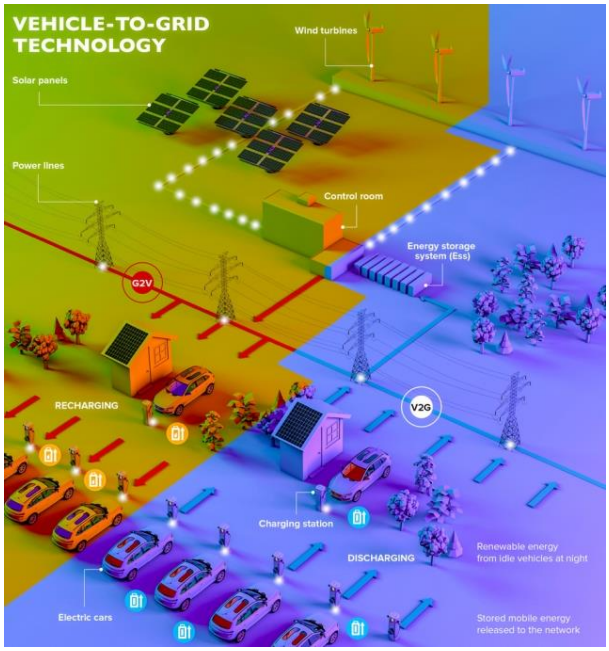


Рисунок 1 – Технологія V2G

Переваги V2G значні як для власника автомобіля, так і для мережі. Для власника вигодою є можливість використовувати свій електромобіль не просто як транспортний засіб, а й як резервний генератор для дому, якщо станеться відключення електроенергії чи інша катастрофа. Крім того, власник транспортного засобу може компенсувати витрати, продаючи надлишок енергії свого електромобіля назад у мережу.

З точки зору мережевої інфраструктури, технологія V2G може зняти навантаження на мережу, дозволивши електромобілю продавати назад частину своєї накопиченої енергії, коли мережа досягає пікового попиту. Коли попит нижчий або поблизу виробляється відновлювана енергія, електромобіль може заряджатися самостійно.

Технологія V2G досі вважається рідкістю для транспортних засобів на сьогоднішньому ринку, але вона набирає обертів, оскільки впроваджується в нових пропозиціях електромобілів, таких як повністю електричний Ford F-150.

Підключення V2N. Після підключення V2G підключення V2N є надзвичайно цінною новою технологією електромобілів. V2N – інша форма підключення електромобілів, означає здатність транспортного засобу стати підключеною частиною Інтернету, здатною спілкуватися з будь-чим іншим у мережі. У контексті електромобілів цей вид підключення зазвичай стосується підключення автомобіля до внутрішньої мережі виробника та хмарних сервісів. Завдяки підключенню V2N транспортний засіб можна ретельно контролювати, аналізувати та динамічно оновлювати для забезпечення максимальної продуктивності.

Одним із варіантів використання підключення V2N є компанії, яким необхідно отримувати інформації про продуктивність своїх транспортних засобів, щоб дізнатися про такі показники, як пропускна здатність енергії, цикли заряду батареї та запас ходу. Отримавши цей відгук від усіх підключених транспортних засобів у мережі V2N, виробник електромобілів може виконувати статистичний аналіз транспортних засобів, щоб зрозуміти, як їхні транспортні засоби працюють у реальних умовах для покращення продуктивності. Звідси транспортні засоби, підключені до V2N, можуть отримувати оновлення свого програмного забезпечення та мікропрограми по повітрю. Крім того, електромобілі компанії можуть використовувати цю інформацію для інформування про зміни апаратного забезпечення в майбутніх моделях своїх електромобілів.

Однією з компаній, яка займається цим, є Tesla. Вони часто випускають бездротові оновлення щодо функцій автопілоту, а також інших загальних функцій продуктивності. Таким чином, V2N є важливою новою технологією, оскільки вона забезпечує найкращу можливу продуктивність електромобілів як поточного покоління, так і майбутніх поколінь.

Підключення V2V є формою підключення EV, що визначає взаємозв'язок усіх під'єднаних транспортних засобів на дорозі. Завдяки V2V транспортні засоби можуть бездротовим способом обмінюватися інформацією один з одним про швидкість, положення, дорожні умови та іншу інформацію (рис. 2). Мета підключення V2V полягає в тому, щоб дозволити транспортним засобам мати повну інформацію про кожен інший транспортний засіб на дорозі, щоб уникнути небезпечних і небажаних ситуацій, таких як аварії та затори. Крім того, транспортні засоби з підтримкою V2V можуть використовувати інформацію про умови дороги та дорожнього руху в режимі реального часу для досягнення оптимального шляху до пункту призначення, заощаджуючи час, енергію та гроші водія.

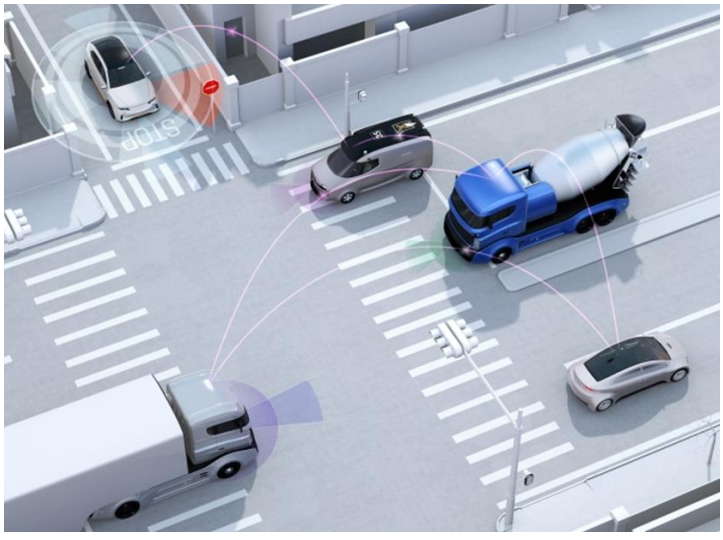


Рисунок 2 – Комунікація V2V

Висновки. Привабливість V2V полягає в тому, що це не така далека від реальності технологія, як здається. З технологічної точки зору можна сказати, що зараз є інфраструктура, необхідна для досягнення V2V завдяки таким технологіям, як 5G і хмарне підключення. Одними з найбільших перешкод на шляху впровадження V2V є безпека та геополітичні виклики.

Технологія V2X – це майбутнє електромобілів. Двадцять п'ять-тридцять років тому неможливо було уявити, що телефони отримають набагато більше функцій і стануть такими важливими аспектами нашого життя. Сьогодні ми стоїмо на тому самому роздоріжжі з електромобілями. Технологія V2X вдихає нове життя в технології електромобілів та надає їм набагато більше, ніж тривіальне водіння.

Список використаних джерел.

1. J. Torriti, Demand Side Management for the European Supergrid: Occupancy variances of European single-person households / Energy Policy, vol. 44, pp. 199-206, 2012.

2. Yih-Fang Huang; Werner, S.; Jing Huang; Kashyap, N.; Gupta, V. State Estimation in Electric Power Grids: Meeting New Challenges Presented by the Requirements of the Future Grid / Signal Processing Magazine, vol.29, no.5, pp.33-43, 2012.

3. Tomoiagă, B.; Chindriş, M.; Sumper, A.; Sudria-Andreu, A.; Villafafila-Robles, R. Pareto Optimal Reconfiguration of Power Distribution Systems Using a Genetic Algorithm Based on NSGA-II / Energies, vol. 6, pp. 1439-1455, 2013.

4. F.R. Yu, P. Zhang, W. Xiao, and P. Choudhury Communication Systems for Grid Integration of Renewable Energy Resources / Network, vol. 25, no. 5, pp. 22-29, 2011.

5. Mohsen Fadaee Nejad, Amin Mohammad Saberian and Hashim Hizam Application of smart power grid in developing countries / 7th International Power Engineering and Optimization Conference, 2013.

6. The History of Electrification: The Birth of our Power Grid. Edison Tech Center, 2013.

7. Berger, Lars T. and Iniewski, Krzysztof Smart Grid - Applicacions, Communications and Security, 488 p., 2012.

8. N.A. Sinitsyn. S. Kundu, S. Backhaus Safe Protocols for Generating Power Pulses with Heterogeneous Populations of Thermostatically Controlled Loads / Energy Conversion and Management, vol.67, pp. 297-308, 2013.

9. Energy Future Coalition, "Challenge and Opportunity: Charting a New Energy Future," Appendix A: Working Group Reports, Report of the Smart Grid Working Group. Why the Smart Grid Won't Have the Innovations of the Internet Any Time Soon: Cleantech News and Analysis.

10. National Energy Technology Laboratory. NETL Modern Grid Initiative – Powering Our 21st-Century Economy. United States Department of Energy Office of Electricity Delivery and Energy Reliability, 17 p, 2007.

SOC ДЛЯ ВИРОБНИКІВ АВТОМОБІЛІВ

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

Abstract. There are many factors to consider when auto OEMs decide whether to go with a customized SoC or “off-the-shelf” products. Some questions include whether the car is intended for a broad-based market with little differentiation from others, which key IP should be brought in-house versus relying on external providers, and what are the trade-offs in terms of power, performance, size and costs. In the end, automotive vendors must decide what is most suitable to them, based on the options available.

Вступ. Питання того, чи знадобляться додатки ADAS для досягнення успіху в майбутньому, не «якщо», а «коли». Платформи для автономного водіння наступного покоління вимагають вищих рівнів продуктивності, щоб приймати рішення за частки секунди. Автомобіль повинен розуміти, транслювати та точно сприймати навколишнє середовище та реагувати на зміни якомога швидше та найбезпечніше.

Майбутні ADAS і автономні реалізації (рис.1) вимагають найвищої продуктивності, периферійних обчислень у реальному часі з можливостями обробки ШІ, а також інтерфейсів з високою пропускною спроможністю для безлічі датчиків високої роздільної здатності, включаючи радар, LiDAR і камеру.

Удосконалення можливостей «бачення/зору» передових систем допомоги водієві (ADAS) виходить за рамки камер і LiDAR, включаючи інтелектуальні датчики для обробки складних сценаріїв водіння, які в автомобільній промисловості називають 4 рівнем, або «високою» автоматизацією.

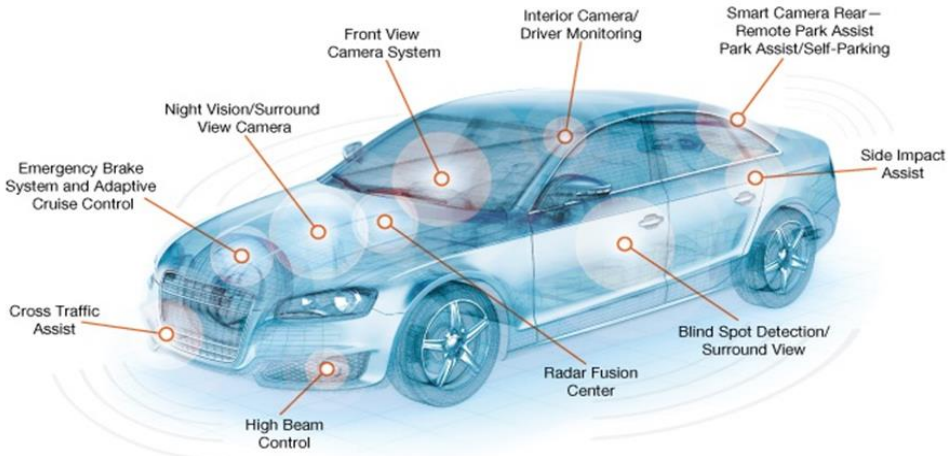


Рисунок 1 – ADAS і автономне водіння потребують кількох датчиків

Основна частина. Темпи зростання ринку автомобільних SoC у першому півріччі 2022 року показують збільшення на 60%. Удосконалення автоматизації транспортних засобів, такі як можливості GPS-радарів, аудіо та відео допомога, а також збільшення інвестицій у дослідження та розробку автоматизації транспортних засобів, щоб впоратися зі зростаючими вимогами споживачів щодо безпечного водіння, стимулюють ринок автомобільних SoC.

Фактори, що сприяють різкому зростанню, включають суворі правила безпеки транспортних засобів, попит на вищий рейтинг безпеки, підвищення обізнаності споживачів разом із зниженням вартості компонентів. Крім того, зростаючий ринковий попит на автономні транспортні засоби з ультразвуковими датчиками та камерами високої чіткості сприяє подальшому зростанню ринку.

Автомобільні системи на процесорі допомагають створювати кілька спеціалізованих блоків обробки на одному кристалі, який виконує кілька одночасних завдань, таких як керування рухом, камери огляду та відображення інформації. Інформаційно-розважальна система дозволяє водієві керувати багатьма функціями централізованого визначення місцезнаходження, вхідними, вихідними, конференц-дзвінками та багатьма іншими. Він надає інформацію та розваги водієві, а також пасажиру через відео та аудіо інтерфейси, елементи керування, такі як панель кнопок, сенсорний екран, голосові команди тощо. Таким чином, протягом багатьох років зростає впровадження інформаційно-розважальної системи з метою підвищення безпеки автомобіля, кращих рішень для підключення та покращення взаємодії з користувачем автомобіля, щоб підвищити попит на інформаційно-розважальну систему.

Індивідуальні SoC проти OTS (готових) рішень. Є багато факторів, які слід враховувати, коли виробники автомобілів вирішують використовувати налаштований SoC, чи «готові» продукти. Деякі питання включають наступне: чи призначений автомобіль для широкого ринку з незначною диференціацією від інших, яку ключову IP слід надати власному рішенню, чи покладатися на зовнішніх постачальників, і які компроміси з точки зору потужності, продуктивності, розміру і витрат. Зрештою, постачальники автомобілів повинні вирішити, що їм найбільше підходить, виходячи з наявних варіантів.

Переваги індивідуальних рішень SoC перед стандартними рішеннями на базі типових мікропроцесорів і мікро контролерів. Нижче наведено причини, чому індивідуальні рішення SoC можуть бути оптимальним вибором під час проектування вашого наступного автомобільного застосування:

1. Користувальницькі SoC побудовані на основі багатоцільових IP-блоків, які спеціально розроблені та інтегровані для досягнення запланованих функцій відповідно до вимог прикладної програми. Вони

спеціально розроблені для досягнення оптимального рівня продуктивності та ефективності при одночасному зменшенні розміру та загальних витрат на специфікацію.

2. Стандартні OTS або «готові» кремнієві рішення призначені для використання на більш широкому ринку. Таким чином, типові кремнієві пристрої OTS підтримують функції, які не повністю оптимізовано для потреб автовиробників, або в деяких випадках взагалі не використовуються. Це часто призводить до збільшення займаної площі, непотрібного споживання енергії та неефективності продуктивності.

3. Індивідуальні рішення SoC надають виробникам комплектного обладнання та Tier-1 можливість повністю володіти ключовими диференційованими технологіями в сферах ADAS та автономності. Запатентовані мікросхеми пропонують компаніям можливість отримати глибокі знання та власний досвід, забезпечуючи більший контроль над майбутнім дизайном та продуктами реалізації.

Ланцюг постачання – головний фактор, який слід враховувати при розробці нового обладнання, в тому числі електроніки сучасної автомобільної техніки.

Перебої в ланцюзі постачання є головною проблемою для виробників оригінального обладнання. Непередбачені події можуть порушити потік поставок, наприклад стихійні лиха, блокада міжнародних кордонів, урядові санкції, економічні спади, геополітичні та соціальні заворушення. Постачання матеріалів ніколи не гарантується, однак шанси на продовження виробництва більш сприятливі, коли компанії не потрібно конкурувати з кількома іншими, щоб отримати той самий продукт.

Все більше і більше виробників автомобілів розуміють, що мікросхеми загального призначення пропонують функції, які обслуговують багатьох клієнтів, обмежуючи конкурентоспроможність їхньої продукції та обмежуючи їх термінами та графіком доставки постачальників.

В чому переваги користувальницьких SoC? Час від часу з’являється нова компанія, яка змінює звичну та сталу бізнес-модель. Наприклад, Tesla на ранній стадії усвідомила важливість оновлень програмного забезпечення OTA (Over-the-Air) для додавання певних функцій і підвищення безпеки та продуктивності. Компанія розробляла власні процесори з 2016 року. Tesla разом з іншими технологічними гігантами, такими як Google, Amazon, Cruise та багатьма іншими, вирішили розробити власні платформи автономного водіння.

Також Tesla була однією з перших компаній, які впровадили технології автономного водіння, запустивши свій автопілот 1 покоління в 2016 році. Щоб побудувати самокерований автомобіль, виробникам автомобілів потрібна комбінація апаратного, програмного забезпечення та даних, щоб працювати разом, щоб тренувати глибокі нейронні мережі, які

дозволяють транспортному засобу сприймати навколишнє середовище та безпечно переміщатися в ньому. Глибинні нейронні мережі є двигуном штучного інтелекту. Він містить низку алгоритмів, спеціально розроблених для імітації роботи нейронів у людському мозку. Вони є основою глибокого навчання. Еволюція автопілоту Tesla та функцій повного автономного керування змусила виробників автомобілів уважніше придивитися до використання камер та ультразвукових датчиків.

Рішення SoC. Для створення запатентованої мікросхеми потрібна складна, добре структурована будова з повною системою підтримки для кожного етапу процесу розробки. Більшість компаній, які прагнуть розробляти власні мікросхеми, не мають у своєму розпорядженні таких можливостей. Їм потрібна допомога від вузькоспеціалізованих компаній, які володіють великими інженерними навичками, ноу-хау та досвідом, щоб підтримувати проектування, розробку та реалізацію SoC на повному системному рівні.

Багато виробників пропонують комбінацію IP разом із необхідним досвідом проектування та підтримкою розробки для впровадження широкомасштабних, повністю налаштованих автомобільних рішень SoC, щоб відповідати найвибагливішим і найсуворішим вимогам до продуктивності автомобільних програм.

Такий підхід до виробництва автомобільних SoC, забезпечує функціональну безпеку, прискорюючи розробку програмного забезпечення та перевірку системи.

Висновки. Автомобільні SoC – це власна або зовнішня функція, яка може досліджувати, контролювати та допомагати покращувати стан безпеки автопарків. SoC можуть бути використані для вдосконалення автоматизованих структур, які пропонують найсучасніші можливості для водія або клієнта.

Список використаних джерел.

1. Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles, SAE International, pp. 41, 2021.

2. Jennifer Shuttleworth SAE Standards News: J3016 automated-driving graphic update / SAE International, 2019.

3. SAE International Expands Global Footprint with Acquisition of SMi Group Ltd / SAE International, 2020.

4. Alexander Borodin, Vladimir Karnaushenko FPGA Nano Structures for Vehicle Electronics / XII International Scientific Conference «Functional Basis of Nanoelectronics», September 9-13, Odesa, Ukraine, pp., 2021.

УНІВЕРСАЛЬНИЙ ПРОГРАМНО-АПАРАТНИЙ ІНТЕРФЕЙС ЗВ'ЯЗКУ З МНОЖИНОЮ ВБУДОВАНИХ ПРИСТРОЇВ

студентка Гетьман К.Р., асистент Шевцов І.О.
Харківський національний університет радіоелектроніки,
кафедра МТС, м. Харків, Україна
e-mail: kseniia.hetman@nure.ua, ivan.shevtsov@nure.ua

Abstract. The object of research is multiformat hub for embedded systems used in IoT (Internet of Things). The effective development of IoT is not only about the penetration of "connected" devices in all aspects of life, but also about the creation of a technological ecosystem, unified solutions for collecting, transmitting, aggregating data on a platform that allows processing data and using it to implement effective solutions. Availability of many inexpensive sensors and peripherals with different interfaces and communication protocols to work with IoT controllers. Standardized interfaces and communication protocols of most automation controllers impose restrictions on the use of many devices. At the same time, it is often not possible to use interface converters to connect an unsupported device to the automation controller.

Вступ. На сьогоднішній день ми спостерігаємо потужний спалах інтересу до інтернету речей саме в останні кілька років, концепція технології існує з 1999 року, і вже тоді відчувалася масштабність її характеру. Агрегування даних з підключених пристроїв і датчиків допомагає оптимізувати бізнес-процеси, і отримувати більш персоналізовані і якісні послуги/інфраструктуру споживачам.

Основна частина. Відлагоджувальні плати виробництва компанії STMicroelectronics надають користувачам можливість швидко, ефективно і з мінімальними матеріальними витратами створювати прототипи, гнучкі до зміни і додаванню нового функціоналу. Також, ці плати мають відносно невисоку вартість [1-3].

Безкоштовне програмне забезпечення також значно спрощує процес створення рішень на базі контролерів STM32, а широкий спектр документації, зменшує інформаційні труднощі освоєння контролерів на первинних етапах до мінімуму [1].

Для проектування ПО будемо використано відлагоджувальну плату Nucleo F767-ZI. Обрана відлагоджувальна плата підтримує безліч інтерфейсів UART, SPI, I2C, CAN і т.д. Однак не всі інтерфейси можна одночасно використовувати. Обмеження, в даному випадку, накладає те, що сигнальні ланцюга різних інтерфейсів можуть бути виведені на один і той же вивід мікросхеми. При цьому програмно необхідно вибрати, який це буде інтерфейс. Також обмеження на використання всіх інтерфейсів накладає те, що частина виводів мікроконтролера на відлагоджувальній платі спочатку задіяна на певні функції, наприклад USB, і оцінний UART.

На базі обраної плати було реалізовано такі інтерейси зв’язку: CAN (стандарт промислового мережі, орієнтований, перш за все, на об'єднання в єдину мережу різних виконавчих пристроїв і датчиків), RS-48 (стандарт фізичного рівня для асинхронного інтерфейсу), Ethernet (сімейство технологій пакетної передачі даних між пристроями для комп'ютерних і промислових мереж), CSMA/CD (Carrier Sense Multiple Access with Collision Detection – множинний доступ з прослуховуванням несучої і виявленням колізій – технологія множинного доступу до загального передавального середовища в локальній комп'ютерній мережі з контролем колізій), RS-232 (Recommended Standard 232 - фізичний рівень для асинхронного (UART) інтерфейсу), I2C (послідовна шина даних для зв'язку інтегральних схем, розроблена фірмою Philips на початку 1980-х як проста шина внутрішнього зв'язку для створення керуючої електроніки).

Також реалізована підтримка таких протоколів: UART (універсальний асинхронний приймач і передавач) та USART (універсальний синхронний і асинхронний приймач і передавач), SPI (Serial Peripheral Interface - це протокол послідовного зв'язку синхронного типу, який складається з двох ліній даних (MOSI і MISO), однієї тактової лінії (SCK) і лінії вибору підлеглих (SS)), I2C (Inter-Integrated Circuit - синхронний протокол послідовного зв'язку або двопровідний інтерфейс).

Висновки. Використання універсальних пристроїв сполучення значно спрощує проєктування систем автоматизації, робототехніки та IoT, що також призводить до скорочення часу розробки. Використання цього класу пристроїв дає змогу розробникам абстрагуватися від роботи з периферійними інтерфейсами в контролерах верхнього рівня.

Виконана робота дає нам можливості збільшити зручності під час використання хабу, не тільки за рахунок мультиінтерфейсності, а і мультиформатності, що значно зменшує кількість проміжних пристроїв під час передачі даних.

Список використаних джерел.

1. 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.

2. I. Shevtsov, I. Svyd, V. Chumak, A. Sierikov. Practical Aspects of Software Optimization for MCUs with RTOS. // IV International Scientific and Practical Conference Theoretical and Applied Aspects of Device Development on Microcontrollers and FPGAs (MC&FPGA-2022), Kharkiv, Ukraine, 2022, pp. 35-36, doi: 10.35598/mcfpga.2022.012.

3. 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.

ПІДСИСТЕМА ІДЕНТИФІКАЦІЇ ВИБУХОНЕБЕЗПЕЧНИХ ПРЕДМЕТІВ

доцент, к.т.н. Хрустальов К. Л., студент Сергієнко А. С.
Харківський національний університет радіоелектроніки,
кафедра КІТАМ, м. Харків, Україна
e-mail: kirill.khrustalev@nure.ua, andrii.serhiienko@nure.ua

Abstract. This work is devoted to modern developments in the field of detection of explosive objects. This article presents the relevance of the explosive ordnance detection system. The main components of the system and their interaction are shown and described. A block diagram of the developed system is attached. The main problem with existing systems is that in it a person must be in close proximity to be detected. The subsystem that is being developed will be used on the robot that will be controlled remotely. When an explosive device is detected, it will warn where it is located.

Вступ. В умовах воєнного стану мінування приміщень ворогом є однією з найактуальніших проблем у сучасному світі. Для того, щоб уникнути травм і зберегти життя саперам використовують спеціальні прилади, роботи для виявлення вибухонебезпечних ознак, які допомагають виявити їх. Грамотне застосування технічних засобів для пошуку вибухових речовин може сприяти зниженню ймовірності отримати травми під час розмінування приміщень.

Основна частина. До ознак вибухонебезпечних приладів ставляться: наявність характерних металевих і пластмасових деталей, напівпровідникових приладів (діодів, транзисторів, інтегральних мікросхем) підривних пристроїв, провідних ліній, антен, певна форма корпусу (циліндр, паралелепіпед) тощо [1].

Історія розвитку засобів пошуку вибухонебезпечних речовин та вибухонебезпечних приладів склалася так, що в даний час найбільшого розвитку отримали засоби, робота яких заснована саме на виявленні цих ознак. Найбільш широкою номенклатурою представлені металошукачі (металодетектори, індукційні міношукачі), перші зразки яких були створені у 30-х роках минулого століття. Вони призначені для виявлення вибухонебезпечних предметів за наявності металевих корпусів чи досить масивних (більше 3-5 г) деталей детонатора [2]. Функціонування металошукачів засноване або на гармонійному методі, що дозволяє виявити металеві об'єкти за рахунок вимірювання параметрів наведеного в них сигналу (фаза і амплітуда), що збуджується гармонічним струмом, або на методі перехідних процесів, що дозволяє виявити металеве тіло по згасаючому в ньому вторинному імпульсу.

Переносні індукційні металошукачі зазвичай складаються з датчика та блоку обробки сигналу із системою індикації, конструктивно розміщених

на штанзі. Живлення приладів здійснюється від акумуляторних батарей напругою 6-12 В [3]. Основним недоліком використання металошукачів є те, що людина повинна знаходитися в безпосередній близькості від неї, що ускладнює розмінування території, оскільки вибухонебезпечний пристрій може детонувати.

Для вирішення цієї проблеми розроблена підсистема за допомогою якої можна буде керувати приладом із безпечного для сапера місця. Основними елементами підсистеми є циліндричний датчик металошукача, який буде виявляти вибухонебезпечне пристрій по металевих елементах. Аналого-цифровий перетворювач, буде перетворювати аналоговий сигнал у цифровий і передавати його в мікроконтролер, який визначатиме чи є пристрій вибухонебезпечним. Також пропонується після виявлення металодетектором вибухонебезпечного пристрою здійснити додатковий візуальний огляд території за допомогою камери, яка буде встановлена на роботі. За допомогою GPS-трекера будуть записані координати місцезнаходження вибухонебезпечного пристрою які будуть передані саперам. Це значно убезпечить роботу саперів та прискорить розмінування території. Структурна схема підсистеми ідентифікації вибухонебезпечних предметів наведена на рисунку 1.

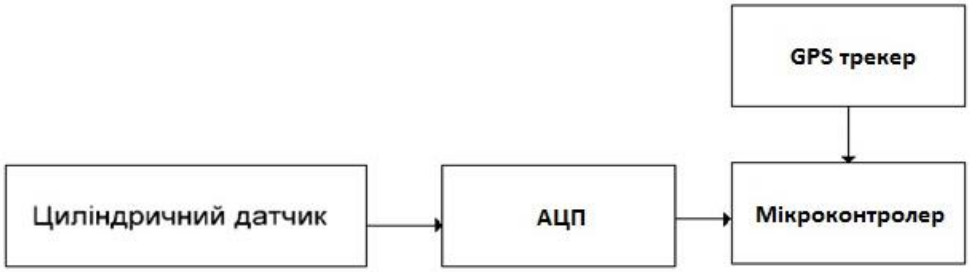


Рисунок 1 – Структурна схема підсистеми ідентифікації вибухонебезпечних предметів

Висновки. Запропонована підсистема ідентифікації вибухонебезпечних предметів дозволить здійснювати керуванням роботом з безпечної відстані, записувати та передавати координати місцезнаходження потенційно небезпечних предметів, що полегшить та зробить безпечнішою роботу саперів та прискорить процес розмінування території.

Список використаних джерел.

1. Ewing R. G., Atkinson D. A., Eiceman G. A., Ewing G. J. A critical review of ion mobility spectrometry for the detection of explosives and explosive related compounds. *Talanta*. 2001. Volume 54. P. 515-529.

2. Rothman L. S., Gamache R. R., Tipping R. N. e.a. The HITRAN Molecular Database: edition of 1991 and 1992. *JQSRT*. 1992. Volume 48. P. 469-507.

3. Jensen W. A. Binomial reliability demonstration tests with dependent data. *Quality Engineering*. 2015. Volume 27. P. 253-266.

4. Danila O., Steiner S. H., Mackay R. J. Assessing a binary measurement system. *Journal of Quality Technology*. 2008. Volume 40. P. 310-318.

СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ УПРАВЛІННЯ ФІНАНСОВИМ КАПІТАЛОМ ВИРОБНИЧИХ ПІДПРИЄМСТВ

доцент, к.т.н. Хрустальова С. В., студент Пономаренко Д. С.
Харківський національний університет радіоелектроніки,
кафедра КІТАМ, м. Харків, Україна
e-mail: sofiia.khrustalova@nure.ua, dmytro.ponomarenko@nure.ua

Abstract. The proposed a decision support system for managing the financial capital of the enterprise, implemented as a software tool. The purpose is to increase the efficiency of decision-making in the management of the financial capital of manufacturing enterprises by using specific indicators to calculate the company's compliance with the value investment strategy. The object of research is the decision-making process for management financial capital of production enterprises. The subject of research is software for financial management capital of production enterprises.

Вступ. Збереження фінансового капіталу підприємства є дуже важливою частиною будь-якого бізнесу. Одним із способів зберігання, і навіть збільшення, капіталу є інвестування. На сьогоднішній день існує безліч інструментів інвестування коштів: депозити, пенсійні фонди, дорогоцінні метали, нерухоме майно, державні облігації, криптовалюти та ін. Але з усіх інструментів виділяються акції великих підприємств. Інвестування в акції може бути дуже прибутковим. Важливою частиною інвестування є фундаментальний аналіз цінних паперів підприємств, які потенційно можуть бути придбані в інвестиційний портфель. Автоматизація цього процесу підвищить якість аналізу, виключить людський фактор з прорахунків, а також заощадить багато часу, що також є корисним при аналізі сотень потенційних елементів інвестиційного портфелю.

Основна частина. На сьогоднішній день існує безліч систем підтримки прийняття рішень, в тому числі економічних. Такі системи реалізовані у вигляді програмних засобів (найчастіше – веб-додатків або десктопних програм), наприклад, таких як yahoo.finance або finviz [1,2]. ористуючись цими сервісами, можливо знайти велику кількість історичної інформації, графіків, новин, експертних статей та аналітики. Однак, вони не пропонують користувачу жодної стратегії для того, яким чином йому використовувати цю інформацію. Тому, пропонується система підтримки прийняття рішень (рис. 1), яка дозволяє користувачу, з використанням пошукового поля, аналізувати цінні папери підприємств і перевіряти відповідність підприємства під стратегію вартісного інвестування.

Вартісне інвестування – стратегія інвестування, яка заснована на виявленні недооцінених цінних паперів за допомогою фундаментального аналізу, запропонована Бенджаміном Гремом та Девідом Доддом. Цінні

папери, що відповідають стратегії, повинні мати низку критеріїв, за допомогою яких інвестор може оцінити відповідність стратегії.

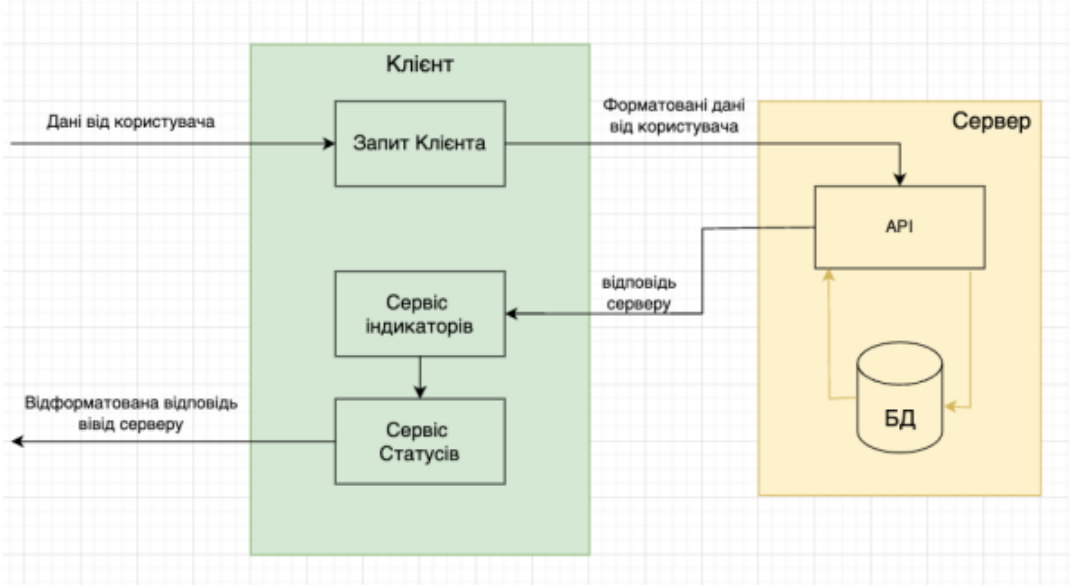


Рисунок 1 – Структурна схема системи підтримки прийняття рішень управління фінансовим капіталом виробничих підприємств

Робота системи починається з отримання даних від користувача за допомогою пошукового поля. Після отримання даних, клієнт програмного засобу обробляє їх до того формату, який розуміє сервер, і відправляє відповідні запити. Сервер, в свою чергу, робить відповідні запити до бази даних, для того щоб також обробити їх і відправити клієнту необхідну відповідь. Після того, як клієнт отримує відповідь від серверу, дані проходять два рівні обробки – через сервіс індикаторів та сервіс статусів, в яких вже відбувається бізнес-логіка програмного засобу – прорахунок індикаторів та співставлення кожного індикатора з таблицею відповідностей для того, щоб сформувати статус індикатора і віддати вже сформовані дані для рендеру у HTML.

Розроблено алгоритм роботи програмного засобу управління фінансовим капіталом виробничих підприємств, який наведено на рис. 2.

Після того, як користувач ввів ключове слово для пошуку підприємства і натиснув на будь-яке підприємство у наданому листі співпадінь, відправляється запит на API для того, щоб отримати відповідь з серверу з відповідною інформацією. Програмний код перевіряє, чи прийшов 200 статус у відповіді, і тільки в цьому разі програма продовжує розрахування з даними з серверу.

В будь-якому іншому разі, користувач побачить повідомлення про те, що сервер не має змоги повернути коректні дані. В такому разі користувач може спробувати повторити свої дії або спробувати обрати іншу компанію у листі, що відображається після введення ключового слова для пошуку.

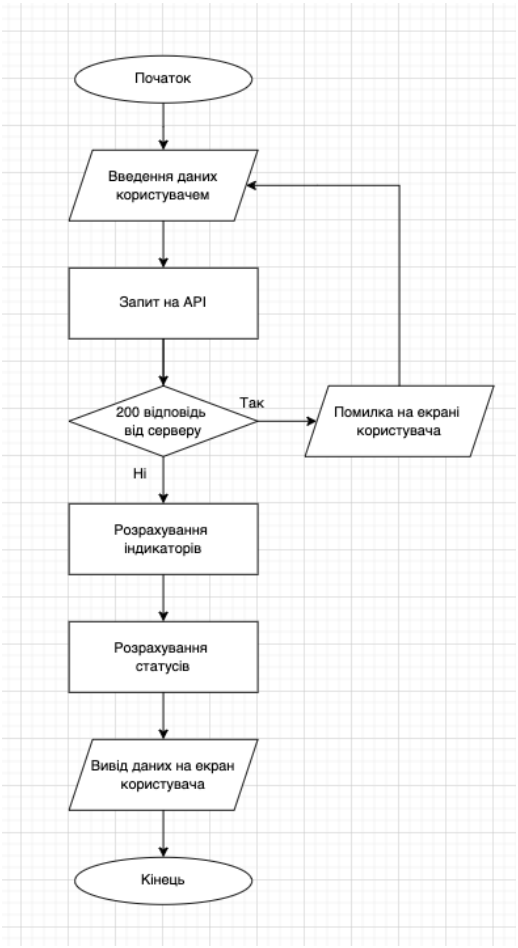


Рисунок 2 – Алгоритм роботи програмного засобу управління фінансовим капіталом виробничих підприємств

За даними «Альфа-банку», найбільшою популярністю в українських інвесторів користувалися акції Apple, Coca-Cola, Intel, Microsoft. Аналіз даних цінних паперів, станом на 18.10.2022 показав, що жодна з цих акцій не має відмінних результатів в кожному з критеріїв, хоча деякі індикатори і вказують на задовільні результати.

Висновки. Таким чином, використання розробленої системи дозволило підвищити ефективність прийняття рішень при управлінні фінансовим капіталом виробничих підприємств шляхом використання специфічних індикаторів для розрахунку відповідності підприємства стратегії вартісного інвестування.

Список використаних джерел.

1. Yahoo.finance, веб-сайт. URL: https://finance.yahoo.com/ (дата звернення 29.10.2022).

2. Investing, веб-сайт. URL: https://www.investing.com/ (дата звернення 29.10.2022).

3. Грем Б. Розумний Інвестор. Стратегія вартісного інвестування. Київ: Наш Формат, 2019, 123 с.

ВИКОРИСТАННЯ IOT ПРИСТРОЇВ НА ОСНОВІ ESP32 ЯК СПОСІБ АВТОМАТИЗАЦІЇ ВНУТРІШНІХ ПРОЦЕСІВ МЕРЕЖІ ЗАРЯДНИХ СТАНЦІЙ ДЛЯ ЕЛЕКТРОМОБІЛІВ

студентка Сігута Д.К., старший викладач Широкопетлєва М.С.
Харківський національний університет радіоелектроніки,
кафедра ПІ, м. Харків, Україна
e-mail: diana.sihuta@nure.ua, marija.shirokopetleva@nure.ua

Abstract. Automation of all possible processes is an integral part of technological development in any field and charging stations network is not an exception. It is proposed to take into consideration a ESP32 development board and compare it with other devices. Obviously, the main task of the charging stations network is to provide drivers with the service of charging their electric vehicles. The ESP32 device should be considered as the control processor of the hardware part which manages all the processes while charging and makes just-in-time reports about station activity.

Вступ. Автоматизація усіх можливих процесів є невід'ємною складовою технологічного розвитку у будь-якій сфері. І мережа зарядних станцій для електромобілів не є виключенням. Більше того, ефективність її функціонування напряму залежить від рівня впровадження IoT пристроїв. Їхня мета полягає у мінімізації людської участі та підвищенні якості взаємодії кінцевого користувача з програмною системою.

Основна частина. Головне завдання даного дослідження полягає у виборі конкретного IoT пристрою та визначенні задач, які мають бути автоматизовані. Перш за все, розглянемо 3 серії мікроконтролерів від різних виробників: ESP32, Arduino та STM32.

Особливу увагу зосередимо на характеристиці пристроїв ESP32:

- тип «система на чипі» (усі функціональні складові розміщуються на одній мікросхемі);
- використання 32-розрядного мікропроцесору в 2-ядерних та 1-ядерних варіаціях, що працює на 160 або 240 МГц;
- наявність інтегрованих Wi-Fi та Bluetooth модулів;
- низький рівень енергоспоживання [1].

IoT пристрій має підтримувати зв'язок по мережі, тому ключовою характеристикою є наявність вбудованого Wi-Fi модулю. Пристрої Arduino та STM32 мають низку своїх переваг, але даний модуль у них відсутній. Це вимагає купівлю окремих компонент, що підвищує собівартість пристроїв. А ESP32 пристрої наділені унікальним набором рис, необхідних для даної предметної області за відносно низьку ціну, тому зупинимось на цій серії.

Тепер визначимо, яку множину функціональних можливостей має забезпечувати IoT пристрій в контексті обраної предметної області. Очевидно, що ключовою задачею мережі зарядних станцій є надання

водіям послуги підзарядки їхніх електромобілів. Даний процес має виконуватись виключно за участю та власною ініціативою водія. Це, у свою чергу, усуває необхідність працевлаштування додаткових робітників. З іншого боку, дана взаємодія має бути добре спроєктованою, щоб клієнт з докладанням мінімальних зусиль досягнув бажаного результату.

Для вирішення цієї проблеми приходить на поміч мікроконтролер ESP32, котрий слід розглядати в якості керуючого процесору апаратної частини окремо взятої зарядної станції. Свою роботу він починає зі з'єднання по HTTPS-протоколу з сервером відповідної програмної системи, після чого переходить в режим очікування від нього певних команд. Окрім того, до його функціональності входить:

- розпізнавати підключення/ відключення електромобіля;
- контролювати початок та кінець подання електроенергії;
- слідкувати за прогресом зарядки;
- вести підрахунок обсягу витраченої електроенергії;
- зупиняти процес зарядки у разі досягнення 100-відсоткового заряду електромобіля.

Варто зазначити, що наведеними вище пунктами роль ESP32 пристрою не обмежується. Також він має контролювати діяльність зарядної станції, щоб у режимі реального часу повідомляти користувачам про її статус або звітувати про будь-які збої та помилки. Завдяки цьому мережа зарядних станцій становитиме дійсно налагоджену систему, яка ставить собі за мету вчасно вирішувати виникаючі проблеми, задовольняючи цим потреби кінцевих користувачів.

Не менш важливим є те, що мікроконтролер ESP32 підтримує механізм OTA (Over The Air Updates) – це метод бездротового розповсюдження на кінцеві пристрої для оновлення їхньої мікропрограми, конфігурації або пов'язаних із безпекою протоколів [2]. Це надає можливість дистанційного виправлення помилок та впровадження нового функціоналу у встановлені IoT пристрої одразу по всій мережі без необхідності зосередження уваги на окремих зарядних станціях.

Висновки. Таким чином, було визначено, що мікроконтролер ESP32 може відіграти вирішальну роль в автоматизації внутрішніх процесів мережі зарядних станцій для електромобілів, що значно покращить користувацький досвід та взаємодію з системою в цілому. Застосування подібних рішень безумовно розвиває дану індустрію та слугує рушієм створення і впровадження новітніх технологій.

Список використаних джерел.

1. ESP32 Wi-Fi & Bluetooth MCU | Espressif Systems [Електронний ресурс] – Режим доступу до ресурсу: https://www.espressif.com/en/products/socs/esp32 (дата звернення: 05.10.2022).

2. Over The Air Updates (OTA) – ESP32 | ESP-IDF Programming Guide latest documentation – Режим доступу до ресурсу: https://docs.espressif.com/projects/esp-idf/en/latest/esp32/api-reference/system/ota.html (дата звернення: 05.10.2022).

ДОСЛІДЖЕННЯ БЕЗПЕКИ ХМАРНИХ СЕРВІСІВ

Довбня А.А., к.т.н., доц. Горелов Д.Ю.
Харківський національний університет радіоелектроніки,
кафедра КРіСТЗІ, м. Харків, Україна
e-mail: andrii.dovbnia@nure.ua

Abstract. The subject of the study is data located in the cloud infrastructure that requires the appropriate level of security and privacy, which is a priority need of clients served in public clouds.

У сучасному динамічному світі найбільш важлива конкурентна перевага компаній – їх ефективність, яка визначається швидкістю реакції на зміни умов ведення бізнесу та додавання нового функціоналу. Для багатьох використання хмарних сервісів стає найбільш виправданим вибором. Хмарні сервіси дозволяють:

1) істотно збільшити швидкість виділення ресурсів, необхідних для розвитку сервісу чи додавання нового функціоналу;

2) підвищити ефективність використання ресурсів, спрогнозувати необхідні витрати та врахувати їх у вартості послуг;

3) вирішити проблеми забутих активів та застарілого обладнання, яке може бути задіяне зловмисниками при проведенні атак.

Однак переваги хмарних сервісів супроводжуються новими ризиками, які потрібно мати на увазі при ухваленні рішення про міграцію у хмару.

Ризик №1. Конфіденційність даних або ймовірність несанкціонованого доступу до конфіденційної інформації (баз даних, віртуальних серверів, даних, що передаються у незахищеному вигляді, інші об'єкти орендованої хмари) з боку провайдера послуг. Це пов'язано з тим, що обробка інформації здійснюється на обладнанні провайдера, без можливості фізично контролювати його дії.

Для мінімізації цього ризику рекомендується вживати наступні заходи.

1. Шифрувати конфіденційні дані, що зберігаються у базі даних. Якщо неможливо гарантувати безпеку даних, що зберігаються на фізичному рівні, то потрібно зробити такий доступ не вартим зусиль. Цей захід також дозволить мінімізувати ризик несанкціонованого доступу до опублікованої бази даних. При цьому шифрування можна реалізувати як на рівні програмного забезпечення (ПЗ), так і вбудованими засобами бази даних.

2. Шифрувати дані під час передачі. Імовірність цього ризику мала через високу складність здійснення атаки. Проте, якщо вартість даних висока, то логічним буде використання шифрування на рівні ПЗ, оскільки ціна такого заходу порівняно невелика. Такий захід пред'являє підвищені вимоги до процесів управління ключами та сертифікатами шифрування, оскільки при раптовому закінченні терміну дії сертифіката робота сервісу може бути порушена.

3. Видаляти системних користувачів та/або пакети, створені провайдером, з віртуальних серверів. Дуже часто провайдер додає до віртуальних серверів та інших сервісів додаткові облікові записи або програми для забезпечення можливості зручного адміністрування всіх сервісів прямо з консолі управління хмарною інфраструктурою. Тому використання цього заходу потрібне лише у випадку, коли забезпечення конфіденційності є головним пріоритетом (наприклад, у сегменті обробки даних банківських карток).

4. Заборонити на рівні мережевих сегментів публічний доступ до баз даних. З метою уникнення можливості випадкової публікації бази даних в Internet рекомендується використовувати архітектурні обмеження. Наприклад, коли доступ з Internet можливий лише до одного мережного сегменту, в якому заборонено розміщувати бази даних та інші подібні послуги.

5. Моніторинг подій на рівні хмари. З метою своєчасного виявлення порушень вимог щодо публікації баз даних або ознак компрометації облікових записів необхідно контролювати все, що відбувається у хмарній інфраструктурі. Як правило, провайдер надає спеціалізовані сервіси, що дають змогу реалізувати такий моніторинг (наприклад, Cloudtrail або Audit Trails). Всі події з цих сервісів можна експортувати до SIEM та налаштувати там необхідні правила обмеження доступу.

6. Обов'язково використовувати багатофакторну аутентифікацію для доступу до хмари. Цей захід є обов'язковим при використанні хмари, оскільки при компрометації привілейованого облікового запису можна повністю втратити контроль над хмарою і, отже, усіма бізнес-процесами, реалізованими за допомогою хмарних сервісів.

7. Контролювати цілісність контейнерів та ПЗ. Використання принципів безпечної розробки – найважливіший фактор забезпечення необхідного рівня безпеки сучасних веб-сервісів. Оскільки впровадити шкідливий код можна на всіх етапах життєвого циклу ПЗ, дуже важливо забезпечити безпеку коду, починаючи з етапу проектування та розробки та до введення додатка в експлуатацію.

Ризик № 2. Несанкціонована зміна програмного забезпечення. В умовах використання хмарних сервісів дуже важливо забезпечити цілісність програми, від написання первинного коду до запуску цього коду на сервірі. При використанні зовнішніх сервісів з'являються такі додаткові загрози, як внесення несанкціонованих змін у зібрані контейнери та використання шкідливого коду в процесі компіляції. Для мінімізації даного ризику слід забезпечити повний контроль за репозиторієм первинного коду та регістром контейнерів, а також за цілісністю програмного забезпечення протягом усього його життєвого циклу.

Ризик № 3. Доступність хмарного сервісу або ймовірність порушення доступності сервісу (обмеження доступу через санкційні

обмеження, будь-яка інша відмова у наданні послуги з боку провайдера, технічний збій на устаткуванні провайдера) з вини провайдера.

Для мінімізації цього ризику рекомендується вживати наступні заходи.

1. Обов'язкове резервування даних, первинного коду програм та опису інфраструктури в місці, що не залежить від поточного провайдера хмарних сервісів. Якщо виникне ситуація, коли доступ до хмари стане неможливим, це означатиме втрату всього, що знаходиться в хмарі. При цьому для відновлення роботи сервісу на інших ресурсах обов'язково необхідно мати резервну копію даних та первинного коду вживаних сервісів. Якщо ці дані відсутні, то роботу сервісу практично неможливо відновити. Резервні копії необхідно зберігати в незалежному від хмари місці, наприклад, в іншому хмарному сервісі або власному фізичному сервері. Для прискорення процесу відновлення роботи сервісу інших ресурсах рекомендується використовувати підхід "Інфраструктура як код" з обов'язковим резервуванням опису використовуваної інфраструктури.

2. Заборона використання рутового облікового запису для адміністрування. Рутовий обліковий запис – це обліковий запис, який використовувався для реєстрації в хмарному сервісі. Він має найширші права, і якщо його втратити, то буде вкрай складно відновити контроль над хмарою. Тому рекомендується максимально знизити ризик компрометації такого облікового запису, що виникає при використанні його для адміністрування або виконання інших задач.

3. Моніторинг повідомлень від провайдера про технічне обслуговування або деградацію обладнання. Провайдер досить часто здійснює технічне обслуговування обладнання, іноді це пов'язано, наприклад, з деградацією жорстких дисків. Буває, що для проведення робіт провайдеру потрібно вимкнути сервіс. Як правило, він попереджає про це, щоб можна було оперативно перейти на резервне обладнання. Але якщо ігнорувати повідомлення провайдера, то можлива ситуація, коли сервіс перестане працювати через те, що ключовий сервер раптом вимкнувся.

4. Окремі організаційні підрозділи (Organizational Units) для адміністраторів, фахівців з безпеки, тестувальників, розробників та основної інфраструктури. Розділяти функціонал важливо як мінімум з двох причин. Насамперед, інфраструктура, що використовується для розробки або тестування, дуже часто змінюється, а нижчі вимоги безпеки підвищують можливість компрометації сервісів або облікових записів. Тому відділення цих сегментів від виробничого дозволить мінімізувати вплив даних сегментів на роботу сервісу. Щодо відділення функцій безпеки в окремий сегмент, то це насамперед необхідно для забезпечення безпеки журналів аудиту.

Ризик № 4. Висока вартість. Простота та швидкість виділення ресурсів у хмарі – незаперечна перевага такого підходу. Це дозволяє

швидко масштабувати послуги зі збільшенням кількості запитів від клієнтів. З іншого боку, важливо пам'ятати, що не обмеження виділення ресурсів призведе до значного росту вартості використовуваних ресурсів. Особливо гостро проблема необмеженого масштабування проявляється під час DDoS-атак. Якщо сервіс намагатиметься обробити всі запити, то це призведе до того, що вартість ресурсів перевищить можливі межі, а бази даних будуть забиті марною інформацією.

Важливо звернути увагу на ефективність використання ресурсів. Якщо, наприклад, були орендовані потужні сервери, які завантажені менш ніж на 10%, це також призведе до зниження прибутку.

Для мінімізації можливих наслідків слід:

– лімітувати сервіси, що масштабуються (як правило, всі хмарні послуги виділяють ресурси в рамках квот, тому достатньо вказати такі значення квот на ресурси, вартість яких буде прийнятною);

– використовувати засоби захисту від атак на прикладному рівні (ця вимога є обов'язковою як мінімум з двох причин: по-перше, запити від зловмисників не приносять жодного доходу, отже, немає сенсу витрачати ресурси на їх обробку, по-друге, відсутність захисту на прикладному рівні істотно підвищує ризик успішної атаки на сервіс. При цьому можливі різні варіанти реалізації захисту на прикладному рівні, починаючи від опенсорсного або промислового міжмережевого екрану програмного рівня та закінчуючи сервісами очищення трафіку);

– контролювати завантаження віртуальних серверів (при оренді віртуального сервера сплачується його вартість. Отже, чим менш завантажений сервер, тим дорожче в результаті обходиться його експлуатація. Дані щодо використання ресурсів можна отримати із логів операційної системи сервера).

Список використаних джерел.

1. Tari, Z. Security and Privacy in Cloud Computing. IEEE Cloud Comput. 2014, 1, 54–57.

2. Mollah, M.B.; Azad, M.A.K.; Vasilakos, A. Security and privacy challenges in mobile cloud computing: Survey and way ahead. J. Netw. Comput. Appl. 2017, 84, 38–54.

3. Abdulsalam, Y.S.; Hedabou, M. Decentralized Data Integrity Scheme for Preserving Privacy in Cloud Computing. In Proceedings of the 2021 International Conference on Security, Pattern Analysis, and Cybernetics (SPAC), Chengdu, China, 18–20 June 2021; pp. 607–612.

4. Sgandurra, D.; Lupu, E. Evolution of attacks, threat models, and solutions for virtualized systems. ACM Comput. Surv. 2016, 48, 1–38.

5. Subramanian, N.; Jeyaraj, A. Recent security challenges in cloud computing. Comput. Electr. Eng. 2018, 71, 28–42.

6. Cook, A.; Robinson, M.; Ferrag, M.A.; Maglaras, L.A.; He, Y.; Jones, K.; Janicke, H. Internet of cloud: Security and privacy issues. In Cloud Computing for Optimization: Foundations, Applications, and Challenges; Springer: New York, NY, USA, 2018; pp. 271–301.

7. Zhang, Y.; Xu, C.; Lin, X.; Shen, X.S. Blockchain-based public integrity verification for cloud storage against procrastinating auditors. IEEE Trans. Cloud Comput. 2019, 9, 923–937.

ДОСЛІДЖЕННЯ МОЖЛИВОСТЕЙ ВИКОРИСТАННЯ ВИПАДКОВИХ СИГНАЛІВ В ЗАДАЧАХ ПОШУКУ ПРИСТРОЇВ НЕСАНКЦІОНОВАНОГО ЗНІМАННЯ ІНФОРМАЦІЇ

Загута Є.А., к.т.н., доц. Горелов Д.Ю.
Харківський національний університет радіоелектроніки,
кафедра КРіСТЗІ, м. Харків, Україна
e-mail: yevhenii.zahuta@nure.ua

Abstract. The purpose of thesis is theoretical study of the structure of the response of a nonlinear diffuser under the action of random RF signal of a nonlinear radar to ensure the effective identification of the latter.

Однією з найскладніших задач у галузі технічного захисту інформації є пошук закладних пристроїв, які не використовують радіоканал для передачі інформації, а також радіозакладок, що перебувають у неактивованому стані. Такі традиційні засоби виявлення, як панорамні радіоприймачі, аналізатори спектру або детектори поля, у цьому випадку виявляються неефективними. Нелінійний радіолокатор дозволяє визначати наявність, стан та природу об'єктів за рахунок використання явищ нелінійного відбиття (розсіювання) радіохвиль цими об'єктами. Серед реальних об'єктів нелінійні властивості найсильніше виражені у напівпровідникових переходів та контактів метал-оксид-метал (МОМ), що виникають в результаті корозії, апроксимуються багаточленом третього ступеня.

Схема математичного експерименту: передавач локатора випромінює випадковий сигнал $x(t)$ з заданими характеристиками (гаусова випадкова величина з математичним сподіванням $m = 0.5$ та СКВ $\sigma = 1.67$, об’єм значень випадкової величини складає 2000). Випромінений сигнал впливає на нелінійний елемент, перевипромінюється і приймається антеною приймача локатора, причому характеристики сигналу перетворюються у відповідності до вольт-амперної характеристикою нелінійного елемента. У якості нелінійних елементів розглядались напівпровідниковий діод з квадратичною вольт амперною характеристикою (ВАХ), структура МОМ з кубічною характеристикою та тунельний діод з поліноміальною ВАХ. У якості моделі миттєвих значень шумового сигналу було використано випадкову величину з рівномірною густиною ймовірності в діапазоні $[0; 1]$, об’єм значень випадкової величини складав 2000. Моделювання складалось зі 100 чисельних експериментів.

Дія випадкового процесу на нелінійне коло призводить до зміни форми його густини ймовірності, тому в першому дослідженні порівнювались коефіцієнти асиметрії та ексцесу. Оскільки кожен експеримент було проведено 100 раз, то були побудовані гістограми

моментів випадкового процесу. Аналіз гістограм коефіцієнту асиметрії та коефіцієнту ексцесу дозволяє виробити наступне вирішальне правило:

$\begin{cases} As(z(t)) \le 0.5 \\ Es(z(t)) \le 0.3 \end{cases}$	Нелінійності немає	Ймовірність пропуску нелінійного елементу 0%
$\begin{cases} 0.5 \le As(z(t)) \le 1.2 \\ 0.3 \le Es(z(t)) \le 2.1 \end{cases}$	Присутня нелінійність типу напівпровідниковий діод	Ймовірність виявлення нелінійного елементу 100%; ймовірність пропуску нелінійного елементу 0%; ймовірність хибної тривоги, тобто реєстрація МОМ структури 5%; ймовірність хибної класифікації, тобто пропуск тунельного діода 6%
$\begin{cases} As(z(t)) \ge 1.2 \\ 2.1 \le Es(z(t)) \le 10 \end{cases}$	Присутня нелінійність типу «метал-окисел-метал»	Ймовірність виявлення нелінійного елементу 100%; ймовірність пропуску нелінійного елементу 0%; ймовірність пропуску цілі, тобто пропуск напівпровідникового діода 0%; ймовірність пропуску цілі, тобто пропуск тунельного діода 38%
$\begin{cases} As(z(t)) \text{ } будь-який \\ Es(z(t)) \ge 10 \end{cases}$	Присутня нелінійність типу тунельний діод	Ймовірність виявлення нелінійного елементу 100%; ймовірність пропуску нелінійного елементу 0%; ймовірність хибної тривоги, тобто реєстрація МОМ структури 3%; ймовірність хибної класифікації, тобто пропуск напівпровідникового діода 0%

Дія випадкового процесу на нелінійне коло призводить до зміни форми його спектральної густини середньої потужності, тому в другому дослідженні порівнювались спектрально-кореляційні властивості відбитих сигналів. Аналіз гістограм коефіцієнтів кореляції Пірсона зондувального сигналу з сигналом, відбитим від лінійного об'єкту, напівпровідникового діода, МОМ-структури та тунельного діода дозволяє виробити наступне вирішальне правило:

$$\text{якщо } R(s(t), z(t)) \ge 0.97 \implies \text{нелінійність відсутня,}$$
$$\text{якщо } 0.93 \le R(s(t), z(t)) \le 0.97 \implies \text{напівпровідниковий діод,}$$
$$\text{якщо } 0.85 \le R(s(t), z(t)) \le 0.93 \implies \text{МОМ} - \text{структура,}$$
$$\text{якщо } R(s(t), z(t)) \le 0.4 \implies \text{тунельний діод.}$$

Аналіз гістограм нормованої ефективної ширини спектру відбитих сигналів дозволяє виробити наступне вирішальне правило:

$$\text{якщо } \Delta F(z(t)) \le 1.1 \implies \text{нелінійність відсутня,}$$
$$\text{якщо } \Delta F(z(t)) \ge 1.4 \implies \text{МОМ} - \text{структура,}$$
$$\text{якщо } 1.1 \le \Delta F(z(t)) \le 1.4$$
$$\implies \text{напівпровідниковий або тунельний діод}$$

ІНФОРМАЦІЙНА БЕЗПЕКА ДІЯЛЬНОСТІ У ДИСТАНЦІЙНОМУ ФОРМАТІ

Литвиненко О.В., к.т.н., доц. Горелов Д.Ю.
Харківський національний університет радіоелектроніки,
кафедра КРіСТЗІ, м. Харків, Україна
e-mail: oleksandr.lytvynenko@nure.ua

Abstract. The subject of the study is methods for increasing the level of cybersecurity of user activities in remote mode.

У 2020 р. державні та комерційні компанії по всьому світу були змушені оперативно переводити багатьох співробітників на віддалену роботу, що призвело до масового використання найбільш очевидних заходів захисту – міжмережевого екранування та двофакторної аутентифікації. Таким чином, ігнорувалося багато актуальних загроз безпеці.

1. Загрози перехоплення облікових даних, що вводяться в ізольованому середовищі.

Одним із заходів захисту інформації при організації віддаленої роботи у випадку, якщо співробітник використовує особистий пристрій, є віртуалізація робочих місць та публікація програм на термінальному сервері з подальшою ізоляцією середовища.

Справді, якщо на власному пристрої співробітника буде встановлено шкідливе програмне забезпечення, воно не зможе впливати на робоче середовище або робочі програми.

Однак навіть якщо і для найвіддаленішого підключення використовується альтернативна автентифікація, у разі підключення до віртуалізованого робочого місця (VDI) та термінального додатка (наприклад, за RemoteApp) висока ймовірність того, що програма вимагатиме авторизації за допомогою логіну та паролю. У такому разі шкідливе програмне забезпечення може перехопити натискання клавіш, обчислити коректне поєднання «логін-пароль», і зловмисник вже по іншому каналу зможе отримати доступ до конфіденційних даних.

Для нейтралізації цієї загрози рекомендується використовувати рішення класу Single Sign-On (SSO) спільно з рішеннями альтернативної посиленої аутентифікації. Рішення SSO має бути встановлене на офісних робочих місцях, до яких співробітник підключається з VDI, або на термінальному сервері. Далі для підтвердження аутентифікації в корпоративних додатках система вимагатиме пред'явлення альтернативного фактора аутентифікації, після чого SSO самостійно надасть ресурсу необхідні облікові дані.

Таким чином, на особистій робочій станції навіть за наявності кейлоггера не перехоплюються логіни та паролі, що вводяться.

2. Загрози порушення доступності корпоративних ресурсів.

2.1. Дистанційне блокування облікових даних.

Найчастіше для доступу до корпоративних ресурсів використовуються публічні веб-сервіси, доступні через Інтернет, наприклад, веб-клієнт пошти.

Часто ім'я поштової скриньки збігається з ім'ям доменного облікового запису. Зловмисник може спробувати розгадати пароль шляхом підбору. Для нейтралізації цієї загрози включається блокування облікового запису після кількох невдалих спроб введення пароля.

Однак зловмисник може перебирати паролі для цілеспрямованого блокування доменного облікового запису. Така атака може призвести до часткового паралічу деяких бізнес-процесів.

З метою часткової нейтралізації цієї загрози можна скористатися спеціалізованим рішенням для двофакторної аутентифікації (2FA), наприклад, одноразовими паролями. При цьому навіть якщо здійснюється спроба перебору, буде заблоковано другий аутентифікатор, а не обліковий запис.

Таким чином, співробітник збереже можливість отримання доступу до корпоративних ресурсів, щоправда, лише через альтернативне з'єднання або при локальній роботі.

2.2. Втрата чи поломка захищеного носія ключової інформації.

Виконуючи робочі обов'язки, віддалені співробітники можуть користуватися цифровими сертифікатами, наприклад, для підпису документів або підключення до сторонніх веб-сервісів. При цьому у разі втрати або поломки пристрою з'являється задача його оперативної заміни, яка не зможе бути реалізована, особливо якщо співробітник територіально віддалений від офісу.

Для нейтралізації загрози можна скористатися спеціалізованими рішеннями, що реалізують віртуальну смарт-картку (тобто без зберігання ключової інформації на захищеному пристрої, що знімається).

У такому разі зберігання ключової інформації здійснюватиметься у таких контейнерах: 1) на серверній стороні всі операції з ключами виконуються на сервері; 2) контейнер у спеціалізованому модулі всередині пристрою – Trusted Platform Module.

Використання подібних рішень вважається менш безпечним, ніж знімні захищені апаратні носії, проте ці рішення найбільш гнучкі і підходять для описаної нештатної ситуації. Після заміни ключового носія можна відключити віртуальну смарт-карту.

Таким чином, навіть у разі втрати чи поломки ключового носія простою у бізнес-процесах компанії не буде.

3. Загрози відмовлення від авторства дій, які призвели до інциденту.

3.1. Спірні ситуації у разі збою критичного ресурсу.

За будь-якої роботи з IT-ресурсами з боку привілейованих користувачів завжди існує ризик помилок через людський фактор. Самі дії можуть призвести до збою критичного ресурсу.

Навіть при роботі безпосередньо в приміщенні організації буває складно розібратися, що сталося і хто є відповідальним за збій. У разі віддаленого доступу ситуація ускладнюється багаторазово. Подібні розбори інцидентів не лише негативно впливають на робочу атмосферу, коли відбуваються спроби звинуватити невинних, а й витрачають багато часу фахівців на непродуктивні дії.

Використання SIEM дозволить дізнатися, хто підключався до ресурсу, але навряд чи дозволить точно визначити відповідального, не кажучи вже про відсутність даних про послідовність дій, які спричинили збій.

Однак при використанні рішень класу Privileged Access Management (PAM) всі підключення привілейованих користувачів до критичних ресурсів фіксуються у різних форматах (відео- та текстовий запис, знімки екрана, натискання клавіш, передані файли). Далі, використовуючи записи дій, можна оперативно визначити, яка послідовність дій призвела до збою, виявити відповідального за інцидент і визначити чинник навмисності.

3.2. Спроба уникнути відповідальності.

Бувають ситуації, коли в компанії працює інсайдер – внутрішній зловмисник, який цілеспрямовано здійснив дії, що спричинили збій або порушення роботи критичного ресурсу. Саме собою завдання виявлення відповідального вже є складним, проте з допомогою рішення класу PAM можна оперативно знайти винного.

При спробі притягти співробітника до відповідальності, він може сказати, що у нього були вкрадені відповідні дані для доступу до його облікового запису. Ні для кого не секрет, що парольна автентифікація дуже вразлива для загрози розголошення, а сам факт розголошення може бути виявлений після інциденту.

Очевидно, що в такій ситуації будь-який керівник може замислитися про те, що співробітник справді невинний, а те, що сталося, – просто невдалий збіг обставин.

Для нейтралізації цієї загрози рекомендується спільно з рішенням PAM використовувати рішення для 2FA співробітників. Тоді, якщо співробітник дійсно є інсайдером і мав місце інцидент, йому буде важко уникнути відповідальності. Якщо все-таки співробітник заявить, що у нього вкрали телефон, на якому стоїть генератор одноразових паролів, йому буде поставлене логічне запитання: "Чому ви оперативно не повідомили про це службу безпеки?"

РОЗШИРЕННЯ ФУНКЦІОНАЛУ SIEM СИСТЕМ

Мінін Д.О., к.т.н., доц. Горелов Д.Ю.
Харківський національний університет радіоелектроніки,
кафедра КРіСТЗІ, м. Харків, Україна
e-mail: dmytro.minin@nure.ua

Abstract. The subject of the study is undeclared capabilities of Security information and event management systems.

Багато компаній використовують SIEM-системи для виявлення інцидентів інформаційної безпеки різного ступеня складності і часто навіть не уявляють усі можливості власної системи моніторингу. Це пов'язано з тим, що співробітники відділу інформаційної безпеки часто не замислюються над додатковими функціями та можливостями, хоча ці знання могли б істотно допомогти в автоматизації цілого ряду процесів у відділі інформаційної безпеки (ІБ) або всієї компанії в цілому.

До основних таких недекларованих можливостей відносяться:

1) запуск зовнішніх скриптів та програм;
2) використання скорингової моделі;
3) застосування нейромереж для виявлення інцидентів ІБ.

Запуск зовнішніх скриптів і програм. Використовується, наприклад, для:

1) сканування хоста, у якому стався інцидент інформаційної безпеки;
2) запису в сторонні ресурси інформації про інцидент;
3) реалізація команд на віддаленій системі з метою виконання дій над користувачем або вузлом, що фігурує в інциденті ІБ.

Розглянемо докладніше перший сценарій – сканування хоста – і розглянемо ситуацію, при якій відбувається інцидент, пов'язаний зі спробами нелегітимних дій щодо очищення журналу аудиту та/або створення адміністративної групи на Linux-системі. При виявленні цієї події запускається скрипт збору з вузла додаткової інформації, пов'язаної з користувачем або групою. Результати роботи скрипта повертаються назад до SIEM-системи для фіксації всієї отриманої інформації про користувача або групи. Якщо інцидент призводить до його появи в системі управління інцидентами (Case Manager), то аналітику з ІБ буде набагато простіше прийняти рішення про критичність даного інциденту.

За такої реалізації робота вирішального правила про сканування хоста стає максимально продуктивною. Але варто враховувати той факт, що всі правила, які здійснюють запуски зовнішніх команд, повинні пройти етапи тестування та налагодження для мінімізації помилкових спрацьовувань та оптимізації завантаження системи. Для цього у SIEM-системі створюються механізми автоматичної перевірки коректності роботи правил та частоти їх спрацьовувань.

Використання скорингової моделі. Часто словосполучення "скорингова модель" асоціюється з антифрод-системами та боротьбою з фінансовими шахраями. Але реалізація скорингової моделі в інформаційній безпеці та SIEM-системі наразі є тією необхідністю, без якої повнота картини виявлення інцидентів ІБ не буде вичерпною.

Для використання складних кореляційних логік та виявлення складних ланцюжків інцидентів необхідно реалізовувати скорингову модель для підрахунку балів по кожному користувачеві та вузлу, що бере участь в інцидентах ІБ.

Так, наприклад, при спрацьовуванні правила Brute Force проводиться занесення до списку підрахунку скорингу як користувача, так і хоста, у якому відбувається спроба підбору пароля. При фіксації ряду інцидентів з користувачем або вузлом, що перебувають у аркуші скорингу, сумарний бал підвищується залежно від критичності інциденту. Таким чином, підсумовуючи бали за кожен інцидент, можна наочно оцінювати картину того, що відбувається, а також у разі реалізації додаткових механізмів можна контролювати інциденти, що відбуваються, і накладати на життєвий цикл кібератак Kill Chain з наступною класифікацією за MITRE.

Розглянемо наступний приклад. Створюється два списки (аркуші) з назвами User List та Host List:

– поля у User List – користувач, скоринг, дата;

– поля Host List – вузол, скоринг, дата.

Додаються до правил, що виявляють інциденти ІБ, дії щодо занесення користувача або хоста у відповідний лист, а також скорингове значення. Таким чином, у разі виявлення інцидентів у аркуші додається інформація про користувачів та хостів, що фігурують в інцидентах, а також підраховується скоринг по кожному користувачеві та хосту.

Такими діями можна створити додатковий механізм аналізу та можливості зміни критичності виявлення інцидентів, пов'язаних з тим чи іншим хостом або користувачем. У разі грамотно побудованої моделі можна активно реагувати на будь-які інциденти з ІБ.

Застосування нейромереж. Наразі все більший оборот набирає використання математичних моделей у сфері інформаційної безпеки, одним із прикладів яких є нейромережі.

Пропонується використовувати потужності SIEM-систем для генерації частини наборів даних для навчання нейромережі та мінімізації трудовитрат фахівців зі збирання та аналізу даних. Архітектура побудови інтеграції полягає в налаштуванні SIEM-системи в частині правил кореляції, мінімізації їх хибних спрацьовувань та подальшому вивантаженні кореляційних подій на набір даних (dataset) через шину даних. Для наочності розглянемо наступний приклад.

1. Треба навчити математичну модель для аналізу доменів третього рівня щодо наявності ряду артефактів, які можуть бути в запиті (наприклад

довжина доменного імені третього рівня понад 20 символів є підозрілою; не людино-читані слова в доменному імені є додатковою ознакою аномалії; фіксація доменного імені у репутаційних базах – ознака інциденту ІБ).

2. Здійснюється підключення DNS до SIEM та налаштування правил кореляції на виявлення довжини доменів третього рівня, у разі перевищення довжини запиту список доменів міститься в аркуші.

3. Аркуш відправляється на API лінгвістичного аналізу для отримання семантичного коефіцієнта розпізнання імені домену.

4. Як додатковий захід здійснюється надсилання запиту на платформу Threat Intelligence для аналізу доменного імені.

Таким чином, можна отримати багаторівневу систему аналізу доменних імен та складання списків "нормальних" та "ненормальних" імен для подальшого завантаження в набір даних (dataset).

Основна ідея цього прикладу полягає у демонстрації необхідності застосування автоматичних інтеграцій із сервісами, які можуть зменшити час підготовки набору даних для навчання моделі та заощадити ресурси фахівців DS/DM.

Зростання ефективності.

У докладі на конкретних прикладах було продемонстровано недекларовані можливості, що використовуються в SIEM-системах, і те, як вони дозволяють підвищити ефективність ситуаційного центру ІБ у цілому. Необхідність автоматизації процесів обробки інцидентів ІБ є одним із наріжних каменів у роботі будь-якого підрозділу захисту інформації. Щоб ефективно керувати системами моніторингу подій ІБ, необхідно перципувати (сприймати) і вміти використовувати весь спектр можливостей SIEM-систем.

Список використаних джерел.

1. Обзор решений SIEM (Security information and event management). Режим доступу: https://habr.com/ru/company/roi4cio/blog/528770/ (дата звернення 11.01.2022).

2. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. Режим доступу: https://www.manaraa.com/Book/174707/security-information-and-event-management-(siem)-analysis-tr (дата звернення 11.01.2022).

3. Evaluation of Local Security Event Management System vs Standard Antivirus Software. Режим доступу: https://www.mdpi.com/2076-3417/12/3/1076/htm (дата звернення 11.01.2022).

ПОРІВНЯЛЬНИЙ АНАЛІЗ ТРАДИЦІЙНИХ БІОМЕТРИЧНИХ МЕТОДІВ КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПОМ

Леушина А.А., к.т.н., доц. Горелов Д.Ю.
Харківський національний університет радіоелектроніки,
кафедра КРіСТЗІ, м. Харків, Україна
e-mail: anastasiia.leushyna@nure.ua

Abstract. The research in thesis described the novel comparison based upon various aspects to make easy selection for biometric device deployment in specific environment. Proposed a comparison among all kind of biometric system available in the society.

Відповідно до дослідження «Global biometric system market revenue forecast from 2017 to 2022» [1] на світовому ринку біометричних систем активно застосовуються технології, засновані на розпізнаванні та використанні наступних біометричних даних: відбитки пальців (non-AFIS); зображення райдужної оболонки ока; геометрія долоні; зображення обличчя; рисунок вен долоні; відбитки пальців (AFIS); голос; рукописний та клавіатурний почерк.

Кожна біометрична технологія має свої переваги і недоліки, тому безпосередньо їх порівнювати складно. Дослідники визначають кілька факторів для подібного порівняння [2-3]: унікальність, стабільність, універсальність, вимірюваність, порівняльність, стандартність, інвазивність, продуктивність, прийнятність, стійкість, конфіденційність, вартість, новітність, популярність, простота використання, швидкість обробки, точність (FAR, FRR та EER), розмір біометричного шаблону, технологія побудови біометричного сканера, стабільність біометричної характеристики, ймовірність відмови реєстрації біометричного зразка, ймовірність того, що біометрична система не виявить біометричні дані при правильному їх представленні.

Згідно проведеного аналізу ідентифікація за геометрією обличчя має не найкращі інтегральні показники серед статичних біометричних технологій. Проте, основні недоліки цього методу відносяться технічних показників – швидкості обробки, розміру біометричного шаблону та точності ідентифікації. Зі зростанням потужності обчислювальної здатності біометричних систем ці показники також будуть зростати, що демонструє сучасна картина біометричного ринку. У 2021 р. одразу декілька європейських столиць впровадили тестові системи оплати проїзду у метро за допомогою FaceId. Крім того, системи ідентифікації за FaceId легко можуть бути інтегровані у вже існуючі системи відео спостереження. Також перспектив використання цієї технології можна додати зручність у користуванні (оскільки можна так розмістити камери, що від людини взагалі не вимагається жодних дій), можливість проведення скритного та

неперервного моніторингу, а також легку інтеграцію з іншими біометричними модальностями у мультибіометричні системи.

Технологія ідентифікації за відбитком пальця non-AFIS має більші перспективи ніж райдужна оболонка ока та малюнок вен. Наразі основними недоліками технології є: порівняно невисока точність, порівняно невисока стійкість до зламу, неможливість функціонування у запилених приміщеннях, не сприйняття технології з-за «дактилоскопічного минулого». Перші два недоліки будуть подолані впродовж декількох років. Наразі стандартною роздільною здатністю FingerPrint сканерів є 200 точок на квадратний дюйм та побудова біометричного зразка за 12-14 мінуціями. Використання сканерів з роздільною здатністю 1000 точок на квадратний дюйм дозволить враховувати до 40 мінуцій, тим самим значно покращити точність технології. Використання ультразвукових сканерів замість оптичних дозволить не тільки отримувати тримірні зображення пальця (тим самим захистити від класичного зламу за допомогою скотчу), а й реєструвати в процесі сканування мікрорухи шкіри пальця, викликані звані кровотоком (тим самим реєструвати отримання біометричного зразка від живої людини, а не предмету з нанесеним на нього папілярним візерунком). Використання високошвидкісних камер дозволить здійснювати безконтактне сканування одразу декількох пальців, що дозволить будувати мультизразкові біометричні системи. Подальший зріст користувачів смартфонів з вбудованими сканерами відбитка пальця буде, по-перше, створювати умови для здешевлення технології, по-друге, зменшенню людей, що не сприймають дану технологію з-за її «дактилоскопічного минулого».

Жоден динамічний метод не може бути використаний у якості основної технології біометричної ідентифікації. Їх задача – збільшити точність ідентифікації за рахунок допоміжного алгоритму у мультибіометричних системах. З огляду на тенденції розвитку телекомунікаційних технологій голос залишиться тільки у сфері онлайн банкінгу та IoT за стосунках. Рукописний текст трансформується у підпис комп’ютерною мишкою і разом з клавіатурним почерком знайде своє місце у UEBA системах.

Найменші перспективи до розвитку має ідентифікація за геометрією долоні. Низькі точність і стабільність не можуть бути покращені за рахунок нових технологій сканування чи побудови біометричних зразків.

Список використаних джерел.

1. Global biometric system market revenue forecast from 2017 to 2022, by technology.

2. P. Tripathi. A Comparative Study of Biometric Technologies with Reference to Human Interface. International Journal of Computer Applications (IJCA), vol. 14, no. 5, 2011.

3. Padma Manivannan. Comparative and Analysis of Biometric Systems. International Journal on Computer Science and Engineering (IJCSE,) vol. 3, no. 5, pp. 2156-2162, 2011.

ПОРІВНЯЛЬНИЙ АНАЛІЗ ПЕРСПЕКТИВНИХ БІОМЕТРИЧНИХ МЕТОДІВ КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПОМ

Леушина А.А., к.т.н., доц. Горелов Д.Ю.
Харківський національний університет радіоелектроніки,
кафедра КРіСТЗІ, м. Харків, Україна
e-mail: anastasiia.leushyna@nure.ua

Abstract. The research in thesis described the novel comparison based upon various aspects to make easy selection for biometric device deployment in specific environment. Proposed a comparison among all kind of biometric system available in the society.

Огляд наукових та науково-популярних джерел з біометричної ідентифікації дозволяє виділити наступні перспективні технології: ідентифікація за структурою поту на пальцях; ідентифікація за рухами губ; ідентифікація за запахом; ідентифікація за мікровібраціями пальців; ідентифікація за геометрією серця або за параметрами серцебиття; ідентифікація за термограмою обличчя; ідентифікація за формою вушної раковини; ідентифікація за динамічними параметрами ходи; ідентифікація за акустичним відгуком середнього вуха; ідентифікація за біоакустичними параметрами долоні; ідентифікація власників смартфонів за особливостями взаємодії з пристроєм; ідентифікація за геометрією носа; ідентифікація користувачів комп'ютерних мереж за особливостями взаємодії з програмним забезпеченням; ідентифікація за динамічними параметрами електроенцефалограми; RFID ідентифікація за допомогою імплантованих біочіпів; мультимодальна ідентифікація.

Якщо з зазначених вище біометричних технологій контролю та управління доступом у якості перспективних вибрати лише ті, що наразі представлені у вигляді тестових макетів та можуть у майбутньому широко використовуватись у приватних та комерційних рішеннях, то залишаються наступні: ідентифікація за рухами губ; ідентифікація за параметрами серцебиття; ідентифікація за термограмою обличчя; ідентифікація за формою вушної раковини; ідентифікація за динамічними параметрами ходи; ідентифікація за біоакустичними параметрами долоні; ідентифікація власників смартфонів за особливостями взаємодії з пристроєм; ідентифікація за геометрією носа; ідентифікація користувачів комп'ютерних мереж за особливостями взаємодії з програмним забезпеченням; RFID ідентифікація за допомогою імплантованих біочіпів; мультимодальна ідентифікація.

Ідентифікація за структурою поту на пальцях та ідентифікація за запахом можуть забезпечити високу точність, але не зможуть отримати великого розповсюдження через високу чутливість до зовнішніх факторів. Ідентифікація за мікровібраціями пальців скоріш за все в у майбутньому

стане частиною ультразвукових сканерів відбитка пальця, як додаткова модальність. Ідентифікація за акустичним відгуком середнього вуха та ідентифікація за динамічними параметрами електроенцефалограми знову ж мають високу точність ідентифікації людини, проте не відповідають умові широкого та зручного використання.

Ідентифікацію за рухами губ, за геометрією носа, за формою вушної раковини та за динамічними параметрами ходи можна віднести до технологій середньої точності. Проте вони дуже легко інтегруються с ідентифікацією за геометрією обличчя, виступаючи додатковою модальністю, і можуть значно підвищити точність біометричної системи, особливо в сценаріях, коли забезпечити відео-зйомку облич анфас неможливо.

Аналогічно ідентифікація за параметрами серцебиття, за біоакустичними параметрами долоні та ідентифікація власників смартфонів за особливостями взаємодії з пристроєм також забезпечують середню точність, проте легко інтегруються, навіть за сучасного стану розвитку мобільних технологій, у смартфони. Таким чином, ідентифікацію за відбитком пальця або FaceId можна використовувати для розблокування смартфону, а зазначені технології ідентифікації забезпечать неперервну ідентифікацію власника смартфона.

Ідентифікація за термограмою обличчя забезпечує вискоку точність ідентифікації та може використовуватись як одно модальних біометричних системах. Єдина перешкода на шляху масового поширення технології – досить вартісні інфрачервоні тепловізійні відеокамери.

Ідентифікація користувачів комп'ютерних мереж за особливостями взаємодії з програмним забезпеченням вже зараз широко використовується в системах User and Entity Behavior Analytics з метою виявлення кіберзагроз. З плином часу кількість подібних систем на ринку буде тільки зростати.

RFID ідентифікація за допомогою імплантованих біочіпів наразі також широко використовується в приватних цілях. Питання декількох років – і цю технологія з переліку «перспективних» перейде до переліку «традиційних».

Мультимодальній ідентифікації відповідає найвищий рівень точності, оскільки використовується кілька біометричних технологій ідентифікації людини. Оскільки наразі головними вимогами до біометричних систем є точність, зручність і максимальний захист від зламу в перспективі усі біометричні системи будуть мультимодальними.

Список використаних джерел.

1. Advanced Biometrics. David Zhang,Guangming Lu,Lei Zhang. Springer International Publishing, 2018.

2. Biometrics: Concepts, Methodologies, Tools, and Applications. Information Resources Management Association. 2016.

ПІДВИЩЕННЯ НАДІЙНОСТІ БІОМЕТРИЧНИХ ПАСПОРТІВ ЗА РАХУНОК ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТРИХОВОГО КОДУВАННЯ

Пилявських Є.А., к.т.н., доц. Горелов Д.Ю.
Харківський національний університет радіоелектроніки,
кафедра КРіСТЗІ, м. Харків, Україна
e-mail: yevhenii.pyliavskykh@nure.ua

Abstract. An algorithm for receiving and processing facial biometric information directly from a face image and a method for recording them in the structure of QR-codes are proposed.

Серед застосувань штрихового кодування інтерес представляють системи біометричної ідентифікації. Це обумовлено тим, що біометричні технології можуть забезпечити точну перевірку аутентичності людини, а технології штрихового кодування забезпечують автоматизацію всіх біометричних процесів, уніфікацію, каталогізацію і захист документів (наприклад, посвідчень особи) від прямого доступу до них, а також безпомилковий обмін даними по стандартним каналам зв'язку.

Особливої важливості задача поєднання біометрії та штрих-кодів надбала в останні роки з широким впровадженням біометричних паспортів. Складовою частиною будь-якого біометричного паспорта є RFID-чіп, у якому записані особисті дані людини. Це може бути фотографія власника паспорта в Австралії, Великій Британії, Канаді та США, або один / кілька відбитків пальця в країнах Шенгенської угоди.

Надійність біометричних паспортів викликає певні побоювання, оскільки в мережі Internet можна знайти емулятори е-паспортів, а просканувати та скопіювати дані з RFID-чіпу – ще простіше. З цього погляду штрих-коди більш захищені, оскільки нічого не випромінюють і можуть мати дуже малі розміри.

В роботі пропонується алгоритм поєднання технологій штрихового кодування та лицьової біометрії.

Серед різноманіття цифрових методів антропометрії обличчя з урахуванням, по-перше, використання мінімального обсягу інформації для опису геометрії обличчя (обмежений об'єм даних, що можна помістити у штрих-код) і, по-друге, вимоги мінімальних обчислювальних витрат з метою ідентифікації онлайн та за допомогою мобільних пристроїв, було обрано координати антропометричних точок обличчя та фенотип обличчя.

В такому разі алгоритм представлення біометричної та документальної інформації в рамках шрих-кодів наступний.

1. Згідно стандартів лицьової біометрії 68 координат антропометричних точок обчислюються по зображенню обличчя, приведеному до розміру 320×240.

2. Складається інформативне поле:

$$ANTRO = 'x1\ x2\ x3 \ldots x68\ \#\ y1\ y2\ y3 \ldots y68'.$$

3. На основі інформативного поля ANTRO формується бінарний (чорно-білий) QR-код QR-ANTRO.

4. Розраховуються значення яскравості (від 0 до 255) для кожної з колірних компонент «red», «green», «blue» кольорового зображення обличчя в координатах антропометричних точок.

5. Складається інформативне поле:

$$PHENO = 'r1\ r2 \ldots r68\ \#\ g1\ g2 \ldots g68\ \#\ b1\ b2 \ldots b68'.$$

6. На основі інформативного поля PHENO формується бінарний (чорно-білий) QR-код QR-PHENO.

7. Складається інформативне поле *INFO*, в якому може міститись додаткова інформація про людину, наприклад, дані, що дублюють інформацію про відбиток пальця у біометричному паспорті, або ж індивідуальні риси обличчя, як-то татуювання, шрами, родимі плями, родимки на обличчі тощо.

8. На основі інформативного поля INFO формується бінарний (чорно-білий) QR-код QR-INFO.

9. Сформовані бінарні коди QR-ANTRO, QR-PHENO і QR-INFO об’єднуються в один кольоровий QR-код. Використання кольорових штрих-кодів вирішує проблему ємності штрих-кодів. Кольорові двовимірні штрих-коди можуть містити три і більше шарів. Наприклад, кольоровий QR-код із трьома шарами є за фактом кольоровим зображенням, кожен шар якого є окремим QR-кодом. Ємність такого коду становить приблизно 21000 буквено-цифрових знаків.

Якщо на паспорті розмістити такий код, то за вкладеною в нього інформацією можна в режимі онлайн на мобільному сканері відновити зображення обличчя людини та порівняти її, по-перше, з фото у паспорті, а по-друге, із самою людиною. Крім того, якщо додати четвертий шар код, що містить зашифрований SHA hash, то можна захистити код від підробки.

Список використаних джерел.

1. Кухарев Г.А., Казиева Н., Цымбал Д.А. Технологии штрихового кодирования для задач лицевой биометрии: современное состояние и нове решения // Научно-технический вестник информационных технологий, механики и оптики. 2018. Т. 18. № 1. С. 72–86.

2. Kaziyeva N., Kukharev G.A., Matveev Y.N. Barcoding in biometrics and its development. Lecture Notes in Computer Science. 2018. Vol. 11114. pp. 464-471.

3. Кухарев Г. А., Матвеев Ю. Н., Щеголева Н. Л. Формирование штрих-кода по изображениям лиц на основе градиентов яркости // Научно-технический вестник информационных технологий механики и оптики, 2014, 90 (3), с. 89-96.

ПРОТОТИПУВАННЯ БЕЗПАРОЛЬНОЇ СИСТЕМИ АУТЕНТИФІКАЦІЇ З ВИКОРИСТАННЯМ ОЗНАК BROWSER FINGERPRINTS

Федотов В.В., к.т.н., доц. Горелов Д.Ю.
Харківський національний університет радіоелектроніки,
кафедра КРіСТЗІ, м. Харків, Україна
e-mail: vitalii.fedotov@nure.ua

Abstract. The scenario of using the Browser Fingerprints collection and analysis system to build a password-free authentication system for web-resource users is proposed.

В останні роки з метою підвищення інформаційної безпеки користувачів у мережі Internet розробляються нові методи ідентифікації з динамічною конфігурацією факторів, що дозволяють ефективно визначити, чи користувач є легітимним.

Одним із підходів до реалізації подібних систем є визначення унікального багатокомпонентного цифрового сліду користувача, що базується на оцінці різних статичних та поведінкових ознак профілю суб'єкта доступу – ознак Browser Fingerprints [1-2]. У межах побудови такого профілю можуть бути використані наступні групи ознак: дані про браузер; дані про операційну систему, апаратне та програмне забезпечення; службова інформація про сеанс користувача – web-сервер; дані про користувача тощо.

Використовувати тільки ознаки Browser Fingerprints для ідентифікації користувачів неможливо з-за порівняно невисокої точності. Так точність ідентифікації за часом відвідування, парою «логін – пароль», IP-адресою користувача, рядком-ідентифікатором UserAgent (містить відомості про назву та версію використовуваного браузера, операційну систему і апаратну платформу комп'ютера, мову використовуваної операційної системи, версію верстки web-сторінки, кодове найменування та версію програмного забезпечення, що перетворює вміст web-сторінок і інформацію про форматування в інтерактивне зображення на екрані), переліком плагінів, що встановлено в браузері, роздільною здатністю екрану в пік селях та списком встановлених шрифтів становила 85 % [3]. Проте аналіз та збір ознак Browser Fingerprints можуть бути використані для створення безпарольних систем аутентифікації. Алгоритм роботи подібної системи може бути наступним.

1. Перевірка IP на предмет знаходження його у внутрішній дозволеній базі IP адрес (white list) або на наявність в базі адрес зловмисників, які використовуються для злому (black list). Якщо буде виявлено небезпеку, то автоматична аутентифікація припиняється.

2. Кожному профілю мережі відповідає ідентифікатор і при вході профіль перевіряється на його існування в каталозі дозволених. Якщо дану відповідність не доведено, то доступ може бути відхилений або ж спрямований на систему багатофакторної аутентифікації. Зловмисники часто створюють нові профілі, щоб можна було легко вписуватися в повсякденний трафік і уникати виявлення. Тому потрібно позначати такі профілі.

4. Аналіз місця розташування користувача. Якщо запит на аутентифікацію надійшов з місця розташування, де у організації немає відомих співробітників, клієнтів або партнерів, то він може бути відхилений або перенаправлений на систему багатофакторної аутентифікації.

4. Аналіз неможливих подій. Якщо доступ був зареєстрований вранці в одній точці країни, а потім через годину зовсім в іншому місці, то система запідозрить зловмисні дії і пере направить користувача на систему багато факторної аутентифікації.

5. Аналіз геолокації. Для забезпечення безпеки можна поставити географічний бар'єр і всі запити ззовні, повинні будуть проходити додаткові етапи підтвердження особистості.

6. Зчитування всіх доступних ознак Browser Fingerprints. Аналіз ознак Browser Fingerprints та ідентифікація за ними користувачів.

7. Аналіз поведінкових шаблонів. З часом у кожного користувача формується унікальний біометричний шаблон. Він створюється на основі взаємодії (апаратної та програмної) користувача зі своїм пристроєм. Ці характеристики так само унікальні, як і відбиток людського пальця. Досить точна імітація зловмисниками подібних нюансів практично неможлива.

Таким чином, через деякий час роботи в подібній системі аутентифікації потреба в паролі відпадає, оскільки він замінюється на індивідуальні користувацькі та поведінкові шаблони. Також створюється додатковий захист, оскільки, після отримання доступу, дії користувача відстежуються, і при відхиленні від еталонного профілю – блокуються.

Список використаних джерел.

1. The Security of HTTP-Headers. Режим доступу: https://www.contextis.com/en/blog/security-http-headers (дата звернення 10.01.2022).

2. Antoine Vastel, Pierre Laperdrix, Walter Rudametkin, and Romain Rouvoy. FP-STALKER: Tracking Browser Fingerprint Evolutions. In IEEE Symposium on Security and Privacy (S&P) (2018-05-21). 728–741.

3. Бессонова Е.Е., Метод идентификации пользователей в сети Интернет с использованием компонентного профиля // Материалы диссертационной работы на соискание ученой степени кандидата технических наук. Санкт-Петербург, 2014. 115 с.

АВТОРСЬКЕ ПРАВО НА КОМП'ЮТЕРНУ ПРОГРАМУ

Леушина А.А., ст. викладач Олейнікова О.І.
Харківський національний університет радіоелектроніки,
кафедра КРіСТЗІ, м. Харків, Україна
e-mail: anastasiia.leushyna@nure.ua

Abstract. This report examines the terms and object of copyright. Inform about an efficient way of protecting a computer program. The theses is exploring benefits of intellectual property protection.

Авторське право – це сукупність прав, які належать автору у зв'язку зі створенням і використанням твору літератури, науки, мистецтва. Авторське право забезпечує захист особистих немайнових і майнових прав авторів [1].

У статті 8 Закону України «Про авторське право і суміжні права» пропонується перелік об'єктів авторського права. До них належать: літературні письмові твори; усні твори у вигляді виступів, лекцій, промов, проповідей; музичні і музично-драматичні твори, у тому числі хореографічного характеру; аудіовізуальні твори, твори образотворчого мистецтва, архітектури, фотографії і твори прикладного мистецтва, ілюстрації, карти, плани, ескізи, пластичні твори, сучасні обробки творів, перекладів, аранжування та інші переробки творів, збірники творів, бази даних, комп'ютерні програми тощо [2].

На даний час, існують три реальні і дієві способи захисту програмного продукту (комп'ютерної програми, сайту, бази даних тощо) від неправомірного використання:

– охороняти вихідний код програми за допомогою авторського права;

– охороняти алгоритми, які використовуються в програмах, як способи вирішення конкретних завдань;

– охороняти назву програми [3].

У ст. 1 Закону України «Про авторське право і суміжні права» наводиться визначення комп'ютерної програми, відповідно до якого комп'ютерна програма – це набір інструкцій у вигляді слів, цифр, кодів, схем, символів чи у будь-якому іншому вигляді, виражених у формі, придатній для зчитування комп'ютером, які приводять його у дію для досягнення певної мети або результату (це поняття охоплює як операційну систему, так і прикладну програму, виражені у вихідному або об'єктному кодах)[4].

Авторське право на комп'ютерну програму, виникає з моменту його створення і обов'язкова реєстрація його не вимагається.

Реєстрація авторського права надає цілий ряд незаперечних переваг, перед незареєстрованими правами. Перш за все, в Україні існує презумпція авторства, відповідно до якої, автором є особа, зазначена як автор на

оригіналі або примірнику твору. Проте, особа, яка має свідоцтво про реєстрацію авторського права, перебуває у значно вигіднішому становищі, на випадок якихось розбіжностей, несподіваних ситуацій чи зловживань. Поряд з цим, буває й таке, що авторське право реєструється з метою привласнення твору (комп'ютерної програми, бази даних тощо) з метою отримання вигоди. На підставі свідоцтва може бути складено ліцензійний договір із особами, зацікавленими використати твір, і автор, якщо вчасно не подбає про захист свого права, залишиться ні з чим. По своїй суті, свідоцтвом про реєстрацію авторського права можна захищатися, як найнадійнішим аргументом у спорі за права володіння програмними продуктами.

Наявність свідоцтва дозволить вільно розпорядитися своїм правом на програмний продукт, базу даних, чи інший твір або делегувати право третій особі. Для отримання матеріальної вигоди, як правило, складається авторський договір, і як обов'язковий додаток до цього виступає свідоцтво про реєстрацію авторського права, що засвідчує авторські права на те, що він передає [3].

Переваги захисту комп'ютерної програми авторським правом:

– простота та доступність охорони;

– авторське право поширюється як на всю програму, так і на її окремі частини;

– строк дії захисту авторським правом досить значний і на практиці значно перевищує строк технічної експлуатації комп'ютерної програми;

– доведення порушення авторського права та визначення розміру компенсації за таке порушення, як правило, є менш складним [5].

Список використаних джерел.

1. Закревська Юлія Олександрівна. Авторське право// URL: https://patentpoltava.com/copyright.html (дата звернення: 17.02.2022).

2. Коссак В. М., Якубівський І. Є. Право інтелектуальної власності: Підручник. — К.: Істина, 2007. — 208 с.

3. Яновський Олексій. Реєстрація і захист прав інтелектуальної властності на комп'ютерну програму// URL: https://zkg.ua/yak-vidbuvajetsya-rejestratsiya-avtorstva-na-kompyuternu-prohramu

4. Закон України «Про авторське право і суміжні права»// URL:https://zakon.rada.gov.ua/laws/show/3792-12#Text

5. Наталія Грушевська. Правова охорона комп'ютерних програм: як правовласнику захистити свої прав а// URL: https://yur-gazeta.com/publications/practice/zahist-intelektualnoyi-vlasnosti-avtorske-pravo/pravova-ohorona-kompyuternih-program-yak-pravovlasniku-zahistiti-svoyi-prava.html (дата звернення: 18.02.2022)

СПОСОБИ МАСКУВАННЯ ТА ВИЯВЛЕННЯ ТЕХНІЧНИХ ЗАСОБІВ ВІДЕОСПОСТЕРЕЖЕННЯ

Гребенчук М.В., ст. викладач Олейнікова О.І.
Харківський національний університет радіоелектроніки,
кафедра КРіСТЗІ, м. Харків, Україна
e-mail: maksym.hrebenchuk@nure.ua

Abstract. This work is devoted to the issue of video surveillance and possible ways to hide video surveillance devices. Below are some of the most popular options based on the research of modern scientists. As the number of atrocities in the world has increased in the 21st century, the world needs to be guarded and protected from terrorism and misconduct. As practice shows, video surveillance devices help to solve this problem.

Протягом останніх років збільшилася кількість випадків воєнних, політичних та соціальних диверсій в Україні. Внаслідок цього безпека громадян стає питанням державного масштабу. Необхідною мірою захисту від несподіваних та незапланованих маніпуляцій, є забезпечення цілодобового чи тимчасового спостереження за режимними об’єктами, громадськими місцями, транспортними сполученнями, військовими і медичними закладами, закладами освіти, тощо.

Більшість людей звикли зустрічати камери відеоспостереження у супермаркетах, державних установах, школах чи університетах, метрополітені. Однак, якщо камер відеоспостереження не було б помітно у видимому просторі, люди б цього не помітили. Маскування є методом структурного приховування об'єкта захисту шляхом зміни його видових ознак під ознаки інших об'єктів (фону).

Один з найбільш очевидних недоліків неприхованої системи відеоспостереження є ризик її пошкодження зловмисниками. Сьогодні грабіжники дуже добре розуміються на технологіях, що дозволяє їм обходити системи безпеки, перехоплювати сигнал або пошкоджувати їх на відстані [1]. Одним зі способів маскування засобів відеоспостереження є фарбування технічного засобу, проте і воно буває різних типів. Маскувальне фарбування реалізується просто, але його ефект залежить від сезонних та інших змін навколишнього середовища. Для маскування без фарбування створюються спеціальні конструкції [2] або використовуються найбільш зручні місця для обладнання відеоспостереження.

Захисне фарбування поверхні відеокамер проводиться однобарвною фарбою під колір і середню яскравість фону навколишньої місцевості та предметів біля контрольованого об'єкта. Кольори захисного фарбування залежать від ландшафту, а найбільш розповсюдженими є: хакі, жовтувато-сірий, сіро-зелений, голубувато-сірий, оливковий. Вони відносяться до так званих універсальних, які погано виділяються на тлі різноманітних об'єктів

[1]. Тож для нагляду за об’єктами біля лісосмуг, садиб, полів, контрольно-пропускних пунктів, місць тимчасової стоянки військової техніки, залізничних шляхів чи мостів цей варіант маскування найдоцільніший.

Для міста дещо важче підібрати потрібний колір, тому можна використовувати конструкції чи архітектуру будівель для маскування камер на фасаді, навісах, порогах, балконах та вікнах зовні і об’ємні люстри, плафони, інформаційні стенди, колони чи будь які інші елементи інтер’єру всередині будівель.

Існує три основних способи маскування технічних засобів відеоспостереження:

1. Встановлення компактних, невеликих камер.

2. Використання ландшафту. Відмінний спосіб приховати встановлені по периметру відеокамери – це розмістити їх у правильних, непомітних місцях, замаскувати під навколишній простір. Зовні та всередині контрольованих приміщень є безліч предметів, які можуть бути укриттям для камер. Їх можна сховати серед рослин, розсипу каміння, замаскувати під лампочку.

3. Камуфляж для відеокамер. Поряд з використанням елементів ландшафту можна маскувати корпуси камер. Це може бути як тонкий кожух, що повторює форму камери, пофарбований у спеціальний колір, так і плівка, яка наклеюється на камеру. Наприклад, якщо камера встановлюється на дерево, їй можна надати колір кори, а якщо в кущах – хакі забарвлення. Стельові камери можна обклеїти білою плівкою так вони стануть практично невидимими.

Для виявлення технічних засобів відеоспостереження використовуються оптичні виявники - універсальні прилади, за допомогою яких можна знайти і увімкнену, і вимкнену приховану камеру. Ці пристрої випускаються у формі монокулярів та бінокулярів з одно- або двоколірним підсвічуванням. Вони призначені для виявлення об'єктива камери незалежно від його діаметра. Є головним та максимально ефективним засобом. Професійні моделі оптичних виявників оснащені потужним підсвічуванням, оптичним збільшенням та досить широким кутом огляду [3].

Список використаних джерел.

1. ТОР-Безпека м.Київ URL: https://tor-safety.com (дата звернення 21.02.2022)

2. Торокін А.А. Основи інженерно-технічного захисту інформації. - М.: Ось-89, 1998 р. - 336 с.

3. Как найти скрытую камеру: средства для выявления несанкционированного видеонаблюдения. URL: https://detsys.ru/article/kak_nayti_skrytuyu_kameru (21.02.2022)

НОРМАТИВНО-ПРАВОВИЙ ЗАХИСТ КОМЕРЦІЙНОЇ ТАЄМНИЦІ В УКРАЇНІ

Горецький О.В., ст. викладач Олейнікова О.І.
Харківський національний університет радіоелектроніки,
кафедра КРіСТЗІ, м. Харків, Україна
e-mail: oleksii.horetskyi@nure.ua

Abstract. The need for legal protection of trade secrets is due to the needs of the market economy and ensuring a competitive environment in business. The right to trade secrets is based on the de facto monopoly of the owner of the information, not on the legal monopoly on its use.

В умовах інтенсивного розвитку ринкових відносин важливого значення набуває цивільно-правовий обіг інформації. Інформація охоплює всі сторони життя і є дуже важливим і необхідним елементом діяльності людини, суспільства і держави в соціально-економічній, духовній та політичній сферах.

Необхідність правової охорони комерційної таємниці зумовлена потребами ринкової системи господарювання та забезпечення конкурентного середовища у підприємницькій діяльності. На відміну від винаходів, права на які охороняються на основі їх державної реєстрації за допомогою патентів, правова охорона комерційної таємниці побудована на основі забезпечення секретності відповідної інформації. Комерційній таємниці властива універсальність. Особа може віднести до комерційної таємниці навіть потенційно патентоспроможні рішення, які правоволоділець не бажає оприлюднювати та патентувати.

Строк дії охорони прав на комерційну таємницю обмежує лише строк існування сукупності ознак комерційної таємниці (ст. 508 ЦК). Права на комерційну таємницю діють, поки зберігається фактична монополія особи на конфіденційну інформацію, що лежить в основі комерційної таємниці.

Комерційна таємниця не потребує офіційного визнання її охороноспроможності, державної реєстрації та виконання інших формальностей, а також сплати державних зборів чи мита.

Варто зауважити, що сьогодні в Україні немає спеціального закону про право інтелектуальної власності на комерційну таємницю, як це має місце щодо більшості об'єктів права інтелектуальної власності.

Визначення комерційної таємниці закріплене у ст. 505 ЦК України: комерційною таємницею є інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить [1]. Відповідно до ч. 2 ст. 505 ЦК України об'єктом комерційної таємниці може бути технічна, комерційна, організаційна, виробнича чи будь-яка інша інформація. Якщо інформацію

створено внаслідок певних інтелектуальних зусиль людини, її можна розглядати як об'єкт прав інтелектуальної власності.

Комерційна таємниця має відповідати таким вимогам [2]:

1) інформація, невідома іншим особам;
2) відсутній вільний доступ до інформації на законній підставі;
3) вжито заходів для охорони конфіденційності інформації.

Відомості, які не становлять комерційної таємниці визначені Постановою від 09.09.1993 року № 611. До них належать:

- установчі документи;
- документи, що дають право здійснювати підприємницьку діяльність;
- відомості за встановленими формами звітності про фінансово-господарську діяльність та інші для перевірки правильності обчислення, сплати податків і т.д.;
- документи про платоспроможність;
- відомості про чисельність, склад працівників, їхню заробітну плату та умови праці;
- документи про сплату податків та інших обов'язкових платежів, а також відомості про забруднення довкілля, порушення антимонопольного законодавства, дії, що заподіють шкоду здоров'ю населення [3].

Суб'єктом прав інтелектуальної власності на комерційну таємницю є особа, яка правомірно визначила інформацію комерційною таємницею (ч. 2 ст. 506 ЦК України). Тобто суб'єкт, у якого є певна інформація, що відповідає визначеним у ч. 1 ст. 505 ЦК України ознакам, самостійно приймає рішення про визначення такої інформації комерційною таємницею.

Право на комерційну таємницю базується на фактичній монополії володільця інформації, а не на юридичній монополії на її використання. Забороняється лише посягати на цю монополію за допомогою незаконних заходів.

Список використаних джерел.

1. Цивільний кодекс України : URL: https://zakon.rada.gov.ua/laws/show/435-15/ru/ed20131011#Text (дата звернення: 23.02.2022).

2. Коссак В. М., Якубівський І. Є. Право інтелектуальної власності: Підручник. – К.: Істина, 2007. – 208 с.

3. Комерційна таємниця на підприємстві: основні правила. URL: https://profpressa.com/articles/komertsiina-taiemnitsia-na-pidpriiemstvi-osnovni-pravila. (дата звернення: 21.02.2022).

ФОТОГРАФІЧНА РОЗВІДКА ЯК ЗАГРОЗА ІНФОРМАЦІЇ, ЩО ВІЗУАЛІЗУЄТЬСЯ НА ОБ'ЄКТІ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

Рябіченко В.С., к.т.н., доцент Заболотний В.І.
Харківський національний університет радіоелектроніки,
кафедра БІТ, м. Харків, Україна
email: vadym.riabichenko@nure.ua

Abstract. This work is devoted to assessing the capabilities of technical means of photographic intelligence. The main technical characteristics of photographic systems are considered. The formulas according to which the coefficients of these characteristics are calculated are given.

Нова ера інформаційних технологій все більше піддається загрозам збоку фотографічної (ФР) розвідки. Мається на увазі зняття зображень інформації з екранів моніторів та проекторів на об'єкті, фотографування паперової секретної документації тощо. Тому, щоб протистояти таким загрозам інформаційній безпеці слід розуміти основні технічні характеристики фотографуючих систем. Основними характеристиками засобів фоторозвідки є масштаб фотографічного зображення, контрастність одержуваного зображення та роздільна здатність.

Масштаб фотографічного зображення характеризує ступінь зменшення зображуваних на знімку об'єктів. При фотографуванні об'єкти розвідки часто знаходяться на великій відстані від фотоапаратури а їх зображення отримуємо у фокальній площині об'єктива. Якщо позначити лінійні розміри об'єкту як l, а його зображення як l` то масштаб зображення M, як наведено на рисунку 1, буде:

$$\mathrm{M} = \frac{l`}{l} = \frac{f_{\text{об}'\text{єкта}}}{H}.$$

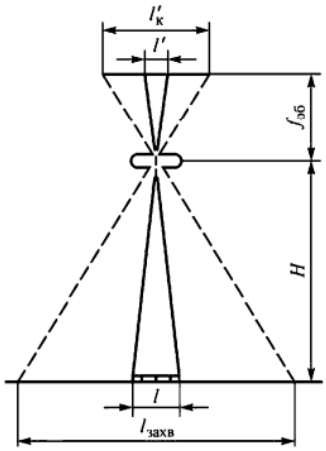


Рисунок 1 – Визначення масштабу фотографічного зображення

Проте, на практиці, масштаб фотографування обирається з розрахунком на те, щоб не тільки отримати достатню деталізацію об’єкта, але й забезпечити необхідну полосу захвату внутрішнього простору виділеного приміщення на ОІД. А ширина захвату $l_{\text{захв}}$ залежить від розміру кадру фотоапаратури $l`_{\text{к}}$ і масштабу зображення:

$$l_{\text{захв}} = \frac{l`_{\text{к}}}{\text{М}}.$$

Тобто, слід розуміти, що чим менший масштаб тим більша полоса захвату. Фотографування через вікно при розвідці проводиться зазвичай у масштабі 1:20000 – 1:10000. Хоча деякі об’єкти фотографуються і в масштабі від 1:5000 до 1:2000.

Наступна характеристика – контрастність, яку знаходять за формулою:

$$\text{К}_{\text{вид}} = 1 - (\text{B}_{\min\text{еф}} + \text{B}_{\text{д еф}}\text{B}_{\text{ф}\,max} + \text{B}_{\text{д}\,max}).$$

Де, $\text{B}_{\min\text{еф}}$ – мінімальна яскравість об’єкту, $\text{B}_{\text{д еф}}$ – ефективна яскравість атмосферної димки, $\text{B}_{\text{ф}\,max}$ – максимальна яскравість фону, $\text{B}_{\text{д}\,max}$ – максимальна яскравість атмосферної димки.

Коефіцієнт контрастності фотографуючої системи залежить від типу світлочутливої матриці. Найбільш поширені мають коефіцієнт контрастності від 1.5 до 2.5. При збільшенні висоти використовують слід збільшити коефіцієнт контрастності. Таким чином, компенсується зниження контрастності зображення внаслідок впливу серпанку.

Роздільна здатність фотографуючої системи характеризує здатність фотошару відтворювати дрібні деталі об'єктів та виражається максимальним числом паралельних штрихів, що роздільно передаються фотошаром, на білому тлі, що припадають на 1 мм знімка. Для її визначення використовують спеціальний тест-об'єкт. Таким чином, була встановлена залежність для роздільної здатності при відтворенні деталей малої контрастності:

$$R_K = R_{K=1}\sqrt{K/(2-K)},$$

де К – контрастність деталей за ефективними яскравостями; $R_{K=1}$ – роздільна здатність при контрасті деталей К = 1;

Таким чином, для подальшого більш розгорнутого розгляду даної теми необхідно провести додаткові дослідження характеристик освітлення паперових носіїв, яскравості моніторів тощо.

Список використаних джерел.

1. Теоретические основы технических разведок / Ю.К. Меньшаков / Под редакцией Ю.Н. Лаврухина. – Москва / Издательство МГТУ им. Н.Э. Баумана, 2008. - 529 с.

2. Хорошко В.О. Основи інформаційної безпеки / В.О. Хорошко, В.С. Чередниченко, М.Є. Шелест /За ред. проф. В.О. Хорошка. – К.: ДУІКТ, 2008. – 186 с.

ПРО ПІДВИЩЕННЯ БЕЗПЕКИ ОБМІНУ ФАЙЛАМИ У ВІДЕОКОНФЕРЕНЦІЯХ

Філімонов Д.А., д.т.н., проф. Антіпов І.Є.
Харківський національний університет радіоелектроніки,
кафедра КРіСТЗІ, м. Харків, Україна
e-mail: denis.filimonov@nure.ua

Abstract. Theses are about the files protecting that are transferred within the videoconference. Onion nesting and file encryption are suggested. According to algorithm, one of the layers contains a mechanism for comparison the real and expected IP-address. In case of a match, the inner protective layer is removed and the file becomes available. If there is a mismatch, the data will be destroyed. The algorithm will make it impossible to intercept attached files from a media stream that is weakly protected.

Актуальність відеоконференцій (ВК) є незаперечною. В наш час вони використовуються повсюдно від навчання та проведення судових засідань до міждержавних переговорів на найвищому рівні. ВК реалізуються через комп'ютер, планшет чи телефон і можуть супроводжуватися додатковим показом презентації, демонстрацією екрану та ін. Ряд сервісів дозволяють також обмінюватися файлами.

У доповіді запропоновано спосіб підвищення безпеки обміну файлами, що передаються у рамках ВК. Для його реалізації необхідно знати IP-адресу одержувачів – учасників даної ВК, які з'ясовуються на етапі їхньої авторизації при підключенні до відповідного сервісу.

Алгоритм формування даних, що передаються, наступний. Перед передачею файлу, він попередньо зашифровується за допомогою алгоритму AES. Потім відбувається інтеграція очікуваних IP-адрес одержувачів і механізму їх перевірки в передані дані, які ще раз зашифровуються AES. В результаті формується масив, схематично показаний на рис. 1. Після чого він передається по мережі разом із медіапотоком.

Механізм перевірки, що входить до складу масиву, являє собою програмний код, який вбудований таким чином, що після шифрування разом з IP-адресами утворює з ними єдине ціле. Цей масив може бути модифікований без порушення працездатності механізму перевірки. Рисунок 1

У постійному вигляді вказаний масив проходить по мережі до адресата. При отриманні файлу миттєво та автоматично запускається первинний механізм дешифрування, який перевіряє IP-адреси на відповідність до очікуваних. У разі збігу очікуваної та реальної IP-адреси відбувається зняття «внутрішнього» шару шифрування та вилучення вихідного файлу, що схематично представлено на рис. 2. Усі процедури відбуваються у клієнтській частині додатку для ВК.

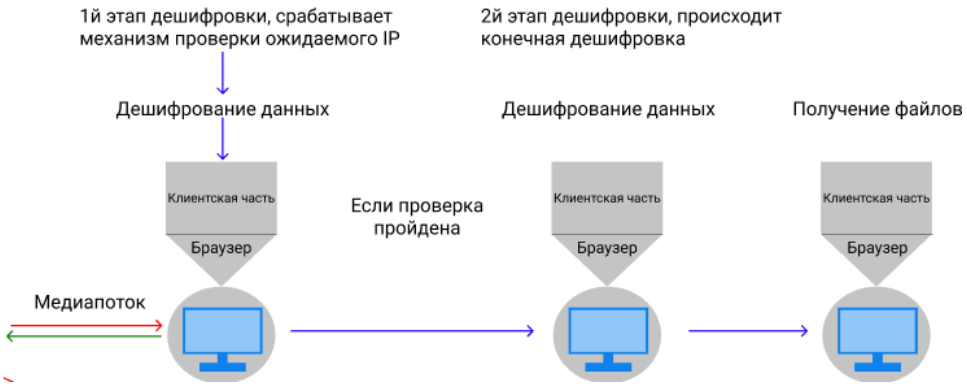


Рисунок 2

Особливостями WEB-протоколів, що використовуються при організації ВК, є те, що, по-перше, «недоставка» даних не впливає на продовження трансляції, а по-друге, не існує механізму перевірки адрес усіх одержувачів медіапотоку. Це дозволяє зловмиснику перехоплювати дані, залишаючись при цьому непомітним.

Але при отриманні зловмисником файлу, зашифрованого пропонованим способом, після запуску механізму дешифрування виявляється розбіжність реальної IP-адреси і тієї, яка закладена в механізм перевірки. І тут зняття «внутрішнього» шару шифрування немає, а отриманий масив даних знищується, що схематично представлено на рис. 3.

Оскільки всі процедури відбуваються в клієнтській частині спеціальної програми, то зловмисник не має змоги отримати доступ до даних після зняття «зовнішнього» шару шифрування.

Хоча даний алгоритм розроблений саме для файлів, що передаються в рамках ВК, при певному доопрацюванні він може бути застосований і для медіапотоку.

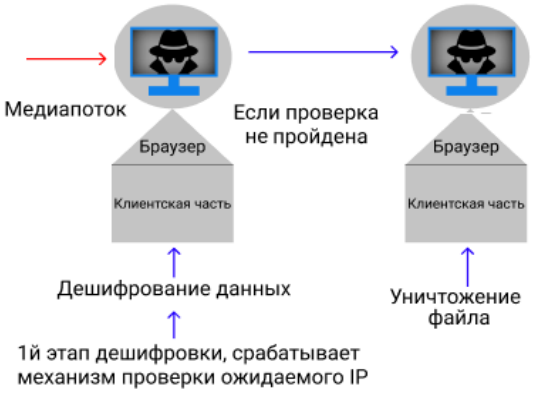


Рисунок 3

ПОРІВНЯЛЬНА ХАРАКТЕРИСТИКА СЕРВІСІВ ВІДЕОКОНФЕРЕНЦІЙ З ТОЧКИ ЗОРУ БЕЗПЕКИ

Філімонов Д.А., д.т.н., проф. Антіпов І.Є.
Харківський національний університет радіоелектроніки,
кафедра КРіСТЗІ, м. Харків, Україна
e-mail: denis.filimonov@nure.ua

Abstract. Theses are about the comparative characteristics of well-known videoconferencing services. The fundamental vulnerability of such services, due to the peculiarities of network data transfer protocols, is noted. The comparison focuses on end-to-end encryption, two-factor authentication, and the ability to manage data on the client side and on the server. The comparison results are presented in a table. According to the analysis results, the most secure services are Cisco Webex Meetings and GoToMeeting.

Роль та значення відеоконференція (ВК) останніми роками суттєво зросли. Так, у світі нині існують десятки різних сервісів ВК із сумарною добовою аудиторією понад 1.6 млрд. користувачів. Численність сервісів свідчить, по-перше, про їх затребуваність, а, по-друге, говорить про те, що не існує ідеального рішення на всі випадки життя. Різні сервіси поряд з основною послугою – передача відео- та звукового потоку даних – надають додатковий набір послуг, такий як можливість обміну файлами, демонстрація екрана або слайдів, спільне редагування документів, запис ВК та інші. Ряд сервісів працюють безпосередньо з браузера, для деяких потрібна установка спеціальної програми. Існують обмеження за тривалістю ВК та за кількістю учасників, причому ці обмеження можуть відрізнятися для платного та безкоштовного варіантів одного й того ж сервісу.

Робота присвячена порівняльній характеристиці вразливості різних сервісів ВК до загрози несанкціонованого доступу. Web-протоколи, що використовуються для ВК, мають ряд особливостей, пов'язаних із передачею відео- та аудіоданих: трансляція може продовжуватися незалежно від доставки або недоставки медіапотоку одержувачам; крім того, не існує механізму перевірки адрес усіх тих, хто його отримує. Це дає можливість зловмисникам здійснювати атаки на ВК, організовуючи помилкові запити APR, здійснюючи хибну маршрутизацію або перехоплюючи з'єднання TCP. У результаті вони можуть отримати доступ до даних ВК, залишаючись при цьому непомітними для її учасників. Також не слід забувати про невиявлені вразливості в самих сервісах і про те, що дані можуть зберігатися і на серверах ВК, і на пристроях користувачів досить довго.

Тому при порівнянні різних сервісів ВК, основна увага приділяється наявності наскрізного шифрування, двофакторної аутентифікації,

можливості керування даними на стороні клієнта та на сервері, а також наявності так званої «кімнати очікування» – можливості, яка дозволяє адміністратору в ручному режимі схвалювати підключення кожного окремого учасника ВК.

У таблиці представлено порівняльну характеристику найбільш популярних сервісів ВК за вказаними критеріями та виставлено узагальнену оцінку ступеня захищеності за 5-бальною шкалою.

Таблиця – Порівняльна характеристика сервісів ВК

Сервис	Активних користувачів млн./день	Наскрізне шифрування	Двофакторна автентифікація	Кімната очікування	Управління даними на стороні клієнта	Управління даними на сервері	Оцінка ступеня захищеності
Cisco Webex Meetings	300	+	+	+	+	–	5
FaceTime	220	+	+	–	+	+	3
Slack	70	–	+*	–	–	–	3
Webinar Meetings	50	–	–	+	+	+	3
Zoom	260	–	–	+	+	–	2
Proficonf	10	–	–	–	–	–	1
Trueconf	90	–	+	–	+	–	2
Messenger Rooms	100	–	+**	–	+	+	3
WhatsApp	180	+	+	–	+	+	3
Microsoft Teams	75	–	+	+	+	+	2
Skype	140	–	+	–	+	+	1
GoToMeeting	40	+	+	+	+	–	5
Google Meet	100	–	+	+	+	+	4

* – з використанням ПЗ IOS;

** – через Facebook

При виставленні підсумкової оцінки ступеня захищеності використовувалися також дані про алгоритми і довжину ключа шифрування та ряд факторів, які не увійшли до таблиці. Слід зазначити, що іноді з'являється інформація про успішну атаку хакерів на той чи інший сервіс і про виявлення в ньому вразливостей. З урахуванням цієї обставини, на мій погляд, слід віддавати перевагу сервісам з більшою аудиторією, оскільки для них оновлення програмного забезпечення з урахуванням вимог безпеки відбувається частіше.

За підсумками аналіз найбезпечнішими є сервіси Cisco Webex Meetings та GoToMeeting. У доповіді зазначені характеристики та обґрунтування оцінок буде розглянуто докладніше.

ІНФОРМАЦІЙНИЙ КОМПЛЕКС РОЗПОДІЛЬНИХ ЕЛЕКТРОМЕРЕЖ

Павленко Я.С., асистент Булага В.А.
Харківський національний університет радіоелектроніки,
кафедра КРіСТЗІ, м. Харків, Україна
e-mail: yan.pavlenko@nure.ua

Abstract. The IR RES set is designed to monitor the main technical parameters of normal and emergency modes of 10 (6) kV distribution electrical networks (voltage, the appearance of an interphase short circuit current), as well as meteorological conditions (temperature and relative humidity) in the places of operation and data transmission to control room through the GSM networks of operating operators. The IR RES set is used to optimize the search and localization of the place of damage to overhead power lines with voltage 10(6) kV, as well as to prevent emergency conditions as a result of the influence of climatic factors.

Робота електромереж пов’язана з різними факторами які перешкоджають її безперебійному функціонуванню. Для оптимізації роботи електромереж доцільно використовувати інформаційний комплекс розподільних електромереж.

Інформаційний комплекс розподільних електромереж складається з наступних систем:

1) система моніторингу розподільних електромереж 6/10 кВ;
2) система контролю ожеледиці;
3) система контролю підстанцій, що не обслуговуються, 35/10кВ;
4) система відеоспостереження.

Система моніторингу розподільних електромереж 6/10 кВ С призначена для оперативного моніторингу та контролю аварійного значення метеопараметрів. Вона допомагає здійснювати оперативний пошук та локалізацію місць ушкоджень.

Використання цього обладнання дозволяє:

1) зменшити витрати на пошук місць несправностей;
2) зменшити кількість недовідпущеної електричної енергії споживачам;
3) мінімізувати небезпеку ураження електричним струмом від пошкодженої лінії.

Система контролю ожеледиці виконує наступні завдання:

1) періодичне вимірювання температури та вологості, вагове навантаження в точці підвіски дроту та передачу інформації на блок диспетчерський;
2) фіксацію та передачу на блок диспетчерської аварійної інформації про перевищення заданих критичних значень метеорологічних параметрів

та вагового навантаження у точці підвіски дроту, зумовлених утворенням ожеледиці;

3) усереднення результатів за період збору даних;

4) прийом та обробку інформації з розпізнаванням адреси відправника;

5) програмне встановлення критичних параметрів, а також періодів збору та передачі інформації;

6) відображення та збереження результатів моніторингу на комп'ютері.

Система контролю підстанцій, що не обслуговуються, 35/10кВ призначена для автоматизованого збору, обробки та передачі на центральний диспетчерський пункт інформації про аварійні та нормальні режими роботи підстанцій (включаючи інформацію щодо замикання на землю в мережі із ізольованою нейтраллю). Система дозволяє здійснювати функцію охоронної сигналізації на території підстанції. Використання даної системи дозволяє підвищити ефективність експлуатації розподільних мереж, оперативно та достовірно контролювати стан обладнання.

Система відеоспостереження призначена для:

1) забезпечення безпечного стану об'єкта та всього, що до нього входить людей, обладнання, цінностей нематеріального характеру;

2) боротьби з тероризмом, бандитизмом та розкраданнями з проникненням, наявність камер відеоспостереження є заходами мінімізації ризиків наступу таких подій;

3) оперативного інформування про появу нештатних ситуацій від проникнення осіб зі зброєю до вибухів, пожеж, раптових руйнувань тощо;

4) створення бази даних про події на об'єкті, що охороняється за певний період часу.

Список використаних джерел.

1. Крухмалёв, В.В., Гордієнко, Н.В., & Моченов, А.Д. (2004). Основи побудови телекомунікаційних систем і мереж. Горячая линия – Телеком.

2. Іпатов, В.П., Орлов, В.К., Самойлов, І.М., & Смирнов, В.Н. (2003). Системи мобільного зв'язку. Горячая линия – Телеком.

3. Тепляков, І.М. (2004). Основи побудови телекомунікаційних систем і мереж. Радио и сввязь.

4. Гаранін, М.В., Журавльов, В.І., & Кунегін, С.В. (2001). Системи та мережі передачі інформації. Радио и связь.

5. Волков, Л.Н., Неміровскій, М.С., & Шінаков, Ю.С. (2009). Системи цифрового радіозв'язку: базові методи і характеристики. Еко-трендз.

6. Bulaga, V. (2021) “Digital System for customs inspection of baggage in high security areas,” 2021 III International Scientific and Practical Conference Theoretical and Applied Aspects of Device Development on Microcontrollers and FPGAs. DOI: https://doi.org/10.35598/mcfpga.2021.015.

ТЕХНІЧНІ ЗАСОБИ АКУСТИЧНОЇ РОЗВІДКИ

Філоненко Я. С., к.т.н., проф. Олейніков А.М.
Харківський національний університет радіоелектроніки,
кафедра КРіСТЗІ, м. Харків, Україна
e-mail: yaroslav.filonenko@nure.ua

Abstract. To build an effective system of information protection, it is necessary, as one of the points, to explore all possible technical means of intelligence that can be used, technical means of acoustic intelligence - including. The class of technical meansof acoustic intelligence, in particular, include narrow microphones. The main characteristic of the acoustic antenna, as a structural part of the acoustic receiver, is the characteristic of the direction.

Для побудови ефективної системи захисту інформації необхідно, як один із пунктів, дослідити усі можливі технічні засоби розвідки що можуть бути використані, технічні засоби акустичної розвідки (ТЗАР) – в тому числі. До класу технічних засобів акустичної розвідки, зокрема, відносять вузькоспрямовані мікрофони.

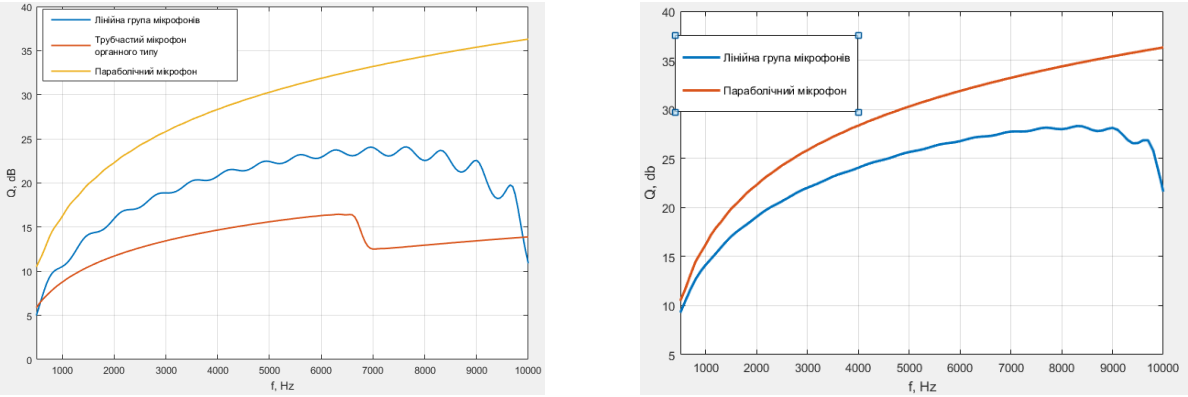
Акустомеханічний перетворювач(акустична антена), як структурна частина акустичного приймача, найбільше впливає на кінцеві характеристики мікрофону в цілому і тому, ключовим є те, які параметри він матиме. Основною характеристикою акустичної антени є характеристика спрямованості – вона визначає вплив акустичної завади на сигнал з напрямку що не співпадає з напрямком на джерело звуку.

Існує декілька типів вузькоспрямованих мікрофонів: рефлекторні (параболічні) мікрофони, лінійні групи мікрофонів, трубчасті мікрофони органного типу, трубчасті щілинні мікрофони, комбіновані акустичні приймачі - усі вони відрізняються за характеристикою спрямованості.

В роботі було досліджено характеристику спрямованості для кожного типу мікрофонів, її залежність від частоти, вплив на розбірливість мови, залежність характеристики спрямованості від габаритів мікрофону і т.д. У випадку лінійної групи мікрофонів і трубчастого мікрофону органного типу також було прийнято до уваги кількість одиничних мікрофонів, кількість трубок у конструкції, відповідно, та відстань між крайніми приймачами, котрі визначають максимальну частоту прийому акустичних коливань.

У доповіді досліджено залежність індексу спрямованості мікрофонів, як ключової характеристики, від частоти, у випадку лінійної групи мікрофонів та трубчастого мікрофону органного типу описується також залежність індексу спрямованості від кількості приймачів відносно відстані між приймачами.

Наприклад, при порівнянні індексу спрямованості ТЗАР на частотах до 5600 Гц котрі включають 95% енергії мовного сигналу, при габаритних обмеженнях 50 см, виходить наступний графік (рис.1). Для лінійної групи мікрофонів значення індексу спрямованості можна збільшити за рахунок використання одиничних мікрофонів з характеристикою спрямованості у вигляді гіперкардіоїди (С = 0,75) та використання цифрової обробки сигналів[1].



а) б)

а) параболічні мікрофони, лінійні групи мікрофонів, трубчасті мікрофони органного типу; б) параболічні мікрофони, лінійні групи мікрофонів(з приймачами з характеристикою спрямованості у вигляді гіперкардіоїди)

Рисунок 1 – Графік залежності індексу спрямованості від частоти:

Використовуються наступні алгоритми ЦОС: алгоритм затримки та підсумовування, алгоритм надспрямованості, алгоритм пост-фільтрації Вінера, алгоритм придушення бокових пелюсток [2].

Алгоритм затримки та підсумовування базується на затримці сигналів від окремих мікрофонів. Алгоритм дозволяє здійснити качання променя за рахунок фазової затримки. Алгоритм надспрямованості об’єднує у своїй структурі диференційну мікрофону решітку та алгоритм затримки та підсумовування. Алгоритм пост-фільтрації Вінера дозволяє компенсувати некогерентні завади, а також компенсувати когерентні завади з бічних пелюсток. Основною метою цього дослідження є порівняння різних типів мікрофонів з метою визначення найоптимальнішої конструкції з точку зору ефективності використання (дальність розвідки, розбірливість мови).

Список використаних джерел.

1. Олейников, А.Н., Войтенко, А.О. Сравнительная характеристика параметров узконаправленных микрофонов // Радиотехника. – 2013. – Вып. № 173. – С. 224-231.

2. Олейников, А.Н., Бородавка, А.В. Основные направления совершенствования средств акустической разведки // Радиотехника. – 2017. – Вып. № 189. – С. 189-194.

ЦИФРОВА СИСТЕМА ДЛЯ МИТНОГО КОНТРОЛЮ РУЧНОГО БАГАЖУ В АЕРОПОРТАХ ТА ЗОНАХ ПІДВИЩЕНОЇ НЕБЕЗПЕКИ

Сердюк С.Л., асистент Булага В.А
Харківський національний університет радіоелектроніки,
кафедра КРіСТЗІ, м. Харків, Україна
e-mail: serhii.serdiuk@nure.ua

Abstract. This article discusses the development of a three-energy digital system for customs inspection of luggage and hand luggage in airports and high-security areas, which will provide not only easy monitoring of luggage and hand luggage, but also security screening. The peculiarity of such a system is the use of scintillation crystals in the control systems of customs baggage inspection. And also the scheme of three-energy digital radiographic system has been developed, which gives the possibility of fast and safe luggage monitoring.

Вступ. Сцинтилятори - це особливі речовини, що мають здатність випромінювати світло при поглинанні іонізуючого випромінювання, такого як, наприклад, гамма-кванти. На відміну від, наприклад, люмінесценції, тут збудження відбувається саме з допомогою іонізації, а не з допомогою механічного впливу. Причому в основному висвічування світла відбувається швидко, у формі миттєвого спалаху для ока.

Сцинтилятори мають мертвий час порядку мікросекунд або десятків наносекунд. Це можна віднести швидше до переваг сцинтилятора, тому що в якості центрових детекторів у іонізаційних камер і багатьох інших детекторів мертвий час істотно більший. До недоліків сцинтиляторів відноситься складність експлуатації частини з них. Так багато сцинтиляторів гідроскопічні, а намокнувши (або поглинувши водяну пару з повітря) перестають світити. Іншим потрібна низька температура. Втім, це проблема взагалі більшої частини детекторів, і саме в цьому відношенні сцинтиляторні детектори менш вибагливі, ніж інші, яким часто потрібна і низька температура і високий вакуум.

Виходячи з вище сказаного, була розроблена система схема цифрової радіографічної системи для контролю багажу і поштових відправлень. Принцип роботи установки, заснований на застосуванні методу скануючого рентгенівського променя полягає: об'єкт, що підлягає контролю, лягає на стіл установки, нерухомий рентгенівський генератор (Re з MXF) за допомогою механізмів юстування налаштовується щодо досліджуваного об'єкта, спеціальний колімуючий пристрій формує вузький (близько 1° по товщині) віялоподібний пучок рентгенівських променів, що по вертикалі має кут близько 60°. Рентгенівські промені, що пройшли крізь об'єкт контролю за допомогою спеціальної детекторної лінійки, перетворюються на електричні сигнали, які після відповідної обробки в блоці обробки інформації, записуються пристроєм цифрової відеопам'яті, а

потім надходять на відеоконтрольний пристрій монітор, що трансформує їх у видиме зображення на екрані телебачення.

З великої різноманітності сцинтиляторів для спектрометричного режиму необхідні ті, які мають: малі часи висвітлення (5мкс) і післясвітіння, що знижують спотворення форми спектрів амплітудного розподілу за рахунок накладання імпульсів; високий світловихід і максимальне спектральне узгодження з ФД для забезпечення високого відношення сигнал-шум у низькоенергетичній області; високу термостабільність люмінесцентних характеристик для досягнення стабільності положення піків повного поглинання при зміні температури навколишнього середовища; можливо більше значення Zеф для створення високоефективних гамма-детекторів; високі волого- та механічна стійкість, що визначають технологічність виготовлення детекторів та можливість тривалої експлуатації. Під дані вимоги найбільше підходять кристали ZnSe(Te), які виготовляють у НТК «Інститут монокристалів», розташованому в Харкові. Також дані СЦ не мають гігроскопічності, є радіаційно-стійкими, відносно твердими і добре стійкими до механічних впливів.

Висновки. ФД як фотоприймач має ряд переваг, наприклад: малі габарити і вага, низьковольтне живлення, висока радіаційна стійкість, механічна міцність і не схильний до впливу магнітних полів. Зі збільшенням обсягу СЦ зростає площа його поверхні і для поліпшення умов світлозбирання сцинтиляцій необхідно збільшувати світлочутливу поверхню ФД, які випускаються з певними розмірами світлочутливого майданчика. З урахуванням вимог і обраного СЦ кристала, вартості фото-діода, його чутливості та малої ємності, ми використовували вітчизняний ФД - ФД-263.

Список використаних джерел.

1. F. Bohapov, "Simulation of X-Ray Television System Output Signal Based on CMOS-Matrixes", *Electronic and Acoustic Engineering*, vol. 3, no. 4, pp. 53-58, 2022. doi: 10.20535/2617- 0965.2020.3.4.200608.

2. L. Kyyda, "The Adaptation of Customs Legislation to the International Standards of the Simplified Customs Control of Citizens When Crossing the Customs Border of Ukraine", *Public Policy and Ecnomic Development*, no. 2, pp. 93-98, 2014. doi: 10.14746/pped.2022.02.21.

3. Customs system [Electronic resource]: Access mode: http://student.zoomru.ru/tamoj/problemy-i-perspektivy-razvitiya-tehnicheskih/1.html 25.02.2022. Customs System.

4. Liquid Scintillators [Electron resource]: Access mode: http://nuclphys.sinp.msu.ru/students/scint/index.htm 15.02.2022. Scintillation detectors/

5. V. Bulaga, “Digital System for customs inspection of baggage in high security areas,” *2021 III International Scientific and Practical Conference Theoretical and Applied Aspects of Device Development on Microcontrollers and FPGAs*, 2021. DOI: 10.35598/mcfpga.2021.015

АНАЛІЗ МЕТОДІВ ОПТИМІЗАЦІЇ КОМПЛЕКСНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Румянцева О.В., к.т.н., с.н.с. Пшеничних С.В.
Харківській національний університет радіоелектроніки,
кафедра Інфокомунікаційної інженерії ім. В.В. Поповського,
м. Харків, Україна
e-mail: olha.rumiantseva@nure.ua

Abstract. The report reviews well-known optimization methods that can be used to solve the problem of choosing from a set of available tools of such a set that will ensure the neutralization of all potential information threats with the best quality and the lowest possible cost of resources. The report also reviews issues related to the choice of performance indicators and optimality criteria for a comprehensive information security system. It also considers the evaluation of the effectiveness of the functioning of a comprehensive information security system, which is carried out based on the results of the analysis.

Одним з найважливіших завдань оптимальної побудови комплексної системи захисту інформації (КСЗІ) є вибір із безлічі наявних засобів такого їх набору, який дозволить забезпечити нейтралізацію всіх потенційно можливих інформаційних загроз із найкращою якістю та мінімально можливими витраченими на це ресурсами.

Відомо, що найефективніше завдання захисту інформації вирішуються у межах попереджувальної стратегії захисту, коли на етапі проектування оцінюються потенційно можливі загрози і реалізуються механізми захисту від них. При цьому на етапі проектування системи захисту інформації розробник, не маючи статистичних даних про результати функціонування системи, змушений приймати рішення про склад комплексу засобів захисту (КЗЗ) інформації, перебуваючи в умовах значної невизначеності.

Водночас прорахунки у виборі комплексу засобів захисту інформації на етапі проектування ведуть до невиправданого збільшення збитків від реалізації деструктивних впливів. Крім того, у процесі проектування системи захисту інформації на об'єкті інформатизації найбільш трудомісткими та найменш забезпеченими у методичному плані є етапи оцінки ефективності та вибору оптимального проектного варіанту.

Створення системи комплексного захисту вимагає тривалого часу, залучення великої кількості експертів. Термін служби комплексної системи захисту інформації є тривалим. Протягом терміну служби кілька разів може змінитись склад її технічних засобів. Виходячи з цього, одним з основних питань, які вирішуються розробником комплексної СЗІ, є оптимізація складу комплексу засобів захисту, що забезпечує збереження ефективності її функціонування протягом життєвого циклу. Одним з

найскладніших є завдання оптимізації складу засобів захисту на етапі проектування.

Розглядаючи завдання побудови оптимального КЗЗ у СЗІ як завдання проектування складного технічного об'єкта, її математичну постановку можна представити у наступному вигляді. Необхідно знайти безліч засобів захисту $X_{opt} \in X$ таке, що

$$X_{opt} = \underset{X}{arg\ extr}\, I(X, Y, t),$$

де $I(X,Y,t)$ – узагальнений показник ефективності функціонування комплексу засобів захисту.

Потрібно сформувати склад засобів захисту інформації з багатьох доступних, які забезпечують виконання всіх необхідних функцій за умови досягнення оптимуму обраного критерію та виконання відповідних обмежень. Крім того, такий набір засобів захисту повинен задовольняти вимогам нормативних документів та вимогам сумісності.

При цьому приймаються такі припущення та обмеження:

– час аналізу захищеності поставлено ($t = T$);

– безліч потенційно можливих загроз Y визначено і є кінцевим;

– зловмисник є інформаційним суб'єктом, здатним до навчання;

– витрати на експлуатацію КСЗІ постійні, а їх надійність абсолютна;

– випадки появи різних ненавмисних загроз є незалежними випадковими подіями.

У доповіді розглядаються відомі методи оптимізації, які можуть бути використані для вирішення завдання вибору оптимального складу засобів захисту інформації у КСЗІ, а також питання, що стосуються вибору показників ефективності та критеріїв оптимальності КСЗІ.

Як показник ефективності КСЗІ найчастіше використовується залишковий ризик реалізації загроз інформаційної безпеки, а критерій оптимальності визначається співвідношенням ефективності КСЗІ та вартості самого комплексу з урахуванням витрат на його експлуатацію та підтримання у робочому стані.

Оцінка ефективності функціонування КСЗІ здійснюється за результатами аналізу, що здійснюється за допомогою моделювання.

Список використаних джерел.

1. Горохов Д.Е. (2009). Методика оптимизации комплекса средств защиты на основе априорной оценки риска. Информация и безопасность, (4), 603 – 606.

2. Пиявский С.А. (2014). Простой и универсальный метод принятия решений в пространстве критериев «Стоимость–эффективность». Онтология проектирования, 3 (10), 89–102.

ПЕРСПЕКТИВИ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ 6G

Лозовська Г.О., к.т.н., доц. Горелов Д.Ю.
Харківський національний університет радіоелектроніки,
кафедра МІРЕС, м. Харків, Україна
e-mail: hanna.lozovska@nure.ua

Abstract. The paper discusses the applications use cases based on 6g networks.

Окрім широкосмугової передачі даних мережі 5G стали кроком вперед до високонадійного безпровідного доступу з малою затримкою, що дозволило організовувати складні та розподілені мережі Інтернету речей. Введення мереж 6G, які використовують штучний інтелект для покращення якості зв'язку та забезпечують покриття, що виходить за межі земної поверхні, призведе до появи нових сценаріїв використання систем зв'язку (рис. 1).

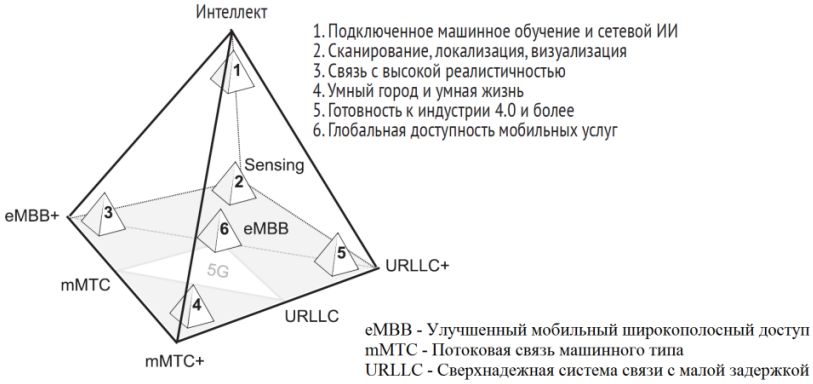


Рисунок 1

Зв'язок з високою реалістичністю. Використання за стосунків доповненої реальності (AR, VR та MR), а також голографічного зв'язку, вимагає значного підвищення роздільної здатності дисплеїв. Подібні дисплеї потребують надвисоких швидкостей передачі даних, які мережі 5G не здатні забезпечити. Також надзвичайно низьких затримок в мережі вимагає тактильний зворотний зв'язок у реальному часі при телеуправлінні.

Сканування, локалізація та зйомка. Надвисоких швидкостей обміну даними вимагають високоточна навігація, розпізнавання жестів, відображення та реконструкція зображень. Порівняно зі зв'язком, для оцінки якості сканування, локалізації та візуалізації використовують інші критерії, такі як роздільна здатність сканування та точність вимірювання діапазону, кута або швидкості. Вони також включають новий набір показників якості роботи, таких як ймовірність неправильного виявлення та помилкової тривоги.

Повнофункціональна індустрія 4.0. Хоча 5G був розроблений з

низькою затримкою та високою надійністю, деякі з сценаріїв висувають надзвичайно високі вимоги (наприклад, точне управління рухом), що перевищують можливості 5G. У свою чергу, 6G дозволить реалізувати ці варіанти використання за рахунок технологій, що реалізують надвисоку надійність та надзвичайно низьку затримку. Разом з тим, по мірі того, як нові методи взаємодії людини та машини на основі ШІ стануть життєздатними, майбутні автоматизовані виробничі системи будуть орієнтовані на спільну роботу роботів, коботів або навіть кіборгів.

Розумне місто та розумне життя. Величезну кількість датчиків буде розгорнуто для потреб розумного транспорту, будівництва, охорони здоров'я, автомобілів, заводів та міст. Ці датчики будуть збирати великі дані для алгоритмів для надання ШІ як послуги, тобто автоматизація та інтелект будуть створені в кіберсвіті та доставлені у фізичний світ через безпровідні мережі 6G.

Глобальне покриття для мобільних послуг. За для забезпечення вимога безперебійних та безрозривних мобільних послуг по всій земній поверхні у мережах 6G передбачена інтеграція наземного та неназемного зв'язку. У такій інтегрованій системі мобільний користувач за допомогою одного пристрою може отримати доступ до послуг мобільного широкосмугового доступу як у міських, так і в сільських районах або навіть на літаках і кораблях. У цих сценаріях постійно відбувається динамічний вибір оптимальних каналів наземних та неназемних мереж без переривання поточних послуг. Безпілотні транспортні засоби матимуть можливість використовувати безрозривну високоточну навігацію у будь-якій точці планети. До можливих варіантів використання глобального покриття відносяться також IoT-підключення для захисту навколишнього середовища в реальному часі та точного ведення сільського господарства.

Мережевий ШІ. Повноцінне використання можливостей ШІ є фундаментальним принципом функціонування 6G. По суті, з одного боку, можливості ШІ можуть бути розширені та інтегровані у більшість функцій та додатків 6G. З іншого боку, майже всі додатки 6G будуть засновані на ШІ, при цьому ШІ також зможе розширювати всі попередні варіанти використання безпровідних мереж, вносячи до них просунуту автоматизацію. Таким чином, повне підключення розподілених агентів машинного навчання через мережу 6G призведе до появи мережевого інтелекту та кращого захисту конфіденційності даних.

Список використаних джерел.

1. Saad, W.; Bennis, M.; (2020). "A Vision of 6G Wireless Systems: Applications, Trends, Technologies, and Open Research Problems". IEEE Network. 34 (3): 134–142.

2. Alwis, Chamitha De; Kalla, Anshuman; Pham, Quoc-Viet; (2021). "Survey on 6G Frontiers: Trends, Applications, Requirements, Technologies and Future Research". IEEE Open Journal of the Communications Society. 836–886.

3. Yang, H.; Alphones, A.; Xiong, Z.; Niyato, D.; Zhao, J.; Wu, K. (2020). "Artificial-Intelligence-Enabled Intelligent 6G Networks". IEEE Network. 34 (6): 272–280.

ОГЛЯД ТА АНАЛІЗ ЗАСОБІВ СТВОРЕННЯ ІНТЕРФЕЙСУ МОБІЛЬНИХ ДОДАТКІВ

Калина О.М., к.т.н., проф. Колендовська М.М.
Харківський національний університет радіоелектроніки,
кафедра МІРЕС, м. Харків, Україна
e-mail: oleksandra.kalyna@nure.ua

Abstract. Mobile technology is ingrained in our lives - we can now pay directly from the phone, the simplest built-in applications have replaced paper books, newspapers, wallet and calendar, music players, cameras, calculators and computers. This growing popularity of mobile devices has now forced business owners to turn their attention to the mobile market, which, although part of the Internet, plays by its own rules.

З моменту народження Інтернету минуло більше 50 років, і за цей час мережа стала не тільки всесвітньою і загальнодоступною, але й перетворилась у потужний маркетинговий інструмент – власники бізнесів розгледіли у Інтернеті хороший ринок збуту і спосіб реклами своєї продукції. Кількість користувачів всесвітньої мережі безупинно росла, а разом з нею росло і розмаїття послуг і сервісів в мережі.

З появою перших кишенькових персональних комп'ютерів світ технології став ближче, а розповсюдження смартфонів з сенсорним дисплеєм дозволило користувачеві виконувати складні операції кількома рухами пальцю. За статистикою на 2021 рік кількість унікальних користувачів інтернету у світі дорівнює 4.95 мільярду людей, що проводять у інтернеті у середньому 7 годин на добу. В Україні процент користувачів сягнув вище 50%, що, у цілому, відповідає світовій статистиці. Тим часом, близько 92.1% користувачів інтернету виходять у мережу за допомогою мобільних пристроїв (а з комп'ютерів або ноутбуків – 71.2%) – за останні 5 років відсоток мобільних користувачів зріс майже на 15%.

Мобільні технології щільно закоренилися у нашому житті – за їх допомогою ми тепер можемо заплатити прямо з телефону, найпростіші вбудовані додатки замінили паперові книжки, газети, гаманець і календар, програвачі музики, фотокамери, калькулятори і комп'ютери. Цей ріст популярності мобільних пристроїв тепер змусив власників бізнесів звернути свою увагу і на мобільний ринок, який хоч і є частиною інтернету, але грає за власними правилами. Власники мобільних девайсів, яких зараз більше ніж 6 мільярдів, проводять у середньому 4.5 години користуючись свої телефоном, з яких 92.5% часу проводять у мобільних додатках, а не в браузері, що диктує бізнесу ще одну умову – складні сайти вже не такі популярні, користувач скоріше за все обере доступ до улюбленого сервісу через мобільний додаток, ніж через мобільну версію сайту.

Мобільний інтерфейс додатку – це інструмент взаємодії між користувачем та програмою. Дослідження показали, що для того, щоб сприйняття користувачем додатку було вільним, необхідно знизити когнітивне навантаження на людину. Досягти легкості користування додатком можна у такі способи:

- Спрощувати і розбивати задачі: поділ задач на прості, короткі блоки допомагає з'єднати різні дії в логічний сценарій, який легше сприймається користувачем.
- Використовувати стандарти платформи: кожна мобільна операційна система має ряд навігаційних патернів, які використовуються у кожному нативному додатку, задокументовані гайдлайнами системи – збірка правил і рекомендацій до використання елементів у додатках. Операційній системі Android відповідають Material Design Guidelines, а iOS – Human Interface Guidelines.
- Адаптувати: При проектуванні додатку варто враховувати не тільки особливості ОС і технічні переваги і недоліки пристрою, але й культурні особливості різних народів, швидкість або вірогідність відсутності інтернет з’єднання тощо.
- Використання зрозумілих заголовків та іконок.
- Інформувати: Важливо повідомляти користувача про його статус у додатку, у тому числі, хід завантаження, оновлення, місце у навігації і причини виникнення помилок – це допоможе запобігти невірному використанню додатку, яке призведе до негативного досвіду користування.
- Проектувати для користування руками. Також варто враховувати те, що додаток може бути використаний «на ходу»: у транспорті, на вулиці тощо, а це означає, що найважливіші елементи управління необхідно сконцентрувати в зоні доступу великого пальцю однієї руки.
- Враховувати кольорову сліпоту: Колір не повинен використовуватися як єдиний візуальний засіб передачі інформації, варто використовувати пояснюючі іконки, написи й зображення, щоб дати однозначне повідомлення навіть людині з особливостями сприйняття кольору.
- Не зупиняти дизайн-процес. Тестування, робота над помилками і пошук нових рішень – є невід’ємними частинами процесу розробки будь-якого проекту.

Таким чином, мобільні додатки – це логічний етап розвитку інтернету, технологій і сервісів, від якого може залежати статус компанії і економічна прибутковість бізнесу. Розробка інтерфейсу мобільного додатку – складний, технічний процес, який потребує великої кількості досліджень аудиторії і конкурентів. Технологій не зупиняються на місці, темпи життя сучасної людини збільшуються, тож найважливішою задачею дизайнерів і розробників є не створення ефективного і зручного користувацького досвіду.

ВИКОРИСТАННЯ AR-ТЕХНОЛОГІЙ ПРИ ВИЯВЛЕННІ БПЛА

Крамський І.А., к.т.н, проф. Олейніков В.М.
Харківський національний університет радіоелектроніки,
кафедра МІРЕС, м. Харків, Україна
e-mail: ihor.kramskyi@nure.ua

Abstract. The use of augmented reality is a promising direction in the modern world. AR can be applied in various fields of science and technology. Also, for the convenience of displaying various objects in space, you can use AR elements.

The ability to see an unmanned aerial vehicle in real time somewhere in the sky on a computer monitor or other display device can speed up the process of locating the drone and eliminating it.

Доповнена реальність (Augmented Reality, AR) - результат введення в поле сприйняття будь-яких сенсорних даних з метою доповнення відомостей про оточення та покращення сприйняття інформації [1].

Доповнена реальність (AR) – проектування будь-якої цифрової інформації (зображення, відео, текст, графіка тощо) поверх екрана будь-яких пристроїв. В результаті реальний світ доповнюється штучними елементами та новою інформацією. Може бути реалізована за допомогою додатків для звичайних смартфонів та планшетів, окулярів доповненої реальності, стаціонарних екранів, проекційних пристроїв та інших технологій.

Загальна схема створення доповненої реальності завжди така: камера пристрою AR знімає зображення реального об'єкта; програмне забезпечення (ПЗ) пристрою проводить ідентифікацію отриманого зображення, вибирає або обчислює відповідне зображення візуальне доповнення, поєднує реальне зображення з його доповненням і виводить підсумкове зображення на пристрій візуалізації.

Основними способами виявлення безпілотних літальних апаратів (БПЛА) в електромагнітному (ЕМ) спектрі є:

- використання тепловізора інфрачервоного діапазону ЕМ хвиль;
- використання камер оптичного діапазону ЕМ хвиль;
- використання радіолокаційних станцій;
- здійснення радіомоніторингу.

Для виявлення об'єктів з температурою, що відрізняється від навколишнього середовища, використовуються інфрачервоні тепловізійні камери, що дозволяє вести спостереження з допомогою за БПЛА навіть в умовах обмеженої видимості і в темний час доби.

Для отримання найбільш інформативних та стабільних результатів можливе точне поєднання тепловізійних знімків із видимим зображенням.

Для цього застосовується тепловізор та фотокамера для одночасного ведення аерофотозйомки у видимому діапазоні.

Для виявлення БПЛА в оптичному діапазоні ЕМ хвиль існує активні та пасивні методи. Активними методами вважається метод анагліфів та метод визначення координат БПЛА у просторі. Пасивні методи включають у свій склад метод візуального спостереження та метод комбінованого стереоефекту.

Радіомоніторинг є отримання інформації з використанням технічних засобів на ділянці її проходження по лініях радіозв'язку [2].

В основному, включає діяльність з вивчення радіообстановки, пошуку, виявлення і контролю різних каналів зв'язку, інших джерел радіовипромінювань. Завданнями радіомоніторингу ефіру є:

- панорамний спектральний аналіз у реальному часі;
- пошук випромінювань від БПЛА, вимір їх параметрів, порівняння з базою даних визначення їх приналежності;
- запис радіосигналів зі службовими параметрами (частота, час, рівень сигналу, спектрограма тощо) та подальше їх відтворення;
- технічний аналіз радіосигналів у реальному часі та при відкладеній обробці;

Данні, які були отримані з різних джерел при виявленні БПЛА, передаються до програмного забезпечення (ПО) доповненої реальності. Також до ПО надсилаються відеозображення з камер у реальному часі. Різноманітні координати отримані завдяки відбитим сигналам є маркерами для промальовки БПЛА у AR. У ПО є базовий пресет 3D моделей БПЛА різного розміру, завдяки чому на дісплеї можна побачити приблизні розмірі та знаходження виявленого апарату.

Список використаних джерел.

1. Технологии и концепции Industry - Augmented Reality. URL: https://www.it.ua/ru/knowledge-base/technology-innovation/dopolnennaja-realnost-ar. 22.02.22

2. Годунов А. И., Шишков С. В., Юрков Н. К. Комплекс обнаружения и борьбы с малогабаритными беспилотными летательными аппаратами // Надежность и качество сложных систем. 2014. № 2 (6). С. 62–70. URL: https://cyber leninka.ru/ article/v/kompleks-obnaruzheniya-i-borby-smalogabaritnymi-bespilotny mi-letatelnymi-apparatami-1. 23.02.22

ВИКОРИСТАННЯ СИСТЕМИ АКУСТИЧНИХ ДАТЧИКІВ ДЛЯ ВИЯВЛЕННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

Воропаєв В.Ю., к.т.н., доц. Олейніков В.М.
Харківський національний університет радіоелектроніки,
кафедра МІРЕС, м. Харків, Україна
e-mail: vladyslav.voropaiev@nure.ua

Abstract. Review of methods for detecting unmanned aerial vehicles (UAVs). Detection of UAVs using an acoustic information channel. Methods of UAV detection using acoustic sensors are analyzed. Possibilities and advantages of using acoustic sensors for UAV detection are described. Advice and recommendations for improving UAV detection systems using acoustic sensors are given.

Використання безпілотних літальних апаратів (БПЛА) швидко зростає в широкому діапазоні споживчих застосувань, оскільки вони виявляються зручними та гнучкими в різних сферах діяльності та завданнях. Однак ця універсальність та простота використання призводить до швидкого розвитку загроз з боку зловмисників, які можуть використовувати БПЛА для злочинної діяльності, перетворюючи їх на пасивні або активні загрози. Необхідність захисту критичних інфраструктур та важливих подій від таких загроз, призвела до прогресу систем протидії БПЛА.

Нещодавні досягнення засобів протидії БПЛА пропонують системи, які включають велику кількість інтегрованих датчиків для виявлення загроз, за допомогою радіолокаційних, електрооптичних/теплових і акустичних датчиків. Електрооптичні і теплові камери пропонують високі можливості класифікації з точною локалізацією та дальністю, але обидві чутливі до параметрів навколишнього середовища. Радіолокаційні датчики традиційно є надійним вибором для виявлення, але їх класифікаційні можливості не є оптимальними. З іншого боку, акустичні датчики, як правило, надійні до умов навколишнього середовища та мають високі можливості виявлення та класифікації БПЛА. З недоліків можна виявити обмежений ефективний діапазон виявлення.

Система спостереження на основі акустичних датчиків використовує масиви мікрофонів, для отримання унікального акустичного портрету виявлених БПЛА [1]. Зазвичай БПЛА забезпечують унікальні акустичні портрети в певному діапазоні частот. Акустичні особливості виявленого БПЛА можна виділити з часової та частотної області. Методи, що базуються на акустиці, можуть покладатися на певні математичні методи аналізу акустичних сигналів, які здатні виділити сигнал виявленого БПЛА із фонового шуму.

БПЛА у польоті генерує акустичні хвилі, що приймаються акустичними мікрофонами, які перетворюють акустичне тиск на

електричний сигнал. Джерелами звукових хвиль, як правило, є рухові установки і лопаті повітряних гвинтів. У БПЛА з електричним двигуном основним джерелом звуку є видавлене лопаті повітряних гвинтів, а двигун майже не випромінює шуму.

Для виявлення акустичних сигналів БПЛА використовують решітки мікрофонів, оскільки для визначення місця знаходження БПЛА в просторі необхідно мінімум чотири мікрофони. Акустичні антенні решітки можуть ефективно використовуватися для виявлення та супроводу низько літаючих БПЛА на тактичних відстанях. У той самий час акустичні решітки, крім просторового накопичення сигналів, дозволяє оцінювати час приходу фронту акустичної хвилі у різні точки простору, що, своєю чергою, сприяє оцінці кута поширення хвилі щодо решітки, тобто. можна обчислити пеленг джерела випромінювання.

Показники спрямованості – одне з найважливіших показників джерел шуму авіації [2]. Чинники спрямованості випромінювання різних джерел застосовують у класичних підходах авіаційної акустики до розрахунку очікуваних рівнів шуму літаків на місцевості. Ці методи розрахунку також входять до методики прогнозу меж чутності та помітності малорозмірних безпілотних літальних апаратів з гвинтомоторною установкою.

Підсумовуючи вище сказане, можна вважати, що використання акустичних систем для виявлення БПЛА є перспективним методом, що має безліч позитивних сторін, а також можливості для нарощування потенціалу в дальності виявлення та точності місця визначення, що вирішується вибором масивів і конфігурацій мікрофонних решіток та їх ефективної обробки.

Список використаних джерел.

1. Карташов В.М., Олейников В.Н., Шейко С.А., Бабкин С.И., Корытцев И.В., Зубков О.В., Анохин М.А. Информационные характеристики звуковых сигналов малых беспилотных летательных аппаратов// Радиотехника. Всеукр. Межвед. Науч.-техн. Сборник. Вып 191. - Харьков, 2017. - С. 181-187.

2. Олейников В.Н., Шейко С.А., Бабкин С.И. Исследование характеристик акустического излучения малых беспилотных летательных аппаратов// Сборник научных трудов VI Международного радиоэлектронного форума “Прикладная радиоэлектроника. Состояние и перспективы развития (МРФ-2017)” Международная научная конференция “Радиолокация. Спутниковая навигация. Радиомониторинг”. 24-26 октября 2017 г. Харьков, Украина. – Изд. “Точка”. С.107- 110.

МІСЦЕ СТОРІТЕЛЛІНГУ У РОЗРОБЦІ ЕФЕКТИВНОГО ДИЗАЙНУ

Огієнко А.Є., к.т.н., проф. Колендовська М.М.
Харківський національний університет радіоелектроніки,
кафедра МІРЕС, м. Харків, Україна
e-mail: anastasiia.ohiienko@nure.ua

Abstract. Storytelling - the technology of creating a story and transmitting the necessary information to influence the emotional, motivational, cognitive sphere of the user. With its help, professionals in the field of visual content and design have the opportunity to communicate, share information and establish relationships with the user. This is a universal tool for creating the right impression of the product.

Під час створення та розробки веб та мобільних додатків, веб-сайтів одним з найважливіших процесів, який регулюють дизайнери є сторітеллінг. Сторітеллінг – технологія створення історії та передачі за її допомогою необхідної інформації з метою впливу на емоційну, мотиваційну, когнітивну сфери користувача.

За допомогою нього професіонали в області візуального контенту та дизайну мають можливість спілкуватися, обмінюватися інформацією та будувати взаємовідносини з користувачем. Це універсальний інструмент для створення правильного враження від продукту.

Для того, щоб побудувати якісний сторітеллінг, контент-менеджери та дизайнери використовують певну схему та модель роботи: на початку роботи над проектом моделюються портрети користувачів, визначаються їх болі та драматичні точки, а вже потім за допомогою правильного, логічного та послідовного дизайну створюються сценарії щодо вирішення проблем клієнтів. Тож, говорячи про історії, користувачі описують своє емоційне враження, тобто щось, що вплинуло на них на глибокому особистому рівні.

Таким чином, емоції відіграють важливу роль у сприйнятті сайтів, додатків та всього продукту у цілому. Згідно досліджень Дональда Нормана,професора когнітології та консультанта з юзабіліті компанії Nielsen Norman Group, вплив дизайну на враження людини від продукту відбувається на трьох рівнях та відповідає трьом сторонам дизайну.

Інтуїтивний дизайн — цей вид дизайну відбувається на підсвідомому та біологічному рівні мислення. Тобто людина може автоматично полюбляти чи ненавидіти певні об’єкти або предмети та це є початкова реакція на зовнішню оболонку.

Поведінковий дизайн — це те, як продукт чи додаток працює, функціонує, відчуття від їх використання, юзабіліті - тобто загальне враження користувача від їх використання.

Рефлективний дизайн — те, як продукт чи додаток змушують людину почуватися себе вже після початкової реакції та взаємодії з ним, коли клієнт асоціює цей продукт зі своїм життєвим досвідом та наділяє його значенням та цінністю.

Звідси зрозуміло, що важливо не тільки створити враження комфорту та функціональсті, але й знайти та створити між дизайном та користувачем легкий та зрозумілий зв'язок.

На базовому рівні створення історії та створення враження у користувача мають спільні елемнти: планування, дослідження та створення контенту. Сторітеллінг надає розробникам можливість зрозуміти суть та зміст продукту та цільову аудиторію. Історії допомагають ефективно донести до людей найбільш складні ідеї.

Сторітеллінг може надати наступні можливості, які допоможуть поліпшити процес створення продукту та враження від нього:

- Надання людського обличчя сухим даним;
- Спрощення складних ідей для команди;
- Підвищення ефективності спільної роботи команди;
- Визначення мети;
- Можливість зрозуміти первинного користувача;
- Швидке визначення задач проекту (напрямків, у яких повинен рухатися проект);
- Спрощення внутрішньої комунікації у великих організаціях;
- Надання інформації змісту та ценності для користувача.

Сторітеллінг допомагає командам розробників глянути на все з іншого боку. Здатність дотримуватися певного процесу залежить від багатьох факторів, який включає графік роботи, бюджет та мету.

Сторітеллінг — це спосіб швидко налагодити контакт між командами розробників, глибше проникнути в суть проекту та зрозуміти його. Враження та емоційне забарвлення, яке створює людина, отримує форму завдяки дизайну, контенту та взаємодії з користувачем. Оповідачі вміли налагоджувати контакт з людьми раніше, ніж були створені веб-сайти, — що робить сторітеллінг найціннішим інструментом дизайну для бізнесу.

Таким чином, сторітеллінг є одним з найважливіших інструментів для створення необхідного для користувача враження від продукту у будь-якій сфері життя. Він допомагає розробникам глибше пізнати суть продукту та точніше влучити у потреби клієнта. Завдяки сторітеллінгу дизайнер може відтворити правильний, чіткий та логічний сценарій щодо користування веб-сайтом та, як результат, залучити більшу кількість потенційних клієнтів продукту, що вказує на ефективність цього способу налагодження контакту між користувачем та розробником.

WEB-ДИЗАЙН, ЯК ПОЄДНАННЯ ПСИХОЛОГІЇ ТА МУЛЬТИМЕДІА

Гречко А.В., к.т.н., проф. Колендовська М.М.
Харківський національний університет радіоелектроніки,
кафедра МІРЕС, м. Харків, Україна
e-mail: anna.hrechko@nure.ua

Abstract. This article discusses several basic concepts of psychology used in interface design and web resources. Brief examples of the use of these concepts are given. Visual cues, Gestalt principles, short-term memory, the concept of motivation, and the concept of examples are just a few examples of how psychology influences web resource design. Psychology helps in choosing fonts, color palette and creating a website framework. Drawing up a portrait of the user and testing the prototype also do not do without the basics of psychology. Describes why a skilled web designer and designer should learn today.

З кожним роком Інтернет все глибше проникає в наше повсякденне життя, особливо, в умовах карантину. З'являється потреба переходу сфери послуг в цифровий простір. Щоб цей перехід був максимально продуктивним та вигідним для бізнесу, на допомогу приходять UI/UX дизайнери та розробники веб-ресурсів.

User Experience – важливий блок розробки ресурсу будь-якого характеру (інтернет-магазину, інформаційного ресурсу, реклами). На цьому етапі в гру вступає психологія.

Розробник повинен знайти баланс між цілями бізнесу та потребами користувачів. Якщо з цілями замовника (власника бізнесу) визначитись просто, то для розуміння потреб майбутніх користувачів необхідно провести кілька циклів досліджень, проектувань, тестувань, правок та нових досліджень.

Базові знання психології допомагають дизайнерам зрозуміти, як люди діють та чому діють саме так. Будь-які аспекти дизайну інтерфейсу користувача можуть бути суб'єктивними, проте психологія не може бути оскаржена.

Коли вперше користувач знайомиться з новим інтерфейсом, він розгублений. Щоб підвищити ефективність першої взаємодії рекомендовано використовувати психологічну концепцію візуальних підказок. Яскравим прикладом є іконографіка.

Завдяки розповсюдженим символам, до яких звик кожен з нас, інтерфейс стає інтуїтивно зрозумілим.

Психологічна концепція «принципі Гештальта» (закони близькості, подоби, симетрії та замикання) – засновані на інтуїтивному прагненні людей узагальнювати об'єкти на основі їхнього візуального компонування.

Групувати елементи керування необхідно в безпосередній близькості до вмісту, на який вони будуть впливати.

Потрібно враховувати, що людина не здатна утримувати велику кількість елементів у пам'яті. По можливості усувайте необхідність запам'ятовування інформації, зробивши її видимою або доступною. Наприклад, якщо користувач неправильно заповнив інформаційне поле, покажіть йому яке поле було невірним і чому. Необхідно демонструвати, як попередні рішення впливають на нинішню ситуацію.

Концепція мотивації. У 2010 році вчені в галузі маркетингу, соціальної психології та мотивації – Мінджунг Ку і Айєлет Фішбах – провели дослідження та встановили, що люди, швидше за все, будуть мотивовані, щоб закінчити завдання, якщо вони бачать, що ще необхідно зробити, а не те, що вони вже зробили.

Ця концепція використовується, наприклад, у процесі оформлення замовлення: розділити на етапи, показати скільки кроків залишилося, цим показуючи, що користувач майже завершив дію.

Концепція прикладів. Краще 1 раз побачити, ніж 100 разів почути – приказка, яка розкриває сутність концепції. Коли ви вводите нові функції в проект, продемонструйте, як ними користуватись (відео-інструкція, підказка, тощо).

Це тільки декілька прикладів як психологія впливає на дизайн веб-ресурсів. Під час збору цільової аудиторії необхідно зрозуміти, кому буде корисний майбутній ресурс, які потреби користувачів він повинен закривати, як зробити взаємодію комфортною та результативною.

User Interface також будується на основах психології: підсвідоме сприйняття кольорової палітри, розміру шрифтів, патернів. Тестування прототипів – ще один важливий етап проектування. Розуміння, як виправити недоліки дизайну та покращити usability продукту – справа психології.

Таким чином, можна зробити висновок, що бути просто дизайнером сьогодні – не достатньо. Сучасний висококваліфікований спеціаліст – ще й психолог, верстальник, соціолог та емпат.

Список використаних джерел.

1. Kirill Lipovoy. (2018, 22 червня). 10 психологічних концепцій для дизайнерів. https://cloudmakers.ru/10-psihologicheskih-kontseptsii-dlya-dizajnerov.

2. Susan M. Weinschenk (2011) 100 Things Every Designer Needs to Know About People (Voices That Matter). New Riders Publishing.

3. Jon Yablonski (2020) Laws of UX: Using Psychology to Design Better Products & Services 1st Edition. O'Reilly Media, Inc.

ОГЛЯД АСПЕКТІВ ЗАСТОСУВАННЯ СУЧАСНИХ ТЕХНОЛОГІЙ ДЛЯ СТВОРЕННЯ СЦЕНАРІЮ ТА ТРЕЙЛЕРУ ГРИ

Бірюков Д.К., к.т.н., проф. Колендовська М.М.
Харківський національний університет радіоелектроніки,
кафедра МІРЕС, м. Харків, Україна
e-mail: dmytro.biriukov@nure.ua

Abstract. This paper presents the classification of scripting genres, detailed analysis of systems for writing computer game scripts in the genre of "visual novel", detailed analysis of software for writing scripts, comparison of software for writing scripts, detailed analysis of software for creating video-trailer created video -trailer using pre-created animations.

Візуальні романи або новели (visual novel, скорочено - VN) користуються величезною популярністю в Японії і давно стали там одним з провідних жанрів. Як це часто буває, на Заході про настільки великої галузі ігрової індустрії багато хто навіть і не здогадуються. А ті, хто все-таки хоче вникнути в її суть, стикаються з великими потоками інформації і контенту. Для початку розберемося що це і в чому ж суть цих візуальних новел.

Розглянемо жанр ігор - візуальні новели. Ігри в жанрівізуальні новели – це симбіоз між книгою, фільмом та грою.

Найчастіше гравець просто поглинає кілотонни тексту, супроводжуваного всілякими спрайтами персонажів, декоративних тканин, спеціальними зображеннями і відео. Часом зустрічаються сюжетні розвилки. Залежно від вибору сюжет йде в своє русло, тому за одне проходження (або прочитання, як хочете) весь контент не помітити. Справжня кінцівка в більшості випадків відкривається лише після того, як ви познайомитеся з усіма сюжетними лініями, які називають рутами. Однак ніхто не змушує розробників дотримуватися єдиної формули. Деякі вважають за краще зовсім позбавляти гравця можливості вибору, і тоді сюжет слід суворої структурі, вплинути на нього ніяк не можна. Такі новели називають кінетичними, відсутність розвилок вони компенсують загальної опрацюванням всього, навіть другорядних дрібниць.

У теперішній час написання сценарію за будь-якої потреби займає набагато менше часу завдяки технологічному розвитку цієї галузі. Існує багато програмних засобів для робот из сценарним текстом. Я обрав декілька відомих мені для порівняльного аналізу: Microsoft Word, Final draft, Scrivener та Ultra Otliner.

Microsoft Word - Microsoft Word (часто - MS Word, WinWord або просто Word) - текстовий процесор, призначений для створення, перегляду, редагування та форматування текстових статей, ділових паперів, а також інших документів, з локальним застосуванням

простейших форм таблично-матричних алгоритмів. Випускається корпорацією Microsoft у складі пакетів Microsoft Office. Текуча версія є Microsoft Office Word 2019 для Windows та macOS, а також веб-версія Word Online (Office Online), не вимагає встановлення програм на комп'ютері.

Final draft – це програма для написання та форматування сценаріїв відповідно до стандартів подання, встановлених театральною, телевізійною та кіноіндустрією. Програма також може бути використана для написання таких документів, як сценографії, листи-запити, романи, графічні романи, рукописи та основні текстові документи. Програма допомагає спростити написання імен персонажів, місць дії. Присутні картки і робота зі сценами.

Scrivener- програма обробки текстів, розроблена спеціально для авторів (Scrivener надає систему організації для документів, заміток і метаданих. Це дозволяє користувачеві організовувати замітки, концепції, дослідження і цілі документи для легкого доступу та довідок (документи включають в себе текст, зображення, PDF, аудіо, відео, веб-сторінки і т.і.).

Ultra Outliner – програма яка дозволяє сценаристам відмовитися від паперових карток на користь віртуальних вже на етапі чернетки. З її допомогою можна істотно оптимізувати розробку історії, ґрунтуючись на ідеях Роберта Маккі і Сіда Філда. Ultra Outliner заснований на ідеї паперових карток, які можна перекладати на столі. Віртуальні картки можуть бути легко налаштовані і розфарбовані в процесі роботи.

У даній роботі наведено класифікацію жанрів сценаріїв, детальний аналіз систем для написання сценарії комп’ютерної гри в жанрі «візуальна новела», детальний аналіз програмного забезпечення для написання сценарію, порівняння програмного забезпечення для написання стценарію, детальний аналіз програмного забезпечення для створення відеороліку-трейлерустворено відеоролік-трейлер з використанням попередьо створених анімацій.

Список використаних джерел.

1. Офіційний сайт бази даних візуальних новел. [Електронний ресурс] URL: https://vndb.org/v?f=&o=a&p=12&s=rel (дата звернення: 17.02.2022).

2. Сторінка гри на сайті БДВН. [Електронний ресурс]
URL: https://vndb.org/v945 (дата звернення: 17.02.2022).

3. Сторінка гри на сайті БДВН. [Електронний ресурс]
URL: https://vndb.org/v751 (дата звернення: 18.02.2022).

ОГЛЯД АСПЕКТІВ ЗАСТОСУВАННЯ ІГРОВИХ ТЕХНОЛОГІЙ ДЛЯ СТВОРЕННЯ ВІЗУАЛЬНОЇ НОВЕЛИ

Зіноватна Д.В., к.т.н., проф. Колендовська М.М.
Харківський національний університет радіоелектроніки,
кафедра МІРЕС, м. Харків, Україна
e-mail: daryna.zinovatna@nure.ua

Abstract. This paper presents the classification of game genres, classification of game mechanics, detailed analysis of systems for creating graphic elements, detailed analysis of engines for creating games, review of methods for creating game scenes, description of functional requirements, developed graphical application interface, developed algorithm for dialogue.

Такий напрям комп'ютерних ігор, як «Візуальні новели» зародився ще в 1980 році, за базою даних візуальних романів [1]. На той момент цей напрям був виключно японським. Але він поступово розвивався і набрав обертів в 1993-х. Розробка візуальних новел на просторах країн СНД зародилася ще в 2011-х роках. Але особливий фурор в цьому жанрі стався після виходу «Нескінченного літа» в 2013 році. Тоді ж і стався не тільки фурор серед читачів, але і розробників, що прийшли в цей жанр комп'ютерних ігор.

Візуальний роман - жанр комп'ютерних ігор, підвид текстового квесту, де глядачеві демонструється історія за допомогою графічних елементів - статичних (або анімованих) зображень персонажів та фону, виведення на екран тексту, а також звукового і (або) музичного супроводу. Нерідко використовуються і вставки повноцінних відеороликів. Візуальні романи включають в себе велику кількість жанрів - наукову фантастику, фентезі, пародійні комедії, жахи, любовні романи. Так само, деякі візуальні новели створені для навчання дітей наукам, соціальним аспектам, фінансової грамотності, тощо.

Візуальні новели унікальні тим, що це інтерактивна історія, в якій цікавий сюжет і здатність творчої команди створити якісне оповідання є запорукою успішності гри. Однак на відміну від розробників ігор, компанії-видавці візуальних новел продають не «інтерактивність», а історію. Читач не взаємодіє з сюжетом ВН досить активно (виключаючи суміші з візуальних новел і інших ігрових жанрів).

Візуальні новели поділяються по механиці. Існують з виборами, кінетичні, звукові та симулятори побачень. Проаналізуємо їх.

- Візуальна новела з виборами – найпопулярніший вид візуальних новел, де рушієм сюжету є вибір читача.

Приклади: Katawa Shoujo, Rewrite, Clannad.

- Кінетична новела (Kinetic Novel) - характерною рисою цього підвиду візуальних новел є повна відсутність розгалужень сюжету, вибору варіантів.

Приклади: A Requiem For Innocence, Umineko no Naku Koro ni Chiru, Planetarian ~Chiisana Hoshi no Yume~.

- Звукова новела (Sound Novel) – підвид кінетичної новели, за умовою що це новела, в якої більша увага приділяється звуковому супроводу.

Приклади: Higurashi no Naku Koro ni, Umineko no Naku Koro ni.

- Симулятор побачень – метою даного жанру є досягнення певних відношень між головним героєм та одним з персонажів.

Приклади: Шкільні дні, The Second Reproduction, Maji de Watashi ni Koishinasai.

- RPG візуальні новели – візуальні новели з елементами РПГ-ігор. Вони складаються з двох частин: 1 – розповідь сюжету виконується шляхом діалогів у жанрі «візуальних новел», 2 - рух по сюжету виконується у жанрі РПГ, де головний герой подорожує по локаціям і виконує певні дії. Перевага надається жанру РПГ.

Приклади: Undertale: Forgotten Story, Нарака, Devil of the mirror.

- ADV візуальні новели – жанр схожий на РПГ новелу, але в ньому переважають риси притаманні візуальним новелам, а подорож через локації гри здійснюється шляхом натискання кнопок на екрані, а не на клавіатурі, як у випадку з РПГ новелами.

Приклади: Clannad, Ever 17: The Out of Infinity, Planetarian.

Механіки візуальних (з вибором, кінетичних та симуляторів) та Adventure новел можна поділити за часом. Розрізняють 5 видів: менш 2 годин; від 2-х до 10-ти годин; від 10-ти до 30-ти годин; від 30-ти до 50-ти годин; більше 50-ти годин.

Для реалізації комп’ютерної гри в жанрі «Візуальна новела» було обрано механіку звичайної новели з виборами, але невеликою за часом проходження (від 2-х до 10-ти годин). Це більше підходить для цілей гри, краще сприймається користувачами і має більш розширену цільову аудиторію.

У даній роботі наведено класифікацію жанрів гри, класифікацію механік гри, детальний аналіз систем для створення графічних елементів, детальний аналіз движків для створення гри, огляд методів створення ігрових сцен, опис функціональних вимог, розроблено графічний інтерфейс додатку, розроблено алгоритм діалогу, розроблено алгоритм вибору.

Список використаних джерел.

1. Офіційний сайт бази даних візуальних новел. [Електронний ресурс] URL: https://vndb.org/v?f=&o=a&p=12&s=rel (дата звернення: 17.02.2022).

ВИКОРИСТАННЯ МУЛЬТИМЕДІЙНИХ ТЕХНОЛОГІЙ ДЛЯ СТВОРЕННЯ АНІМАЦІЙНИХ ФІЛЬМІВ

Кащавцев М.В., к.т.н., проф. Колендовська М.М.
Харківський національний університет радіоелектроніки,
кафедра МІРЕС, м. Харків, Україна
e-mail: maksym.kashchavtsev@nure.ua

Abstract. The entertainment industry is not the only area in which 2D and 3D graphics are in demand. It is widely used in education, health, architecture and, of course, advertising. 3D animation has become the most popular among all types of animation, especially among the younger generation.Viewers usually like 3D animation: they are bright, attractive, and convey emotions well. Therefore, many brands prefer to tell stories, create a trusting image and attract new customers with the help of videos with 3D animation.

In this paper we will consider the methods and possibilities of creating different kinds of films, their development and current opportunities.

У сучасному світі 2D та 3D графіка є звичною частиною індустрії розваг. За допомогою нього можна робити гри, мультфільми та фільми. С розвитком комп'ютерних технологій 3D графіка стала більш динамічною, чіткої і класною.

Індустрія розваг не єдина сфера, в якій затребувана 2D та 3D графіка. Вона знайшла широке застосування в сфері освіти, охороні здоров'я, архітектурі і, звичайно, рекламі. 3D-анімація стала найпопулярнішою серед всіх видів анімації, особливо у молодого покоління.

Глядачам звичайно подобається 3D-анімації: вони яскраві, привабливі, добре передають емоції. Тому багато брендів вважають за краще розповідати історії, створювати довірчий імідж і залучати нових клієнтів саме за допомогою роликів з 3D-анімацією.

В цій роботі розглянемо методи та можливості створення різного роду фільмів, їх розвиток та сучасні можливості.

І зараз в наш час, майже у кожної людини є комп'ютер і програми за допомогою яких можна створити мультфільм на 2D або 3D графіку. На даній роботі ми будемо робити короткий мультфільм, зроблений на 3D програмою і відео редакторі.

Важливе поняття грає розуміння як зробити мультфільм щоб він усім сподобався. Для дітей зазвичай грають мультфільми з веселими персонажами з веселою і (або) повчальною історією. Також ці історії бувають корисні і для дорослих. Для такого роду існують такі студії як Disney, Pixar, Ghibli, Netflix і автори деяких каналів на YouTube каналах.

Сюжет - Подія або ряд пов'язаних між собою і послідовно розвиваються подій, які становлять зміст художнього твору [1-3].

Сценарій - літературно-драматичний твір (що містить докладний опис дії і текст промов персонажів), на основі якого створюється фільм [1-3]. Тут також розкривається, і інша частина фільму яка може підійти до дорослого.

Після сценарію йде створення персонажа, спочатку малюємо на папері, робимо ескіз персонажа, потім цей малюнок переносимо в 3D програму і моделюємо персонажа або можна зліпити його, (в програмі є скульптування або можна взяти таку програму як Zbrush, це найкраща програма для скульптування) . Після того як змоделювали персонажа, наносимо кольору і робимо клунь.

3D-анімація - це створені за допомогою комп'ютерної графіки об'єкти, що рухаються в тривимірному просторі. Такі можливості є в програмних продуктах 3D Max і 3D Maya, а також Houdini і на Adobe Premier Pro.

Ріг - термін в комп'ютерній анімації, який описує набір залежностей між керуючими і керованими елементами, створений таким чином, щоб керуючих елементів було менше, ніж керованих. Призначення - спростити маніпуляцію великою кількістю об'єктів.

Після Рігг ми створюємо сцени і об'єкти, а потім ставимо туди персонажа і анімуємо його. Пізніше йде рендер по частинах відео.

Робота в відео редакторі простіше ніж в 3D. Потрібно всього лише розставити ті частини відео по порядку і видалити непотрібні фрагменти. Додаємо звук (під звуком мається на увазі музичний супровід) і теж редагуємо. У коні ми створюємо Рендер відео і відео готово.

Список використаних джерел.

1. Ріггінг і позування персонажа в Blender - URL: https://www.3dtoday.ru/blogs/argon/rigging-and-posing-the-character-in-blender (дата звернення: 18.02.2022).

2. Використання Драйверів - URL: http://blender3d.org.ua/tutorial/%D0%94%D1%80%D0%B0%D0%B9%D0%B2%D0%B5%D1%80%D1%8B_%D0%B2_Blender_25x.html (дата звернення: 18.02.2022).

3. Уроки по blender - URL: http://blender3d.com.ua/ (дата звернення: 03.02.2022).

4. Чем отличается 3D от 2D (мнение профессионалов)? - URL: https://www.hwp.ru/articles/CHem_otlichaetsya_3D_ot_2D__28mnenie_professionalov_29__82586/ (дата звернення: 18.02.2022).

5. Основи анімації в Animate - URL: https://helpx.adobe.com/ru/animate/using/animation-basics.html (дата звернення: 14.02.2022).

ФРАКТАЛЬНІ МЕТОДИ ІДЕНТИФІКАЦІЇ МАЛОРОЗМІРНИХ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ ПО АКУСТИЧНОМУ ВИПРОМІНЮВАННЮ

Зінченко М.Р., к.т.н., доц. Олейніков В.М.
Харківський національний університет радіоелектроніки,
кафедра МІРЕС, м. Харків, Україна
email: d_res@nure.ua

Abstract. The paper discusses methods for analyzing the fractality of acoustic radiation from UAVs. An experimental dependence of the Hurst exponent on the engine speed is obtained.

Специфічні властивості БПЛА - відносно невисока вартість, економічність, простота експлуатації, оперативність розгортання та введення в дію - ці фактори призводять до масовості застосування БПЛА в протиправній діяльності. У зв'язку з цим актуальною стає задача оперативної ідентифікації БПЛА і застосування спеціальних технічних засобів, які забезпечують ефективну адекватну відповідь на виникаючу загрозу. На цей час існує ряд методів ідентифікації - методи мел-кепстральних коефіцієнтів, спектрального аналізу, фрактальні методи. Але не існує абсолютно ефективних і надійних методів виявлення БПЛА тому потрібно шукати, розглядати і досліджувати нові методи і алгоритми та вдосконалювати вже існуючі.

Останнім часом отримали розвиток методи дослідження часових рядів, згідно яких часові послідовності змінювання досліджуваних сигналів розглядаються як сукупність періодичних та хаотичних процесів. Хаотична компонента в таких сигналах міститься як в змінюванні частот так і в динаміці форми запису сигналу [1]. Для порівняння фрактальних властивостей різноманітних процесів часто застосовують метод Херста. В цьому методі для аналізу часових рядів використовується безрозмірний показник, який визначається відношенням розмаху R накопиченого відхилення від середнього до середньоквадратичного відхилення S (R/S) [2]. Апроксимуючи визначену фрактальну функцію прямою лінією можно визначіти кутовий коефіцієнт H, який називають показником Херста.

Застосування показника Херста для частотних та енергетичних спектрів аналізованих динамічних процесів являє собою гарний приклад комбінованої методики застосування теорії фракталів та вейвлет-аналізу для виявлення особливостей часових рядів [3]. При цьому аналізуються множини, що характеризують частотний спектр і енергії частотних складових.

На основі експериментальним даних, отриманих у різних режимах польоту БПЛА, проведен аналіз на предмет хаотичності та фрактальних ознак. Для цього використовувався показник Херста, як міра фрактальної

розмірності. Проведемо аналіз залежності показнику Херста від частоти обертання повітряного гвинта. Для цього на етапі експериментального дослідження було проведено акустичні записи роботи лабораторних моделей БПЛА для повітряних гвинтів розміром 6 та 8 дюймів. В результаті проведених розрахунків було отримано графіки, на яких побудовані лінії нахилу, на основі яких розраховується показник Херста.

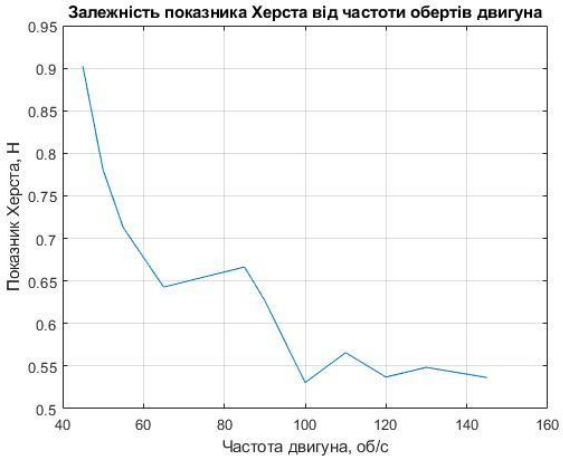


Рисунок 1

На основі проведених розрахунків можна зробити наступні висновки. Для гвинта діаметром 6 дюймів спостерігаються коливання показнику Херста близько до значення *H=0,83* і зі зміною частоти обертів гвинта серйозних змін не спостерігається. На рис. 1 побудовано графік залежності показнику Херста від обертів частоти обертів двигуна, де видно поступове зниження показнику Херста від *H=0,90* при частоті обертів гвинта 45 об/с, до *H=0,53* при частоті обертів гвинта 145 об/с. При чому при перевищенні повітряним гвинтом частоти 100 об/с показник Херста майже перестає змінюватись і коливається в межах *H=0,52* до *H=0,56*, що може вказувати на перехід сигналу в шумоподібний.

На основі представлених результатів можна зробити висновки, що отримані акустичні сигнали є персистентними, тобто мають ознаки хаотичного сигналу, так як показник Херста має значення *H>0,5*. Отже можна припустити, що на показник Херста в більшій ступені має вплив розмір гвинта, а зміна швидкості його обертання суттєво не змінює представлення про об’єкт спостереження. Дані результати були отримані в лабораторних умовах при роботі з макетами БПЛА, тому вони не повністю відображають характеристики БПЛА під час польоту.

Список використаних джерел.

1. Р.С. Ахметханов, Е.Ф. Дубинин, В.И. Куксова - Анализ временних рядов в диагностике технических систем. URL:https://mospolytech.ru/mio/iblock/908/ – 20.12.2021 р.

2. Федер Е. Фракталы : пер с англ.. – М.:Мир, 1991. – 254 с.

3. Агарев К.М., Ахметханов Р.С., Дворецкая Т.Н.,Юдина О.Н. Комплексный анализ особенностей и устойчивости спектрального состава временного ряда: // Проблемы машиностроения и автоматизации. 2006. №2. С. 24-32.

КЛЮЧОВІ ТЕХНОЛОГІЇ СИСТЕМ ЗВ'ЯЗКУ ШОСТОГО ПОКОЛІННЯ

Лозовська Г.О., к.т.н., доц. Горелов Д.Ю.
Харківський національний університет радіоелектроніки,
кафедра МІРЕС, м. Харків, Україна
email: hanna.lozovska@nure.ua

Abstract. The paper discusses possible technologies that will be deployed for 6G communication. 6G communication systems should be designed with native AI and machine learning support to ensure optimum efficiency. Blockchain will be-come an important database management technology.The use of SWIPT provides a solution to a number of problems that can lead to significant gains in terms of energy consumption, spectral efficiency and management of wireless interfer-ence.

Вимоги до мереж, які можна назвати повноцінними мережами шостого покоління, поки що не сформовані, проте Китай ще в 2018 році оголосив про початок розробок, які дозволять зробити якісний прорив. Нещодавно компанія Samsung опублікувала документ, який показує, що можна чекати від цієї технології. Основними користувачами 6G будуть люди та машини. Головними технологіями стануть розширена реальність, високоякісна мобільна голограма і цифрові репліки. Якщо при розробці 5G основний акцент робився на підвищенні швидкості пересилання, у 6G, вважають у Samsung, варто зосередитися на трьох аспектах. Це продуктивність, архітектура і надійність. Швидкість пересилання даних у мережах 6G зросте до 50 разів: з 20 Гбіт/с до 1000 Гбіт/с. Затримки в пересиланні повинні знизитися на порядок, а саме з 1 мс до 0.1 мс.

Виходячи з цих вимог розглянемо технології, які стануть базою для побудови мережах зв'язку 6G.

Штучний інтелект (ШІ). Хоча структура базової мережі 5G підтримує інтелектуальні функції, вводячи новий тип мережевих функцій (наприклад, аналітику мережевих даних), можливості використання ШІ в мережевих операціях та управлінні обмежені. Тобто 5G надає ШІ як послугу надвисокого рівня. Натомість системи зв'язку 6G повинні бути спроектовані з нативною підтримкою ШІ та машинного навчання – не лише як базової функціональності, а й для забезпечення оптимальної ефективності. З погляду архітектури, запуск розподіленого ШІ на периферії може забезпечити максимальну продуктивність, одночасно вирішуючи проблеми управління даними окремих осіб та підприємств. Вбудована підтримка ШІ в 6G спрямована на надання послуг ШІ в будь-якому місці та в будь-який час і постійно покращуватиме продуктивність системи та зручність роботи користувачів за рахунок постійної оптимізації. Отже, мережева архітектура 6G з нативною підтримкою ШІ

принесе «мережевий ШІ», відійшовши від сьогоднішнього централізованого «хмарного ШІ».

Для підтримки нових технологій доповненої реальності (AR/VR/MR) необхідні надвисокі швидкості передачі даних до десятків Тбіт/с. Субтерагерцовий і міліметровий діапазони будуть базовими в мережах 6G, у той час як смуга нижнього ТГц-діапазону (0.3-1.0 ТГц) буде основним кандидатом для передачі даних на короткі відстані, наприклад, для використання всередині приміщень або в каналах пристрій-пристрій. ТГц-діапазон дозволить використовувати широкий спектр додатків, вимогливих до якості зв’язку та чутливих до затримок.

Технології OWC, такі як оптичний зв'язок, зв'язок у видимому світлі, зв'язок із оптичною камерою та зв'язок FSO на основі оптичного діапазону – це технології передачі поза радіочастотним діапазоном, що дозволють мінімізувати вплив електромагнітного поля на навколишні об'єкти. Зв'язок, заснований на оптичних бездротових технологіях, може забезпечити дуже високі швидкості передачі даних, низькі затримки та безпечний обмін даними.

Блокчейн стане важливою технологією управління базами даними у майбутніх системах зв'язку. Розподіл даних по численним вузлам чи обчислювальним пристроям забезпечить їх безпечну автономну взаємодію та надійність підключення масштабних мереж Інтернету речей.

3D-мережі. Система 6G інтегруватиме наземні та бортові мережі для підтримки зв'язку для користувачів у вертикальному напрямку. Саме тому безпілотні літальні апарати (БПЛА) стануть важливим елементом 6G мереж. БПЛА можуть служити декільком цілям, таким як покращення мережевого підключення, моніторинг навколишнього середовища, побудова крупно масштабних систем управління транспортом тощо.

Одночасна бездротова передача інформації та енергії (SWIPT) є новітньою технологією, що дозволяє бездротовим вузлам зв'язку перезаряджати свої батареї від радіочастотних сигналів при декодуванні інформації. Крім того, використання даної технології забезпечує вирішення низки проблем у бездротовій передачі енергії, що може призвести до помітних виграшів з погляду енергоспоживання, спектральної ефективності та управління завадами бездротового зв'язку.

Список використаних джерел.

1. Сети 6G. Путь от 5G к 6G глазами разработчиков. От подключенных людей и вещей к подключенному интеллекту. / пер. с англ. В. С. Яценкова. – М.: ДМК Пресс, 2022. – 624 с.

2. T.D. Ponnimbaduge Perera, D.N.K. Jayakody, S.K. Sharma, S. Chatzinotas, J. Li. Simultaneous Wireless Information and Power Transfer (SWIPT) Recent Advances and Future Challenges. IEEE Commun. Surv. Tutorials, 20 (1) (2018), pp. 264-302.

3. B. Kazi, G. Wainer. Next Generation Wireless Cellular Networks : Ultra-Dense Multi-Tier and Next generation wireless cellular networks : ultra-dense multi-tier and multi-cell cooperation perspective. Wirel. Networks, 25 (4) (2019), pp. 2041-2064

ОГЛЯД ТЕХНОЛОГІЙ БЕЗПРОВІДНОЇ ПЕРЕДАЧІ СИГНАЛІВ ТА ЕНЕРГІЇ

Путівцев А.П., к.т.н., доц. Горелов Д.Ю.
Харківський національний університет радіоелектроніки,
кафедра МІРЕС, м. Харків, Україна
e-mail: d_res@nure.ua

Abstract. The article deals with technologies for wireless transmission of information and energy using electromagnetic waves. Concepts are provided about the existing four kinds of system configuration for realizing wireless signal and power transmission, such as separate receiver, time interruptions, power separation, and antenna switching.

Інтеграція технологій передачі мікрохвильової енергії (ПМЕ) та безпровідних комунікацій відкрила нову дослідницьку область, звану безпровідну передачу сигналів та енергії (БПСЕ). Через високе послаблення поширення радіохвиль БПСЕ досі в основному використовувались в невеликих безпровідних мережах з вузлами малої потужності, такими як RFID та сенсори. Однак, з розвитком мереж зв’язку п'ятого покоління, нові безпровідні технології, такі як невеликі сенсорні мережі та MIMO, можуть значно скоротити витрати на поширення за рахунок скорочення відстаней зв'язку. У той же час очікується, що споживання енергії безпровідними пристроями буде постійно знижуватися. Тому прогнозується, що БПСЕ стане незамінним будівельним блоком для багатьох комерційних та промислових безпровідних систем у майбутньому.

Наразі існує чотири типові системні конфігурації для реалізації БПСЕ.

Роздільний приймач.

У цій архітектурі схеми збору енергії та декодування інформації реалізовані у двох роздільних приймачах, як показано на рис. 1, а). Ця архітектура приймача може бути реалізована з використанням готових компонентів для приймачів збирання енергії та приймачів інформації. Ця архітектура дозволяє одночасно і незалежно виконувати як збирання енергії, так і декодування інформації. Інформація про стан каналу і зворотний зв'язок з приймачем можуть бути використані для оптимізації між потрібним рівнем збору енергії і швидкістю передачі інформації.

Часове перемикання (ЧП).

Архітектура ЧП, зображена на рис. 1, b), використовує одну антену для збору енергії та декодування інформації. Приймач, який використовується в цій архітектурі, містить модуль збору енергії, декодер інформації та перемикач для перемикання між модулем збору енергії та декодером інформації в системі. Потужність передачі сигналу та коефіцієнт ЧП можуть налаштовуватися для різних цілей проектування

системи на основі вимог якості зв'язку.

Поділ потужності (ПП).

У цьому режимі приймач, зображений на рис. 1, c), до виконання операції обробки сигналу ділить прийнятий сигнал на два потоки різних рівнів потужності із заданим співвідношенням поділу потужності. Після цього обидва сигнали передаються в декодер інформації та схему збору енергії відповідно. У цій архітектурі не потрібно жодних додаткових змін у конструкції звичайних систем зв'язку, крім схеми приймача. У кожній приймальній антені співвідношення розподілення потужності може бути оптимізовано таким чином, що швидкість передачі інформації та зібрана енергія будуть збалансовані відповідно до вимог системи.

Комутація антен.

Перемикання антени між збиранням енергії та обробкою інформації є нескладним процесом і може використовуватися для реалізації БПСЕ, як показано на рис. 1, d). Наприклад, у той час як більшість антен у приймачі зайнято процесом обробки інформації, решта антен може працювати для збирання енергії. Порівняно з часовим перемиканням і поділом потужності, перемикання антен порівняно простіше та привабливіше для практичних проектів, що реалізують протокол БПСЕ. Крім того, при оптимальному режимі комутації антен можна легко розширити цю архітектуру, включивши до неї більше антен для підтримки нових технологій, таких як масиви з багатоканальним входом / багатоканальним виходом (MIMO).

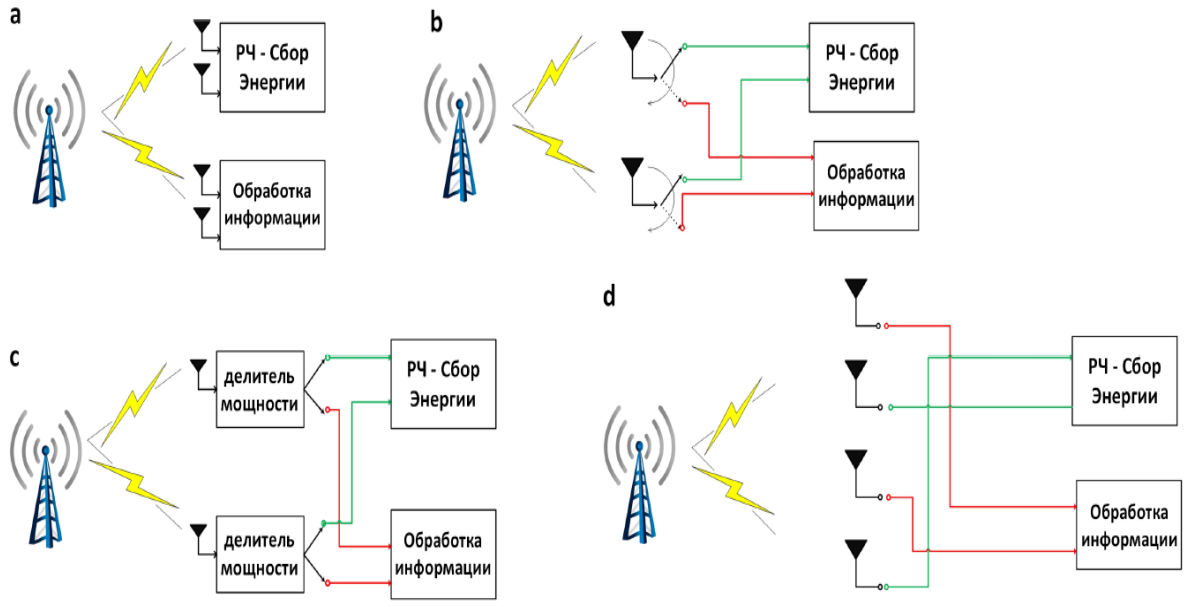


Рисунок 1

Незважаючи на швидкий прогрес з теоретичної точки зору, реалізація БПСЕ, як і раніше, стикається з багатьма проблемами. Спроби дослідників з подолання теорії та практики МБПСЕ призвели до нещодавньої появи нових тенденцій: використання багато частотних МБПСЕ, когнітивне радіо з підтримкою БПСЕ, повно дуплексний зв'язок з підтримкою БПСЕ, бістатичні радіолокаційні системи з підтримкою БПСЕ, БПСЕ з попереднім кодуванням рівнів сигналу, неортогональний множинний доступ з БПСЕ, сенсорні мережі з підтримкою БПСЕ, мережі D2D з підтримкою БПСЕ.

Список використаних джерел.

1. Yuen C. et al. Feature Topic on Energy Harvesting Communications. IEEE Commun. Mag. Vol. 4 and 6. Apr. and June 2015.

2. Zhang R. and Ho C. MIMO Broadcasting for Simultaneous Wireless Information and Power Transfer. IEEE Trans. Wireless Commun. Vol. 12. № 5, 2013. P. 1989-2001.

3. Димитров Г.Л. Беспроводная передача информации и энергии на основе микроволн // Научный журнал. 2017. № 9. С. 11-21.

ВПЛИВ ШВИДКОСТІ РУХУ БПЛА НА ТОЧНІСТЬ ВИЗНАЧЕННЯ КООРДИНАТ ПАСИВНИМ СОДАРОМ

Голозубов Р.О., к.т.н., доц. Олейніков В.М.
Харківський національний університет радіоелектроніки,
кафедра МІРЕС, м. Харків, Україна
email: d_res@nure.ua

Abstract. Using the method of simulation modeling, the influence of the speed of movement of the UAV on the accuracy of determining the coordinates is analyzed. The source of this error is the Doppler effect.

Виявлення та визначення координат малих безпілотних літальних апаратів (БПЛА) ускладнюється їх низькою помітністю як в електромагнітному, так і в оптичному діапазоні довжин хвиль, а також особливістю траєкторії їх польоту. Акустичні методи спостереження забезпечують виявлення та визначення координат БПЛА практично у будь-яких погодних умовах незалежно від часу доби [1]. Пасивний метод акустичної локації визначення координат має деякі обмеження, які можна досліджувати методом імітаційного моделювання. Удосконалення методів пеленгації БПЛА шляхом прийому та обробки їх акустичних сигналів є актуальним завданням.

Для вимірювання кутових координат джерела акустичного випромінювання БПЛА у пасивних содарах використовується масив мікрофонів різної конфігурації, який дозволяє приймати акустичні сигнали і отримувати первинні координати. Використовуючи функцію взаємної кореляції поміж сигналами у кожній вимірювальній базі можна визначити напрямок на джерело акустичного випромінювання.

У залежності від вигляду первинних координат, що визначають, розрізняють кутомірний, різніцево-дальновимірний і комбінований методи. Різніцево-дальновимірний метод або метод гіперболічного позиціонування забезпечує вимірювання кутових координат і дальності до джерела випромінювання. Для реалізації різніцево-дальновимірного методу визначення просторових координат використовується не менш як чотири мікрофона, які дозволяють отримати три незалежних різниці дадьностей до джерела випромінювання. Геометричне місце точок для двовимірного випадку, яке відповідає визначеної різниці часу приходу до двох мікрофонів, - це гіпербола, а місце розташування джерела випромінювання на площині - це точка перетину двох гіпербол.

Для перевірки ефективності алгоритму, який застосовується, для розрахунку координат содару створена імітаційна модель пересування БПЛА у просторі та формування широкосмугового акустичного випромінювання. Для проведення розрахунків вводяться розміри, орієнтація баз та місце розташування содара. У процесі моделювання

безперервно, для кожної дискрети часу, розраховуються затримки акустичного сигналу, які з'являються під час прийому сигналу, у кожному мікрофоні мікрофонної решітки пасивного содару.

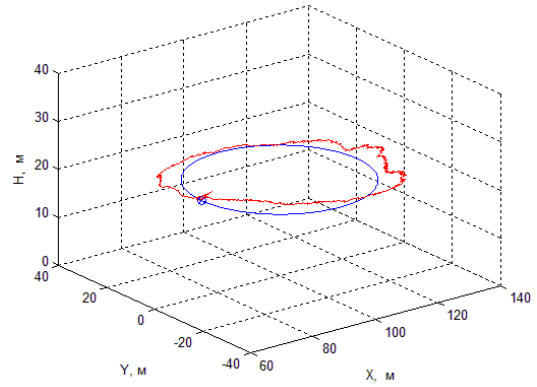


Рисунок 1

Надалі задається необхідне відношення сигнал/шум сигналу, що обробляється, вводиться врахування відбиттів від земної поверхні з коефіцієнтом відбиття, який потрібен.

У разультаті роботи програми, яка реалізує імітаційну модель, формуються аудіофайли, аналогічні аудіофайлам на виході мікрофонної решітки содара. Зіставляючи задані траєкторні параметри руху БПЛА у імітаційній моделі та результати розрахунку координат БПЛА за даними содара, можна отримати значення абсолютних значень похибки алгоритму, який використовується, для визначення місця розташування і умов проведення модельного експерименту.

Задамо у модельному експерименті рух БПЛА по колу радіусом 25 м, віддалення центру кола від содару 100 м, висоту польоту 20 м, тривалість польоту 5 с, швидкість руху 31,4 м/с. Максимальна швидкість руху квадрокоптера DJI Phantom 3 PRO складає 20 м/с, але у модельному експерименті, для отримання більш виражених результатів, можно задати більш високі значення швидкості. Так, на рис.1 представлені результати, отримані у моделі пасивного содара. Задана траєкторія - синій колір лінії, вимірена содором - червоний колір лінії. Спостерігається помітне відхилення траєкторії, яка вимірена содаром, від заданої у експерименті. Кругова траєкторія руху БПЛА трансформується у еліптичну. З підвищенням швидкості відмінності зростають. Причиною цього явища є ефект Доплера. Це відбувається тому, що радіальні швидкості джерела звуку відносно двох мікрофонів вимірювальної бази содара різняться з-за розносу мікрофонів у просторі. Відповідно, існує різниця швидкостей Доплера між першим і другим мікрофонами для кожної пари мікрофонів вимірювальної бази содара. Це, у свою чергу, приводить до додаткового зсуву положення ВКФ і модифікації координат, визначених содаром.

Список використаних джерел.

1.Kartashov V.M., Oleynikov V.N, Sheyko S.A., Babkin S.I., Koryttsev I.V., Zubkov O.V., Anokhin M.A. Information characteristics of sound radiation of small unmanned aerial vehicles. Telecommunications and Radio Engineering (English translation of Elektrosvyaz and Radiotekhika), V.77(10), 2018, pp. 915-924.

ОГЛЯД ТА АНАЛІЗ ЗАСОБІВ 3D-МОДЕЛЮВАННЯ

Рогинский С.В., к.т.н., проф. Колендовська М.М.
Харківський національний університет радіоелектроніки,
кафедра МІРЕС, м. Харків, Україна
e-mail: serhii.rohynskyi@nure.ua

Abstract. In computer graphics, 3D modeling is the process of developing a mathematical representation of any three-dimensional surface of an object using specialized software. The simulation product is a 3D model. It can be represented as program code or displayed in a viewport as a 3D model, as well as a two-dimensional image created by a rendering process. 3D models can be created manually or automatically, including using a 3D scanner. Making models by hand is similar to creating a sculpture in the plastic arts.

У комп'ютерній графіці 3D-моделювання — це процес розробки математичного представлення будь-якої тривимірної поверхні об'єкта за допомогою спеціалізованого програмного забезпечення. Продукт моделювання є 3D-модель. Вона може бути представлена у вигляді програмного коду або відображена у в’юпорті чи в’ювері, як 3D-модель, а також за допомогою двовимірного зображення, що створюється за допомогою процесу рендерингу. 3D-моделі можуть створюватись вручну або автоматично, у тому числі за допомогою 3D-сканера. Виготовлення моделей вручну є подібним до створення скульптури в пластичному мистецтві.

3D-моделі представляють 3D-об'єкт використовуючи набір точок в 3D-просторі, поєднаних між собою різноманітними геометричними об'єктами, як от трикутниками, лініями тощо.

На сьогодні в літературі розглянуті наступні категорії алгоритмів 3D моделювання:

1. Сплайнове моделювання (термін «сплайн» означає криві, що бувають різних типів): NURBS — поверхні NURBS визначаються кривими, на які впливають «важкі» контрольні точки. Крива слідує за точками (але не обов'язково дотикається до них). Збільшення ваги точки притягне криву ближче до неї. NURBS є насправді гладкими поверхнями, а не їхніми імітаціями за допомогою маленьких плоских поверхонь, тому цей метод часто застосовують для моделювання органічних форм. Часто термін NURBS використовується для позначення усіх методів сплайнового моделювання, перерахованих нижче:
   - Патчі і криві Безьє — простий тип NURBS;
   - Бі-сплайни (англ. Bi-spline) — це спеціальний тип сплайнів, які можуть бути швидко обчислені, як сума базових функцій;
   - Rational;

- Non-uniform (нерівномірні) — дозволяє можливість нерівномірної параметризації вздовж поверхні;

2. Полігональне моделювання — точки в 3D-просторі, вершини (англ. Vertex), з'єднані між собою лінією — ребром (англ. Edge), утворюють поверхню (англ. Faces) за законами створення геометричних площин. Набір об'єднаних площин називають полігональною сіткою (англ. Polygon mesh). Більша частина 3D-моделей сьогодні будується як текстуровані багатокутні моделі, оскільки вони досить гнучкі і комп'ютер може відрендерити їх досить швидко. Однак, багатокутники є плоскими й можуть тільки приблизно передати вигнуті поверхні, використовуючи багато багатокутників. Процес перетворення гладких поверхонь в багатокутники називається тесселяцією;
3. Моделювання за допомогою сабдивів (англ. Subdivision surfaces) — один із сучасних алгоритмів, який прогресивно розвивається і все більш нарощує конкуренцію двом попереднім.
4. Процедурне моделювання — таке моделювання дозволяє оперувати масштабними проектами, вимагає у більшості пайплайну, тому використовується великими студіями комп'ютерної графіки;

Таким чином, в роботі розглянуті та перераховані математичні підходи, що інтегровані в тому чи іншому вигляді у програмне забезпечення і виділяють за своїми можливостями різні алгоритми для створення однієї і тієї ж моделі, кожна із яких має своєрідні властивості.

Список використаних джерел.

1. M. Ivanov, O. Sergiyenko, V. Tyrsa, P. Mercorelli, V. Kartashov, W. Hernandez, S. Sheiko, M. Kolendovska. Individual scans fusion in virtual knowledge base for navigation of mobile robotic group with 3D TVS // Proceedings of 44th Annual Conference of IEEE Industrial Electronics Society (IECON). -2018. – Washington DC, USA. -S. 3187-3192. ISBN 978-1-5090-6683-4/18/.

2. Habr [інтернет ресурс]. – Режим доступу: https://habr.com/ru/post/341050/ (дата звернення: 17.02.2022).

3. Yuexiang SU The application of 3D technology in video games – College of Software Engineering, Beijing University of Technology 2018, p. 392. ISBN 978-1-5090-6683-4/18/.

4. 80.lv [інтернет ресурс]. – Режим доступу: https://80.lv/articles/wargamings-3d-modeling-workflow/ (дата звернення: 17.02.2022).

SELECTION OF ELEMENTS FOR THE DEVELOPMENT OF A BEDSIDE PATIENT MONITOR

st. Shugai V.V., as. Chumak V.S.
Kharkiv National University of Radio Electronics,
Department of MTS, Kharkiv, Ukraine
e-mail: valeriia.shuhai@nure.ua, valeriia.chumak@nure.ua

Abstract. The bedside monitor is a modern high-tech device, without which not a single intensive care unit of an inpatient and intensive care unit of a hospital can do today. All the increased requirements for patient care and safety, for the quality of diagnostics of diseases [1-5], for control over the conduct of medical procedures, make the bedside monitor an indispensable medical equipment in modern hospitals.

The bedside monitor occupies its niche in the Ukrainian medical equipment market. Today, many manufacturers offer consumers a large selection of bedside monitors, which differ in their capabilities and equipment, size, screen diagonal, and price. Improvement of the base unit of the bedside monitor with the help of a modern element base makes it possible to increase the technical and metrological indicators of the control of vital physiological parameters of a patient and ease of maintenance.

At all times, doctors used different methods of treatment, but all had one goal - human health. Our lives very often depend on doctors. Until a few centuries ago, medicine was powerless to treat many diseases and there were no special devices to help doctors detect the disease in the early stages of its development. Now, it has become much easier to control treatment processes thanks to new technologies.

After a special examination, we can detect the disease in its early stages and begin treatment in time. Many hospitals are already equipped with modern equipment, which has gained popularity and has become indispensable in resuscitation. The bedside monitor [6-7] has become an indispensable assistant for all patients.

The bedside monitor is a high-tech device that monitors the patient's condition, and in case of deterioration of the patient's condition, doctors, thanks to this monitor, will be able to provide the necessary assistance in a timely manner. The bedside monitor is needed not only in the intensive care unit, but in any modern ward, as well as high-quality medical clothing. A monitor can help determine how effectively a patient is being treated. We can monitor the cardiovascular and respiratory systems. The purpose of work – the improvement of the basic block of the bedside monitor for control of vital physiological parameters of the patient due to use of the newest element base. The resuscitation monitor is intended for control of vital physiological parameters of the patient: the electrocardiogram; the heart rate; the non-invasive and invasive

blood pressure; the body temperature; the respiratory rate; the saturation of oxygen in the blood; the photoplethysmogram observation; the observation of capnogram; the measurements of CO2 content in exhaled air. The base unit includes: the module "CS" for coupling with the central station; the "VIDEO" module for pairing with external video monitors; the color TFT display; the inverter for display backlight lamps; the thermal printer; the capnograph; the blood pressure module; the CPU board; the invasive pressure module; the module of oxygen saturation in the blood.

As an element based we choose the following elements as [8]:

UC3843BD1G - a high performance fixed frequency current mode controller, designed for Off−Line and DC−DC converter applications offering the designer a cost−effective solution with minimal external components;

MAX8546EUB - voltage-mode pulse-width-modulated step-down DC-DC controller, have a wide 2.7V to 28V input range, and do not need any additional bias voltage;

PIC16F628 - FLASH-Based 8-Bit CMOS Microcontroller, have enhanced core features, eight-level deep stack, and multiple internal and external interrupt sources;

AD8541 -single rail-to-rail input and output single-supply amplifier featuring very low supply current and 1 MHz bandwidth, guaranteed to operate from a 2.7 V single supply as well as a 5 V supply, provide 1 MHz bandwidth at a low current consumption of 45 mA per amplifier;

LM339 - Quad Single Supply Comparator, designed for use in level detection, low–level sensing and memory applications in consumer automotive and industrial electronic applications;

HCF4013BE and HCF4013BM - two-stroke D-flip-flops, a monolithic integrated circuit fabricated in metal oxide semiconductor technology available in PDIP14 and SO14 packages;

MAX1640 and MAX1641 - step-down pulse-width-modulation controller use an external Pchannel MOSFET switch and an optional, external N-channel MOSFET synchronous rectifier for increased efficiency, CMOS, adjustable-output, switch-mode current sources operate from a + 5.5 V to + 26 V input, and are ideal for microprocessor-controlled battery chargers;

LM809M3-2.63/NOPB - microprocessor supervisory circuits provide a simple solution to monitor the power supplies in microprocessor and digital systems and provide a reset during power-up, power-down, and brown-out conditions.

When choosing a bedside monitor, it is important not just to compare the cost of different systems, but be sure to correlate the price, functionality and quality of equipment. Calculations of the coupling of elements with the nodes of the electrical schematic diagram of the base unit, developed assembly drawing of the printed circuit board of the base unit and the drawing of the printed circuit

board indicating the technical requirements for thickness and width of printed conductors, distance between conductors.

References.

1. В.С. Чумак, И.В. Свид. Перспектива использования продукта FPGA в медицинских системах. // XIII Міжнародна науково-практична конференція магістрантів та аспірантів «Теоретичні та практичні дослідження молодих науковців» (19–22 листопада 2019 року): матеріали конференції. – Харків : НТУ «ХПІ», 2019. – 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. Малахова О. Ю. Електроміограф на FPGA / О. Ю. Малахова, І. О. Шевцов, науковий керівник : В. С. Чумак // Авіація, промисловість, суспільство: матеріали III Міжнар. наук.-практ. конф., 12 трав. 2022 р. – Харків : ХНУВС, 2022. – С. 117-120.

4. Сусловець Р. І. Розробка системи вимірювання параметрів літієвої батареї електромобіля на базі мікроконтролера stm32 / Р. І. Сусловець, наук. керівник: Чумак В. С., Воргуль О.В. // Авіація, промисловість, суспільство: матеріали III Міжнар. наук.-практ. конф. (м. Кременчук, 12 трав. 2022 р.) / МВС України, Харків. нац. ун-т внутр. справ, Кременчуц. льотний коледж., Наук.парк «Наука та безпека». – Харків : ХНУВС, 2022. – С. 133-135.

5. Луценко А. В. Генетичний алгоритм реконфігурації ПЛІС типу FPGA в медичних системах / А. В. Луценко, О. В. Воргуль // Наука, технології, інновації: тенденції розвитку в Україні та світі: матеріали міжнародної студентської наукової конференції, 4 червня, 2021 рік. – Харків, Україна: Молодіжна наукова ліга. – С. 131-132.

6. RADfarm [Електроний ресурс]. Монітор пацієнта URL: https://radfarm.com.ua/diagnostika/monitori-paciyenta (Дата звернення: 20.10.2022).

7. Meditor [Електроний ресурс]. Meditor: провідний дистриб’ютор медичного обладнання для діагностики та реабілітації URL: https://heaco.ua/catalog/patient_monitors/monitor_patsienta_heaco_g3l.html (Дата звернення: 20.10.2022).

8. Trebovetska R.V., Tychkov V.V., Halchenko V.Ya., - Cherkasy, IV International Scientific-Practical Conference "Information Technologies in Education, Science and Technology" (ITEST-2018) CLTU, 2018 y., p. 134.

МОДЕЛЮВАННЯ РАДІОЛОКАЦІЙНИХ СИСТЕМ У MATLAB

аспірант Сєріков А.О., доц., к.т.н. Свид І.В.
Харківський національний університет радіоелектроніки,
кафедра МТС, м. Харків, Україна
e-mail: anton.sierikov1@nure.ua, iryna.svyd@nure.ua

Abstract. The peculiarities of using the Matlab application program package for the study of radar systems as components of airspace control, control and surveillance of airspace are considered. It is shown that Matlab is a flexible and powerful package that allows for mathematical and simulation modeling of practical guidance.

Вступ. Радіолокаційні системи займають вагоме місце у системах управління повітряним простором, контролю повітряного простору та спостереження повітряного простору [1-4].

Радіолокаційне спостереження визначається як спосіб своєчасного виявлення повітряних об’єктів (ПО) та визначення їхнього місцезнаходження (а за потреби й отримання додаткової інформації, що стосується ПО) і своєчасного надання цієї інформації користувачам, щоб забезпечити підтримку безпечного управління, виходячи з визначеної сфери інтересів [5-14].

Основна частина. Для дослідження та моделювання радіолокаційних систем можна використовувати Matlab [15]. Цей пакет прикладних програм містить велику кількість вбудованих функцій спрямованих на моделювання радіолокаційних систем та окремих вузлів, що мають змінні параметри.

Розглянемо деякі функції. Функція *radar_eq.m* реалізує радіолокаційні втрати, що визначаються, як зменшення загального відношення сигнал/завада. Синтаксис такий:

[snr] = radar_eq (pt, freq, g, sigma, te, b, nf, loss, range).

Основні параметри функції наведено у табл. 1.

Функція *radar_eq.m* розроблена таким чином, що вона може приймати одне значення для вхідного діапазону або вектор, що містить багато значень діапазону.

Також можна легко змінити функцію Matlab *radar_eq.m*, щоб вона вирішувала рівняння для максимальної дальності виявлення, як функції мінімально необхідного відношення сигнал/завада (SNR) для заданого набору параметрів радара.

Таблиця 1 – Параметри функції radar_eq.m

Знак	Опис	Одиниці виміру	Статус
pt	пікова потужність	Ватт (Watts)	Введення
freq	центральна частота радара	Герц (Hz)	Введення
g	посилення антени	Децибел (dB)	Введення
sigma	цільовий поперечний переріз	Метри квадратні (m^2)	Введення
te	ефективна шумова температура	Кельвін (Kelvin)	Введення
b	пропускна здатність	Герц (Hz)	Введення
nf	коефіцієнт шуму	Децибел (dB)	Введення
loss	втрати радіолокації	Децибел (dB)	Введення
range	цільовий діапазон (може бути або одиничним значенням, або вектором)	Метри (meters)	Введення
snr	SNR (одиничне значення або вектор, в залежності від вхідного діапазону)	Децибел (dB)	Вихідні дані

Крім того, рівняння радіолокатора

$$\mathrm{SNR}_0 = \frac{P_t G^2 \lambda^2 2\sigma}{(4\pi)^3 k T_e B F L R^4} \quad (1)$$

можна модифікувати для обчислення ширини імпульсу, необхідного для досягнення певного відношення сигнал/завада для даного діапазону виявлення. У цьому випадку радіолокаційне рівняння можна записати як

$$\tau = \frac{(4\pi)^2 k T_e F L R^4 SNR}{P_t G^2 \lambda^2 \sigma}. \quad (2)$$

Такий запис для моделювання може бути корисний для наступної ситуації. Радарні системи часто використовують кінцеву кількість імпульсів для виконання всіх призначених режимів роботи. Деякі з цих сигналів використовуються для пошуку та виявлення, інші можуть використовуватися для відстеження, тоді, як обмежена кількість широкосмугових сигналів може використовуватися для розрізнення цілі. Під час пошукового режиму роботи, наприклад, виявлення певної цілі з певним значенням характеристики відбиваючої здатності (RCS) цілі встановлюється на основі заздалегідь визначеної ймовірності виявлення P_D. Імовірність виявлення, P_D, використовується для обчислення необхідного відношення сигнал/завада виявлення.

Після обчислення необхідного відношення сигнал/завада, рівняння (2) можна використати для знаходження найбільш підходящого імпульсу (або хвилі), який досягає необхідного відношення сигнал/завада (або

еквівалентно необхідного P_D). Часто може бути так, що жоден з доступних радіолокаційних сигналів не може гарантувати мінімально необхідне відношення сигнал/завада для конкретного значення RCS у певному діапазоні виявлення. У цьому випадку радар повинен чекати, поки ціль не підійде достатньо близько в діапазоні, щоб встановити виявлення, інакше можна використовувати імпульсну інтеграцію (когерентну або некогерентну). В якості альтернативи можна використовувати кумулятивну ймовірність виявлення.

Висновки. Контроль повітряного простору став однією з найважливіших задач усіх країн світу, як кожної окремо, з точки зору забезпечення їх національної безпеки і оборони, так і усіх разом, з точки зору забезпечення безпеки польотів авіації і поєднання міжнародних зусиль у боротьбі з тероризмом у цій сфері.

Для розвитку радіолокаційних систем на етапі дослідження, модернізації, оновлення тощо доцільно використовувати пакет прикладних програм Matlab. Що дозволить забезпечити проведення якісних науково-практичних досліджень.

Список використаних джерел.

1. Свид І. В., Обод І. І. Завадостійкість радіолокаційних систем ідентифікації за ознакою «свій-чужий»: монографія. / І. В. Свид, І. І. Обод. Харків : Друкарня Мадрид, 2021. 254 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. 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", In: Ageyev D., Radivilova T., Kryvinska N. (eds) 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.

4. I. Svyd, I. Obod and O. Maltsev, "Interference Immunity Assessment Identification Friend or Foe Systems", In: Ageyev D., Radivilova T., Kryvinska N. (eds) 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. I. Svyd, I. Obod, O. Maltsev, G. Zavolodko, D. Pavlova, H. Maistrenko, "Fusion of Airspace Surveillance Systems Data", 3rd IEEE International Conference on Advanced Information and Communication Technologies (AICT), Lviv, Ukraine, 2019, pp. 430-433, doi: 10.1109/AIACT.2019.8847916.

6. О.П. Черних, І.І. Обод, І.В.Свид. Інформаційне забезпечення на основі мереж спостереження повітряного простору. Eastern-European Journal of Enterprise Technologies, 2/9(50) 2011 - Харків, 2011. С. 23-25. doi:

10.15587/1729-4061.2011.1850.

7. V. Semenets, I. Svyd, I. Obod, O. Maltsev, W. Wójcik, M. Tkach, S. Starokozhev, "Method of Increasing the Relative Throughput of Requesting Radar Systems", Przegląd Elektrotechniczny, ISSN 0033-2097, R. 98 NR 11/2022, 2022, pp. 97-101, doi: 10.15199/48.2022.11.17.

8. I. Svyd, I. Obod, O. Maltsev, O. Vorgul, I. Shevtsov and O. Bilotserkivets, "Optimizing the Request Signals Detection of Aircraft Secondary Radar System Transponders," 2022 IEEE 41st International Conference on Electronics and Nanotechnology (ELNANO), 2022, pp. 652-657, doi: 10.1109/ELNANO54667.2022.9926991.

9. I. Svyd, I. Obod, O. Maltsev, O. Romanov, O. Zhuk and O. Nesmiian, "Estimation of The Throughput of The Channel for Measuring The Distance of Short-Range Radio Engineering Systems," 2022 IEEE 41st International Conference on Electronics and Nanotechnology (ELNANO), 2022, pp. 646-651, doi: 10.1109/ELNANO54667.2022.9927005.

10. I. Svyd, I. Obod, O. Maltsev, O. Vorgul, V. Chumak and A. Sierikov, "Analysis of the Impact of Interference on the Time Position of Signals in Requesting Airspace Observation Systems," 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T), 2021, pp. 470-474, doi: 10.1109/PICST54195.2021.9772138.

11. I. Svyd, I. Obod, O. Maltsev, O. Vorgul, V. Chumak and B. Bakumenko, "Estimation of the Spatial Coordinates of Air Objects in Synchronous Radar Networks for Airspace Observation," 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T), 2021, pp. 425-428, doi: 10.1109/PICST54195.2021.9772227.

12. M. K. Abdul-Hussein, O. Strelnytskyi, I. Obod, I. Svyd and H. Alrikabi, "Evaluation of the Interference's Impact of Cooperative Surveillance Systems Signals Processing for Healthcare", International Journal of Online and Biomedical Engineering (iJOE), vol. 18, no. 03, pp. 43-59, 2022. doi: 10.3991/ijoe.v18i03.28015.

13. Свид І.В., Семенець В.В., Мальцев О.С., Ткач М.Г., Старокожев С.В., Даценко О.О., Шевцов І.О. Порівняльний аналіз методів визначення координат повітряних об'єктів системами широкозонової мультилатерації. Радіотехніка. 2022. Вип. 209. С. 162-177. doi: 10.30837/rt.2022.2.209.16.

14. Свид І.В., Ткач М.Г., Сєріков А.О., Коротіч О.В., Дацько С.В., Сухоруков Д.О., Мачоніс Т.С. Обробка інформації мереж радіолокаційних систем спостереження повітряного простору. Радіотехніка. 2022. Вип. 210. С. 137-145. doi: 10.30837/rt.2022.3.210.11.

15. B. R. Mahafza and A. Z. Elsherbeni, MATLAB simulations for radar systems design by Bassem R. Mahafza and Atef Z. Elsherbeni. London: Chapman & Hall / CRC Press, 2004.

АЛФАВІТНИЙ ПОКАЖЧИК

А

Алєксєєв В.О. 42
Антіпов І.Є. 124, 126

Б

Бондаренко А.О. 54
Бондаренко А.С. 66
Бенько Т.Г. 71
Булага В.А. 128, 132
Бірюков Д.К. 148

В

Вадурін К.О. 20, 22
Вирвихвост О.В. 46
Васильєв Ю.С. 75, 79, 83
Воропаєв В.Ю. 142

Г

Горбенко Є.О. 75, 79, 83
Гетьман К.Р. 87
Горелов Д.Ю. 96, 100, 102, 105, 108, 110, 112, 114, 136 ,156, 158
Гребенчук М.В. 118
Горецький О.В. 120
Гречко А.В. 146
Голозубов Р.О. 161

Д

Довбня А.А. 96

З

Заболотний В.І. 122
Загута Є.А. 100
Зубков О.В. 8
Зубков А.О. 8
Зіноватна Д.В. 150
Зінченко М.Р. 154

І

Ісаєва О.А. 30
Іванов Л.С. 50

К

Кухаренко Д.В. 20, 22
Кавецький В.С. 28
Карнаушенко В.П. 75, 79, 83
Калина О.М. 138
Колендовська М.М. 138, 144, 146, 148, 150, 152, 163
Крамський І.А. 140
Кащавцев М.В. 152

Л

Луценко А.В. 26
Литвиненко О.В. 102
Леушина А.А. 108, 110, 116
Лозовська Г.О. 136 ,156

М

Малахова О.Ю. 24
Мещан К.А. 69
Міщеряков Ю.В. 69
Мінін Д.О. 105

Н

Новоселов С.П. 4, 12, 16

О

Олейнікова О.І. 116, 118, 120
Олейніков А.М. 130
Олейніков В.М. 140, 142, 154, 161
Огієнко А.Є. 144

П

Пятайкіна М.І. 75, 79, 83
Пащенко Є.В. 4
Пугач К.О. 32
Першин Є.В. 38
Пономаренко Д.С. 91
Пилявських Є.А. 112
Павленко Я.С. 128
Пшеничних С.В. 134
Путівцев А.П. 158

Р

Рудніченко М.Д. 66
Рябіченко В.С. 122
Румянцева О.В. 134
Рогинский С.В. 163

С

Свид І.В. 168
Славгородський Я.В. 34
Сєріков А.О. 168
Сичова О.В. 12
Сергієнко А.С. 89
Сігута Д.К. 94
Сердюк С.Л. 132

Т

Теслюк С.І. 16

Ф

Факас О.В. 36
Федотов В.В. 114
Філімонов Д.А. 124, 126
Філоненко Я.С. 130

Х

Хрустальов К.Л. 89
Хрустальова С.В. 91

Ц

Цехмістро Р.І. 38

Ч

Чумак В.С. 24, 26, 28, 30, 32, 34, 36, 165
Чикота В.Ю. 58

Ш

Шугай В.В. 165
Шаповалов С.В. 38
Шафоростов Д.Д. 62
Шевцов І.О. 87
Широкопетлєва М.С. 94

Ю

Юрків В.Л. 71

Я

Янушкевич Д.А. 46, 50, 54, 58, 62

ЗМІСТ

Новоселов С.П., Пащенко Є.В. *Автоматизація контролю виконання монтажних операцій* 4

Зубков О.В., Зубков А.О. *Особливості реалізації Web серверів на модулях ESP8266 ТА ESP32 У Arduino IDE* 8

Новоселов С.П., Сичова О.В. *Використання віртуальних лабораторних макетів для налагодження технологічних програм ПЛК* 12

Новоселов С.П., Теслюк С.І. *Автоматизація прокладення шляху в просторі на основі даних з сенсорів мобільних роботів* 16

Вадурін К.О., Кухаренко Д.В. *Розробка принципової схеми блока живлення мобільного робота-графопобудовник* 20

Вадурін К.О., Кухаренко Д.В. *Розробка принципової схеми блока датчиків ліній робота-графопобудовника* 22

Малахова О.Ю., Чумак В.С. *Реєстрація електроміографічних біопотенціалів на базі мікроконтролерної системи* 24

Луценко А.В., Чумак В.С. *використання FPGA для реалізації штучної нейронної мережі* 26

Кавецький В.С., Чумак В.С. *Система глибинного зондування на базі мікроконтролера серії STM32* 28

Ісаєва О.А., Чумак В.С. *Аналіз дерматоскопічного зображення під час УФ-відеодерматоскопії* 30

Пугач К.О., Чумак В.С. *Використання кристалів в технологіях оптичного зв'язку* 32

Славгородський Я.В., Чумак В.С. *Підключення мікроконтролера до локальної мережі за допомогою модуля на мікросхемі ENC28J60* 34

Факас О.В., Чумак В.С. *Переваги використання AVR мікроконролерів* 36

Цехмістро Р.І., Шаповалов С.В., Першин Є.В. *Особливості перспектив використання безбатарейних джерел додаткового живлення для мікропроцесорних пристроїв із інтегрованими GSM/GPS/GPRS модулями* 38

Алєксєєв В.О. *Ректена з трифазною схемою випрямлення для IoT додатків* 42

Вирвихвост О.В., Янушкевич Д.А. *Технології створення робототехнічних комплексів для гуманітарного розмінування* 46

Янушкевич Д.А., Іванов Л.С. *Сучасні підходи до системи управління якістю підприємства на принципах концепції Quality 4.0* 50

Бондаренко А.О., Янушкевич Д.А. *Моделювання процесу гуманітарного розмінування із застосуванням робототехнічних комплексів* 54

Чикота В.Ю., Янушкевич Д.А *Система локації та картографування територій, забруднених вибухонебезпечними предметами* 58

Шафоростов Д.Д., Янушкевич Д.А. *Технології виявлення та класифікації вибухонебезпечних предметів* 62

Рудніченко М.Д., Бондаренко А.С. *Концепція інтелектуальної інформаційної системи аналізу та обробки антропометричних даних* 66

Мещан К.А., Міщеряков Ю.В. *Сучасні методи надання персоналізованих рекомендацій в інформаційних системах* 69

Бенько Т.Г., Юрків В.Л. *Уніфікований портативний зарядний пристрій на основі сонячних елементів* 71

Васильєв Ю.С., Горбенко Є.О., Карнаушенко В.П., Пятайкіна М.І. *Головні тенденції у виробництві електроніки* 75

Горбенко Є.О., Васильєв Ю.С., Карнаушенко В.П., Пятайкіна М.І. *Інформаційні технології в транспортних додатках* 79

Пятайкіна М.І., Васильєв Ю.С., Горбенко Є.О., Карнаушенко В.П. *SoC для виробників автомобілів* 83

Гетьман К.Р., Шевцов І.О. *Універсальний програмно-апаратний інтерфейс зв'язку з множиною вбудованих пристроїв* 87

Хрустальов К.Л., Сергієнко А.С. *Підсистема ідентифікації вибухонебезпечних предметів* 89

Хрустальова С.В., Пономаренко Д.С. *Система підтримки прийняття рішень управління фінансовим капіталом виробничих підприємств* 91

Сігута Д.К., Широкопетлєва М.С. *Використання IoT пристроїв на основі ESP32 як спосіб автоматизації внутрішніх процесів мережі зарядних станцій для електромобілів* 94

Довбня А.А., Горелов Д.Ю. *Дослідження безпеки хмарних сервісів* 96

Загута Є.А., Горелов Д.Ю. *Дослідження можливостей використання випадкових сигналів в задачах пошуку пристроїв несанкціонованого знімання інформації* 100

Литвиненко О.В., Горелов Д.Ю. *Інформаційна безпека діяльності у дистанційному форматі* 102

Мінін Д.О., Горелов Д.Ю. *Розширення функціоналу SIEM систем* 105

Леушина А.А., Горелов Д.Ю. *Порівняльний аналіз традиційних біометричних методів контролю та управління доступом* 108

Леушина А.А., Горелов Д.Ю. *Порівняльний аналіз перспективних біометричних методів контролю та управління доступом* 110

Пилявських Є.А., Горелов Д.Ю. *Підвищення надійності біометричних паспортів за рахунок використання технологій штрихового кодування* 112

Федотов В.В., Горелов Д.Ю. *Прототипування безпарольної системи аутентифікації з використанням ознак Browser Fingerprints* 114

Леушина А.А., Олейнікова О.І. *Авторське право на комп'ютерну програму* 116

Гребенчук М.В., Олейнікова О.І. *Способи маскування та виявлення технічних засобів відеоспостереження* 118

Горецький О.В., Олейнікова О.І. *Нормативно-правовий захист комерційної таємниці в Україні* 120

Рябіченко В.С., Заболотний В.І. *Фотографічна розвідка як загроза інформації, що візуалізується на об'єкті інформаційної діяльності* 122

Філімонов Д.А., Антіпов І.Є. *Про підвищення безпеки обміну файлами у відеоконференціях* 124

Філімонов Д.А., Антіпов І.Є. *Порівняльна характеристика сервісів відеоконференцій з точки зору безпеки* 126

Павленко Я.С., Булага В.А. *Інформаційний комплекс розподільних електромереж* 128

Філоненко Я.С., Олейніков А.М. *Технічні засоби акустичної розвідки* 130

Сердюк С.Л., Булага В.А *Цифрова система для митного контролю ручного багажу в аеропортах та зонах підвищеної небезпеки* 132

Румянцева О.В., Пшеничних С.В. *Аналіз методів оптимізації комплексних систем захисту інформації* 134

Лозовська Г.О., Горелов Д.Ю. *Перспективи використання технологій 6G* 136

Калина О.М., Колендовська М.М. *Огляд та аналіз засобів створення інтерфейсу мобільних додатків* 138

Крамський І.А., Олейніков В.М. *Використання AR-технологій при виявленні БПЛА* 140

Воропаєв В.Ю., Олейніков В.М. *Використання системи акустичних датчиків для виявлення безпілотних літальних апаратів* 142

Огієнко А.Є., Колендовська М.М. *Місце сторітеллінгу у розробці ефективного дизайну* 144

Гречко А.В., Колендовська М.М. *WEB-дизайн, як поєднання психології та мультимедіа* 146

Бірюков Д.К., Колендовська М.М. *Огляд аспектів застосування сучасних технологій для створення сценарію та трейлеру гри* 148

Зіноватна Д.В., Колендовська М.М. *Огляд аспектів застосування ігрових технологій для створення візуальної новели* 150

Кащавцев М.В., Колендовська М.М. *Використання мультимедійних технологій для створення анімаційних фільмів* 152

Зінченко М.Р., Олейніков В.М. *Фрактальні методи ідентифікації малорозмірних безпілотних літальних апаратів по акустичному випромінюванню* 154

Лозовська Г.О., Горелов Д.Ю. *Ключові технології систем зв'язку шостого покоління* 156

Путівцев А.П., Горелов Д.Ю. *Огляд технологій безпровідної передачі сигналів та енергії* 158

Голозубов Р.О., Олейніков В.М. *Вплив швидкості руху БПЛА на точність визначення координат пасивним содаром* 161

Рогинский С.В., Колендовська М.М. *огляд та аналіз засобів 3D-моделювання* 163

Shugai V.V., Chumak V.S. *Selection of elements for the development of a bedside patient monitor* 165

Сєріков А.О., Свид І.В. *Моделювання радіолокаційних систем у Matlab* 168

МАТЕРІАЛИ

IV ФОРУМУ
«Автоматизація, електроніка та робототехніка.
Стратегії розвитку та інноваційні технології»
AERT-2022

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.