

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЗАПОРІЗЬКА ПОЛІТЕХНІКА»

ТИЖДЕНЬ НАУКИ-2025
Факультет інформаційної безпеки та електронних комунікацій

Збірник тез доповідей
щорічної науково-практичної конференції серед студентів, викладачів,
науковців, молодих учених і аспірантів
14–18 квітня 2025 року

Електронне видання на DVD-ROM

Запоріжжя • НУ «Запорізька політехніка» • 2025

УДК 621.3+004+519.6

T39

*Рекомендовано до видання Вченою радою
Національного університету «Запорізька політехніка»
(Протокол № 10 від 27.05.2025 р.)*

Упорядник: Сергій Лізунов

Редакційна колегія:

Вадим ШАЛОМЄЄВ, д-р техн. наук, професор, (відпов. ред.)

Олексій КУЗЬКІН, д-р техн. наук, професор;

Василь ГЛУШКО, канд. техн. наук, доцент;

Євген ПАРАХІСВИЧ, канд. техн. наук, доцент;

Микола АНТОНОВ, канд. техн. наук, доцент;

Віра САВЧЕНКО, канд. техн. наук, доцент;

Наталія ФУРМАНОВА, канд. техн. наук, доцент;

Микола КАСЬЯН, канд. техн. наук, доцент;

Микола ДЄДКОВ, канд. іст. наук, доцент;

Олена ВАСИЛЬЄВА, д-р екон. наук, професор;

Світлана КОКАРСЬВА, канд. наук з фіз. вих. і спорту, доцент;

Юрій ФІЛЕЙ, канд. юр. наук, професор;

Таїсія ГАЙВОРОНСЬКА, канд. філос. наук, доцент;

Наталія ВИСОЦЬКА, в.о. начальника НДЧ;

Наталія САВЧУК, начальник редакційно-видавничого відділу;

Сніжана ВИЧУЖАНІНА, керівник відділу наукової роботи студентів;

Юлія ЧУШКІНА, провідний фахівець відділу наукової роботи студентів

Сергій ЛІЗУНОВ, відповідальний на факультеті ФІБЕК.

T39

Тиждень науки-2024. Факультет інформаційної безпеки та електронних комунікацій. Тези доповідей науково-практичної конференції, Запоріжжя, 14–18 квітня 2025 р. [Електронний ресурс] / Редкол. : Вадим ШАЛОМЄЄВ (відпов. ред.) Електрон. дані. – Запоріжжя : НУ «Запорізька політехніка», 2025. – 103 с. – 1 електрон. опт. диск (DVD-ROM); 12 см. – Назва з тит. екрана.

ISBN 978-617-529-501-4

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

УДК 621.3+004+519.6

ISBN 978-617-529-501-4

© Національний університет
«Запорізька політехніка»
(НУ «Запорізька політехніка»), 2025

ЗМІСТ

СЕКЦІЯ «ІНФОРМАЦІЙНА БЕЗПЕКА ТА НАНОЕЛЕКТРОНІКА»

Pogosov V.V. On the work of single-electron transistorS	7
Матюшин В.М. Стимулювання дифузійних процесів в напівпровідниках в результаті збудження електронної системи при протіканні приповерхневої екзотермічної хімічної реакції	9
Карпуков Л.М., Воскобойник В.О. Метод реалізації у процедурі синтезу мікрохвильових шлейфних фільтрів	11
Кривоус А.С., Сніжної Г.В., Солодовник А.І. Вплив окислення на стабільність прямої напруги силових діодів притискної конструкції	13
Лізунов С. І., Верещака М.П., Філобок Є.В. Роль соціальної інженерії у сучасних кібератаках та методи протидії	15
Лізунов С. І., Філобок Є.В., Верещака М.П. Методи та інструменти цифрової криміналістики в розслідуванні сучасних кіберінцидентів	17
Неласа Г.В., Аль-Хамад Н.А. Дослідження та аналіз схеми шифрування відкритого ключа k-рке в стандарті fips 203	22
Бережний О.Ю., Корольков Р.Ю. Дослідження методів обходу антивірусного захисту microsoft defender	25
Нагорна Н.М. Захист надвеликих інтегрованих схем і систем на кристалі від несанкціонованого втручання.....	27
Кутовий І.А., Корольков Р.Ю., Коротун А.В. Загасання електромагнітних хвиль у метаматеріалах	29
Сніжна К.Г., Скляр М.С., Сніжної Г.В. Використання технології Eye detect у поліграфічних дослідженнях	32
Тюрін М.М., Василенко О.В. Модернізація фрезерних станків на базі програмного забезпечення	34

Єршов М.О., Василенко О.В., Шумейко П.Д. Отримання оптимальних параметрів нанорозмірних пігментів ксераліків	36
--	----

СЕКЦІЯ «ТЕЛЕКОМУНІКАЦІЇ ТА РАДІОТЕХНІКА

Бугрова Т.І., Горохов Є.П. Застосування машинного зору для підвищення ефективності frv дронів.....	38
Бугрова Т.І., Мулін О.С. Особливості турнікетних антен у складі систем РЕБ	40
Бугрова Т.І., Мулін О.С., Проваторов С.М. Квадрифілярні антени для джамерів	42
Костенко В.О. , Фокін Д.О. Мікропроцесорна техніка у модернізації пекарного обладнання	44
Логачова Л.М, Овчинніков В.В. Застосування метаматеріалів у техніці надвисоких частот	46
Гладун К.В., Самойлик С.С. Вимірювання висоти цілі методом Matrix Pencil	48
Калиніченко Д.В. , Мороз Г.В. Підвищення дальності дії комерційних безпілотних літальних апаратів (БПЛА)	50
Плетінь Д.Ю., Мороз Г.В. Передача інформації за допомогою лазерних технологій	52
Плетінь Д.Ю.1, Мороз Г.В. Метод відновлення стільникового зв'язку Пологівського району.....	54
Сумарюк С.Г., Чорнобородов М.П. , Мороз Г.В. Алгоритм розташовування елементів аудіомережі на місцевості з урахуванням «недоступних зон»	56
Чорнобородова Н. П., Чорнобородов М. П., Комінов Є. Є. Визначення придатності "промислових" антен до їх застосування підрозділами зсу	58
Чорнобородова Н. П., Чорнобородов М. П., Маслов О. О. Визначення напруги живлення підсилювача.....	60

СЕКЦІЯ «ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ЕЛЕКТРОННИХ ЗАСОБІВ»

Костяной П.А., Фарафонов О.Ю. Алгоритмічне забезпечення попередньої обробки з безпілотних апаратів для побудови тривимірної карти місцевості.....	63
Malyi Oleksandr I, Vychuzhanina Snizhana DRFM type Digital devices for storing and reproducing radar signals in radio jamming	65
Гарачук С.А., Онищенко В.Ф. Розробка системи цифрової передачі відео з використанням WiFi 6E.....	67
Vlasenko Pavlo. A Method for Source-Side Authentication in Analog Video Transmission.....	70
Онищенко В.Ф., Магльованний В.А. Оптимізація маршрутів наведення БПЛА за допомогою рекурентних нейронних мереж	72
Фурманова Н.І., Поспеева І.Є. Формування інноваційних компетентностей майбутніх інженерів засобами робототехніки	74
Ярошенко К.Р., Малий О.Ю. Розробка електронного блоку для радарної системи виявлення дронів	75
Кобець М.К., Миронова Н.О. Розробка апаратного та програмного забезпечення для автомобіля на базі Raspberry Pi з архітектурою зв'язку UDP Socket	78
Черніговцев М.О., Миронова Н.О. Автоматизація управління інвентарем університету на основі технологій радіочастотної ідентифікації та бездротового позиціонування	81
Баранова О.А., Миронова Н.О. Дослідження підходів реалізації систем віддаленого моніторингу промислових робіт	82
Шевченко Т.В., Миронова Н.О., Єфименко М.В. Дослідження функціональних можливостей станка LumenPnP та фідерних систем для автоматизованої установки SMD-компонентів	84
Немудрий К.І., Куляба-Харитонова Т.І. Використання штучного інтелекту в таргетованій рекламі	85

Хохлов В.С., Миронова Н.О., Молочков Д.Є. Розробка системи визначення просторового положення об'єктів у робочій зоні робота	87
Девяткін О.К.1, Миронова Н.О. Розробка апаратного та програмного забезпечення зовнішнього дисплею для відображення інформаційних віджетів.....	88
Давиденко Д.В., Миронова Н.О. Розробка мобільного людино-машинного інтерфейсу для промислового робота	90
Малий О.Ю., Жулай А.О. Розробка розумної колонки з українським напрямом.....	91
Манько Д.В., Шаптала С.В. Розробка алгоритмів синхронізації 3D-моделі цифрового двійника робототехнічного пристрою з потоковими IoT-даними	93
Резниченко П.О., Фурманова Н.І., Яковенко В.В. Проєктування багатофункціональної автоматизованої поворотної платформи	95
Тарасов Є.П., Поспєєва І.Є., Піроженко О.О. Розробка конструкції та плати обробки сигналів фазованої решітки	97
Пономарьов Є.А., Фурманова Н.І. Економічна ефективність та сталий розвиток автоматизованих систем адаптивного пакування	99

ON THE WORK OF SINGLE-ELECTRON TRANSISTORS

The effect of the Coulomb blockade in a single-electron transistor, a device where Fermi-liquid leads are mediated by a quantum dot, plays an essential role in condensed matter physics, mesoscopics, and open quantum systems. The Coulomb spectroscopy and transport through a quantum dot are sensitive to the precise nature of the nonequilibrium steady state, the mechanisms of relaxation, electronic interactions, and topological order [1]. The “orthodox” theory of the Coulomb blockade is based on rate equations formulated in the basis of different charged states in the island [2]. Such states are well defined for almost isolated quantum dots which have weak tunnel coupling to the leads, i.e., with a small dimensionless conductance. In this theory, the distribution function in the island is not affected by the coupling to contacts; i.e., the internal relaxation in the island is assumed to prevail on the characteristic tunneling time scale.

The elementary tunnel design schematically represents a kind of sandwich: a massive gold film (emitter) with a deposited dielectric; islands of monatomic height (disc-shaped clusters) [3] or spherical-like gold clusters [4] are formed on the dielectric film; a tunneling microscope tip (STM), also coated with gold, was used as the third electrode (collector). Measured $I-V$ characteristics have a plateau of the zero current (a current gap).

In the limit of weak tunnelling, the probability P_n of detecting “on average” n excess electrons on the island determined by the master equation in the stationary limit. The current flowing through the quantum island (with a limitation on the Coulomb instability [2]) was defined as

$$I = -e \sum_{n_{\min}}^{n_{\max}} P_n (\overrightarrow{\omega_n} - \overleftarrow{\omega_n}) \quad (1)$$

where $\overrightarrow{\omega_n}$ are the electron flows to the island from left to right and from right to left.

In this work, in comparison with [1], the dependence of the tunnel rate

$$\Gamma(d_c) = \Gamma_0 \exp\left(-\frac{2d_c \sqrt{2mW}}{\hbar}\right) \quad (2)$$

on the island-collector distance (d_c) is taken into account for calculating the reduced current $\tilde{I} \equiv I / (eP_0\Gamma_0)$; W is the work function of electrons from gold. In this manner we have restored the correct dependence $I(V, d_c)$ missed in our previous article [2].

The width of the current gap ΔV_{is} is determined by the threshold voltages V_{0+} / V_{0-} from the condition of equality of zero collector current on the forward/reverse branches of the I - V characteristic. In the low-temperature limit ($k_B T_{eff} \ll \Delta \varepsilon_F$) for the current gap of almost isolated island (weak coupling) an analytical expression is obtained,

$$\Delta V_{is} = V_{0+} - |V_{0-}|, |V_{0\pm}| = \frac{1}{2 - \eta^\pm(d_c)} \left(\frac{1}{2e} \tilde{E}_c + \frac{1}{e} \Delta \varepsilon \right) \quad (3)$$

where $\eta^\pm(d_c)$ are the fractions of the voltage, $\tilde{E}_c$ is the Coulomb charging energy of island, and $\Delta \varepsilon \equiv \varepsilon^{\text{HO}} - \mu_{is} \geq 0$. Here ε^{HO} and μ_{is} are highest occupied electron level and the chemical potential of electrons in the island, respectively.

For the case of “strong quantization” the size of the current gap for non-magic clusters is equal to zero explicitly, because the emitter Fermi level is in line with the closed levels in the cluster. In this regime, the expression (2) describes the experimental values well.

In the experiment [4] for the structure based on the magic disk with a radius of $R \cong 22 a_0$ a feature was discovered: the current gap varies as $0.8 \rightarrow 0.4 \rightarrow 0.7$ V for cyclic variation of $d_c \cong 2 \rightarrow 4 \rightarrow 2 a_0$, respectively. Such small values of d_c , smaller than the radius of a gold atom, indicate that this situation is associated with a strong tunneling coupling regime between the island and the collector. This leads to the fact that the values of $\tilde{E}_c$ and $\eta^\pm(d_c)$ become indefinite from the point of view of electrostatics. In this regard, formula (3) becomes inapplicable to this case.

REFERENCES

1. D. S. Shapiro, A. D. Mirlin, A. Shnirman, Phys. Rev. B 107, 125404 (2023)
2. V.V. Pogosov, E.V. Vasyutin, Nanotechnology. 17, 3366 (2006)
3. J. G. Hou, B. Wang, J. Yang, X. R. Wang, H. Q. Wang, Q. Zhu, X. Xiao, Phys. Rev. Lett. 86 5321 (2001)
4. T. Ohgi, Y. Sakotsubo, Y. Ootuka, D. Fujita, Appl. Phys. Lett. 84, 604 (2004)

УДК 539.219.3

Матюшин В.М.¹

¹д-р фіз.-мат. наук, проф. НУ «Запорізька політехніка»

СТИМУЛЮВАННЯ ДИФУЗІЙНИХ ПРОЦЕСІВ В НАПІВПРОВІДНИКАХ В РЕЗУЛЬТАТІ ЗБУДЖЕННЯ ЕЛЕКТРОННОЇ СИСТЕМИ ПРИ ПРОТІКАННІ ПРИПОВЕРХНЕВОЇ ЕКЗОТЕРМІЧНОЇ ХІМІЧНОЇ РЕАКЦІЇ

Стимулювання локальної дифузії є актуальною в електронній технології. Перспективним напрямком приповерхневого стимулювання є дія енергії, що виділяється в результаті протікання на поверхні напівпровідникового кристала екзотермічної хімічної реакції. При цьому енергія виділяється поблизу поверхні, тобто локально, що дуже важливо при створенні складних напівпровідникових наноструктур.

Найбільш простою для дослідження хімічних процесів на поверхні є реакція рекомбінації атомів водню в молекули, в результаті якої виділяється 4,48 Ев на один акт рекомбінації. Виділення такої великої енергії в малому об'ємі (приблизно 10 нм²) приводить до того, що локальна температура різко підвищується (до декілька тисяч градусів). Це приводить до збудження електронної підсистеми напівпровідникового кристала .

Ефективність генерації вільних електронів при рекомбінації атомів водню складає для германію $\eta=0,16$. При цьому значно збільшується ймовірність межзонного переходу міжвалентною зоною провідності. Це приводить до значного підвищення приповерхневої концентрації електронного газу.

В приповерхневих шарах кристала створюється великий градієнт концентрації рухливих носіїв заряду (вільних електронів).

Вільні електрони швидко дифундують в об'єм кристала. При цьому виникає електричне поле значної напруженості.

Атоми металів, які знаходяться в кристалічній ґратці германію та кремнію, можуть іонізуватися та заряджатися негативно (в вузлах ґратки) і позитивно (в міжвузлях). Тому за наявності постійного електричного поля на домішковий атом в кристалі діє сила : $\vec{F}_I = qE$, где q – заряд іона; E – напруженість електричного поля.

Крім сили $\vec{F}_I$ на іон може діяти й інша сила, обумовлена розсіянням на іонах електронів і дірок, що рухаються до електродів. Сила $\vec{F}_2$ тягне домішкові атоми у напрямку руху електронів і дірок. Захоплення іонів електронами провідності може бути дуже значним, таким, що позитивно заряджені іони будуть рухатися проти поля, подібно до атомів з великим негативним зарядом. Сила, що діє на іон, визначається: $\vec{F} = (e_I - |e|\chi)E$. За відсутності зовнішнього електричного поля розподіл електронів у кристалі (за координатами та імпульсами) є ізотропним, тому результуюча сила, що діє з боку електронів на іон, дорівнює нулю.

Коли накладається зовнішнє електричне поле E , електрони, прискорюючись, набувають додаткового імпульсу. Коли прикладено зовнішнє електричне поле E , електрони прискорюються, набуваючи додатковий імпульс.

Для оцінки заряду захоплення розраховують перетин розсіювання на статичних точкових дефектах. Перетин розсіювання вільного електрона визначається видом потенціалу розсіювання, створюваного точковим дефектом.

Навіть якщо концентрація зарядів n_s становить лише $5 \cdot 10^{13} \text{ см}^{-2}$, енергія електростатичного поля вже дорівнює поверхневій енергії кристала. Зазвичай спостережувана концентрація знаходиться в межах 10^{11} - 10^{13} см^{-2} . У цьому випадку в германії поле поверхні екранується на глибинах 10^{-2} - 10^{-4} см .

В таких умовах напруженість поля, спрямованого від поверхні в атмосферу: $E_{\uparrow}$ =приблизно 10^6 В/см . Напруженість поля, спрямованого вглиб кристала германію: $E_{\downarrow}$ =приблизно $5 \cdot 10^5 \text{ В/см}$. Це знижує потенційний бар'єр дифузії у напрямку від поверхні вглиб кристала при перескоку іона: $\Delta E = Fa = eE_{\downarrow} + (I + Z_I) \cdot a$, де a - середня відстань між сусідніми міжвузлями. Для германію ΔE =приблизно $3 \cdot 10^{-2} \text{ эВ}$.

Коефіцієнт міжвузлової дифузії домішки у напрямку поля внаслідок зниження енергії активації зростає та описується наступним виразом:

$$D_{np}^* = D_0 \cdot \exp\left(-\frac{E_0 - \Delta E}{kT}\right) \quad (1)$$

Таким чином вплив електронного стимулювання дифузійних процесів може бути в цьому випадку дуже значним.

УДК 621.372.852.1

Карпуков Л.М.¹, Воскобойник В.О.²

¹ д-р техн. наук, проф. НУ «Запорізька політехніка»

² канд. техн. наук, проф. НУ «Запорізька політехніка»

МЕТОД РЕАЛІЗАЦІЇ У ПРОЦЕДУРІ СИНТЕЗУ МІКРОХВИЛЬОВИХ ШЛЕЙФНИХ ФІЛЬТРІВ

Традиційні методи розрахунку шлейфних фільтрів, що ґрунтуються на перетворенні низькочастотних фільтрів-прототипів у конструкції на елементах з розподіленими параметрами, не забезпечують оптимальних частотних характеристик. У [1] запропоновано прямий метод синтезу шлейфних фільтрів за функцією фільтрації, для апроксимації якої застосовуються функції Чебишева. Розрахунок хвильових опорів ліній елементів структури фільтра здійснюється у цьому методі шляхом вирішення оптимізаційної задачі, якість якого багато в чому залежить від початкового наближення. У зв'язку з цим інтерес представляє реалізація класичного підходу до синтезу, що включає, крім етапу апроксимації, також процедури формалізації та реалізації.

Структура фільтра представлена на рис. 1, де ρ_0 хвильові опори вхідного та вихідного портів, ρ_c – відрізків ліній, ρ_s – шлейфів.

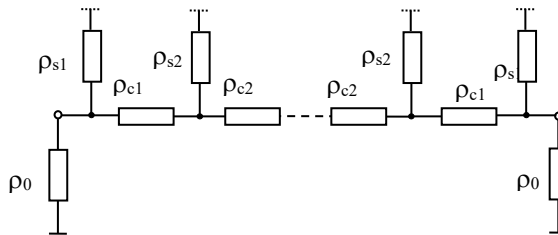


Рисунок 1 – Структура шлейфного фільтра

Чебишевська функція, що апроксимує функцію фільтрації, має, наприклад, для смугового фільтра, наступний вид [1]:

$$F(\theta) = \frac{S_{11}(\theta)}{S_{21}(\theta)} = \frac{\gamma \sum_{k=0}^m a_k \cos(2k\theta)}{\sin(\theta)} \quad (1)$$

де $S_{11}=A_{11}/B$, $S_{21}=A_{21}/B$ – параметри розсіювання фільтра; $m=n_s/2$, $\gamma=\cos(\theta)$ при n_s парному; $m=(n_s+1)/2$, $\gamma=1$ при n_s непарному; n_s – кількість шлейфів.

Етап формалізації полягає у виділенні многочлена $B(z)$, що задовольняє умові фізичної реалізованості, із квадрата модуля $|B(z)|^2=|A_{11}(z)|^2+|A_{21}(z)|^2$ знаменника S -параметрів, що складається за (1), тут $z=\exp(-j2\theta)$, j - уявна одиниця. На етапі реалізації за функцією $S_{11}(z)=A_{11}(z)/B(z)$, складеної при формалізації, розраховуються хвильові опори ланок структури фільтра. У запропонованому методі реалізації використовується формула

$$S_{11}(z)_{n-1} = \frac{A_{11}(z)_e B(z)_n - B(z)_e A_{11}(z)_n}{D(z)_e B(z)_n - A_{11}(z)_e A_{11}(z)_n} \quad (2)$$

яка зв'язує коефіцієнти відображення структур з числом ланок n та $n-1$. У процесі послідовного від'єднання ланок з матрицею розсіювання S_e їх хвильові опори визначаються за умови зменшення на одиницю порядку поліномів (2). Додатковою умовою є: $S_{11}(0)=(1-y_s-y_c)/(1+y_s+y_c)$ для шлейфу або $S_{11}(0)=(1-y_c)/(1+y_c)$ для відрізка лінії на вході структури, $y=1/\rho$.

На рис. 2 представлена ідеальна частотна характеристика, яка отримана за результатами синтезу фільтра, що містить 5 шлейфів і 4 відрізка лінії, для загасань $\alpha_c=0,1$ dB у смузі пропускання, $\alpha_s=40$ dB у смузі згасання та при 50% відносній смузі пропускання.

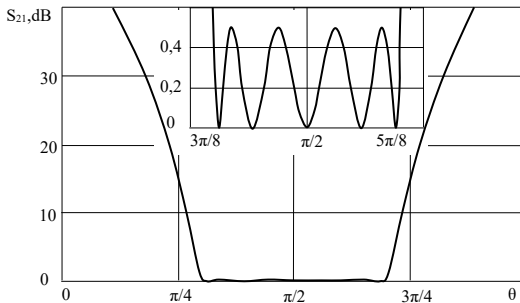


Рисунок 2 – Амплітудно-частотна характеристика фільтра

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Karpukov L., Savchenko Iu., Voskoboynik V. Optimal synthesis of stub microwave filters. // Radio Electronics, Computer Science, Control. 2024. № 2. P 15-23. doi: 10.15588/1607-3274-2024-2-2.

УДК 621.382

Кривоус А.С.¹, Сніжної Г.В.², Солодовник А.І.³

¹ асп. НУ «Запорізька політехніка»

² д-р. техн. наук, проф. НУ «Запорізька політехніка»

³ директор ТОВ «Елемент-Перетворювач»

ВПЛИВ ОКИСЛЕННЯ НА СТАБІЛЬНІСТЬ ПРЯМОЇ НАПРУГИ СИЛОВИХ ДІОДІВ ПРИТИСКНОЇ КОНСТРУКЦІЇ

Важливою вимогою до діодів, які використовуються для паралельного включення в потужних випрямляючих агрегатах, є стабільність значень прямої напруги U_{FM} під час тривалої експлуатації. Неконтрольована зміна значень U_{FM} на окремих діодах призводить до порушення рівномірності розподілення току навантаження в паралельних гілках випрямляючого агрегату і виходу з ладу діодів.

Передбачалось, що головна причина зміни властивостей притискних контактів є поява окисних плівок на поверхні металів під час тривалої експлуатації.

Мета роботи – вивчення впливу окисних плівок різних металів, які використовуються в притискних конструкціях контактів силових напівпровідникових приладах, на пряму напругу U_{FM} силових діодів.

Через тривалий термін експлуатації діодів, було обрано прискорений метод випробувань, тобто зразки контактних матеріалів окислювались при більш високій температурі ($T = 200-300^{\circ}\text{C}$), ніж максимальна робоча температура діода.

Робота проводилась в три етапи. На першому етапі досліджувалось окислення срібних прокладок без покриття, та покритих шаром хрому ($\sim 1-3$ мкм), а також пасивованих в 1% розчині хромпіку. Окислення проводилось при двох режимах:

- 1) окислення в парах води за $T=200^{\circ}\text{C}$ протягом 36 годин;
- 2) окислення на повітрі за $T=200^{\circ}\text{C}$ протягом 120 годин.

Вимірювання U_{FM} проводилось при струмі 6280 А до та після окислення. Для вимірювання було обрано один корпус, один напівпровідниковий випрямляючий елемент та по три комплекти срібних прокладок з різним покриттям. За результатами вимірювань U_{FM} зроблено наступні висновки:

1) окислення срібних прокладок не призвело до збільшення U_{FM} з обома режимами окислення;

2) покриття срібних прокладок хром дало збільшення U_{FM} на 0,12-0,14 В з першим режимом окислення та на 0,09-0,3 В з другим режимом окислення.

Під час другого етапу дослідження впливу окислення на U_{FM} проводили окислення при більшій температурі ($T=300^{\circ}\text{C}$ протягом 24 годин) прокладок з мідної фольги без покриття, з покриттям сріблом, з покриттям хімічним нікелем, з покриттям гальванічним нікелем та з покриттям хромом. Товщина покриття складала 1-3 мкм. Крім того, піддавались окисленню чотири напівпровідникових діодних елементів та вимірювалось на них U_{FM} до окислення та після.

На третьому етапі досліджувався вплив окислення напівпровідникового елемента з напиленим шаром алюмінію товщиною 16-20 мкм на катодну (Si) та анодну сторони (Mo) на значення U_{FM} .

Крім того, на чотири випрямляючи елементи з напиленим алюмінієвим шаром додатково гальванічно осаджувалось срібло товщиною до 3 мкм.

Необхідно зазначити, що срібло осаджувалось лише на анодний бік випрямляючого елемента. Під час третього етапу роботи зробили наступні висновки:

1) випрямляючі елементи з напиленим та впеченим шаром алюмінію на катодній поверхні силіцію та анодній поверхні молібденового диску зібрані в корпус з чистими срібними прокладками практично не збільшили значення своїх U_{FM} після окислення ($T=300^{\circ}\text{C}$ протягом 24 годин);

2) випрямляючі елементи з напиленим та впеченим шаром алюмінію на катодній та анодній поверхні з додатково гальванічно нанесеним шаром срібла на анодну сторону також не збільшили значення своїх U_{FM} після окислення ($T=300^{\circ}\text{C}$ протягом 24 годин).

За результатами проведеного дослідження впливу окислення металів на стабільність значень прямої напруги U_{FM} встановили:

1) молібденовий диск, який передбачений конструкцією силового діода в якості термокомпенсатора, коли окислюється призводить до збільшення значень U_{FM} й скоріше за все є головною причиною збільшення U_{FM} під час експлуатації діодів;

2) напилений та впечений шар алюмінію на силіції та молібденовому диску практично не приводить до збільшення U_{FM} після прискореного окислення ($T=300^{\circ}\text{C}$, $t=24$ години);

3) окислення срібних прокладок також не призводить до суттєвого збільшення U_{FM} ;

4) всі інші варіанти використання металів чистих чи з покриттями нікелем, хромом та ін.. показали після окислення збільшення значень U_{FM} різного ступеню.

РОЛЬ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ У СУЧАСНИХ КІБЕРАТАКАХ ТА МЕТОДИ ПРОТИДІЇ

У сучасному цифровому світі технологічні рішення стають дедалі складнішими та витонченішими, а методи традиційного злому часто блокуються розвиненими системами захисту. Проте найслабшою ланкою в кібербезпеці залишається людина. Саме тому соціальна інженерія стала однією з найпоширеніших тактик серед кіберзлочинців.

Соціальна інженерія – це методика маніпулювання людьми для отримання конфіденційної інформації, несанкціонованого доступу до систем або примушення жертв до виконання дій, що шкодять їхній безпеці. Головна небезпека полягає в тому, що такі атаки не вимагають технічного втручання, а використовують людські слабкості: довірливість, страх (шантаж), образа (помста), підкуп або цікавість. Згідно з дослідженням компанії Verizon, у 2023 році близько 74% кіберзломів включали елементи соціальної інженерії [1].

З розвитком технологій методи соціальної інженерії також еволюціонують. Основними типами атак є:

Фішинг (Phishing) – масові атаки через електронну пошту, соціальні мережі або месенджери, які змушують жертву розкрити свої облікові дані або натиснути на шкідливе посилання.

Вішинг (Vishing) та смішинг (Smishing) – атаки через телефонні дзвінки та SMS-повідомлення. Зловмисники можуть представлятися працівниками банку, техпідтримки або навіть правоохоронних органів.

Бейтинг (Baiting) – використання "приманки", наприклад, заражених USB-накопичувачів або підроблених безкоштовних програм.

Пре-текстинг (Pretexting) – атаки, в яких злочинець вигадусь правдоподібну історію, щоб отримати довіру жертви й змусити її розкрити важливу інформацію.

Атаки через соціальні мережі – створення підроблених акаунтів, маніпуляція довірою, використання персональних даних для цільових атак.

Один із найвідоміших випадків соціальної інженерії стався у липні 2020 року, коли група хакерів отримала доступ до внутрішньої системи Twitter [2]. Використовуючи методи вішингу, зловмисники переконали співробітників компанії передати свої облікові дані, що дозволило їм отримати контроль над акаунтами Ілона Маска, Барака Обами, Білла Гейтса та інших відомих осіб.

Хакери розмістили шахрайські повідомлення, пропонуючи людям перевести Bitcoin на певний гаманець, обіцяючи подвоєння коштів. У результаті атаки вони викрали понад 120 000 доларів США.

Атака на SolarWinds стала однією з найсерйозніших у сфері кібербезпеки за останнє десятиліття [3]. Зловмисники використали методи соціальної інженерії, щоб проникнути в ланцюг постачання компанії. Вони відправляли співробітникам підроблені електронні листи, які містили шкідливі посилання, що призводило до компрометації системи оновлення програмного забезпечення Orion. Ця атака вплинула на понад 18 000 організацій, включаючи урядові установи США та великі корпорації.

У вересні 2022 року Uber став жертвою атаки соціальної інженерії, коли хакер, використовуючи пре-текстинг, отримав доступ до внутрішньої мережі компанії [4]. Він видавав себе за працівника IT-відділу і зміг переконати одного зі співробітників передати йому код двофакторної автентифікації. Це дало хакеру можливість отримати доступ до внутрішніх ресурсів Uber, включаючи інструменти безпеки та фінансові дані.

У грудні 2022 року компанія LastPass, що спеціалізується на керуванні паролями, повідомила про витік даних клієнтів через атаку соціальної інженерії на одного з її співробітників [5]. Зловмисники змогли отримати доступ до зашифрованих резервних копій даних користувачів, що поставило під загрозу мільйони акаунтів по всьому світу.

Для зниження ризику атак необхідно поєднувати технологічні та поведінкові заходи безпеки:

Навчання та тренінги – регулярне проведення симуляцій фішингових атак серед співробітників та користувачів допомагає підвищити обізнаність і зменшити ризик маніпуляцій [6].

Багатофакторна автентифікація (MFA) – навіть якщо зловмисник отримає пароль жертви, йому буде значно складніше пройти додаткову перевірку (SMS-код, біометрія, тощо) [7].

Контроль доступу до критичних систем – принцип мінімальних привілеїв дозволяє уникнути ситуацій, коли компрометація одного облікового запису призводить до зламу всієї системи [8].

Використання ІШ для аналізу поведінки користувачів – сучасні системи кібербезпеки можуть аналізувати дії користувачів і виявляти підозрілу активність, наприклад, спроби входу з незвичних пристроїв або локацій.

Фільтрація електронної пошти та веб-захист – блокування підозрілих повідомлень та посилань на рівні корпоративної безпеки значно зменшує можливість успішних атак.

Соціальна інженерія залишається одним із найнебезпечніших методів атак у кіберпросторі. Зловмисники продовжують використовувати психологічні прийоми, щоб обходити навіть найсучасніші системи безпеки.

Останні реальні випадки, такі як злам Uber, LastPass та атака на SolarWinds, підтверджують, що жодна компанія чи організація не застрахована від подібних загроз.

Ефективна боротьба із соціальною інженерією потребує комплексного підходу, що включає технічні заходи захисту, навчання користувачів та впровадження новітніх методів виявлення підозрілої активності. Використання штучного інтелекту для аналізу поведінки користувачів, багатофакторна автентифікація та регулярне оновлення політик безпеки є ключовими елементами стратегії протидії сучасним кібератакам.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Verizon Data Breach Report 2023 [Електронний ресурс]. – Режим доступу: <https://www.verizon.com/business/resources/reports/dbir/>
2. Twitter Security Incident Report, 2020 [Електронний ресурс]. – Режим доступу: https://blog.x.com/en_us/topics/company/2020/an-update-on-our-security-incident
3. SolarWinds Attack Analysis, 2021 [Електронний ресурс]. – Режим доступу: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-352a>
4. Uber Security Breach Report, 2022 [Електронний ресурс]. – Режим доступу: <https://www.uber.com/newsroom/security-update>
5. LastPass Data Breach Statement, 2023 [Електронний ресурс]. – Режим доступу: <https://blog.lastpass.com/posts/notice-of-security-incident>
6. Cybersecurity Awareness Training, 2023 [Електронний ресурс]. – Режим доступу: <https://www.cisa.gov/cybersecurity-awareness-training>
7. NIST MFA Security Guidelines, 2023 [Електронний ресурс]. – Режим доступу: <https://csrc.nist.gov/pubs/sp/800/63/b/upd2/final>
8. Zero Trust Architecture Guidelines, 2023 [Електронний ресурс]. – Режим доступу: <https://www.cisa.gov/resources-tools/resources/zero-trust-maturity-model>

УДК 004.45

Лізунов С. І.¹, Філобок Є.В.², Верещака М.П.²

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

² асп. НУ «Запорізька політехніка»

МЕТОДИ ТА ІНСТРУМЕНТИ ЦИФРОВОЇ КРИМІНАЛІСТИКИ В РОЗСЛІДУВАННІ СУЧАСНИХ КІБЕРІНЦИДЕНТІВ

У сучасному світі, де інформаційні технології стрімко розвиваються і проникають у всі сфери життя, кількість і складність кіберінцидентів

постійно зростає. Для того щоб ефективно розслідувати такі інциденти, необхідно використовувати спеціальні методи та інструменти цифрової криміналістики, які дозволяють збирати, аналізувати та документувати цифрові докази.

Загальний принцип роботи цифрової криміналістики полягає у систематичному підході до збору та аналізу цифрових доказів з дотриманням юридичних процедур. Фахівці з цифрової криміналістики отримують дані з різних джерел, аналізують їх на відповідність критичним вимогам розслідування і формують доказову базу для подальшого використання в юридичних процесах. Ці методи дозволяють відновити хронологію подій, ідентифікувати зловмисників та визначити механізми атаки.

Розглянемо більш детально різні типи сучасних кіберзагроз та відповідні методи їх розслідування.

Програми-вимагачі (Ransomware)

Програми-вимагачі шифрують дані жертви та вимагають викуп за їх розшифрування. Сучасні варіанти ransomware, такі як Ryuk, Conti та DarkSide, використовують подвійне вимагання – окрім шифрування даних, зловмисники викрадають конфіденційну інформацію та погрожують її оприлюдненням [1].

Методи розслідування атак ransomware включають:

- аналіз зразків шкідливого ПЗ для визначення типу ransomware та можливих вразливостей;

- дослідження журналів подій для встановлення вектору проникнення; аналіз мережевого трафіку для виявлення комунікацій з командними серверами;

- відстеження транзакцій криптовалют та електронних гаманців для ідентифікації зловмисників.

Атаки на веб-додатки

Атаки на веб-додатки, такі як SQL-ін'єкції, Cross-Site Scripting та Cross-Site Request Forgery, залишаються поширеними методами компрометації систем. За даними OWASP, ін'єкційні атаки та неправильна автентифікація є найпоширенішими вразливостями веб-додатків [2].

Методи розслідування атак включають:

- аналіз журналів веб-серверів та додатків;

- дослідження HTTP-запитів та відповідей;

- аналіз коду веб-додатків на наявність вразливостей;

- відтворення атаки у тестовому середовищі.

Інструменти, такі як OWASP ZAP та Burp Suite, дозволяють аналізувати веб-трафік та виявляти вразливості. Спеціалізовані системи моніторингу, зокрема ModSecurity та NAXSI, забезпечують детальне логування спроб атак на веб-додатки.

Методи розслідування мережевих атак

Розслідування мережевих атак вимагає глибокого аналізу трафіку та журналів подій мережевих пристроїв. При виявленні підозрілої активності фахівці з цифрової криміналістики проводять ретельний аналіз PCAP-файлів (Packet Capture), які містять записи трафіку. Цей аналіз дозволяє відновити послідовність дій зловмисника, виявити використані вразливості та визначити скомпрометовані системи [3].

Важливим аспектом розслідування є аналіз DNS-запитів, який може виявити спроби зв'язку з командними серверами або використання технік DNS-тунелювання для прихованої передачі даних. Також досліджуються аномалії в мережевому трафіку, такі як незвичайні обсяги даних, нетипові протоколи або з'єднання з підозрілими IP-адресами та доменами.

Методи аналізу шкідливого програмного забезпечення

Аналіз шкідливого програмного забезпечення є фундаментальним елементом цифрової криміналістики. Цей процес поєднує статичний аналіз (дослідження коду без його виконання) та динамічний аналіз (спостереження за поведінкою шкідливого ПЗ у контрольованому середовищі). Статичний аналіз дозволяє виявити сигнатури, функціональність та потенційні вразливості, тоді як динамічний аналіз демонструє реальну поведінку шкідливого ПЗ, включаючи мережеві комунікації, модифікації файлової системи та реєстру.

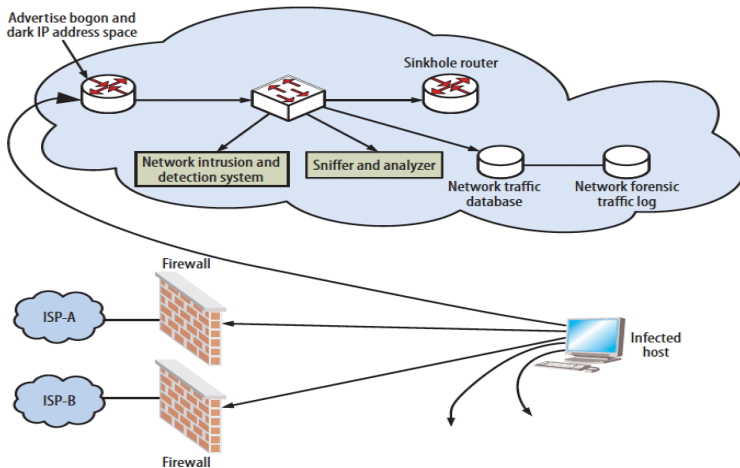


Рисунок 1 – Методологія розслідування мережевих атак

Сучасні методи аналізу шкідливого ПЗ також включають реверс-інжиніринг – процес дослідження бінарного коду для розуміння його

функціональності та механізмів роботи. Це дозволяє виявити приховані функції, механізми ухилення від виявлення та командні сервери, що використовуються для керування зараженими системами.

Аналіз методів мобільної криміналістики

Мобільна криміналістика є одним з найбільш динамічних напрямків цифрової криміналістики, що постійно адаптується до нових технологій та механізмів захисту мобільних пристроїв. Процес розслідування інцидентів, пов'язаних з мобільними пристроями, включає кілька ключових етапів.

Першим кроком є ізоляція пристрою від мережі для запобігання віддаленому стиранню даних або модифікації доказів. Це досягається шляхом активації режиму "польоту" або використання спеціальних екранованих контейнерів, які блокують всі радіосигнали.

Наступним етапом є вилучення даних, яке може здійснюватися різними методами залежно від типу пристрою, рівня захисту та доступних інструментів. Логічне вилучення використовує API операційної системи для доступу до даних, що зберігаються на пристрої. Фізичне вилучення передбачає пряме копіювання вмісту пам'яті пристрою, що дозволяє отримати доступ до видалених даних та обійти деякі механізми захисту.

Основною програмою в цій методиці використовують Cellebrite UFED (Universal Forensic Extraction Device), яка є стандартом в галузі мобільної криміналістики. UFED підтримує вилучення даних з понад 31000 моделей мобільних пристроїв, включаючи смартфони, планшети та GPS-навігатори. Процес роботи з UFED починається з підключення мобільного пристрою до системи через спеціальний кабель або адаптер. Після встановлення з'єднання фахівець обирає тип вилучення (логічне, файлова система або фізичне) та запускає процес [4].

UFED автоматично визначає модель пристрою та пропонує оптимальні методи вилучення даних. Для пристроїв Android система може використовувати ADB (Android Debug Bridge) для логічного вилучення або експлуатувати відомі вразливості для отримання root-доступу та проведення фізичного вилучення. Для пристроїв iOS UFED може створювати резервні копії iTunes, використовувати jailbreak або експлуатувати вразливості bootloader для доступу до зашифрованих даних.

Після вилучення даних UFED проводить їх декодування та аналіз, відновлюючи видалені повідомлення, фотографії, контакти та історію дзвінків. Система також аналізує геолокаційні дані, історію використання додатків та інформацію з соціальних мереж. Результати аналізу представляються у зручному для дослідження форматі з можливістю створення детальних звітів, що включають часові мітки, хеш-суми та інші метадані, необхідні для забезпечення допустимості доказів у суді.

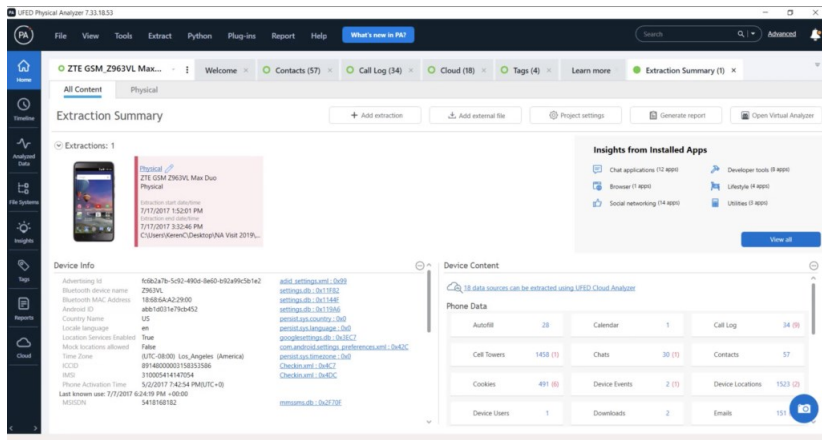


Рисунок 2 – Інтерфейс UFED системи

Важливою функцією UFED є можливість аналізу зв'язків між різними типами даних, що дозволяє відновити хронологію подій та виявити приховані зв'язки. Наприклад, система може пов'язати телефонні дзвінки з повідомленнями, геолокаційними даними та фотографіями, створюючи комплексну картину активності користувача пристрою.

З розвитком технологій та появою нових типів кіберзагроз, методи цифрової криміналістики постійно еволюціонують. Інтеграція штучного інтелекту, розвиток хмарної криміналістики та вдосконалення інструментів аналізу шкідливого програмного забезпечення відкривають нові можливості для ефективного розслідування складних кіберінцидентів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Identity crisis: Why ransomware groups rebrand — and disappear [Електронний ресурс]. — Режим доступу: <https://www.cybersecuritydive.com/news/ransomware-ryuk-conti-revil-2021/608845/>
2. Безпека веб-додатків: найкращі практики та вразливості [Електронний ресурс]. — Режим доступу: <https://itproger.com/ua/news/bezopasnost-veb-prilozheniy-luchshie-praktiki-i-uyazvimosti>
3. Network Forensics: An Analysis of Techniques, Tools, and Trends [Електронний ресурс]. — Режим доступу: <https://www.computer.org/csdl/magazine/co/2012/12/mco2012120036/13rUxBa5qc>

4. How To Use UFED Physical Analyzer 7.33 [Електронний ресурс]. – Режим доступу: <https://www.forensicfocus.com/articles/how-to-use-ufed-physical-analyzer-7-3-3/>

УДК 004.056

Неласа Г.В.¹, Аль-Хамад Н.А.²

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

² асп. НУ «Запорізька політехніка»

ДОСЛІДЖЕННЯ ТА АНАЛІЗ СХЕМИ ШИФРУВАННЯ ВІДКРИТОГО КЛЮЧА К-РКЕ В СТАНДАРТІ FIPS 203

Федеральний стандарт обробки інформації (FIPS) 203 запроваджує механізм інкапсуляції ключів на основі модульної решітки (ML-KEM) для захисту даних від загроз квантових обчислень. Великі компанії, включаючи Google, активно впроваджують постквантову криптографію у свої сервіси, зокрема квантово-безпечні цифрові підписи у Cloud Key Management Service [1].

Мета дослідження: дослідити алгоритми, що складають основу ML-KEM (зокрема схему шифрування відкритого ключа К-РКЕ) та проаналізувати їх функціонування.

Предмет дослідження: стандарт FIPS 203 для побудови безпечного постквантового процесу обміну ключами.

Процес обміну ключами.

В механізмі ML-KEM процес обміну ключами відбувається наступним чином:

Аліса генерує пару ключів – відкритий (інкапсуляції) та секретний (декапсуляції).

Боб, отримавши відкритий ключ Аліси, створює першу копію спільного секретного ключа та зашифрований текст, який асоціюється зі спільним секретним ключем.

Боб надсилає зашифрований текст Алісі.

Аліса дешифрує зашифрований текст і отримує другу копію спільного секретного ключа.

Стандарт FIPS 203 описує спочатку схему шифрування відкритого ключа К-РКЕ, алгоритми якої використовуються як підпрограми в ML-KEM.

КЕМ складається з трьох алгоритмів та колекції наборів параметрів.

Три наступні алгоритми зазначені в стандарті [2]:

- 1) імовірний алгоритм генерації ключів, позначений KeyGen;
- 2) імовірний алгоритм "інкапсуляції", позначений Encaps;
- 3) детерміністичний алгоритм "декапсуляції", позначений Decaps.

Набори параметрів.

ML-KEM включає три набори параметрів, що забезпечують різні рівні безпеки: ML-KEM-512 (категорія безпеки 1); ML-KEM-768 (категорія безпеки 3); ML-KEM-1024 (категорія безпеки 5).

У дослідженні використовувались параметри ML-KEM-512 з наступними значеннями: $k = 2$, $\eta_1 = 3$, $\eta_2 = 2$, $du = 10$, $dv = 4$, а також константи $p = 256$ і $q = 3329$.

Алгоритми в схемі K-PKE.

Алгоритм генерації ключів (K-PKE.KeyGen) приймає випадкове значення в якості вхідних даних.

Основні етапи:

1. Генерація псевдовипадкової матриці A та векторів s та e .
2. Перетворення векторів у область ТЧП (теоретико-числове перетворення).
3. Обчислення вектору $t = As + e$.
4. Кодування отриманих векторів t та s для формування ключів.

Результат: згенеровані ключі ek_PKE (800 байт) та dk_PKE (768 байт).

На рис. 1 наведені результати використання алгоритму K-PKE.KeyGen програмою написаною на Python.

```
1 d = os.urandom(32)
2 ek_PKE, dk_PKE = K_PKE_KeyGen(d)
3 print(f"Keys generated:\n{ek_PKE}\n{dk_PKE}\nwith corresponding lengths:\n{len(ek_PKE)} bytes\n{len(dk_PKE)} bytes")
Keys generated:
b'%16\xd6\xa84\x0c\xbe\xf1\xcb\x92.1P\xff\xf0\x1aT\xacA\xfb\xf8\xa46\xe9\x11\xe4\x88\xcc\x
b'\xfe7\x15\x93\xd2]B\xca\xc1\xc\xd7\xb5\x04\xf6E\x86Z\x1b\x15\xc5\x02\xe9\xc75<\xd9\x91\
with corresponding lengths:
800 bytes
768 bytes
```

Рисунок 1 – Результати генерації ключів

Алгоритм шифрування (K-PKE.Encrypt) приймає ключ шифрування, відкритий текст m та випадкове значення в якості вхідних даних.

Основні етапи:

1. Декодування вектора t та регенерація матриці A .
2. Генерація векторів u , $e1$, $e2$ з використанням випадковості.
3. Обчислення векторів u та v , кодування відкритого тексту m у поліном v .
4. Стиснення та кодування результатів.

Результат: зашифрований текст c розміром 768 байт.

На рис. 2 наведені результати використання алгоритму K-PKE.Encrypt програмою написаною на Python.

Алгоритм дешифрування (K-PKE.Decrypt) приймає ключ дешифрування та зашифрований текст в якості вхідних даних.

```
65 m = os.urandom(32)
66 r = os.urandom(32)
67 c = K_PKE_encrypt(ek_PKE, m, r)
68 print(f"Generated plaintext message m:\n{m}\nwith corresponding length:\n{len(m)} bytes")
69 print(f"Ciphertext generated:\n{c}\nwith corresponding length:\n{len(c)} bytes")
Generated plaintext message m:
b'X\nk\xea\x07\xd9\\\xd9\xf3\xf7\x8f\xd8\xa7\x16\x9be%z)k\xd4q|\xd8\x00\xdb\x81\x1b'!\x01\xcc"
with corresponding length:
32 bytes
Ciphertext generated:
b'\xc2\x0f\x00\xed\xae\xf1\x8f\xd2f\x038\xcd\xeb\xcf96\xee\x0b\xbd\xce\xb7\x16\x8b\x1a\x09\xf2\x89\xca\x98I64\
with corresponding length:
768 bytes
```

Рисунок 2 – Результати шифрування

Основні етапи:

1. Розпакування та декодування значень u та v .
2. Обчислення справжнього постійного значення v та значення $v' - v$.
3. Декодування відкритого тексту m з полінома v .

Результат: вихідне відкрите повідомлення m' .

На рисунку 3 наведені результати використання алгоритму K-PKE.Decrypt програмою написаною на Python.

```
71 m_ = K_PKE_decrypt(dk_PKE, c)
72 print(f"Decrypted original message:\n{m_}\nwith corresponding length:\n{len(m_)} bytes")
Decrypted original message:
b'X\nk\xea\x07\xd9\\\xd9\xf3\xf7\x8f\xd8\xa7\x16\x9be%z)k\xd4q|\xd8\x00\xdb\x81\x1b'!\x01\xcc"
with corresponding length:
32 bytes
```

Рисунок 3 – Результати дешифрування

З наведених результатів на рис. 2 – 3 видно що результуюче відкрите повідомлення m відповідає оригіналу, тобто $m' = m$. Значить реалізовані алгоритми успішно виконують функції схеми шифрування K-PKE зазначеного в стандарті FIPS 203. Розміри ключів та формат в якому вони представленні також відповідають тим, що зазначені в цьому стандарті.

Висновки: В результаті дослідження були побудовані та проаналізовані алгоритми в схемі K-PKE, що є основою для побудови ML-KEM. Реалізовані алгоритми успішно забезпечують обмін ключами з використанням постквантових криптографічних методів. Результати демонструють, що розшифроване повідомлення точно відповідає оригіналу, що підтверджує коректність та ефективність реалізованих алгоритмів відповідно до специфікацій NIST FIPS 203.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Jennifer Fernick, Andrew Foster (February 21, 2025). “Announcing quantum-safe digital signatures in Cloud KMS”: Google Cloud. [Електронний ресурс]. – Режим доступу: <https://cloud.google.com/blog/products/identity-security/announcing-quantum-safe-digital-signatures-in-cloud-kms>
2. National Institute of Standards and Technology (2024) Module-Lattice-Based Key Encapsulation Mechanism Standard. (Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) NIST FIPS 203. [Електронний ресурс]. – Режим доступу: <https://doi.org/10.6028/NIST.FIPS.203>

УДК 004.056.55

Бережний О.Ю.¹, Корольков Р.Ю.²

¹ асп. НУ «Запорізька політехніка»

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

ДОСЛІДЖЕННЯ МЕТОДІВ ОБХОДУ АНТИВІРУСНОГО ЗАХИСТУ MICROSOFT DEFENDER

У сучасних умовах зростання кіберзагроз, пов'язаних як з діяльністю організованих злочинних угруповань, так і зі спеціалізованими державними кіберструктурами, ефективний захист інформаційних систем набуває критичного значення [1]. Найпоширеніша у світі ОС Windows оснащена вбудованим антивірусним засобом Microsoft Defender, здатність якого виявляти сучасні техніки компрометації має вирішальне значення для безпеки користувачів і організацій. У дослідженні перевірено здатність Microsoft Defender виявляти як типові, так і складні методи запуску шкідливого коду у вигляді зворотної оболонки (reverse shell). Експериментальне тестування виконувалося у віртуальному середовищі на базі Windows 11 з активованим Microsoft Defender та Kali Linux як атакувальної машини.

Було реалізовано низку технік, зокрема запуск PowerShell-скриптів, обфускацію команд через кодування в Base64, fileless-виконання, використання легітимних системних компонентів Windows (LOLBins) – таких як regsvr32.exe і msbuild.exe, а також створення кастомного виконуваного .exe-файла з вбудованим корисним навантаженням на C#.

Експерименти показали, що Microsoft Defender ефективно виявляє більшість типових методів запуску зворотної оболонки, зокрема тих, що використовують команду Invoke-Expression, параметр -EncodedCommand, обфусковані PowerShell-скрипти та fileless-техніки виконання. Більшість

таких методів блокуються або на етапі запуску, або за рахунок інтеграції з інтерфейсом AMSI (Antimalware Scan Interface). Найбільш ефективним методом обходу антивірусного захисту виявився запуск шкідливого коду за допомогою msbuild.exe, який є частиною .NET Framework. У цьому випадку XML-файл із вбудованим C#-кодом успішно виконував шкідливий код, який ініціював встановлення зворотного TCP-з'єднання, без виявлення з боку Defender. Додаткове використання режиму прихованого запуску (-w hidden) дозволило здійснити експлуатацію без видимих ознак для кінцевого користувача. Зазначимо, що подібні техніки застосовуються в реальних атаках. Наприклад, хакерські групи Carbanak та FIN7, які спеціалізуються на атаках проти фінансового сектору та підприємств ритейлу, використовували msbuild.exe для прихованого запуску шкідливого C#-коду, що унеможливлювало сигнатурне виявлення з боку Defender [2].

Зведене порівняння протестованих методів, їх виявлення Defender та причин блокування або обходу наведено в таблиці 1.

Таблиця 1 – Порівняння ефективності методів обходу Defender

Метод	Тип виконання	Виявлення Defender	Причина виявлення
msfvenom PowerShell	+ .ps1 reverse shell	Так	Сигнатурне виявлення PowerShell-пейлоаду
Base64 + runner.ps1	Шифрований скрипт + Invoke-Expression	Так	Використання IEX і декодування Base64
TCP reverse shell (чистий PowerShell)	Fileless-скрипт	Так	Поведінковий аналіз + виявлення AMSI
EncodedCommand (.bat)	Прихований запуск PowerShell	Так	Декодування Base64 + команда TCP-клієнта
regsvr32 + .sct (JScript)	LOLBin + скриптова вставка	Так	Активність scriptlet-файлу з TCP-з'єднанням
msbuild + XML (inline C#)	XML із вбудованим C#-кодом	Ні	Відсутність сигнатур на кастомний C#
msbuild + -w hidden	Тихий запуск PowerShell	Ні	Приховане виконання без видимих ознак

Таким чином, отримані результати демонструють наявність реальних векторів обходу захисту Microsoft Defender через легітимні інструменти

Windows. Це підтверджує доцільність впровадження багаторівневої моделі безпеки (Defense in Depth). Такий підхід передбачає використання EDR-рішень із поведінковим аналізом, впровадження політик AppLocker або Windows Defender Application Control (WDAC), обмеження запуску утиліт типу msbuild.exe у середовищах, де їх використання не передбачено, ізоляцію інструментів розробки та виконання коду, а також навчання персоналу виявляти загрози, пов'язані з використанням легітимних системних утиліт (LOLBins) у шкідливих цілях.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. CISA. Russian GRU Cyber Actors Conduct Global Infrastructure Attacks [Електронний ресурс]. – 2024. – Режим доступу: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-249a> – Дата доступу: 03.04.2025.

2. Trend Micro. Carbanak and FIN7 Attack Techniques [Електронний ресурс]. – 2021. – Режим доступу: https://www.trendmicro.com/en_us/research/21/d/carbanak-and-fin7-attack-techniques.html – Дата доступу: 04.04.2025.

УДК 004.056.53

Нагорна Н.М.¹

¹ старш. викл. НУ «Запорізька політехніка»

ЗАХИСТ НАДВЕЛИКИХ ІНТЕГРОВАНИХ СХЕМ І СИСТЕМ НА КРИСТАЛІ ВІД НЕСАНКЦІОНОВАНОГО ВТРУЧАННЯ

Життєвий цикл мікросхеми включає етапи проектування та експлуатації. Вже на першому етапі проектування при формуванні технічного завдання, необхідно позначити вимоги до заходів захисту мікросхеми від непередбачених впливів і визначити рівень безпеки.

Способи захисту можуть бути програмними та апаратними. Апаратні способи дозволяють:

- захистити кристал мікросхеми від механічних впливів при проведенні реінжинірингу;
- захистити блоки пам'яті за допомогою створення блоку керування правами доступу до пам'яті;
- захистити кристал від перевищення номінальних значень електричних параметрів.

Сучасні пристрої типу надвеликих інтегрованих схем (НВІС) і систем на кристалі (СнК) мають захищену інформацію щодо проєкту (ІР-захист) і захищені дані. Такий захист можливий завдяки:

можливості знищення всіх критичних даних у момент несанкціонованого втручання;

завантаженню ключа шифрування користувача за допомогою секретного ключа, вбудованого в мікросхему при її виробництві;

IP-захисту, який не дозволяє вносити зміни до проекту і контролює можливість копіювання проекту.

Наприклад, СнК, реалізовані за технологією SmartFusion2 корпорації Microsemi, мають вбудовані блоки, які виконують наступні функції захисту даних:

- блок недетермінованого генератора випадкових двійкових послідовностей (NRBG);

- блок криптографічного сервісу користувача з виконанням шифрування за стандартами AES 128 / -256, SHA 256 та HMAC;

- апаратні засоби мережевого захисту (firewalls) доступу до пам'яті мікроконтролерної підсистеми.

Визначальною особливістю СНК SmartFusion2, яка дозволяє мати IP-захист і захист даних, є наявність енергонезалежної програмованої логічної матриці, виконаної за флеш-технологією.

У вказаній матриці конфігураційна flash пам'ять рівномірно розподілена площею кристала. Для її роботи не потрібна мікросхема зовнішньої конфігураційної пам'яті, тому не потрібно і завантажувати конфігурацію з неї. Програмована логічна матриця готова до роботи практично відразу після включення.

Крім того, під час конфігурування матриці неможливо підключитися до потоку конфігураційних даних та зчитати його без санкції на зчитування.

На етапі функціонально-логічного проектування НВІС та СнК для захисту пристроїв використовуються методи обфускації у якості апаратного захисту.

В методах обфускації змінюється логічна структура мікросхеми за рахунок додавання до неї додаткових логічних елементів і ключових входів. Вказаний процес називається логічним кодуванням. Він дозволяє змінювати комбінаційну частину функціональних блоків. Функціональний блок працює за заданим алгоритмом, якщо на його ключові входи надходять сигнали у відповідності з секретним ключем, що зберігається у вбудованій пам'яті (рис. 1).

У цьому разі зломиснику, який не має ключа, недоступна внутрішня структура пристрою.

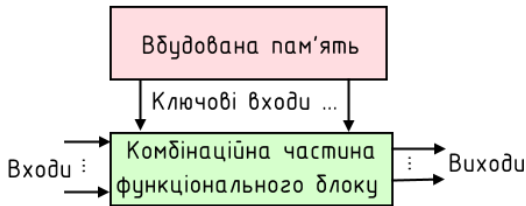
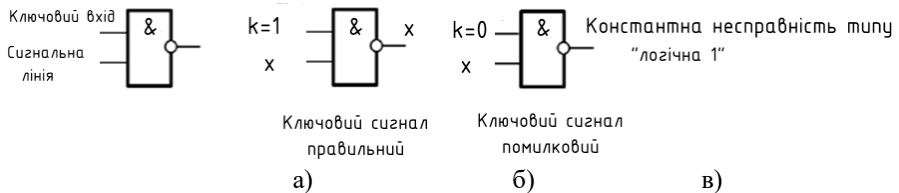


Рисунок1 – Змінення структури функціонального блоку при логічному кодуванні

На рис. 2 на прикладі логічного елемента 2І-НЕ проілюстрований принцип обфускації.



- а) – логічний елемент І-НЕ має додатковий ключовий вхід;
 б) – робота ЛЕ І-НЕ при справжньому ключі;
 в) - робота ЛЕ І-НЕ при несправжньому ключі

Рисунок 2 – Ілюстрація методу логічного кодування

УДК 535.8

Кутовий І.А.¹, Корольков Р.Ю.², Коротун А.В.^{3,4}

¹ студ. гр. БКз-311 НУ «Запорізька політехніка»

² доц. НУ «Запорізька політехніка»

³ проф. НУ «Запорізька політехніка»

⁴ с.н.с. Інституту металофізики ім. Г.В. Курдюмова НАН України

ЗАГАСАННЯ ЕЛЕКТРОМАГНІТНИХ ХВИЛЬ У МЕТАМАТЕРІАЛАХ

Штучні електромагнітні матеріали (метаматеріали) середовища з одночасно від'ємними діелектричною та магнітною проникностями викликають неабиякий інтерес в дослідницькому середовищі. Це пов'язано з можливостями використання вказаних матеріалів для створення гіперлінз та маскуючих покриттів у різних частотних діапазонах, субхвильовій нанолітографії тощо.

Структурними елементами метаматеріалів є тонкі металеві провідники (ENG-матеріали), подвійні розрізані металеві кільця (MNG-матеріали) або сукупність провідників і кілець (DNG-матеріали).

Оскільки структурні елементи метаматеріалів металеві, то в ближньому інфрачервоному оптичному діапазонах спектра суттєвими є втрати енергії, а тому дуже складно одержати штучні матеріали з ідеальними оптичними властивостями.

Проте відомо, що параметри загасання суттєво залежать від геометричних параметрів структурних елементів штучних середовищ, а тому дослідження розмірних залежностей параметрів електричного і магнітного загасання є актуальною задачею.

Частотні залежності діелектричної проникності ENG-матеріалу і магнітної проникності MNG-матеріалу визначаються співвідношеннями

$$\tilde{n}(\omega) = \tilde{n}^\infty - \frac{\omega_{pe}^2}{\omega(\omega + i\zeta_e)}; \quad (1)$$

$$\mu(\omega) = 1 - \frac{F\omega^2}{\omega^2 - \omega_{0m}^2 + i\omega\zeta_m}, \quad (2)$$

де частота електронної плазми та параметр загасання

$$\omega_{pe} = \sqrt{\frac{2\pi c}{\tilde{n}_m R^2 \ln \frac{R}{r_0}}}; \quad \zeta_e = \frac{2\omega_{pe}^2 \tilde{n}_0}{\pi \sigma} \left(\frac{R}{r_0} \right)^2, \quad (3)$$

а резонансна частота кільцевого резонатора та параметр магнітного загасання

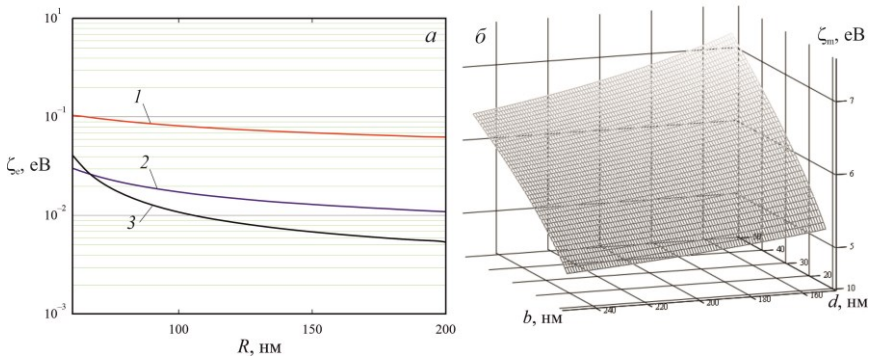
$$\omega_{0m} = \sqrt{\frac{3lc^2}{\pi r^3 \ln \frac{2b}{d}}}; \quad \zeta_m = \frac{2lR_l}{r\mu_0}. \quad (4)$$

У формулах (1) – (4): $\tilde{n}_0$ і μ_0 – електрична і магнітна сталі; $\tilde{n}^\infty$ – внесок кристалічної ґратки в діелектричну проникність металу тонких провідників; $\tilde{n}_m$ – діелектрична проникність оточуючого середовища; c – швидкість світла; r_0 – радіус провідника; R – відстань між осями провідників; σ – питома електропровідність матеріалу провідника; l – відстань між площинами, в яких розташовано подвійні кільця; d – товщина кільця; b –

радіальний розмір кілець та відстань між ними; r – радіус внутрішнього кільця; R_l – погонний опір матеріалу кільця, $F = \pi(r/l)^2$.

Результати розрахунків параметрів загасання для ENG- і MNG-матеріалів із золотими провідниками і подвійними кільцями в тефлоні ($\tilde{n}_m = 2, 3$) наведені на рис. 1.

Встановлено, що параметр загасання для ENG-матеріалів зменшується зі збільшенням відстані між провідниками, а за однакової відстані цей параметр менший у випадку провідників із більшим радіусом. В свою чергу, для MNG-матеріалів параметр загасання зменшується зі збільшенням радіального розміру кілець і зменшенні їх товщини.



a – ENG-матеріал ($1 - r_0 = 10$ нм; $2 - r_0 = 30$ нм; $3 - r_0 = 50$ нм);

b – MNG-матеріал ($l = 100$ нм; $r = 50$ нм).

Рисунок 1 – Розмірні залежності параметра загасання в метаматеріалах різного типу

УДК 535.2: 343.982

Сніжна К.Г.¹, Скляр М.С.², Сніжної Г.В.³

¹ студ. гр. БАД-533 НУ «Запорізька політехніка»

² студ. гр. БК-423 НУ «Запорізька політехніка»

³ д-р. техн. наук, проф. НУ «Запорізька політехніка»

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ EYEDETECT У ПОЛІГРАФНИХ ДОСЛІДЖЕННЯХ

Поліграф (або детектор брехні) широко застосовується в діяльності державних і комерційних структур з метою перевірки лояльності або при розслідуванні будь-яких подій. Згідно ДСТУ 8692:2016 «Поліграфи. Технічні умови» залучення поліграфа спрямовано, в першу чергу, на захист прав фізичних та юридичних осіб у сфері безпеки життя та бізнесу. Дослідження за допомогою поліграфа можуть підтвердити правдивість під час кадрових досліджень або непричетність до правопорушень [1].

Прилад поліграф призначений для вимірювання та реєстрації фізіологічних показників, таких як артеріальний тиск, дихання, пульс та електропровідність шкіри. Це відбувається під час тестування, коли обстежуваному ставлять питання і він надає відповіді. Коли людина обманює, то його тіло реагуватиме несумісним із їх встановленими «нормальними» реакціями чином через нервозність чи страх виявлення. Тому до апаратно-програмного комплексу поліграфа входять датчики контролю за фізіологічними реакціями організму людини. Стандартний комплект такий: датчики дихання, датчик знімання шкірно-гальванічного рефлексу, датчик знімання фотоплетизмограми, датчик тремору, датчик знімання тиску.

Сучасний розвиток цифровізації надав можливість створення і використання особливо розумних датчиків [2], які лежать в основі сучасного моніторингу та автоматизації будь-яких процесів. Задіяння аналізаторів голосової напруги для відстеження зміни в тембрі голосу опитуваного сприяє удосконаленню поліграфа. Застосування нанодатчиків електродермічної реакції, які вживлятимуть безпосередньо в дерму, дозволять більш точно фіксувати зміну електропровідності шкірного покриву людського тіла [3].

Використання високоточних камер дозволить фіксувати розширення та звуження значка, а також зміну площі світлих та темних плям ока. На цьому фізіологічному ефекті побудована технологія «EyeDetect» (дослівно – «виявлення очей», але більш підходяще – «очі не брешуть»), яка використовується в поліграфах нового покоління. Детектор вимірює невеликі зміни у поведінці очей виявлення брехні. Загальна похибка вимірювання та інтерпретації результатів до 10%. Однак ця похибка може бути зменшена при

використанні відеокамер високої роздільної здатності та відповідного програмного забезпечення.

EyeDetect можна використовувати для скринінгових тестів з різних тем у кримінальних чи цивільних справах. Крім детекції брехні, що важливо, є можливість використання зазначеної технології для медичної діагностики.

Немаловажним є, яка використовується методика обробки результатів. Якщо реакція тіла людини (змінюється вологість шкіри, амплітуда та частота дихання, серцебиття та ін.) при брехливих відповідях вивчена досить точно, то поведінка очей потребує додаткових досліджень. Наприклад, можна визначити брехню щодо траєкторії руху очей. Якщо око випробуваного «пішло» ліворуч і вгору, це реакція «правда» на свідомо правдиві питання. Це зона візуальних образів тих об'єктів, які людина колись бачила. Якщо око випробуваного «пішов» праворуч і вгору, то це реакція «брехня» на свідомо неправдиві питання. Це зона візуальних образів тих речей чи явищ, які людина ніколи не бачила раніше. Однак у шульги, в порівнянні з правшою, очі «поводяться» по-різному, що потребує відповідного коригування в інтерпретації результатів.

Моніторинг фізіологічних параметрів людини за допомогою поліграфа та процес отримання відповідної якості результатів може бути покращений за рахунок застосування методів статистичного аналізу і теорії випадкових процесів [4].

Список використаної літератури

1. Градун С. А. Використання поліграфа у діяльності Національної поліції України / С. А. Градун // Правовий часопис Донбасу. – 2024. – № 1 – С. 72–77. <https://doi.org/10.32782/2523-4269-2024-86-72-77>
2. Василенко О. В. Менеджмент цифрового виробництва: монографія / О. В. Василенко, Г. В. Сніжної, Ю. С. Ямненко – Запоріжжя: Національний університет «Запорізька політехніка», 2022. – 120 с. ISBN 978-617-529-374-4.
3. Сніжної Г.В. Нанополіграф: реальність або мрія / Г. В. Сніжної // Всеукраїнська науково-практична конференція «Проведення психофізичних досліджень з використанням поліграфу в умовах воєнного стану: теоретичний та практичний аспекти», 01 червня 2023 р. – Івано-Франківськ: Донецький державний університет внутрішніх справ, Луганський навчально-науковий інститут ім. Е. О. Дідоренка, ГО «Міжнародна асоціація поліграфологів», 2023.
4. Сніжної Г. В. Моніторинг і контроль складних стохастичних систем : монографія / Г. В. Сніжної, О. В. Томашевський, С. М. Степаненко – Запоріжжя: Національний університет «Запорізька політехніка», 2022. – 124 с. ISBN 978-617-529-373-7.

УДК 62-523.8; 519.876.2

Тюрін М.М.¹, Василенко О.В.²

¹ студ. гр. БК-312сп НУ «Запорізька політехніка»

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

МОДЕРНІЗАЦІЯ ФРЕЗЕРНИХ СТАНКІВ НА БАЗІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Впровадження верстатів на базі встановлення числового програмного керування із можливістю подальшої інтеграції верстатів в кібер-фізичну систему виробництва є трендом та необхідною умовою Індустрії 4.0. Ця тенденція спрямована на оптимізацію продуктивності, підвищення ефективності та створення інтелектуальних виробничих систем, так званого Цифрового виробництва [1].

Верстати з ЧПУ відіграють вирішальну роль в автоматизації виробничих процесів, можуть бути інтегровані із такими проривними технологіями І4.0 як робототехніка, машинне навчання, Цифрові двійники. Використання систем машинного зору дозволяє автоматично вирівнювати та перевіряти деталі, скорочуючи час налагодження та покращуючи контроль якості. Підключення до Інтернету речей (IoT) дає можливості моніторити процес в режимі реального часу. Використання моделей Машинного навчання дозволяє не тільки покращувати процеси обробки, але й здійснювати предиктивне обслуговування.

Ще у 70-80-х роках 20 сторіччя інтеграція верстатів із системами автоматизованого проєктування (CAD) і автоматизованого виробництва (CAM) дозволила безпосередньо перетворювати CAD-проєкти в машинні інструкції, що, в свою чергу, значно підвищує точність і ефективність виробничого процесу. На жаль, в українській промисловості досить багато морально застарілих верстатів, зокрема фрезерувальних. Якщо верстати знаходяться в експлуатації, але не забезпечують прийнятної якості та продуктивності, то можна або модернізувати існуючі верстати, або придбати сучасні. Модернізація включає в себе не тільки встановлення програмного забезпечення, але й ремонт/реконструкцію апаратної частини верстата. Необхідність модернізації ґрунтується на певних критеріях якості, які верстати із ЧПУ дозволяють покращити. Серед них:

точність і акуратність завдяки використанню програмного забезпечення для автоматизованого проєктування (САПР) для створення проєктів деталей, які потім безпосередньо переводяться у машинні інструкції для формування траєкторій руху актуаторами (інструментом);

підвищення продуктивності за рахунок безперервного і швидкого виконання програми, зокрема, рутинних операцій;

підвищення складності операцій обробки за рахунок запрограмованих складних траєкторій руху інструменту;

збільшення гнучкості на базі перепрограмування (внесення нових параметрів в готову програму), встановлення нової програми;

збільшення економії в довгостроковій перспективі, оскільки зменшується відходи матеріалу і знижуються витрати на робочу силу;

інтеграція з системами CAD/CAM та кібер-фізичними системами [1] на основі підключення до інформаційно-комунікаційних каналів (і відповідних технологій), збору даних для надбудов та модулів Цифрового виробництва, попереднього моделювання в системах CADAM для оптимізації траєкторій руху інструменту та процесів обробки.

Метою роботи є розробка та дослідження варіантів системи автоматизації фрезерувального станка та узагальнення отриманих результатів до рівня методики. Необхідно виконати синтез роботехнічної системи на основі аналізу варіантів побудови систем на макрорівні, з використанням парадигми синергії та принципів паралельного проектування. Актуальність роботи визначається недостатнім рівнем розкриття питань розробки та дослідження шляхів модернізації багатокоординатних верстатів в парадигмі «м'якої цифровізації».

Для досягнення поставленої мети необхідно пройти ряд етапів та розв'язати наступні задачі: формування критеріїв якості верстату; синтез системи автоматизації та її декомпозиція за різними принципами (структурним та функціональним); вибір програмного забезпечення та формування структурної схеми шляху передачі інформації від CAD до CAM та на актуатори; формування алгоритму функціонування системи; узагальнення отриманих результатів на рівні методики.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Василенко О.В., Сніжної Г.В., Ямненко Ю.С. Менеджмент цифрового виробництва. – Запоріжжя: НУ «Запорізька політехніка», 2021. – 120 с.
2. Василенко О.В. «М'яка» цифровізація підприємств в українських реаліях / О.В. Василенко, Г.В. Сніжної, В.І.Рева, С.А.Івченко // Матеріали VII Міжнар. наук.-техн. конф. Комп'ютерне моделювання та оптимізація складних систем, 3-5 лист. 2021 р. – Дніпро: УДХТУ, 2021. – С. 126-128

УДК 535.6; 539

Єршов М.О.¹, Василенко О.В.², Шумейко П.Д.³,

¹ студ. гр. БК-313сп НУ «Запорізька політехніка»

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

³ канд. техн. наук, доц., ТОВ «ЛКМ ПЛЮС»

ОТРИМАННЯ ОПТИМАЛЬНИХ ПАРАМЕТРІВ НАНОРОЗМІРНИХ ПІГМЕНТІВ КСЕРАЛІКІВ

Для фарб на основі ксераліків (Xirallic paints) характерний сильний ефект блиску з виразним мерехтінням, подібно до перламутру морських раковин. Вперше така фарба була і запатентована дослідниками компанії Merck KGaA в Японії [1] і фактично призвела до революції в галузі покриттів для автомобілів і не тільки. В лабораторіях української фірми «ЛКМ ПЛЮС» проводяться дослідження із ціллю покращення рецептури фарб, підвищення їхньої конкурентоспроможності на ринку сучасних трендових покриттів. Впровадження нової рецептури сучасних фарб на базі ксераліків потребує наукових досліджень в галузі оптичної фізики.

Пігмент ксералік виготовляють із пластинок оксиду алюмінію, покритих оксидом титану. Ці пластинки мають субмікронні розміри і відносяться до нанорозмірних об'єктів, властивості яких, зокрема і оптичні, залежать від багатьох чинників [2]. Серед них збудження атомів та їхня вібрація (фонони), зміщення та деформації кристалічної решітки, переходи серед молекулярних орбіталей, переходи між рівнями енергії (між електронними орбіталями). Окремо слід виділити хвильові процеси: дифракцію, розсіяння, інтерференцію та поляризацію.

Варто також брати до уваги апарат сприйняття оптичної інформації людини, яка має власну спектральну чутливість (обмеження щодо сприйняття хвиль поза межами смуги пропускання), кут зору та електрохімічні процеси, які передують інтерпретації інформації, перетворення її на «картинку», образ, який має сенс.

Сучасний стан комплексного підходу в аналізі оптичних явищ та підвищення вимог до зовнішнього вигляду товару, породив новий науковий напрям, який називається Color Science & Technology, задачами якого є вивчення теорій і методів, що використовуються для проєктування, виготовлення та вимірювання кольорових предметів. Цей напрям є синергією кількох традиційних наукових дисциплін, як фізична хімія, оптика, фізика нанооб'єктів та інших.

Основні фактори впливу фізичних явищ на зовнішній вигляд поверхонь можна представити рисунком 1.

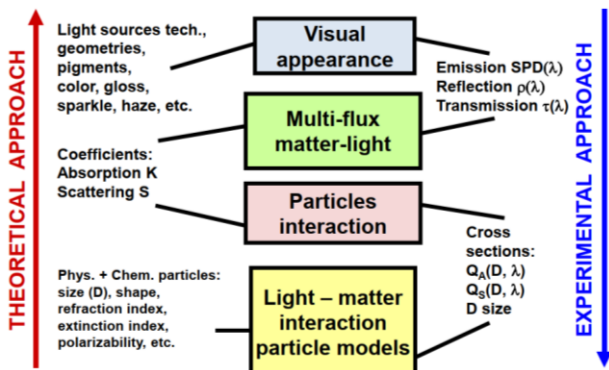


Рисунок 1 – Основні фактори впливу на оптичні феномени [2]

Метою роботи є дослідження та розробка наукових підходів до формування конкурентоспроможних рецептур фарб-ксераліків в умовах українського підприємства. Для досягнення поставленої мети необхідно пройти розв'язати наступні задачі: сформувати теоретичне підґрунтя для аналізу оптичних ефектів ксераліків; провести математичне моделювання оптичних властивостей та багатоваріантний аналіз для пошуку напряму оптимізації параметрів частинок пігменту ксераліків; сформувати критерії для фізико-хімічних процесів формування оптимальних параметрів ксераліків; узагальнити отримані результати на рівні методики для впровадження у серійне виробництво.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Andrea Adelson. Next, a Kandy-Kolored Tangerine-Flake Color-Shifting Baby. [Електронний ресурс] – Режим доступу: <https://www.nytimes.com/2000/09/29/automobiles/next-a-kandy-kolored-tangerine-flake-color-shifting-baby.html?pagewanted=2&src=pm>
2. Francisco Martinez Verdu. The current challenges of Color Physics & Chemistry. [Електронний ресурс] – Режим доступу: https://rua.ua.es/dspace/bitstream/10045/44728/3/Current_challenges_of_Color_Physics_Chemistry.pdf

СЕКЦІЯ «ТЕЛЕКОМУНІКАЦІЇ ТА РАДІОТЕХНІКА»

УДК 621.396.1

Бугрова Т.І.¹, Горохов Є.П.²

¹ доц. НУ «Запорізька політехніка»

² студ. гр. БК-914м НУ «Запорізька політехніка»

ЗАСТОСУВАННЯ МАШИННОГО ЗОРУ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ FPV ДРОНІВ

Машинний зір виконує ключову роль у системах штучного інтелекту, забезпечуючи можливість «бачити» та аналізувати візуальну інформацію. Його основні функції спрямовуються на автоматичне розпізнавання об'єктів, текстур, руху, форм; контроль якості в промисловості (виявлення дефектів); навігацію в автономних системах (роботи, дрони, авто); взаємодію з користувачами (розпізнавання облич, жестів); медичну діагностику, безпеку, агроаналіз тощо. Машинним зором називають алгоритм автоматичного розпізнавання образів на зображенні. Дрон, оснащений такою технологією, запам'ятовує картинку – обриси цілі і орієнтується на неї. Він утримує образ цілі для самонаведення, а також може відслідковувати її в русі.

У більш складних системах машинний зір з допомогою елементів штучного інтелекту може знаходити і розпізнавати об'єкти без участі людини. В умовах війни при дії РЕБ на дрони машинний зір вирішує головну проблему умовних "останніх 100 метрів" до цілі, точніше - термінальної ділянки. Оператор з машинним зором просто підводить дрон до цілі з вільного від перешкод напрямку, виділяє її, натискає "знищити", а далі FPV-дрон все робить самостійно, використовуючи наступну схему керування, яка включає в себе: GPS-модуль — для глобального позиціонування; гіроскоп/IMU — для стабілізації та орієнтації дрона; VIO (Visual-Inertial Odometry) — для точної локалізації в просторі; відстеження траєкторії — для аналізу та корекції маршруту (рис.1).

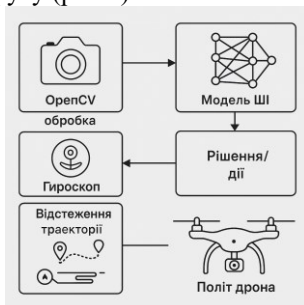


Рисунок 1 – Структурна схема машинного зору для дрона

Апаратне забезпечення включає в себе: основну плату NVIDIA Jetson Nano / Xavier NX, камеру RealSense D435 / Raspberry Pi HQ / ZED mini, GPS-модуль u-blox NEO-M8N, IMU / гіроскоп MPU6050 / BNO055, VIO сенсори Intel T265 / ZED2 / комбіновані камери + IMU. Додатково знадобиться ESC + мотори, живлення (LiPo), рама, модуль Wi-Fi.

Програмне забезпечення включає операційну систему Ubuntu 20.04 + ROS Noetic / ROS 2, машинний зір OpenCV, TensorFlow / PyTorch, YOLOv8, VIO ORB-SLAM2 / VINS-Fusion / RTAB-Map, відстеження траєкторії MAVROS, PX4, ROS Navigation Stack, GPS-навігацію за підтримки MAVLink, GPSD, QGroundControl, керування польотом за допомогою PX4 Autopilot або ArduPilot.

Далі виступає на передній план навчання самого машинного зору за технологіями нейромережі. Його необхідно натренувати для розпізнавання цілі у доволі складних умовах бою.

Виявляється, що розпізнавання бронетехніки, наприклад, танка чи БМП, значно простіша задача, ніж розпізнавання людини. Танк не може впасти на землю, або повністю змінити свою форму, як це може зробити людина, просто піднявши руки чи присівши. Тому навчання машинного зору розпізнаванню людини є складною задачею. На рис.2 показаний результат машинного навчання машинного зору, внаслідок якого здійснюється ідентифікація та захоплення цілі.



Рисунок 2 – Індикація захоплення та супроводження рухомої цілі внаслідок успішного машинного навчання

Наостанок слід зазначити, що реалізація машинного зору не завжди потребує значного підвищення вартості самого дрона. Зокрема, такі рішення є змога реалізувати на комплектуючих вартістю не більше 150 доларів.

Водночас, інтеграція машинного зору дозволяє одночасно вирішити дві основні проблеми ефективності FPV-дронів на полі бою: залежності від впливу РЕБ, бо дрон з машинним зором автоматично наводиться на вказану ціль, а також зліквідувати пряму залежність навченості оператора на результат атаки.

УДК 621.396.1

Бугрова Т.І.¹, Мулін О.С.²

¹ доц. НУ «Запорізька політехніка»

² студ. гр. БК-233_2 НУ «Запорізька політехніка»

ОСОБЛИВОСТІ ТУРНИКЕТНИХ АНТЕН У СКЛАДІ СИСТЕМ РЕБ

З 2022 року ворог використовує комплекс «Комета», який є великою проблемою для вітчизняних засобів РЕБ. Комплекс включає антену з контрольованою спрямованістю прийому (CRPA), навігаційний приймач сигналів глобальних навігаційних супутникових систем (GNSS) у L-діапазоні і встановлюється на ударні (Shahed-136, Герань-2), розвідувальні дрони (Орлан-10, Орлан-30, Грифон-41 для нанесення ударів по території України в зоні активних радіоперешкод від власних та українських засобів РЕБ. Стійкість комплексу до перешкод J/S надзвичайно велика і дорівнює 90 дБ, а відтак, великою є і захищеність навігаційної супутникової системи носіїв.

З 2023 року спостерігається оснащення цим комплексом не тільки безпілотників, крилатих ракет, а й відносно дешевих керованих авіаційних бомб ФАБ-3000 та модулів керування для плануючих бомб (УМПБ, УМПК), які найбільше дошкуляють Силам Оборони на лінії бойового зіткнення і цивільному населенню та інфраструктурі населених пунктів у смузі 30-90 км від лінії фронту внаслідок їх надзвичайної руйнівної дії. Тому створення засобів РЕБ для здійснення невідворотних перешкод згаданому ворожому комплексу з метою втрати ним навігаційного сигналу є актуальною задачею. В галузі антенних систем одним із можливих технічних рішень є застосування турнікетних антен (рис.1) в складі розподіленого в просторі комплексу РЕБ. Ключовим моментом їх успішного застосування є якомога більша кількість комплексів РЕБ.

На рис. 1 показано конструкцію антени «кажан» разом із її 3D і 2D діаграмами спрямованості на частоті 1,4 ГГц, отриманими в програмі симулювання антен 4nec2. З рис.1 видно, що антена добре справляється зі своєю основною задачею створення потужної перешкоди в широкому секторі просторових кутів.

Було також створено декілька варіантів інших турнікетних антен. Результат моделювання в середовищі 4nec2 одного з різновидів хрестоподібного турнікету з екраном на частоті 1,4 ГГц зображено на рис.2. Антена споряджена металевим екраном на відстані у чверть довжини хвилі від турнікету для забезпечення перевипромінювання потужності у бік цілі. Розглядалися екрани двох форм -квадратної та округлої. На рис. 2 наведено порівняння діаграм спрямованості у вертикальному перерізі антен з квадратним (червона крива) та округлим (синя крива) екранами. Очевидно, що квадратний екран ефективніше відбиває випромінювання в бік цілі.

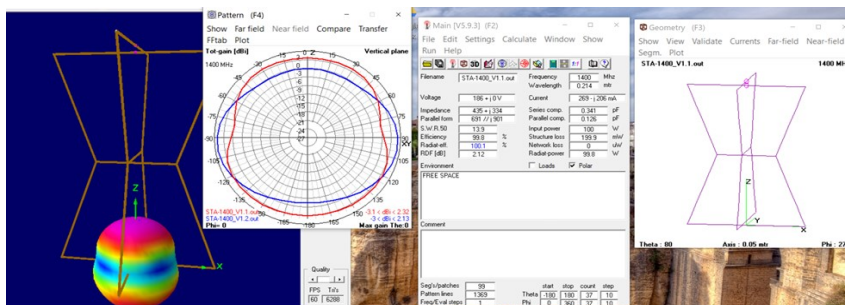


Рисунок 1 – 3D модель турнікетної антени «кажан» з її діаграмою спрямованості

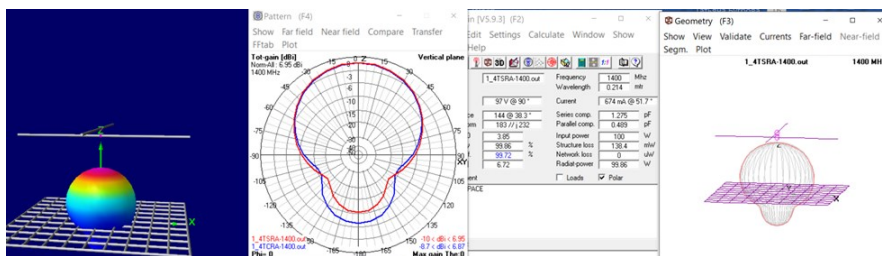


Рисунок 2 – 3D модель хрестоподібної турнікетної антени та її діаграма спрямованості з квадратним (червона крива) та округлим (синя крива) екранами

Таким чином, встановлено, що турнікет з квадратним екраном має більшу ефективність спрямованого випромінювання у вигляді 6,95 dBi підсилення, тоді як підсилення турнікету з круглим екраном дорівнює 6,87 dBi, а у антени типу «кажан» цей показник не підіймається вище 2,32 dBi.

Водночас, надзвичайно велику роль в будь-яких антенах відіграє ступінь узгодження їх із системою живлення. У випадку турнікетів до задачі їх імплансного узгодження додається ще проблема взаємного фазування елементів турнікету. Справа в тім, що, по-перше, лінія живлення є несиметричним типом нап'ямної системи, а кожен з ортогональних один до одного у просторі випромінюючих елементів потребує симетричного живлення. По-друге, для створення поля випромінювання колової поляризації між першим і другим вібраторами треба забезпечити фазовий зсув між джерелами живлення у 90° .

УДК 621.396.1

Бугрова Т.І.¹, Мулін О.С.², Проваторов С.М.³

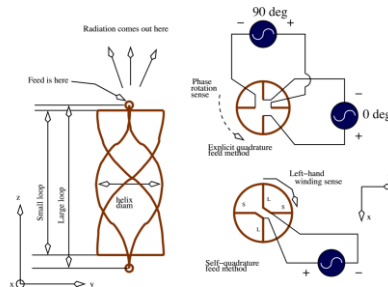
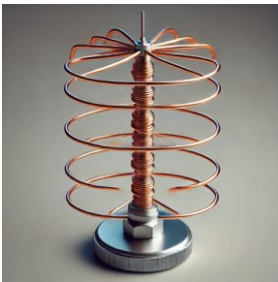
¹ доц. НУ «Запорізька політехніка»

² студ. гр. БК-233_2 НУ «Запорізька політехніка»

³ студ. гр. БК-211 НУ «Запорізька політехніка»

КВАДРИФІЛЯРНІ АНТЕНИ ДЛЯ ДЖАМЕРІВ

Квадрифілярна антена — це спеціальний вид антен, які відрізняються від звичайних спіралей чотирма спіралью закрученими провідниками. Завдяки цій структурі вони забезпечують більш стабільний сигнал в режимі передавання і покращену якість прийому в умовах перешкод (рис.1,а) і двома типами живлення- верхнім і нижнім (рис.1,б). Вони застосовуються, зокрема, в блоках джамерів. Джамер, або jammer, — це електронний компонент, який є основним елементом для створення радіоперешкод. Він працює за принципом перетворення електричної енергії джерел живлення на електромагнітні хвилі, які блокують або порушують роботу систем зв'язку та навігації. Цей компонент подає сигнал через підсилювач, а потім передає його на антену, яка випромінює завади у повітря. Завдяки своїй компактності, джамери часто використовують як частину більш складних систем, таких, як постановники завад.



а

б

Рисунок 1 – Квадрифілярна антена для дрона (а) та два способи її живлення – зверху і знизу (б)

У виробництві систем РЕБ джамери є невід'ємною складовою. Вони встановлюються у стаціонарних та мобільних платформах для створення перешкод у широкому діапазоні частот. Завдяки використанню підсилювачів та адаптивних технологій, джамери можуть налаштовуватись під різні сценарії: від блокування радіозв'язку до придушення GPS-сигналів. Наприклад, у військових автомобілях застосовують модулі завад з кількома джамерами, що працюють одночасно для придушення різних типів сигналів. Це забезпечує гнучкість та ефективність у різних бойових умовах. Складові, такі як генератори білого шуму та високочастотні джерела перешкод, значно розширюють функціонал цих систем. В складі джамерів для дронів використовуються в основному такі типи антен, як всеспрямовані штирєві, конюшина, турнікети і квадрифілярні.

На рис.2 показано результати моделювання квадрифілярної спіральної антени колової поляризації в системі симулювання 4nec2 в околиці частоти 1,575 ГГц. Розраховано параметри узгодження антени з лінією живлення 50 Ом (коефіцієнт стоячої хвилі SWR - синя крива і модуль коефіцієнта відбиття Refl. Coef – червона крива) в діапазоні частот 1400...1700 МГц. Як видно з рис.2, квадрифілярна антена має спрямовану догори грибокподібну діаграму спрямованості і гарно узгоджена з лінією живлення, що підтверджують відповідні значення $SWR=1,42$ і $Refl. Coef=-15,13$ дБ, коефіцієнт підсилення 4,26 dBi на частоті 1560 МГц.

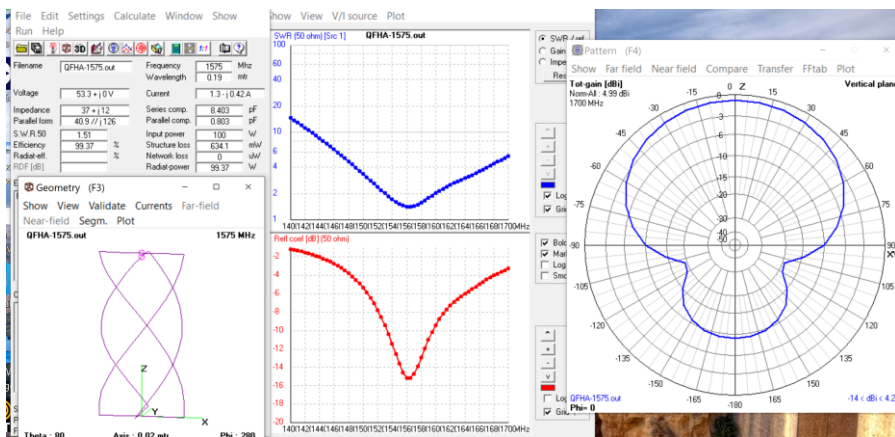


Рисунок 2 – Моделювання квадрифілярної антени в середовищі 4пес2

Наостанок слід зазначити, що квадрифілярні антени є конструктивно нескладним, стійким до механічних пошкоджень при намотуванні на прочному діелектричному каркасі та легкими за вагою випромінювачами. Перевагами цих антен є точна спрямованість завади: квадрифілярна антена створює в просторі над собою сфокусований купол, що ефективно глушить сигнали у вибраному радіусі дальності, який визначається двома факторами: шириною діаграми спрямованості самої антени і потужності передавача, забезпечуючи при цьому високу ефективність; підвищена стійкість до спрямованих атак, тому що через форму діаграми спрямованості така антена може забезпечити кращий захист від дронів, які намагаються пробити заваду з визначеного напрямку; завдяки своїй конструкції квадрифілярні антени зазвичай є більш надійними і стійкими до механічних пошкоджень ніж антени конюшина, проте, є менш надійними, ніж штирьові антени.

УДК 621.791.5

Костенко В.О.¹, Фокін Д.О.²

¹ доц. НУ «Запорізька політехніка»

² студ. гр. БК-914 НУ «Запорізька політехніка»

МІКРОПРОЦЕСОРНА ТЕХНІКА У МОДЕРНІЗАЦІЇ ПЕКАРНОГО ОБЛАДНАННЯ

З відомих причин у багатьох пекарних організаціях використовують зараз застаріле пекарне обладнання фірми «Росс» (м. Харків), яке було виготовлено на початку нульових років. Головним елементом лінійки обладнання є жарочна шафа. В робочій камері цієї шафи проходить випічка при температурі 180-210°C. Для забезпечення необхідного рівня вологості в робочій камері використовувалось додаткове обладнання: парогенератор з окремим каналом електроживлення і керуванням нагрівом. Як правило, ці парогенератори довго не живуть і зараз не працюють, через що виникають певні труднощі.

Авторами запропоновано зовсім відмовитись від використання парогенератора і здійснити керування вологістю в робочій камері за допомогою мікропроцесорної техніки. При цьому треба врахувати, що вимірювання рівня вологості повітря при температурі 200°C за «розумні» гроші не можливо. Тому і організувати кільце зворотного зв'язку для автоматичного керування вологістю не вдається.

Ідея пропозиції полягає в тому, щоб використати накопичений досвід пекарів під час виготовлення різних пекарних виробів, а пар одержувати з крапель води прямо в камері, якщо воду подавати дозовано. При температурі 200°C краплі води миттєво стануть паром, а на поверхні виробів формується тверда корка, яка закріплює об'єм виробу і перешкоджає його росту або зменшенню. Оператору ж пекарної лінії треба дати інструкцію у друкованому вигляді, де будуть вказані номери режимів для різних виробів.

Для здійснення вибраного алгоритму роботи було обрано мікроконтролер Arduino Uno (рис.1), бо він найбільш підходить за своїми габаритами, можливостями, ціною і простотою в реалізації проекту. На рис.2а показано виконавчий елемент системи – електричний водяний клапан, який дозує кількість крапель води у часі. Він відкривається і зачиняється по команді мікропроцесора згідно відповідної програми. Бак з водою поставлено вище клапана, вода подається самопливом. Для узгодження мікропроцесора з електроклапаном використовується стандартний одноканальний реле-модуль (рис.2б).



Рисунок 1 - Arduino Uno



а)

б)

Рисунок 2- Компоненти системи керування а) електричний водяний клапан, б) одноканальний реле-модуль

Розробка програми для мікроконтролера проводилась в середовищі ArduinoIDE.

Проект знаходиться в стадії випробування. Поки не вирішена проблема вибору матеріалу та конструкції трубопроводу подачі води в робочу камеру. По трубочці, якщо вона цільна і металева, виникає канал передачі високої температури. Вода перетворюється в пар раніше попадання в камеру, система «кашляє». Тобто трубопровід на ділянці від клапана до камери повинен мати температурний розрив або ізоляцію.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. <https://doc.arduino.ua/ru/hardware/Uno>
2. <https://easyeda.com/ru>
3. https://biblprog.org.ua/ru/arduino_ide/
4. <https://arduino-master.ru/platy-arduino/arduino-lcd-keypad-shield/>

УДК 621.37

Логачова Л.М¹, Овчинніков В.В²

¹старш. викл. НУ «Запорізька політехніка»

²студ. гр. БК-212сп НУ «Запорізька політехніка»

ЗАСТОСУВАННЯ МЕТАМАТЕРІАЛІВ У ТЕХНІЦІ НАДВИСОКИХ ЧАСТОТ

На даному етапі розвитку сучасної техніки надвисоких частот, систем зв'язку і телекомунікацій, антенної техніки та радіолокації широке застосування знайшли частотно-селективні (частотно-вибіркові) пристрої, що являють собою, переважно, фільтрувальні структури різного типу, які застосовують у широкому мікрохвильовому діапазоні. Як правило, такі мікрохвильові фільтрувальні елементи, вузли та модулі виконуються на основі ліній передачі з розподіленими параметрами: коаксіальних лініях, хвильоводах, мікросмугових лініях та ін., а також у вигляді комбінованих і гібридних пристроїв з розподіленими і зосередженими елементами.

Серед них можна виділити лінії передавання зі спеціальною періодичною структурою поверхні складної форми, що володіють частотно-

селективними властивостями, які в мікрохвильовій техніці часто використовуються як сповільнювальні системи (СС), частотні НВЧ-фільтри і фільтри гармонік.

У сучасній техніці надвисоких частот поліпшення параметрів частотно-селективних пристроїв можна отримати, якщо використовувати в таких конструкціях відносно нові періодичні структури на основі метаматеріалів.

Під метаматеріалами розуміється не природні, а штучно створені макроскопічні композитні середовища, що складаються з періодично розподілених у просторі простих комірок (можливі комірки різної форми).

Існує безліч форм елементів частотно-селективних поверхонь - FSS (Frequency Selective Surfaces).

Рисунок 1 ілюструє деякі з їх найпоширеніших форм, включаючи квадратний патч (а), диполь (б), круглий патч (в), перехресний диполь (г), ерусалимський хрест (д), квадратну петлю і кільце (е), (кругову петлю (ж), квадратну апертуру (з), які під час збудження виявляють властивості, які не зустрічаються в природних матеріалах. Залежно від їхньої конструкції метаматеріали можуть мати одночасно негативні значення як діелектричної, так і магнітної проникностей, що призводить до негативного коефіцієнта заломлення такого середовища.

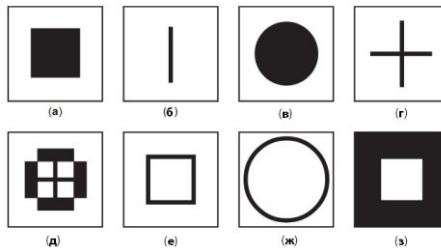
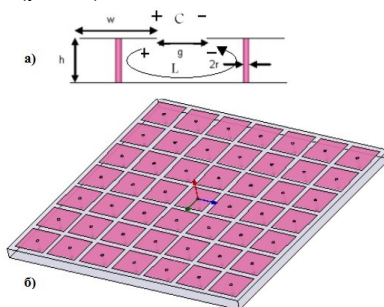


Рисунок 1 - Деякі типові форми елементів FSS

Однією з перших і найбільш відомих частотно-селективних поверхонь є грибоподібна структура (рис. 2).



а) параметри елементарної комірки б) 3D-вигляд
Рисунок 2 - Загальний вигляд грибоподібної структури

Періодична грибоподібна структура складалася з маленьких квадратних металевих осередків з довжиною $w < \lambda$, (де λ - довжина хвилі, що поширюється), сполучених із металевою основою за допомогою вертикальних циліндричних стрижнів - "ніжок", які мають радіус $2r < \lambda$, ширина зазору g , товщина підкладки h , (рис. 2). Залежно від геометрії частотно-селективні поверхні (ЧСП) можуть бути двошаровими або тришаровими. Електромагнітні властивості таких структур можна описати, використовуючи еквівалентну схему з двох елементів - ємності та індуктивності (рис. 2, а).

Способи формування ЧСП можуть бути різними і залежать від розмірів структури і від обраної частоти. Спектральна поведінка ЧСП повністю визначається геометрією поверхні на одиничній комірці при виконанні умови $L \ll \lambda$, де L - період комірки, λ - довжина хвилі, що поширюється. За такої умови кількість комірок на відстані однієї довжини хвилі досить велика, що дає змогу представити таку структуру у вигляді поверхні рівного імпедансу $Z_s(\omega)$. Комбінуючи індуктивні та ємнісні елементи, можна створювати поверхні з різним видом і величиною реактивності та внаслідок цього отримувати різний поверхневий імпеданс, який визначається формулою:

$$Z_s = \frac{j\omega L}{1 - 4\omega^2 LC} \text{УДК 621.396.969}$$

УДК 621.396.969

Гладун К.В.¹, Самойлик С.С.²

¹ асп. НУ «Запорізька політехніка»

² доц. НУ «Запорізька політехніка»

ВИМІРЮВАННЯ ВИСОТИ ЦІЛІ МЕТОДОМ MATRIX PENCIL

Вимірювання висоти цілей у радіолокаційних системах є ключовою задачею для моніторингу повітряного простору, особливо в умовах низької видимості або складного рельєфу. Одним із сучасних методів, що демонструє високу точність у таких задачах, є метод "Matrix Pencil". Цей метод дозволяє вирішувати задачі оцінки параметрів сигналів шляхом обробки багатопроміневих відбиттів і розділення сигналів у частотному домені.

Метод базується на використанні сингулярного розкладу матриць, які формуються з даних сигналу, отриманих за допомогою антенних решіток. Основні етапи робіт при застосуванні методу:

1) Формування матриці даних. Сигнали, що надходять, організовуються у вигляді спеціальних матриць.

2) Розкладання. Метод використовує сингулярне розкладання для виділення незалежних компонент сигналів.

3) Оцінка параметрів. Виділені компоненти аналізуються для визначення висоти цілі шляхом оцінки кута нахилу сигналу.

Перевагою методу "Matrix Pencil" є висока точність вимірювання, а саме, метод ефективно працює в умовах низьких кутів огляду, де багатопроміневі відображення значно впливають на сигнал.

Порівняно з алгоритмами, такими як MUSIC або ESPRIT, метод "Matrix Pencil" забезпечує швидшу обробку, за рахунок малої обчислювальної складності [1].

Також метод "Matrix Pencil" має високу адаптивність, що робить його придатним для використання у складних умовах, таких як нерівномірний рельєф або густий радіохвильовий шум.

Ще однією перевагою метода "Matrix Pencil" є знижена чутливість до перешкод, створених тепловими шумами [2].

Метод "Matrix Pencil" використовується у метрових і дециметрових радіолокаційних системах для визначення низько летючих цілей, які можуть бути приховані через багатопроміневі відбиття; оцінки висоти об'єктів у складних топографічних умовах; підвищення точності в системах з малою шириною променя.

Приклади реалізації методу є роботи [3]-[4]. У роботі [3] досліджується застосування методу для вимірювання висоти за складних умов. Метод використовує комбіновані алгоритми "Matrix Pencil" і MUSIC, які демонструють підвищену точність та зменшення обчислювальної складності. У роботі [4] автори пропонують ефективний алгоритм для оцінки низьких кутів місця в умовах багатопроміневої для МІМО-радарів. Метод базується на методі

"Matrix Pencil" і має на меті подолання проблем, пов'язаних із відбиттями сигналів від поверхні, що можуть призводити до помилок в оцінці кута.

Таким чином метод "Matrix Pencil" є перспективним інструментом для вимірювання висоти цілей у складних умовах. Завдяки точності, низькій обчислювальній складності та адаптивності він широко застосовується в сучасних радіолокаційних системах. Подальші дослідження можуть бути спрямовані на інтеграцію цього методу з технологіями штучного інтелекту для автоматизації процесів обробки сигналів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Pedenko Yu. A. Use of matrix pencil method for radar measurement of elevation angle of low-altitude targets over disturbed sea surface // Radioelectronics and Informatics. 2018. Vol. 23, No. 1. P. 10–18. DOI: 10.15407/rej2018.01.010.

2. Sarkar T. K., Pereira O. Using the matrix pencil method to estimate the parameters of a sum of complex exponential. IEEE Antennas Propag. Mag. 1995. Vol. 37, N 1. P. 48–55.

3. Song, Y., Zheng, G. Height measurement for meter wave polarimetric MIMO radar with electrically long dipole under complex terrain. Remote Sensing, 2023, 15(5), p.1265. DOI:10.3390/rs15051265.

4. Xi E Rong, Liu Zheng, Liu Jun. Fast algorithm for low elevation estimation based on matrix pencil in MIMO radar[J]. Journal of Electronics & Information Technology, 2011, 33(8): 1833–1838. DOI: 10.3724/SP.J.1146.2010.01242.

УДК 654.9

Калиніченко Д.В.¹, Мороз Г.В.²

¹ асп., ст. лаборант центру індустрії 4.0 НУ «Запорізька політехніка»

² старш. викл. НУ «Запорізька політехніка»

ПІДВИЩЕННЯ ДАЛЬНОСТІ ДІЇ КОМЕРЦІЙНИХ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ (БПЛА)

Наразі існує великий попит на безпілотні літальні апарати (БПЛА) у Збройних силах України через можливість їх використання для дистанційної розвідки і моніторингу місцевості, а також для ураження сил супротивника. Попри наявність БПЛА спеціального призначення, виготовлених для військових потреб, все ще існує попит на комерційні БПЛА, що компенсують нестачу спеціальних БПЛА. Однак, основним недоліком комерційних БПЛА є відносно низька дальність дії, яка продиктовується необхідністю виконувати регуляції з використання радіоефіру комерційними пристроями у вільному продажі.

Перш за все, регуляції з використання радіоефіру обмежують максимальну вихідну потужність радіосигналу, яку може генерувати пристрій, що продається у вільному доступі. Приймаючи, що середовище поширення радіохвиль немає втрат, потужність радіосигналу на вході приймача описується залежністю

$$P_{rec} = \frac{P_{tr} G_{tr} G_{rec} \lambda^2}{(2\pi R)^2}, \quad (1)$$

де P_{rec} – потужність на вході приймача, P_{tr} – потужність на виході передавача, G_{tr} і G_{rec} – коефіцієнти підсилення передавальної і приймальної антени

відповідно, λ – довжина хвилі радіохвилі, R – відстань між передавачем і приймачем. Вищезазначена залежність показує, що для збільшення дальності БПЛА треба збільшувати потужність вихідного радіосигналу та/або знижувати поріг чутливості вхідного сигналу.

На даний момент, вже є доступні рішення з модифікації пультів керування БПЛА задля збільшення їх вихідної потужності за межі регуляцій, які нехтуються в бойових умовах. Проте, все ще мало практичних рішень зі збільшення якості радіосигналу з боку БПЛА через необхідність у малих габаритах, незмінності антенної системи БПЛА і обмеженість у споживаній потужності для додаткових ланцюгів підсилення радіосигналів.

Завдяки наявній у продажі елементній базі існує можливість спроектувати малогабаритний підсилювач радіосигналу для встановлення на борту БПЛА на базі інтегральних радіочастотних підсилювачів. Однак, у БПЛА, як і у пульті керування до нього, для передачі та прийому сигналів використовують одий і той самий радіотракт (лінія передачі з антеною). Через це існує необхідність у розробці простого у виконанні методу розрізнення проміжків часу, коли наявний у БПЛА/пульті радіотракт використовується для прийому, а коли – для передачі сигналів. Найпростішим способом є використання направленої відгалуджувача у парі з детектором для виміру потужності радіохвиль, направлених у сторону антени (тобто, на передачу). Тоді, встановлюючи поріг за потужністю передавального сигналу у радіотракті у -5дБм, досягається необхідне переключення «прийм/передача».

Враховуючи вищезазначені рішення, був спроектований та виготовлений підсилювач радіосигналів БПЛА, що працює у смугах частот 2400..2500МГц та 4900..5900МГц (рис.1). Даний прилад має малі габарити (40х24х2мм) і завдяки цьому може бути встановлений усередині корпусу БПЛА.

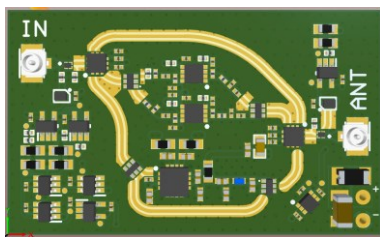


Рисунок 1 – Спроектована плата підсилювача радіосигналів для БПЛА.

Даний прилад підсилює радіосигнали як на прийом, так і на передачу. Результати вимірів (рис.2) показують підсилення вихідних сигналів до потужностей 1.3-1.5 Вт (у порівнянні з початковими 200-300 мВт).

Споживана потужність – менше 3 Вт, що незначним чином впливає на час польоту БПЛА.

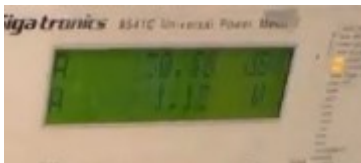


Рисунок 2 – Виміри вихідної потужності радіосигналу БПЛА, додатково оснащеного спроектованим підсилювачем

УДК 621.395

Плетінь Д.Ю.¹, Мороз Г.В.²

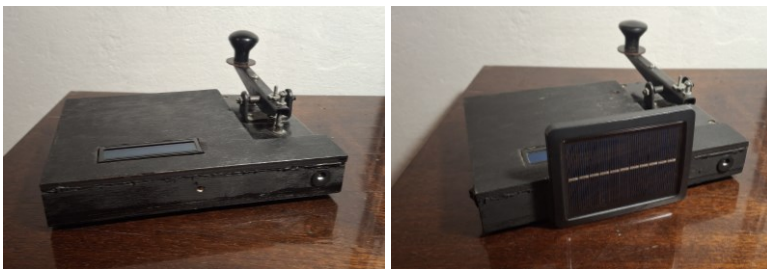
¹ студ. гр. БК-913 НУ «Запорізька політехніка»

² старш. викл. НУ «Запорізька політехніка»

ПЕРЕДАЧА ІНФОРМАЦІЇ ЗА ДОПОМОГОЮ ЛАЗЕРНИХ ТЕХНОЛОГІЙ

Метою роботи є дослідити принципи передачі інформації за допомогою лазерних технологій та продемонструвати їх практичну реалізацію через створення експериментальної моделі лазерного зв'язку. Лазери сьогодні є незамінною технологією, що широко застосовуються в численних сферах. У медицині вони використовуються для хірургічних операцій, офтальмологічних процедурах і дерматологічного видалення шрамів, татуювань чи родимок, у промисловості застосовуються для різання, зварювання матеріалів і 3D-друку металів, а в побуті та професійній діяльності відомі завдяки лазерним принтерам, комп'ютерним мишкам, DVD-дискам та вимірюванню відстаней і створенню 3D-карт у геодезії. Однією з найважливіших сфер їхнього використання є телекомунікації, де лазери використовують для передачі інформації на великих відстанях та магістральних оптичних лініях передачі інформації [1].

У рамках роботи було створено експериментальну модель лазерного зв'язку за принципом роботи азбуки Морзе, яка демонструє принципи лазерної передачі інформації (рис.1).



а – передавач світлового сигналу; б – приймач світлового сигналу.

Рисунок 1 – Оптична модель азбуки Морзе.

Принцип даної моделі базується на передавачі сигналу в корпусі якого вбудований лазерний діод, який активується натисканням телеграфічного ключа, та приймача, котрий оснащений сонячною панеллю, задача якої приймати сигнал від передавача.

Керуючим елементом даної роботи виступає плата Arduino Nano на базі мікроконтролера ATmega328 [3]. У процесі роботи для передавача Arduino Nano було програмовано на керування лазерним діодом за допомогою телеграфічного ключа. Приймальна сторона, також на базі Arduino Nano, була запрограмована для прийому сигналу від лазерного діода через сонячну панель із подальшим декодуванням у текст азбуки Морзе на LCD-дисплеї шляхом ООК-модуляції [2].

Завдяки ООК-модуляції лазерний діод генерує послідовність коротких та довгих імпульсів, що відповідають крапкам та тире азбуки Морзе. Сонячна панель перетворює світлові імпульси в електричні сигнали, які Arduino Nano зчитує та відображає готовий текст на LCD-дисплеї, що свідчить про успішну передачу інформації.

Слід зазначити що сонячна панель є досить чутливою до зовнішнього освітлення, тому було вирішено вбудувати до корпусу приймальної сторони потенціометр, котрий врегульовує поріг при якому для модуляції сигналу буде враховуватися лише сигнал від лазерного діода, для перевірки було використано монітор порту у Arduino IDE (рис.2), де «Значення світла» це значення котре зчитує сонячна панель, «Поріг» це значення яке змінюється потенціометром при якому статус буде змінюватися на негативний «0» якщо значення світла не більше порогового чи позитивний «1» якщо значення світла більше порогового.

Значення світла: 226	Поріг: 380	Статус: 0
Значення світла: 169	Поріг: 380	Статус: 0
Значення світла: 159	Поріг: 380	Статус: 0
Значення світла: 162	Поріг: 380	Статус: 0
Значення світла: 387	Поріг: 380	Статус: 1
Значення світла: 390	Поріг: 380	Статус: 1
Значення світла: 421	Поріг: 380	Статус: 1
Значення світла: 405	Поріг: 380	Статус: 1

Рисунок 2 – Значення зняті з послідовного монітору порту Arduino IDE.

У результаті роботи було досліджено принцип передачі інформації за допомогою лазерних технологій та успішно реалізовано експериментальну модель лазерного зв'язку на базі азбуки Морзе та мікроконтролеру Arduino Nano.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Saleh B. E. A. Fundamentals of Photonics / B. E. A. Saleh, M. C
2. H. Elgala et al.: Indoor Broadcasting via White LEDs and OFDM
3. Banzi M. Getting Started with Arduino / M. Banzi, M. Shiloh.

УДК 621.395

Плетінь Д.Ю.¹, Мороз Г.В.²

¹ студ. гр. БК-913 НУ «Запорізька політехніка»

² старш. викл. НУ «Запорізька політехніка»

МЕТОД ВІДНОВЛЕННЯ СТІЛЬНИКОВОГО ЗВ'ЯЗКУ ПОЛОГІВСЬКОГО РАЙОНУ

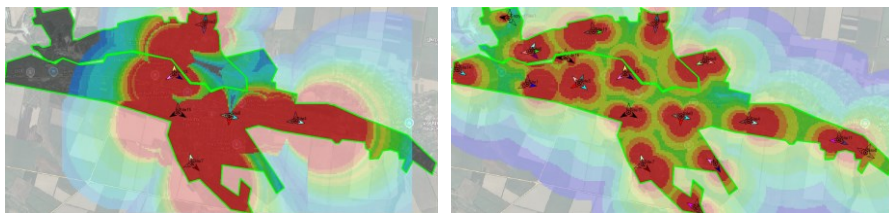
В умовах сучасного світу мобільний зв'язок є важливим компонентом інфраструктури, що забезпечує безперервність комунікацій, розвиток економіки та суспільства, особливо в регіонах із пошкодженнями в наслідок бойових дій, таких як Пологівський район. Метою роботи є аналіз міста та села Пологи для розробки плану розташування базових станцій оператора Vodafone.

Відновлення мережі базується на комплексному підході з використанням програмного забезпечення «Atoll» [2] для моделювання оптимального розміщення базових станцій. Аналіз враховував густоту населення, рельєф місцевості, міську та сільську інфраструктуру, а також джерела перешкод. Для дослідження проекту застосовано обладнання Huawei: базові станції встановлено на окремих вежах і щоглах та дахах будівель, що забезпечило рівномірне покриття у відкритих і густонаселених

зонах. Було використано Антени ADU4518R10v06 які підтримують кілька частот одночасно та частотні діапазони 900 МГц, 1800 МГц, 2100 і 2600 МГц [1].

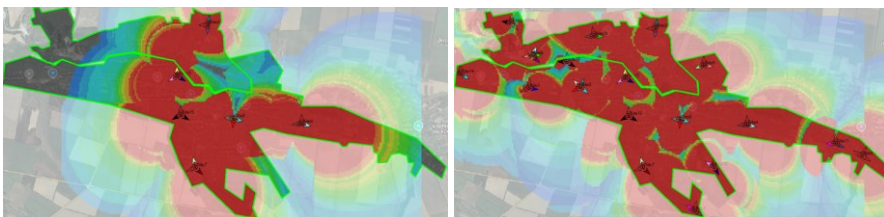
Місто та село Пологи, площа якого сумарно становить 22,98 км², є компактним населеним пунктом із населенням 21 215 осіб. Середня густина населення становить близько 922 осіб на км², що відображає помірну концентрацію жителів у межах міської території. Така густина населення створює попит на якісний мобільний зв'язок, особливо в центральній частині міста та густозаселених районах.

Для роботи із частотами 900 та 1800МГц [3] обрали підсилювач RRU5909, що забезпечували стабільний зв'язок на великих відстанях, а діапазони 2100 і 2600 МГц разом із підсилювачами RRU5517t і RRU5502 підвищили пропускну здатність у густонаселених районах населення. Ефективність даного підходу для покриття та пропускну здатності ілюструє рис.1 та рис.2.



а – покриття до модернізації; б – покриття після модернізації.

Рисунок 1 – Модель покриття для Пологівського району.



а – пропускну здатність до модернізації; б – та після модернізації.

Рисунок 1 – Модель покриття для Пологівського району.

Проведений аналіз щільності забудови, рельєфу та розподілу населення дозволив оптимально розташувати базові станції, забезпечуючи повне

покриття всієї території [4]. Це рішення враховує потреби як центральних районів із високою інтенсивністю зв'язку, так і менш населених зон, де раніше могли спостерігатися проблеми зі зв'язком. Особливу увагу приділено забезпеченню зв'язку в місцях із підвищеним навантаженням, таких як громадські центри, транспортні вузли та житлові масиви. Такий підхід дозволив не лише відновити роботу мережі після збоїв, а й значно покращити її ефективність, надійність і відповідність сучасним стандартам.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Stallings, W. (n.d.). Wireless Communications and Networks.
2. Forsk. (n.d.). Atoll LTE Network Planning and Optimization: Documentation and Materials.
3. Lee, W. C. Y. (n.d.). Mobile Radio Networks: Configurations, Analysis, and Design.
4. Mohammed, E. M., & El-Dosuky, M. M. E. (n.d.). Mobile Network Design and Optimization.

УДК 004.738.5:621.391

Сумарюк С.Г.¹, Чорнобородов М.П.², Мороз Г.В.³

¹ асп. НУ «Запорізька політехніка»

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

³ старш. викл. НУ «Запорізька політехніка»

АЛГОРИТМ РОЗТАШОВУВАННЯ ЕЛЕМЕНТІВ АУДИОМЕРЕЖІ НА МІСЦЕВОСТІ З УРАХУВАННЯМ «НЕДОСТУПНИХ ЗОН»

Моніторинг звукових хвиль має широке використання у різних сферах сучасності [1]. Від моніторингу звуків пострілів в міській забудові для швидшого реагування на правопорушення, використання сенсорів звуку для визначення місцезнаходження бракон'єрів в заказниках та природоохоронних зонах, до визначення місця вибуху міни під час робіт з повоєнного розмінування. Розвиток індустрії персональних літаючих дронів компактних розмірів призводить до появи технічних рішень щодо звукового виявлення подібних виробів для запобігання несанкціонованому використанню або збереженню життів цивільних та військових осіб у разі використання військових дронів.

Просторова локалізація звукових хвиль є нетривіальною задачею яка потребує врахування багатьох параметрів для успішного відпрацювання. Одними з основних чинників, що впливають на поширення звуку на місцевості є просторові характеристики фізичних перешкод [2] (розмір, щільність, положення на місцевості), а також такі особливості місцевості як перепад висот та наявність зон, вкритих водою. Звичайно, для розташовування сенсо-

рів використовують жадібний алгоритм (Greedy algorithm) [3], який засновано на розміщенні множини точок C на площині S , дотримуючись умови, що 2-3 попередніх сенсори мають зони перекриття, визначені радіусом R_{pic} у зоні чутливості кожного нового сенсору. Загальна формула вибору множини точок на площині S виглядає наступним чином:

$$C_i = \text{argp} \in P_{\max}(A_{cov}(C \cup \{p\}) - A_{cov}(C)), \quad (1)$$

де C_i – нове місце розташування сенсору, $\text{argp} \in P_{\max}$ – точка, що лежить у межах потенційних точок, що найсуттєвіше ($P_{\max}$) збільшують площу загального покриття заданої площини S , $A_{cov}(C \cup \{p\})$ – площа площини S після додавання нового сенсору в точці-кандидаті, $A_{cov}(C)$ – площа покриття попереднього етапу.

Кожний вибір точки виходить з набору кандидатів, що обираються за наступним критерієм:

$$P = \bigcup_{c \in C} \{p \mid d(c, p) = R_{pic}, p \in S\}, \quad (2)$$

де C — множина вже розміщених сенсорів, p — потенційна точка для нового сенсора, $d(c, p)$ — відстань між сенсором c та точкою p , R_{pic} – максимальний радіус від попереднього сенсору, в якому дозволено розміщення нового сенсору, S — площа, в межах якої можна розміщувати сенсори.

Точки на відстані R обираються по дискретних кутових напрямках:

$$P = \bigcup_{c \in C} \{(x, y) \mid x = c_x + R_{pic} \cos(\theta), y = c_y + R_{pic} \sin(\theta), \theta \in \Theta\}, \quad (3)$$

де c_x та c_y - координати вже розміщеного сенсора c , Θ - множина дискретних кутів. Це відповідає генерації точок навколо кожного сенсора з певним кутовим кроком.

Для досягнення більш оптимального розміщення аудіосенсорів на місцевості, необхідно врахувати поняття «недоступних зон», які обмежують точки розміщення сенсорів, а також диктують поправки на розміщення сенсорів навколо них. Це в свою чергу дозволить оптимізувати алгоритм, потенційно зменшивши кількість сенсорів для розміщення на площині а також проведенням більш правильного їх розміщення.

Представлено алгоритм, який засновано на Жадібному алгоритмі (Greedy algorithm), який працює із заданою площиною точок розміщення сенсорів, намагаючись розмістити їх таким чином щоб покрити якомога бі-

льшу площу, при цьому мінімізуючи зони які непокриті зоною чутливості сенсорів з урахуванням «недоступних зон»:

$$P = \bigcup_{c \in C} \{p \in S \mid d(c, p) = R \wedge \forall z_i \in Z, d(p, z_i) > r_i\}, \quad (4)$$

де $Z = \{z_1, z_2, \dots, z_m\}$ - множина заборонених центрів, у якій кожна точка z_i має радіус заборони r_i .

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Rossing T. D. Springer Handbook of Acoustics. – Berlin : Springer, 2007. – 1182 с.
2. Taus L., Tsai Y.-H. R. Efficient and robust sensor placement in complex environments // arXiv preprint. – 2023. – arXiv:2309.08545. – 23 p.
3. Piña-Covarrubias E., Hill A. P., Prince P., Snaddon J. L., Rogers A., Doncaster C. P. Optimization of sensor deployment for acoustic detection and localization in terrestrial environments // Remote Sensing in Ecology and Conservation. – 2018. – Vol. 5, No. 2. – P. 180–192. – DOI: 10.1002/rse2.97.

621.396.67.012.12

Чорнобородова Н. П.¹, Чорнобородов М. П.², Комінов Є. Є.³

¹ ТОВ НВФ "Сведа, Лтд"

² доц. НУ «Запорізька політехніка»

³ асп. НУ «Запорізька політехніка»

ВИЗНАЧЕННЯ ПРИДАТНОСТІ "ПРОМИСЛОВИХ" АНТЕН ДО ЇХ ЗАСТОСУВАННЯ ПІДРОЗДІЛАМИ ЗСУ

Державний військово-промисловий комплекс (ВПК), який Україна отримала у спадок від СРСР, як був нездатним пристосовуватись до швидкоплинних змін потреб збройних сил, так і продовжує виробляти не те, що підвищить боєздатність або захищеність військовослужбовця, а винятково те, що вони звикли (з далеких 70-х р.р.) виробляти. Поява дронів докорінно змінила заходи безпеки підрозділів ЗСУ. В умовах цілковитої безпорадності ВПК в плані розробки й виготовлення антен для захисту від БПЛА, виробництвом цих антен зайнялися, здебільшого, «гаражні» ділки - люди без будь-якої освіти, без жодного розуміння сутності справи.

В гонитві за прибутками, ці "виробники" замінюють алюміній на неіржавійку, оцинковку, сталь, не завжди точно дотримуються розмірів й технології. Звісно, через це характеристики антен від "частково" до "істотно" погіршуються, але "виробники" такими речами геть не переймаються - вони просто не підозрюють про це...

Зателефонуйте до будь-якої гаражної контори й спитайте: "Яка ширина діаграми спрямованості Вашого виробу?". Це питання спочатку спантеличить продавця, але, коли він оговтається, після паузи, Ви отримаєте одну з наступних поширених відповідей: "Це - антена на таку-то частоту" або "У неї - купольна діаграма". Шедевром є заява: "Це - антена такого-то типу, тому діаграма у неї - стандартна".

Для захисту від ворожих БПЛА наземних об'єктів (автомобіль, окоп) необхідно мати антену з широкою діаграмою, спрямовану вертикально вгору. Для таких застосувань часто використовують антену Моксона (див. рис. 1).



Рисунок 1 - Антена Моксона

Виробники заявляють ширину діаграми спрямованості від 90° до "верхня півкуля". У переважній більшості випадків, "виробник" не має жодного уявлення про спосіб розрахунку такої антени. І якщо постає задача виготовлення такої антени на новий частотний діапазон, для якого такі антени ще ніхто не робив, то ділки на власний розсуд змінюють розміри антени й продають. Для прикладу, подивимось на рис. 2. Тут наведено експериментальні діаграми спрямованості антени Моксона, виготовленої на робочу частоту 1,5 ГГц.

З рис. 2 видно, що робочою частотою антени є частота 760 МГц (замість заявлених 1,5 ГГц), оскільки на ній форма діаграми спрямованості є звичайною для таких антен (див. мал. 2, а)). На рис. 2, б) .. г) можна побачити процес погіршування характеристики: за збільшування частоти опромінювання антени (приблизно на 90° азимутального кута) формується бічна пелюстка (див. мал. 2, б)), продовжує зростати (див. мал. 2, в)) і на частоті 1230 МГц (див. мал. 2, г)) вона починає перевищувати за рівнем головну пелюстку.

Нажаль, у нас немає технічної можливості здійснювати вимірювання на частотах більших, за 1230 МГц. Тому ми не можемо продемонструвати форми діаграми спрямованості цієї антени на частоті 1,5 ГГц (заявленій робочій). Але на мал. 2, г) можна побачити формування другої бічної пелюстки - приб-

лизно, на 310° азимутального кута. Немає сумнівів, що на частоті 1,5 ГГц у цієї антени буде 3 "головні" пелюстки. Це призведе до того, що лише третину потужності постановника активних завад буде випромінено за призначенням, а дві третини - просто опромінюватимуть навколишніх людей, що не є корисним для їх здоров'я.

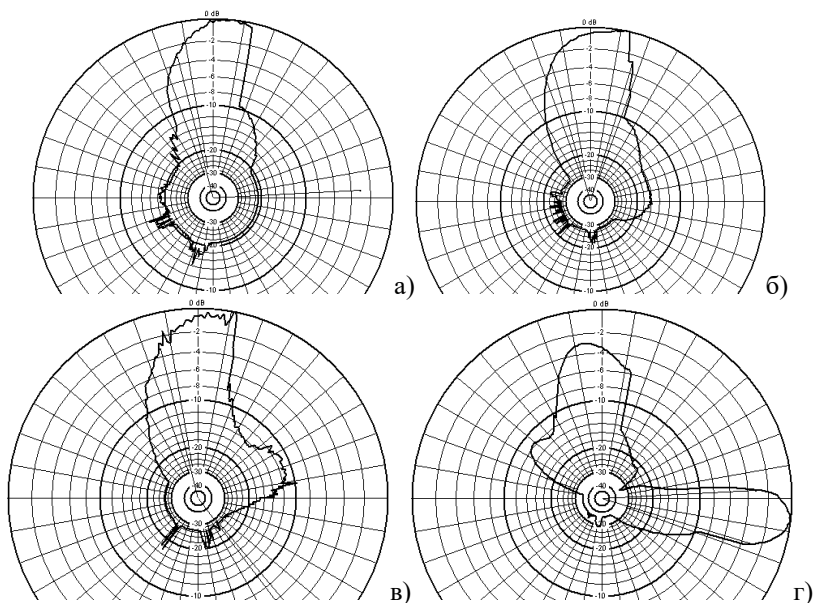


Рисунок 2 - Діаграми спрямованості антени Моксона на частотах:
а) 760 МГц, б) 870 МГц, в) 970 МГц, г) 1230 МГц.

621.375.9:621.376

Чорнобородова Н. П.¹, Чорнобородов М. П.², Маслов О. О.

¹ ТОВ НВФ "Сведа, Лтд"

² доц. НУ «Запорізька політехніка»

³ асп. НУ «Запорізька політехніка»

ВИЗНАЧЕННЯ НАПРУГИ ЖИВЛЕННЯ ПІДСИЛЮВАЧА

Для приймання слабких сигналів використовують підсилювачі з малим коефіцієнтом шуму від різних виробників. AD8317 — це демодульовальний логарифмічний підсилювач, здатний з високою точністю перетворювати

вхідний радіочастотний сигнал у діапазоні від 1 МГц до 8 ГГц. Виробник заявляє безпрецедентну стабільність логарифмічного перетворення незалежно від температури навколишнього середовища за напруги живлення від 3 В до 5,5 В (див. рис. 1 й рис. 2 [1]). Забезпечення належної температурної стабілізації досягається вибором номіналу резистора R_{TADJ} (в залежності від частоти вхідного сигналу).

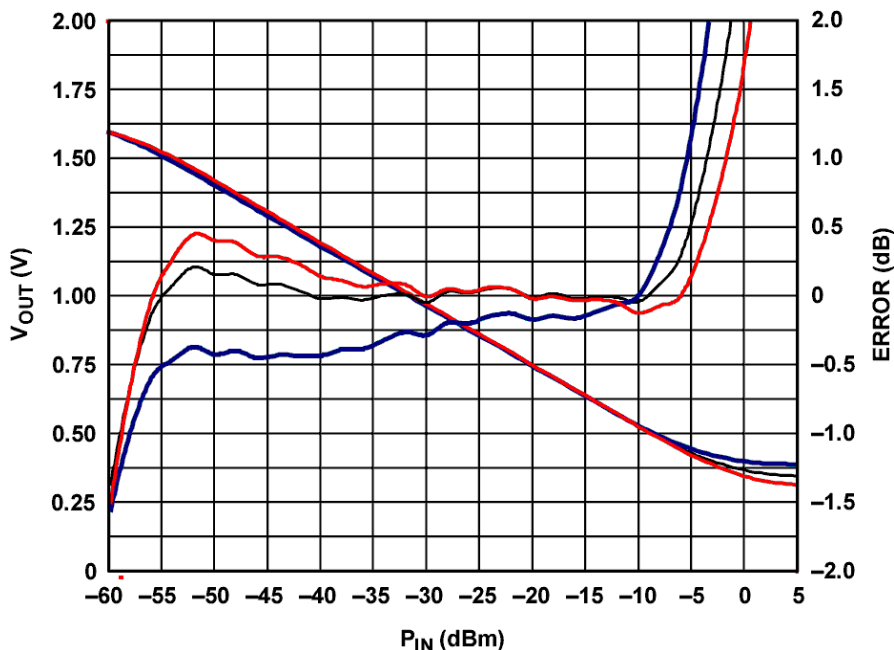


Рисунок 1 - Вихідна напруга V_{OUT} й логарифмічне перетворення в залежності від потужності P_{IN} вхідного сигналу на частоті 1,9 ГГц за $R_{TADJ}=8$ кОм

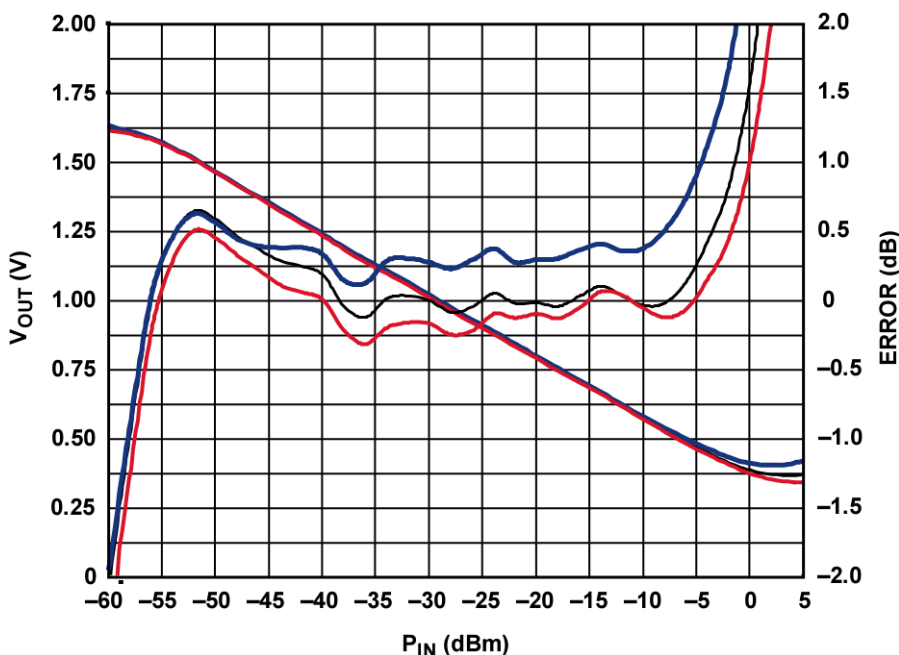


Рисунок 2 - Вихідна напруга V_{OUT} й логарифмічне перетворення в залежності від потужності P_{IN} вхідного сигналу на частоті 5,8 ГГц за $R_{TADJ}=500$ Ом

З рис. 1..2 видно, що за відсутності вхідного сигналу, напруга на виході V_{OUT} мусить бути більшою за 1,6 В. Але в ході дослідження режимів роботи мікросхеми AD8317 було виявлено, що точність логарифмічного перетворення й, відповідно, формування вихідної напруги V_{OUT} , сильно залежить від напруги живлення V_{POS} . У табл. 1 наведено залежність вихідної напруги V_{OUT} від V_{POS} . На підставі отриманих нами даних, рекомендується живити мікросхему від напруги не менше 4 В.

Таблиця 1 – Залежність вихідної напруги V_{OUT} від напруги живлення V_{POS}

V_{POS} , В	V_{OUT} , В	V_{POS} , В	V_{OUT} , В	V_{POS} , В	V_{OUT} , В	V_{POS} , В	V_{OUT} , В
<3,3	0	3,5	0,6	3,8	1,2	4,1	1,69
3,3	0,15	3,6	0,9	3,9	1,4	4,2	1,706
3,4	0,4	3,7	1,1	4,0	1,61	$\geq 4,3$	1,707

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. www.analog.com/media/en/technical-documentation/data-sheets/ad8317.pdf

УДК 004.942:629.735

Костяной П.А.¹, Фарафонов О.Ю.²

¹ асп. гр. А-172.12 НУ «Запорізька політехніка»

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

АЛГОРИТМІЧНЕ ЗАБЕЗПЕЧЕННЯ ПОПЕРЕДНЬОЇ ОБРОБКИ З БЕЗПІЛОТНИХ АПАРАТІВ ДЛЯ ПОБУДОВИ ТРИВИМІРНОЇ КАРТИ МІСЦЕВОСТІ

В останні роки безпілотні літальні апарати (БПЛА) стали незамінними інструментами для швидкого аналізу місцевості, моніторингу навколишнього середовища та реагування на надзвичайні ситуації. Одне з найбільш перспективних застосувань полягає у створенні детальних тривимірних (3D) карт природного та міського середовища. Однак необроблені дані, отримані від датчиків БПЛА, таких як LiDAR, камери RGB і багатоспектральних пристроїв, часто мають різні недоліки. До них належать шум, неточності через рух, дрейф датчика, умови освітлення та неповне покриття. Тому розробка ефективних алгоритмічних методів попередньої обробки є важливою для забезпечення точності та надійності кінцевих 3D-моделей місцевості.

Дослідження досліджували різні методи попередньої обробки для підвищення якості даних, отриманих з БПЛА. Наприклад, в [1] надані вичерпні вказівки для картографування польотів БПЛА та підкреслено важливість підготовки та виконання польоту для забезпечення високоякісного збору даних. Крім того, в [2] представлено надійний інструмент для 3D-картографії залізниць з використанням даних БПЛА, інтегруючи фотограмметрію, штучний інтелект і методи комп'ютерного зору для підвищення точності.

Незважаючи на ці досягнення, залишаються проблеми у стандартизації робочих процесів попередньої обробки, зокрема в обробці зашумлених даних, вирівнювання хмар точок з кількох траєкторій польоту та забезпечення сумісності з різним програмним забезпеченням для картографування. Пропоноване дослідження усуває ці прогалини шляхом розробки модульного конвеєра попередньої обробки, який включає синхронізацію даних, зменшення шуму, вирівнювання хмари точок і стандартизацію формату. Цей підхід спрямований на підвищення точності та надійності 3D-моделей місцевості, створених на основі даних БПЛА.

Новизна цього дослідження полягає в його комплексній та адаптивній структурі, яка не тільки покращує існуючі методи попередньої обробки, але й полегшує інтеграцію як з централізованими, так і з бортовими системами обробки БПЛА. Таким чином, він обслуговує додатки в режимі реального часу в таких сферах, як реагування на стихійні лиха, військова розвідка та сільськогосподарський моніторинг, де швидке та точне картографування місцевості має вирішальне значення.

Це дослідження зосереджено на створенні інтегрованої основи для попередньої обробки даних, зібраних БПЛА, перед створенням 3D-карт. Цей підхід включає кілька ключових етапів: синхронізацію даних, зменшення шуму, видалення викидів, вирівнювання хмари точок і стандартизацію формату. Основна увага приділяється забезпеченню сумісності з широким спектром картографічного програмного забезпечення та інструментів з відкритим кодом, таких як CloudCompare, OpenDroneMap і PDAL.

Алгоритм попередньої обробки складається з п'яти ключових етапів, розроблених для перетворення необроблених даних датчиків у чисту, дослідовну хмару точок, придатну для 3D-моделювання.

Етап 1. Збір даних і синхронізація. Необроблені дані з кількох датчиків БПЛА (LiDAR, RGB, IMU) збираються та синхронізуються за допомогою часових позначок. Параметри калібрування застосовуються для виправлення спотворень датчика.

Етап 2. Зменшення шуму та видалення викидів. Метод видалення статистичних викидів використовується для усунення зашумлених або ізольованих точок. Зменшення дискретизації воксельної сітки зменшує щільність точок, зберігаючи структурні особливості.

Етап 3. Реєстрація хмари точок. Кілька хмар точок об'єднуються за допомогою алгоритму ітеративної найближчої точки (ICP) і методів зіставлення функцій для створення єдиної моделі рельєфу.

Етап 4. Нормалізація формату та фільтрація. Дані конвертуються в стандартні формати (наприклад, LAS, PLY) і обрізаються до відповідних регіонів. Точки з низьким рівнем достовірності відфільтровуються на основі інтенсивності сигналу або помилки позиціонування.

Етап 5. Контроль якості та готовність карти. Щільність точок оцінюється для виявлення розривів покриття. Телеметрія БПЛА аналізується, щоб за потреби рекомендувати додатковий збір даних. Потім остаточна хмара точок експортується для створення цифрової моделі рельєфу (DEM) або створення сітки.

Дослідження також включає порівняльний аналіз різних каналів попередньої обробки на наборах даних, зібраних у різних типах місцевості, таких як лісисті регіони, міські зони та змішані ландшафти. Для оцінки ефективності оцінюються такі показники, як час обробки, повнота карти та

геометрична точність. Результати демонструють, що запропонований алгоритмічний конвеєр підвищує точність 3D-карти на 25% порівняно з необробленими даними, значно підвищуючи якість цифрових моделей висоти (ЦМР) і ортомозаїк.

Важливо те, що модульна структура запропонованого рішення дозволяє інтегрувати як із централізованими наземними системами обробки, так і з бортовими процесорами БПЛА, забезпечуючи додатки в реальному часі в місіях, чутливих до часу. Ця гнучкість особливо цінна під час реагування на стихійні лиха, військової розвідки та моніторингу сільського господарства, де швидке й точне розуміння місцевості має вирішальне значення.

Ця робота представляє алгоритмічну основу для попередньої обробки даних, зібраних БПЛА, закладаючи основу для високоякісного 3D-картографування місцевості. У майбутніх дослідженнях вивчатиметься інтеграція моделей машинного навчання для подальшої автоматизації виявлення аномалій і класифікації в хмарах точок. Запропонований конвеєр відкриває можливість для масштабованого та ефективного аналізу місцевості за допомогою доступних платформ БПЛА, сприяючи розвитку технологій дистанційного зондування.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Maes, W. H. (2025). Practical Guidelines for Performing UAV Mapping Flights with Snapshot Sensors. *Remote Sensing*, 17(4), 606. <https://doi.org/10.3390/rs17040606>
2. Barbero-García, I., Medina-Olivares, H., Sebastián-Pardo, I., & Crespo-Llorca, J. (2025). A new robust tool for 3D rail mapping from UAV: Photogrammetry, AI and Computer Vision integration. *Drones*, 9(3), 120. <https://doi.org/10.3390/drones9030120>

УДК 621.396

Malyi Oleksandr¹, Vychuzhanina Snizhana²

¹ PhD, assistant prof., National University «Zaporizhzhia Polytechnic»

² PhD student, National University «Zaporizhzhia Polytechnic»

DRFM TYPE DIGITAL DEVICES FOR STORING AND REPRODUCING RADAR SIGNALS IN RADIO JAMMING

Today, digital frequency storage and reproduction devices, abbreviated as DRFM, are being developed, manufactured, and operated.

In DRFM devices, the signal is divided into quadrature components. This ensures the constancy of the circuit's output effect at those moments when the signal at the output of the cosine channel is zero, at the output of the sine channel is maximum, and vice versa. At any initial phase, the signal can be decomposed into cosine and sine components, and then restored, preserving all the information, but already in low-frequency oscillation.

The phase of the reference frequencies of the quadrature components is recorded with an accuracy of π , that is, single-bit phase quantization is implemented in the analog-digital device. During signal reconstruction, such a rough phase determination leads to the formation of parasitic sidebands around each spectral component of the reconstructed signal. The level of the bands is only 8 dB below the level of the corresponding principal components. As a result, up to 14% of the power of the reconstructed signal is made up of parasitic sidebands of its spectral components.

When using such a signal to create signal-like interference, the presence of parasitic sidebands is dangerous. Due to these components, it is possible to differentiate signals from interference. The differentiation can be made more difficult by simply increasing the number of bits in the quantization of the phase of the quadrature components. Thus, during two-, three-, four-, and five-bit quantization, the phase intensities of parasitic sidebands are reduced by 9, 17, 23, and 29 dB compared to the case of one-bit quantization. At the same time, the power losses due to parasitic components in the restored signal are reduced from 14 to 2; 0.3; 0.1 and 0.02%, respectively. With the reduction of these losses, the accuracy of signal reproduction increases.

Since increasing the quantization levels is not very difficult, it seems reasonable to immediately use multi-bit quantization in order to eliminate the influence of the factor under consideration on the accuracy of signal reproduction. However, the quantization step cannot be chosen arbitrarily. Ultimately, the choice of step is determined by the intensity of noise and the errors of the signal sensor.

Signal recovery in DRFM occurs in the reverse order of storage. The signal reproduced at the operating reference frequency f_c is filtered and sent to the signal-like interference formation device to be endowed with the appropriate types of interference modulation. From the sequence of such copies of the signal of the radio-electronic device, range-leading, speed-leading, re-targeting and other interferences are formed in it. The false Doppler shift is introduced using a digital frequency synthesizer. There are centimeter-range synthesizers with a frequency tuning step of about units of Hertz, which provide suppression of the true frequency by 60... 70 dB and change of the frequency of the radiated interference signal according to any given law within hundreds of kilohertz.

When generating interference by the speed tracking channel in the described DRFM, it is taken into account that the accuracy of its reproduction of the signal

frequency of the radio electronic device being suppressed is about 1 kHz. The inaccuracy of frequency reproduction can be compensated for, for example, by introducing an initial frequency shift of close to 1 kHz of the reconstructed signal in the direction opposite to that chosen for the direction of frequency change.

Note that other DRFMs may have higher accuracy. In one DRFM, for example, operating in the 7...18 GHz frequency band, an accuracy of at least 50 Hz was achieved, however, when receiving a signal with a duration of 1 ms. When memorizing shorter signals, accuracy, of course, decreases. The generated signal-like interference is amplified by the final power amplifier of the corresponding frequency subrange and radiated by the transmitting antenna of the active interference station towards the suppressed radio-electronic device.

УДК 621.396.67

Гарачук С.А.¹, Онищенко В.Ф.²

¹ старш. викл. НУ «Запорізька політехніка»

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

РОЗРОБКА СИСТЕМИ ЦИФРОВОЇ ПЕРЕДАЧІ ВІДЕО З ВИКОРИСТАННЯМ WIFI 6E

Сучасні безпілотні літальні апарати та мобільні роботизовані платформи все частіше використовують цифрові відеосистеми для реалізації FPV (First Person View), автоматичної навігації, управління завданнями, а також для інтелектуальної обробки даних, яка включає застосування алгоритмів штучного інтелекту та машинного навчання для аналізу відеопотоку, визначення об'єктів і перешкод, прогнозування маршрутів, а також обробки сенсорних даних для забезпечення точної навігації та орієнтації в реальному часі. Сучасні вимоги до таких систем включають необхідність забезпечення високошвидкісного каналу передачі відео з мінімальною затримкою для стабільної передачі інформації в реальному часі. Традиційно для таких завдань використовуються аналогові відеосистеми, що працюють у діапазоні 5.8 ГГц. Хоча ці системи мають хорошу дальність передачі сигналу та простоту використання, вони обмежені у якості відео, адаптивності та здатності до підтримки стабільної цифрової передачі потоку, що є критичним для сучасних дронів та роботизованих платформ. У зв'язку з цим виникає потреба в створенні нових високоякісних відеосистем, здатних працювати на великих відстанях з мінімальною затримкою та інтегруватися з іншими системами управління та моніторингу.

Використання стандарту WiFi 6E відкриває нові перспективи для створення цифрових систем передачі відео, оскільки цей стандарт підтримує

передачу даних у 6-гігагерцовому діапазоні, що дозволяє уникнути перевантаження частотного спектру, який характерний для традиційних аналогових систем. Низька затримка, висока пропускна здатність і можливість стабільної роботи у складних умовах знижують обмеження аналогових систем і дозволяють досягти значно кращих показників якості. Це робить WiFi 6E ідеальним вибором для побудови сучасних цифрових FPV-систем для БПЛА, що не лише відповідають вимогам щодо стабільності передачі, але й перевершують традиційні аналоги за якістю зображення та здатністю до адаптивного управління відеопотоком.

WiFi 6E є розширенням стандарту WiFi 6, що дозволяє використовувати новий 6-гігагерцовий діапазон для бездротової передачі даних. Цей стандарт підтримує до 59 нових 20-МГц каналів, а також ширші канали 40, 80 та 160 МГц для передачі даних з високою швидкістю.

Основними технічними перевагами WiFi 6E є:

- пропускна здатність — до 9.6 Гбіт/с для всієї мережі, з можливістю досягати швидкості ~1-2 Гбіт/с на одному з'єднанні, що дає змогу передавати відео з роздільною здатністю 4K або вище без втрат якості та затримок;

- низька затримка — що дозволяє ефективно використовувати цей стандарт для реального часу, зокрема для керування дронами;

- висока щільність каналів — завдяки використанню нових каналів у діапазоні 6 ГГц, WiFi 6E здатен забезпечити менше перешкод і більше стабільних з'єднань, навіть у щільних міських умовах з великою кількістю користувачів;

- сучасні технології модуляції — використання технологій OFDMA (Orthogonal Frequency Division Multiple Access), MU-MIMO (Multi-User MIMO) та QAM-1024 дозволяє ефективно використовувати доступний спектр частот та передавати дані з високою надійністю.

Незважаючи на переваги, високі частоти в діапазоні 6 ГГц можуть мати більші втрати при поширенні сигналу, що зменшує ефективну дальність передачі порівняно з більш низькими частотами, такими як 5.8 ГГц або 2.4 ГГц. Тому для оптимального функціонування системи необхідно ретельно підбирати антену, враховуючи її спрямованість і потужність передавача.

Порівнюючи цифрову та аналогову передачу відео, можна зробити кілька ключових висновків. Аналогові системи працюють з безперервним електричним сигналом, що дозволяє знижувати затримку до 10 мс, однак вони мають істотні обмеження. Зокрема, аналогові системи не здатні забезпечити високу якість зображення, стійкість сигналу в умовах погіршення зв'язку та можливість адаптації до змінних умов передачі. У порівнянні з ними, цифрові системи надають низку переваг:

- адаптивне кодування — це використання сучасних алгоритмів, таких як H.264 або H.265, дозволяє значно знижувати вимоги до пропускну здатності без втрати якості зображення;

- шифрування трафіку — використовується для забезпечення безпеки даних у критичних сферах (військових чи промислових застосуваннях) цифрові системи підтримують можливість шифрування переданих даних;

- multicast — це цифрові системи, які дозволяють одночасно підключати кілька приймачів до одного джерела відеопотоку, що відкриває нові можливості для багатоцільового використання;

- інтеграція з іншими мережами — це інтегрування в більш широкі інфраструктури, що забезпечує зручність і підвищену безпеку передачі даних.

Для реалізації цифрових відеосистем з високою якістю зображення та можливістю налаштування в реальному часі одним із потужних рішень є Open IPC. Ця відкрита програмна платформа для IP-камер, побудована на базі Linux, надає широкі можливості для управління відеопотоком, кодуванням та мережевими інтерфейсами, що дозволяє адаптувати її під різноманітні умови роботи, зокрема у середовищі безпілотних літальних апаратів (БПЛА).

Open IPC підтримує:

- потокове відео через RTSP, HLS, SRT;

- кодування у форматах H.264, H.265 з можливістю налаштування бітрейту та роздільної здатності;

- вбудовані Web-інтерфейси, CLI та API для зручного керування.

Ця гнучка і масштабована платформа дозволяє інтегрувати цифрові відеосистеми в системи БПЛА, забезпечуючи високоякісну передачу відео з налаштуваннями, що відповідають вимогам реального часу та умовам роботи.

Розробка цифрової системи передачі відео на базі WiFi 6E має великий потенціал для заміни традиційних аналогових FPV-систем у безпілотних літальних апаратах. Така система забезпечує високу якість відео, надійність, безпеку, а також можливість інтеграції в широкую інфраструктуру, що відкриває нові можливості для розширення функціоналу. Платформи на зразок Open IPC сприяють спрощенню розробки таких систем, надаючи інструменти для точного налаштування параметрів відеопотоку та оптимізації його ефективності. Однак для успішної реалізації таких рішень необхідно ретельно оптимізувати апаратне забезпечення та мережеві протоколи, що дозволить досягти високої ефективності в реальних умовах експлуатації.

У зв'язку з цим, дослідження в цьому напрямку має велику актуальність, і передбачає кілька ключових напрямків:

- оптимізація антен — вивчення різних типів антен для покращення дальності та стабільності сигналу в реальних умовах;
- адаптивне кодування — вдосконалення алгоритмів динамічного коригування бітрейту в залежності від стану каналу для оптимізації використання спектру;
- зниження енергоспоживання — дослідження впливу частоти передачі на час роботи БПЛА та розробка енергоефективних рішень;
- інтеграція з телеметрією та автопілотом — розширення можливостей системи завдяки інтеграції з іншими компонентами для передачі даних навігації та автоматизації місій;
- безпека — посилення захисту даних через шифрування для забезпечення безпеки в критичних та оборонних застосуваннях;
- вплив середовища — оцінка завадостійкості та аналіз впливу міських умов і WiFi-шуму на ефективність системи.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Open IPC Documentation. URL: <https://openipc.org/>. (дата звернення: 12.04.2025)
2. "IEEE Standard for Information Technology–Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks–Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 1: Enhancements for High-Efficiency WLAN Standard 802.11ax-2021", May 2021.

УДК 621.391

Vlasenko Pavlo¹

¹ PhD student, National University «Zaporizhzhia Polytechnic»

A METHOD FOR SOURCE-SIDE AUTHENTICATION IN ANALOG VIDEO TRANSMISSION

As previously emphasized by the authors in their prior research [1], the critical role of analog video systems in mission-critical unmanned applications is attributed to their low latency, cost-effectiveness and resilience in noisy environments and signal conditions. However, these systems remain inherently insecure, which highlights the necessity not only for incorporation of strong encryption methods, but also incorporation of reliable mechanisms of signal source verification to counter spoofing and ensure signal origin authenticity.

Historically, the primary focus of analog video protection systems has been on prevention of content unauthorized viewing and copying, rather than origin of the signal verification. Techniques such as Macrovision analog copy protection and

the Copy Generation Management System for Analog (CGMS-A) were designed to defeat duplication devices but lacked any capability to verify the identity of the transmitter. Even more advanced methods, such as watermarking and embedded control bits, did not incorporate cryptographically secure authentication mechanisms, leaving such systems vulnerable to spoofing, relay, and signal injection attacks [2][3]. The absence of standardized asymmetric cryptographic approaches to analog signal source verification represents a critical gap in the design of secure, mission-critical video transmission infrastructure, and presents a viable field of research.

Early conditional-access systems for analog broadcasting were primarily concerned with content encryption and subscriber authorization, using techniques such as session key distribution and scrambling control signals, embedded within VBI lines. However, these mechanisms addressed content confidentiality rather than source authentication. As noted by Yang [4], “one-way authentication is also needed to verify the origin of services” yet implementations were mostly based on symmetrical algorithms and private-key systems that provided no cryptographic proof of transmitter identity. This persistent gap in the analog signal protection model reinforces the need for secure and verifiable methods of source validation in modern unidirectional transmission environments.

The system described in the paper is designed to embed cryptographic metadata, generated using asymmetric algorithms instead of group-master keys system [4], into the video signal path without requiring a reverse communication channel, making it suitable for one-way or offline validation scenarios.

Potential application domains include: (1) multi-source environments where source trust is essential; (2) resistance to spoofing by fake or hijacked transmitters; (3) mitigation of video-based denial-of-service attacks through source-level filtering; (4) secure forensic archiving of analog footage with verifiable origin; (5) lawful or military deployments where source attribution is mandatory.

The proposed signal source authentication method relies on embedding an encrypted and cryptographically signed metadata into the analog signal path at the transmission side. The system architecture includes a source-side cryptographic module that encrypts metadata using receiver public key and generates digital signatures for the data packet, which are then injected into predefined intervals of the signal using amplitude or timing modulation techniques. On the receiver side, the verification unit extracts the metadata, decrypts the payload using receiver private key, and validates the signature using a stored transmitter public key, without the need for two-way communication or direct fixed key sharing. The method is designed to be platform-independent and suitable for integration with existing analog transmission chains. Further technical details, including data encoding formats, error correction methods, synchronization schemes, packet segmentation,

noise resistance and reliability under interference and signal distortion are subjects of ongoing research.

REFERENCES

1. Malyi O., Vlasenko P. The Need of Advanced Analog Video Scrambling Methods for Mission-Critical Unmanned Vehicles Applications. Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій: тези доповідей XII Міжнародної науково-практичної конференції (10–12 грудня 2024 р., м. Запоріжжя). Запоріжжя: НУ «Запорізька політехніка», 2024. С. 22–23. ISBN 978-617-529-487-1.
2. Macrovision Corporation. Analog Protection System: A Presentation to the Analog Reconversion Discussion Group. March 5, 2003. Available at: https://w2.eff.org/IP/DMCA/Macrovision_v_321Studios/20030320_Macrovision_APS.pdf
3. US7162146B2 – System and method for the assertion and identification of rights information in an analog video signal. U.S. Patent. Issued January 9, 2007.
4. Yang C.-H. Design and Implementation of Cryptographic Systems Using 68HC05 Microcontrollers. Proceedings of the APCMTA 2000. Taiwan: National Kaohsiung First University of Science and Technology, 2000. P. 1–4.
5. ISO/IEC 13818-1:2018. Information technology – Generic coding of moving pictures and associated audio information – Part 1: Systems.
6. ISO/IEC 9798-2:2019. Information technology – Security techniques – Entity authentication – Part 2: Mechanisms using symmetric encipherment algorithms.

УДК 004.8:629.735

Онищенко В.Ф.¹, Магльованний В.А.²

¹ канд. фіз.-мат. наук, доц. НУ «Запорізька політехніка»

² асп. гр. А-172.13 НУ «Запорізька політехніка»

ОПТИМІЗАЦІЯ МАРШРУТІВ НАВЕДЕННЯ БПЛА ЗА ДОПОМОГОЮ РЕКУРЕНТНИХ НЕЙРОННИХ МЕРЕЖ

Швидкий прогрес у сфері штучного інтелекту та автономних систем значно вплинув на проектування та розробку безпілотних літальних апаратів (БПЛА). Однією з найважливіших проблем у сучасних додатках БПЛА, особливо в критично важливих сценаріях, є оптимізація маршрутів наведення та навігації в режимі реального часу. Традиційні алгоритми планування шляху часто не в змозі ефективно адаптуватися до динамічного та невизначеного середовища, особливо коли мають справу зі швидкими змінами параметрів, таких як погодні умови, перешкоди та рухомі цілі. Для

вирішення цієї проблеми багатообіцяючим рішенням стали рекурентні нейронні мережі (RNN) завдяки їхній здатності обробляти тимчасові послідовності та вивчати історичні дані. Хоча існуючі дослідження [1, 2] досягли значних успіхів у наведенні та прогнозуванні траєкторії БПЛА, залишається прогалина в інтеграції RNN для адаптивної оптимізації траєкторії в реальному часі, яка враховує енергоефективність, динаміку навколишнього середовища та системні обмеження. Наше дослідження має на меті заповнити цю прогалину шляхом розробки системи наведення на основі RNN, яка покращує можливості прийняття рішень, покращує управління енергією та адаптується до мінливих умов, тим самим просуваючи сферу автономної навігації БПЛА.

У цій роботі досліджується впровадження моделей на основі RNN для оптимізації траєкторій наведення БПЛА. На відміну від нейронних мереж прямого зв'язку, RNN зберігають інформацію про попередні стани, що робить їх особливо придатними для прогнозування майбутніх позицій і динамічного коригування маршрутів на основі даних у реальному часі. Дослідження зосереджено на розробці архітектури RNN, адаптованої до динаміки руху БПЛА та змінних середовища, таких як напрям вітру, тип рельєфу та зони втрати сигналу.

Навчальний набір даних створено за допомогою імітації польоту у віртуальному середовищі, яке включає як статичні, так і динамічні перешкоди. Стратегія навчання з підкріпленням також застосовується в поєднанні з моделлю RNN для покращення процесу прийняття рішень з часом. БПЛА вчиться вибирати оптимальні траєкторії польоту, отримуючи зворотний зв'язок на основі показників успіху місії, ефективності часу та споживання енергії.

Експериментальні результати демонструють значне покращення ефективності та адаптивності маршруту порівняно з класичними методами планування, такими як A* або алгоритм Дейкстри. Крім того, система навігації на основі RNN демонструє надійну продуктивність у раніше невідомих сценаріях, що вказує на потужні можливості узагальнення. Це відкриває двері для автономного прийняття рішень у складних середовищах, зменшуючи потребу у втручанні людини та підвищуючи загальну надійність місій БПЛА.

Підсумовуючи, інтеграція рекурентних нейронних мереж у системи наведення БПЛА пропонує трансформаційний підхід до оптимізації траєкторії. Забезпечуючи прогнозу та адаптивну навігацію, RNN сприяють більш розумній, гнучкій та орієнтованій на місію поведінці в польоті. У майбутніх роботах може бути розглянуто застосування більш просунутих архітектур, таких як довгострокова короткочасна пам'ять (LSTM) або

регульовані повторювані блоки (GRU), для подальшого підвищення продуктивності в режимі реального часу з високим ризиком.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1.Ait Saadi, A., Bhuyan, B. P., & Ramdane-Cherif, A. (2025). Power consumption model for Unmanned Aerial Vehicles using Recurrent Neural Network techniques. *Aerospace Science and Technology*, 157, 108191. <https://doi.org/10.1016/j.ast.2024.108191>

2.Wu, D. (2025). Predictor-based neural network control for unmanned aerial vehicles with input quantization: Design and application. *Artificial Intelligence Review*, 58(47). <https://doi.org/10.1007/s10462-024-11054-0>

УДК 004.89:378.147

Фурманова Н.І.¹, Поспеева І.С.²

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

² старш. викл. НУ «Запорізька політехніка»

ФОРМУВАННЯ ІННОВАЦІЙНИХ КОМПЕТЕНТНОСТЕЙ МАЙБУТНІХ ІНЖЕНЕРІВ ЗАСОБАМИ РОБОТОТЕХНІКИ

У XXI столітті робототехніка перетворилася на одну з найважливіших міждисциплінарних галузей, що інтегрує автоматизацію, мехатроніку, програмування, комп'ютерні технології, штучний інтелект і комп'ютерний зір. Її роль у підготовці інженерів нової генерації особливо актуальна для спеціальностей 174 та 172. Саме через практичне застосування роботизованих систем формується інноваційне мислення, підприємницькі навички та здатність до роботи з реальними технічними викликами.

Інноваційна діяльність у сучасній вищій освіті передбачає розробку та впровадження нових технічних рішень, участь у стартапах, дослідження та освоєння новітніх технологій. Студенти повинні володіти критичним мисленням, технологічною грамотністю, здатністю до командної роботи, підприємництва та самонавчання. Робототехнічні проекти якнайкраще сприяють розвитку саме цих компетентностей.

На кафедрі інформаційних технологій електронних засобів (ІТЕЗ) НУ «Запорізька політехніка» активно впроваджуються різні формати використання робототехніки: у навчальному процесі, дослідницькій діяльності, гуртковій роботі та підготовці кваліфікаційних проєктів. Студенти мають можливість працювати з промисловими маніпуляторами, безпілотними літальними апаратами, 3D-принтерами, системами керування

на ПЛІС, Arduino, Raspberry Pi, а також розробляти моделі цифрових двійників і автономних роботів.

Крім занять, в університеті діють наукові гуртки, у межах яких реалізуються проекти зі створення мобільних роботів, інтерактивних систем, пристроїв на базі IoT та машинного зору. Водночас значна увага приділяється участі студентів у хакатонах, конкурсах інженерних рішень (як-от EВЕС), виступах на конференціях, поданні робіт на стартап-фестивалі, де проекти здобувають відзнаки.

У межах дипломного проектування реалізуються теми, пов'язані з промисловими та комунальними роботами, безпілотними комплексами, розумними сенсорними системами, що дозволяє студентам безпосередньо долучатися до розв'язання актуальних технологічних задач. Розробки охоплюють автоматизацію логістики, моніторинг стану середовища, захисні робототехнічні системи, цифрові моделі виробництва, аналіз енергоспоживання, реалізацію інтерфейсів взаємодії «людина-машина».

Важливою складовою також є участь у міжнародних освітніх проєктах, зокрема Erasmus+, де університет реалізує ініціативи зі створення методологій швидкої підготовки інженерів у сфері робототехніки, дронів і засобів РЕБ. Участь у таких програмах дозволяє інтегрувати досвід провідних європейських університетів, створювати партнерські проєкти з промисловістю та розширювати вплив українських студентів на світовому рівні.

Підсумовуючи, варто зазначити: робототехніка є не лише навчальним інструментом, а потужним фактором розвитку інноваційного потенціалу студентів. Завдяки їй формуються критично важливі компетентності, а студенти готуються до діяльності в умовах Індустрії 4.0. Подальша підтримка цього напряму дозволить підготувати нове покоління висококваліфікованих фахівців, здатних забезпечити інноваційний прорив у промисловості, IT-сфері, медицині, обороні й агропромисловому секторі.

УДК 621.396

Ярошенко К.Р.¹, Малий О.Ю.²

¹ студ. гр. БК-511 НУ «Запорізька політехніка»

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

РОЗРОБКА ЕЛЕКТРОННОГО БЛОКУ ДЛЯ РАДАРНОЇ СИСТЕМИ ВИЯВЛЕННЯ ДРОНІВ

Сучасний розвиток безпілотних літальних апаратів, зокрема дронів, відкриває нові можливості у сферах логістики, сільського господарства,

охорони навколишнього середовища та багатьох інших галузях. Однак зростання кількості дронів у повітряному просторі потребує впровадження ефективних систем для їхнього виявлення, контролю та координації. Особливо важливим це є в умовах інтенсивного використання БПЛА поблизу аеропортів, захищених територій або об'єктів з підвищеним технічним навантаженням.

Метою цієї роботи є створення електронного блоку для радарної системи, який забезпечить точне та своєчасне виявлення безпілотних літальних апаратів у контрольованій зоні. Такий підхід сприятиме підвищенню рівня організації повітряного простору, запобіганню можливим конфліктам між об'єктами та загалом підвищить ефективність роботи систем моніторингу. Робота базується на сучасних технологіях радіолокації та аналізу сигналів, з урахуванням міжнародного досвіду в даній сфері.

Конструкція радіолокаційної системи складається з основних апаратних компонентів: передавача, приймача, антен, підсилювачів, мікшерів, генератора опорної частоти, а також програмованого радіо (Pluto SDR) представлена на рисунку 1.



Рисунок 1 – Конструкція радіолокаційної системи

Передавач генерує сигнал, що подається через підсилювач на антену, яка випромінює його в простір. Відбитий сигнал приймається другою антеною, обробляється в мікшері та надходить на аналого-цифровий перетворювач. Основою є SDR-пристрій, який дозволяє гнучко керувати параметрами сигналу з допомогою програмного забезпечення (наприклад, Python-бібліотека PyADI). Генератор ADF4159 з VCO використовується для формування лінійно змінного сигналу (CHIRP), що дозволяє визначити як відстань, так і швидкість цілі. Принцип дії базується на передаванні та

прийманні частотно-модульованого сигналу. Коли сигнал відбивається від об'єкта, він повертається із затримкою, яка залежить від відстані. Порівнюючи переданий і прийнятий сигнали, утворюється частота биття (f_{beat}), яка дозволяє розрахувати відстань:

$$R = (c * f_{beat}) / (2 * B), \quad (1)$$

де c — швидкість світла, B — ширина смуги частот CHIRP.

Опис елементів конструкції:

Основними апаратними складовими системи є (рис. 2):

- SDR-модуль Pluto SDR — використовується як джерело передачі та прийому сигналів, має високу гнучкість у налаштуваннях частоти та пропускну здатності;
- генератор ADF4159 із зовнішнім VCO — формує лінійно-модульований сигнал (CHIRP), що дозволяє визначати відстань до об'єкта;
- мікшери LTC5548 — здійснюють пониження частоти сигналу до рівня, придатного для обробки;
- підсилювачі ADL8107 — використовуються як підсилювачі потужності (PA) на передачі та малошумні підсилювачі (LNA) на прийомі;
- антенний масив (фазер) — дозволяє формувати напрям прийому.

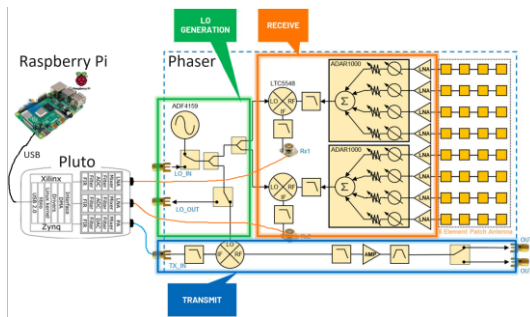


Рисунок 2– Блок схема радарної системи

Принцип дії системи полягає в генерації лінійно-модульованого сигналу (LFM-CHIRP), який випромінюється передавальною антеною. Сигнал відбивається від об'єкта і приймається антеною приймача. Після обробки сигналу на мікшерах і підсилювачах, він надходить до аналого-цифрового перетворювача Pluto SDR. За результатами обробки формується спектр beat-частот, з яких можна визначити відстань та швидкість цілі.

Під час обробки сигналу в Python використовується бібліотека PyADI, яка надає доступ до керування апаратними елементами. Дані аналізуються у частотній області за допомогою швидкого перетворення Фур'є (FFT).

Порівняно з імпульсними радарми, ця система має переваги:

- простіша реалізація без потреби в генерації високовольтних імпульсів;
- вища середня передавальна потужність;
- краща роздільна здатність за рахунок широкої смуги частот;
- можливість безперервного вимірювання швидкості та відстані.

Програмна частина дозволяє реалізовувати різні типи обробки: фільтрацію шумів, побудову спектрограм, трекінг цілей. Можна легко додати логіку класифікації об'єктів на основі амплітудних характеристик або моделей машинного навчання. Серед переваг цієї системи:

- низька вартість реалізації;
- компактність і простота конструкції;
- можливість програмного керування та модифікацій;
- придатність для освітніх цілей і дослідницької роботи;
- ефективність у виявленні малорозмірних об'єктів.

Тож варто зазначити, що реалізована система демонструє практичну можливість створення ефективного радара з використанням доступних засобів. Вона є хорошою основою для подальших вдосконалень і вивчення сучасних методів радіолокації.

Таким чином, запропонована система є не лише ефективною в задачах виявлення малих об'єктів, а й є гнучкою платформою для проведення експериментів та розробки сучасних радіолокаційних технологій.

УДК 004.94

Кобець М.К.¹, Миронова Н.О.²

¹ студ. гр. БК-614м НУ «Запорізька політехніка»

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

РОЗРОБКА АПАРАТНОГО ТА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ АВТОМОБІЛЯ НА БАЗІ RASPBERRY PI З АРХІТЕКТУРОЮ ЗВ'ЯЗКУ UDP SOCKET

Останніми роками попит на автономні та дистанційно керовані роботизовані платформи значно зріс завдяки можливості їхнього застосування в інтелектуальному транспорті, системах безпеки, логістиці та освіті. Використання доступних і гнучких мікрокомп'ютерів, таких як Raspberry Pi, дає змогу створювати масштабовані та ефективні системи, що поєднують апаратну мобільність і мережеве управління. Перспективним підходом є використання UDP-сокет для легкого та швидкого обміну даними між компонентами системи, що робить її високочутливою в умовах реального часу.

Метою роботи є розробка та реалізація прототипу дистанційно керованого роботизованого транспортного засобу, що взаємодіє за архітектурою UDP-сокетів, в якому апаратні та програмні компоненти інтегровані на базі мікрокомп'ютерів Raspberry Pi.

Роботизована платформа працює на базі Raspberry Pi 3 і використовує такі компоненти:

- електродвигуни;
- джерело живлення: батарейний блок 2S1P на основі елементів 18650, керований модулем BMS 20A;
- модуль зарядки: USB Type-C зі струмом зарядки 4A;
- регулювання напруги: DC-DC buck і boost перетворювачі з номіналом 5A;
- драйвери двигунів DRV 8833.

Для спрощення налаштування мережі та уникнення ручного введення IP-адрес, у системі використовується mDNS (Multicast DNS), що дозволяє автоматично знаходити пристрої в локальній мережі.

Програмна реалізація досліджуваної системи базується на багаторівневому програмному стеку, до складу якого входять такі компоненти:

- модулі, реалізовані мовою C++, для клієнтської частини (транспортного засобу) та серверної частини системи керування;
- Java-застосунок для операційної системи Android, що забезпечує графічний інтерфейс користувача з можливістю керування за допомогою віртуального джойстика;
- використання UDP-сокетів як транспортного протоколу з метою забезпечення швидкісного обміну повідомленнями з мінімальною затримкою;
- застосування протоколу mDNS (Multicast DNS) для автоматичного виявлення мережевих сервісів та резолюції IP-адрес без необхідності централізованого DNS-сервера.

Прототип включає робомобіль на Raspberry Pi 3, центральний сервер на Raspberry Pi 5 та Android-смартфон із застосунком для керування. Команди надсилаються через UDP до сервера, який передає їх відповідному транспортному засобу. Архітектура "клієнт-сервер-клієнт" забезпечує централізоване керування, масштабованість та підтримку множинних користувачів і роботів.

Основною проблемою під час розроблення було керування живленням. Спочатку конфігурація з батареєю 1S2P виявилася недостатньою для надійного живлення всіх компонентів. Цю проблему було вирішено шляхом переходу на схему 2S1P з підвищеною струмоємністю. Після кількох замін було обрано надійні драйвери двигунів. Надійність системи було підвищено

завдяки використанню динамічного виявлення сервісів (mDNS) для забезпечення простоти налаштування і можливості повторного використання без складної конфігурації мережі.

Результатом роботи став функціональний прототип роботизованого транспортного засобу на базі Raspberry Pi, що використовує зв'язок через UDP-сокет для керування в реальному часі через мобільний пристрій (рис.1).



Рисунок 1 – Прототип роботизованого транспортного засобу на базі Raspberry Pi

У рамках подальшої модернізації системи передбачається впровадження наступних функціональних розширень:

- виявлення перешкод за допомогою ультразвукових датчиків відстані на передній і задній частинах;
- інтеграція відеокамери для забезпечення візуального зворотного зв'язку, а також створення передумов для реалізації алгоритмів комп'ютерного зору;
- впровадження елементів автономної навігації, заснованої на обробці інформації з бортових сенсорів і можливого застосуванні методів штучного інтелекту.

АВТОМАТИЗАЦІЯ УПРАВЛІННЯ ІНВЕНТАРЕМ УНІВЕРСИТЕТУ НА ОСНОВІ ТЕХНОЛОГІЙ РАДІОЧАСТОТНОЇ ІДЕНТИФІКАЦІЇ ТА БЕЗДРОТОВОГО ПОЗИЦІЮВАННЯ

На сьогодні у навчальних закладах ефективне управління матеріально-технічними ресурсами набуває все більшого значення. Зростаючі обсяги інвентарю, мобільність обладнання та необхідність точного обліку спонукають до впровадження автоматизованих систем управління. Одним із перспективних напрямів у цьому контексті є використання технологій радіочастотної ідентифікації (RFID) у поєднанні з методами бездротового позиціювання. Дані технології дозволяють здійснювати автоматичний облік, моніторинг переміщення та ідентифікацію об'єктів в режимі реального часу

Традиційні методи інвентаризації, що базуються на ручному введенні даних та візуальній перевірці, мають низку суттєвих недоліків. Серед них – висока ймовірність помилок, значні витрати часу, складність у відстеженні переміщення об'єктів та відсутність актуальної інформації. Університетське середовище, де постійно переміщується велика кількість лабораторного, мультимедійного та офісного обладнання, потребує більш ефективного та динамічного підходу до обліку.

Метою даного дослідження є розробка та впровадження автоматизованої системи управління інвентарем університету, що базується на технологіях радіочастотної ідентифікації (RFID) та бездротового позиціювання.

Запропонована система автоматизації управління інвентарем включає наступні компоненти:

- RFID-мітки, закріплені на об'єктах інвентарю: вони містять унікальний ідентифікатор, що дозволяє швидко і точно ідентифікувати кожен об'єкт;
- RFID-зчитувачі, розміщені у ключових точках приміщень університету (лабораторії, аудиторії, склади), вони зчитують дані з міток при їх наближенні та передають інформацію на сервер;
- система бездротового позиціювання (на основі Wi-Fi, Bluetooth або UWB), яка визначає координати об'єкта з точністю до кількох метрів або навіть сантиметрів, залежно від вибраної технології;
- програмне забезпечення для збору, обробки та візуалізації інформації про місцезнаходження та переміщення об'єктів, що дозволить вести історію

переміщень, створювати звіти та сповіщення про порушення режимів зберігання.

Використання RFID у поєднанні з бездротовим позиціюванням дозволяє досягти суттєвого підвищення ефективності обліку. Зокрема, значно скорочується час інвентаризації (до кількох секунд на одиницю), зменшується кількість помилок, підвищується прозорість та контроль за переміщенням обладнання. Система забезпечує своєчасне виявлення втрат або несанкціонованого винесення майна. У контексті університету це особливо актуально для дорогого лабораторного обладнання, яке часто переміщується між корпусами та лабораторіями. Автоматизація дозволяє адміністрації оперативніше реагувати на зміни та оптимізувати логістику використання ресурсів.

Впровадження автоматизованої системи управління інвентарем на основі RFID та бездротового позиціювання є актуальним рішенням для сучасного університету. Така система забезпечує точний, швидкий та надійний облік матеріальних ресурсів, підвищує безпеку та ефективність управління. Перспективами подальших досліджень є інтеграція з системами керування доступом, мобільними застосунками для персоналу та аналітичними модулями на основі штучного інтелекту.

УДК 004.94

Баранова О.А.¹, Миронова Н.О.²

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

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

ДОСЛІДЖЕННЯ ПІДХОДІВ РЕАЛІЗАЦІЇ СИСТЕМ ВІДДАЛЕНОГО МОНІТОРИНГУ ПРОМИСЛОВИХ РОБОТІВ

Роботизовані системи використовуються в багатьох сферах, таких як промисловість, сільське господарство, медицина, а також у військових і дослідницьких цілях. Віддалений моніторинг цих систем став необхідним для забезпечення ефективного управління, своєчасного виявлення помилок і забезпечення безпеки. Віддалене управління роботами дозволяє знижувати витрати на технічне обслуговування і підвищує ефективність роботи в умовах відсутності фізичного доступу до робота.

Системи віддаленого моніторингу можуть бути класифіковані на хмарні, локальні та гібридні в залежності від місця обробки даних:

– хмарний моніторинг є найбільш популярним підходом, де дані з робота передаються на віддалені сервери (AWS, Google Cloud, Azure), де вони обробляються та зберігаються. Це дає змогу моніторити стан робота в реальному часі через веб-інтерфейси або API. Хмарні технології

забезпечують високий рівень масштабованості та доступу до потужних аналітичних інструментів (наприклад, ML та AI), але мають обмеження, пов'язані з безпекою даних та залежністю від стабільного інтернет-з'єднання;

- локальний моніторинг забезпечує обробку даних безпосередньо на пристрої або на локальному сервері, що дозволяє знизити затримки і збільшити безпеку передачі даних. Однак організація такої системи потребує значних інвестицій в інфраструктуру, а також обмежена масштабованість;

- гібридний підхід комбінує переваги обох попередніх моделей, здійснюючи часткову обробку даних на місці та передаючи важливу інформацію в хмару для подальшого аналізу. Це забезпечує високу швидкість обробки критичних даних і знижує навантаження на мережу та сервери.

Одним з основних підходів до організації віддаленого моніторингу є клієнт-серверна модель, де робота (клієнт) збирає дані з сенсорів і передає їх на сервер для обробки та зберігання. Сервер обробляє ці дані та надає доступ до інформації оператору через веб-інтерфейс або мобільний додаток. Перевагою такої моделі є масштабованість, адже один сервер може обслуговувати багато клієнтів одночасно. Однак, такі системи мають високі вимоги до інтернет-з'єднання і мають затримку при передачі даних.

Іншим підходом є пряме підключення, при якому з'єднання між роботом і оператором здійснюється безпосередньо через VPN або WebRTC. Цей метод дозволяє знизити затримки і забезпечити повний контроль над роботом у реальному часі. Однак, цей підхід має обмежену масштабованість і підходить лише для малих систем, де необхідний високий рівень контролю над роботом.

Збір і передача даних у віддаленому моніторингу здійснюється за допомогою різних протоколів зв'язку. Одним із найбільш використовуваних є MQTT – легковаговий протокол для обміну повідомленнями, який використовується в роботизованих системах для передачі телеметрії та команд управління. MQTT добре підходить для передачі даних при нестабільних з'єднаннях або в мережах з низькою пропускну здатністю, таких як LoRaWAN.

WebSocket забезпечує двосторонній зв'язок у реальному часі між клієнтом і сервером, що дозволяє здійснювати інтерактивне управління роботом або передавати відео-стрім у реальному часі. Протокол HTTP(S) використовується для передачі даних через REST API, хоча він має високі затримки і не підходить для реального часу.

Протоколи зв'язку можуть працювати через різні мережеві технології, такі як Wi-Fi, 4G/5G або LoRaWAN, в залежності від специфікацій робота та умов експлуатації.

Вибір підходу до віддаленого моніторингу залежить від кількох факторів, таких як вимоги до безпеки, затримки, масштабованості та

доступності інтернету. Гібридний підхід, що поєднує локальну обробку даних з передачею в хмару, є найбільш оптимальним для багатьох роботизованих систем, оскільки він дозволяє поєднати переваги обох підходів: швидку реакцію та високу масштабованість. Використання сучасних протоколів зв'язку, таких як MQTT і WebSocket, дозволяє забезпечити ефективну передачу даних, знижуючи затримки та забезпечуючи надійний контроль за роботою роботів в реальному часі.

УДК 004.94

Шевченко Т.В.¹, Миронова Н.О.², Єфименко М.В.³

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

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

³ д.-р. техн. наук, проф. НУ «Запорізька політехніка»

ДОСЛІДЖЕННЯ ФУНКЦІОНАЛЬНИХ МОЖЛИВОСТЕЙ СТАНКА LUMENPNP ТА ФІДЕРНИХ СИСТЕМ ДЛЯ АВТОМАТИЗОВАНОЇ УСТАНОВКИ SMD-КОМПОНЕНТІВ

Актуальність теми обумовлена зростаючими потребами підприємств електронної галузі у гнучких, економічно доцільних і адаптивних рішеннях для автоматизації процесів розміщення електронних компонентів. У зв'язку з поширенням відкритих апаратно-програмних платформ, таких як LumenPnP та OpenPnP, з'являються нові можливості для впровадження автоматизації навіть на малих виробництвах.

Мета дослідження – аналіз технічних і програмних можливостей настільного станка LumenPnP та вивчення різновидів фідерних систем, що використовуються для автоматизованої установки SMD-компонентів у малосерійному виробництві.

Об'єкт дослідження – станок LumenPnP, програмне забезпечення OpenPnP, фідери різних типів (ручні, автоматичні, безприводні), а також методи їх інтеграції та налаштування.

Станок LumenPnP – відкритий Pick and Place-пристрій із двома вакуумними маніпуляторами, що значно підвищує швидкість роботи. Має підтримку програмного забезпечення з відкритим кодом OpenPnP, сумісне з різними типами фідерів і контролерів.

Програмне забезпечення OpenPnP – дозволяє виконувати гнучке налаштування фідерів, обробку реперних точок, калібрування плат, а також взаємодію з зовнішніми мікроконтролерами (Arduino Mega 2560) для керування автоматичними фідерами.

Можна виділити наступні типи фідерів:

ручні (стандартні) – прості у виготовленні, проте потребують ручного контролю та корекції;

– автоматичні (механічні та сервокеровані) – забезпечують стабільну подачу компонентів, проте вимагають точного налаштування та живлення;

– безприводні (пасивні) – мають найнижчу вартість і просту конструкцію, але потребують участі маніпулятора для просування стрічки.

У межах дослідження було проаналізовано типи фідерів – ручні, автоматичні та безприводні – їх особливості, принципи роботи, недоліки та можливості вдосконалення. Також розглянуто взаємодію станка з програмним забезпеченням OpenPnP та зовнішніми контролерами (зокрема Arduino Mega 2560), що дозволяє реалізовувати складні схеми керування автофідерами.

Практична частина роботи полягала в автоматизованій установці компонентів на плати блоків живлення типу «20-БМ». Особливу увагу було приділено процесу калібрування, налаштування фідерів, контролю якості встановлення та корекції помилок.

Результати дослідження підтвердили ефективність використання LumenPnP у виробничих умовах. Було запропоновано низку вдосконалень для покращення точності подачі та зниження кількості помилок під час роботи з фідерами. Отримані висновки можуть бути корисними для інженерів, які впроваджують бюджетні автоматизовані рішення у сфері електронного виробництва.

УДК 004.942

Немудрий К.І.¹, Куляба-Харитонova Т.І.²

¹ студ. гр. БК-614м НУ «Запорізька політехніка»

² старш. викл. НУ «Запорізька політехніка»

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ТАРГЕТОВАНІЙ РЕКЛАМІ

Таргетована реклама – це форма маркетингу, що дозволяє досягти конкретної аудиторії на основі її поведінки, інтересів та демографічних характеристик. Завдяки розвитку технологій, особливо штучного інтелекту (ШІ), таргетована реклама значно змінила свої принципи, ставши більш персоналізованою і ефективною. Застосування ШІ дозволяє обробляти величезні обсяги даних і приймати рішення на основі прогнозів, що значно підвищує точність таргетування.

Технології ШІ у таргетованій рекламі ШІ в таргетованій рекламі використовує алгоритми машинного навчання для обробки великих даних про поведінку споживачів. Як зазначають Leventhal та інші у своїй книзі

"Predictive Analytics for Marketers", за допомогою аналізу даних рекламодавці можуть не лише сегментувати аудиторію, а й прогнозувати ймовірність покупки або взаємодії з рекламними оголошеннями. Це дозволяє створювати індивідуалізовані рекламні кампанії, які відображають інтереси та потреби конкретного користувача.

Прогнози машинного навчання допомагають рекламодавцям приймати оптимальні рішення щодо розподілу бюджету. Відомо, що алгоритми, застосовувані у платформах, як Google Ads та Facebook, можуть коригувати стратегії в реальному часі, що сприяє підвищенню ефективності рекламних кампаній і зниженню витрат.

Однією з головних переваг ШІ є значне покращення ефективності реклами. Згідно з дослідженням, опублікованим у "Journal of Business Research", ШІ дозволяє рекламодавцям автоматизувати багато процесів і знижувати витрати на рекламу. Це досягається завдяки більш точному таргетуванню та персоналізації рекламних повідомлень. Рекламодавці можуть спрямовувати свої зусилля на найбільш перспективну аудиторію, що допомагає максимізувати ROI (повернення на інвестиції).

Для прикладу, рекламні кампанії в Google та Facebook використовують алгоритми, які враховують історію пошукових запитів користувачів, їх взаємодію з іншими оголошеннями та навіть поведінку на сайтах, щоб спрогнозувати, які оголошення будуть найбільш релевантними для конкретного користувача.

Попри численні переваги, використання ШІ в рекламі не позбавлене складнощів. Одним з найбільших викликів є питання конфіденційності. ШІ потребує збору великих обсягів персональних даних для точного прогнозування, що підвищує ризики щодо порушення приватності користувачів. Багато користувачів не усвідомлюють, як їхні дані використовуються для створення рекламних оголошень, що викликає етичні питання щодо того, наскільки етичним є збір таких даних. Додатково, алгоритми ШІ можуть мати упередження, якщо їх навчати на історичних даних, які можуть відображати обмежену або не зовсім точну картину. Це може призвести до неефективного таргетування або навіть до дискримінації певних груп користувачів.

Загалом, використання ШІ в таргетованій рекламі має великий потенціал для оптимізації рекламних кампаній, підвищення їх ефективності та персоналізації. Технології дозволяють рекламодавцям знижувати витрати і покращувати результати, однак разом з цим виникають питання етики та захисту даних. Враховуючи ці аспекти, важливо застосовувати ШІ в рекламі з урахуванням етичних стандартів та правових норм. Очікується, що в майбутньому розвиток ШІ в маркетингових стратегіях продовжить сприяти інноваціям і вдосконаленню реклами.

УДК 004.94

Хохлов В.С.¹, Миронова Н.О.², Молочков Д.Є.³

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

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

³ старш. викл. НУ «Запорізька політехніка»

РОЗРОБКА СИСТЕМИ ВИЗНАЧЕННЯ ПРОСТОРОВОГО ПОЛОЖЕННЯ ОБ'ЄКТІВ У РОБОЧІЙ ЗОНІ РОБОТА

Актуальність роботи обумовлена зростаючим інтересом до роботизованих систем, здатних орієнтуватися у просторі та взаємодіяти з об'єктами в реальному часі. У промисловій автоматизації, логістиці, агросекторі та побутових роботах важливою є здатність робота точно визначати положення об'єктів для ефективної взаємодії з ними. Розробка системи визначення просторового положення об'єктів дозволяє підвищити точність маніпуляцій, автоматизувати задачі сортування, захоплення та розміщення предметів. Застосування недорогих сенсорів та алгоритмів комп'ютерного зору робить такі системи доступними для широкого спектра задач.

Мета роботи – розробити прототип системи, що дозволяє визначати просторове положення об'єктів у робочій зоні робота з використанням методів комп'ютерного зору та сенсорних даних.

У межах проектування системи були проаналізовані апаратні рішення, здатні забезпечити отримання просторових координат об'єктів. Розглянуто такі варіанти: стереокамери (Intel RealSense, ZED Camera), LiDAR-сенсори (RPLIDAR A1, Garmin Lidar Lite), 3D-камери на основі ToF (Time-of-Flight), а також глибокі нейромережеві підходи з використанням звичайних RGB-камер. Вибір рішення залежав від бажаної точності, швидкодії, вартості, умов освітлення та розміру робочої зони.

Для реалізації прототипу було обрано стереокамеру Intel RealSense D435, яка поєднує RGB-зображення з глибинною інформацією, забезпечуючи тривимірне сприйняття простору в режимі реального часу. Це дозволяє визначати координати об'єктів відносно робота з високою точністю та мінімальною затримкою.

Програмна частина реалізована з використанням бібліотек OpenCV, Pyrealsense2 та фреймворку TensorFlow. Було впроваджено алгоритм обробки зображення, що включає:

- фільтрацію шумів та покращення контрастності;
- виявлення об'єктів за допомогою попередньо навчених моделей;
- визначення глибини за допомогою стереозображення;

– обчислення просторових координат об'єктів (X , Y , Z) у робочій системі координат.

У разі використання лише RGB-камери, альтернативно може застосовуватись метод монокулярної глибини, заснований на згорткових нейронних мережах (наприклад, MiDaS), що дозволяє оцінити глибину сцени без спеціалізованого апаратного забезпечення, але з меншою точністю.

У результаті було створено функціональний прототип системи визначення просторового положення об'єктів, який дозволяє роботу орієнтуватися у тривимірному просторі та здійснювати точні маніпуляції з об'єктами у своїй робочій зоні. Така система може бути інтегрована у виробничі або дослідницькі роботизовані комплекси для автоматизації рутинних задач

УДК 004.94

Девяткін О.К.¹, Миронова Н.О.²

¹ студ. гр. БК-612сп НУ «Запорізька політехніка»

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

РОЗРОБКА АПАРАТНОГО ТА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ЗОВНІШНЬОГО ДИСПЛЕЮ ДЛЯ ВІДОБРАЖЕННЯ ІНФОРМАЦІЙНИХ ВІДЖЕТІВ

Під час використання комп'ютера для виконання різноманітних завдань – зокрема складних робочих процесів, що вимагають високої концентрації, використання ресурсомістких програм, роботи з повноекранними застосунками або під час відпочинку – доступ до інформації з таких програм, як месенджери, електронна пошта, погодні сервіси та інші подібні, може бути обмеженим. Це створює потребу у додаткових засобах відображення актуальної інформації без відволікання користувача від основного процесу.

Розробка автономного зовнішнього дисплею, здатного працювати у тісній взаємодії з комп'ютером, відкриває нові можливості для підвищення зручності та ефективності роботи користувачів. Такий пристрій може бути особливо корисним в умовах багатозадачності, віддаленої роботи, а також для користувачів, що надають перевагу організованому робочому простору.

Мета роботи – розробити функціональний прототип зовнішнього пристрою з дисплеєм, який здатен виводити інформаційні віджети (повідомлення, календарні події, погоду тощо) та відповідне програмне забезпечення, яке забезпечує взаємодію між комп'ютером і дисплеєм.

У межах виконання роботи передбачено:

- аналіз існуючих рішень у сфері зовнішніх дисплеїв та інтерфейсів виведення інформації;

- вибір оптимального апаратного забезпечення для реалізації пристрою (мікроконтролер, тип дисплею, способи підключення до комп'ютера);

- розробка прошивки для мікроконтролера, що забезпечує відображення даних;

- створення програмного забезпечення для збору, обробки та передавання інформації на дисплей;

- реалізація підтримки базових віджетів: годинник, погода, календар, повідомлення з месенджерів тощо;

- тестування системи на практиці та оцінка її стабільності, енергоспоживання і зручності використання.

Об'єкт дослідження – процес передачі та виведення інформації на додатковий зовнішній дисплей у режимі реального часу.

Предмет дослідження – апаратна і програмна реалізація засобів відображення інформаційних віджетів.

Методи дослідження – аналіз технічної документації, моделювання архітектури пристрою, прототипування апаратної частини, програмування мікроконтролера та програмного забезпечення для комп'ютера, експериментальне тестування.

Очікувані результати роботи:

- розроблений прототип зовнішнього дисплею з апаратною та програмною частиною;

- програмне забезпечення, здатне передавати актуальну інформацію з комп'ютера на пристрій;

- оцінка практичної доцільності використання такого рішення в умовах реального щоденного застосування.

Практична цінність полягає в створенні доступного та зручного інструменту для підвищення продуктивності користувачів шляхом безперервного доступу до важливої інформації без необхідності перемикавання контексту роботи.

УДК 004.94

Давиденко Д.В.¹, Миронова Н.О.²

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

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

РОЗРОБКА МОБІЛЬНОГО ЛЮДИНО-МАШИННОГО ІНТЕРФЕЙСУ ДЛЯ ПРОМИСЛОВОГО РОБОТА

Актуальність дослідження обумовлена стрімким розвитком промислової автоматизації, де ключовою ланкою стають роботизовані системи. Для ефективної взаємодії оператора з роботом використовуються НМІ (Human-Machine Interface) – інтерфейси, які дозволяють зручно управляти, налаштовувати та моніторити робота у виробничому середовищі. Сучасні тренди вимагають мобільності та інтуїтивної зрозумілості інтерфейсів, що спрощують введення команд та контроль за процесами в реальному часі.

Мета роботи – дослідити особливості мобільних НМІ-інтерфейсів для промислових роботів, розглянути існуючі рішення, які сприяють підвищенню ефективності керування та зниженню часу навчання операторів та розробити мобільний людино-машинний інтерфейс для промислового робота.

Мобільні НМІ дозволяють керувати роботами за допомогою планшетів, смартфонів або спеціалізованих переносних консолей. Основні вимоги до таких інтерфейсів: стійкість до промислових умов, простота інтеграції з роботизованою системою, безпечний протокол зв'язку (наприклад, MQTT, OPC UA) та підтримка реального часу.

Серед відомих рішень можна виділити:

- KUKA smartPAD – спеціалізована переносна панель для керування промисловими роботами KUKA, має сенсорний екран, зручний інтерфейс та інтеграцію з KUKA System Software;

- ABB FlexPendant – мобільний інтерфейс компанії ABB, призначений для налаштування і програмування роботів безпосередньо на виробництві, із вбудованими функціями навчання та відлагодження;

- UR PolyScope – інтерфейс від Universal Robots, який доступний як на фізичних панелях, так і через віддалене підключення, дозволяє будувати програми для роботів без глибоких знань програмування;

- Siemens SIMATIC WinCC Unified Mobile – рішення для створення мобільних НМІ-панелей, що дозволяє управляти не лише роботами, а й усією промисловою інфраструктурою через браузер або застосунок.

Мобільні НМІ-інтерфейси значно підвищують гнучкість і безпеку роботи з промисловими роботами, знижуючи навантаження на оператора та спрощуючи процес інтеграції робототехнічних систем у виробничий цикл.

Вибір конкретного рішення залежить від специфіки завдань, типу обладнання та вимог до безпеки.

В роботі планується розробити мобільний людино-машинний інтерфейс для промислового робота.

УДК 621.3

Малий О.Ю.¹, Жулай А.О.²

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

² студ. гр. БК-514м НУ «Запорізька політехніка»

РОЗРОБКА РОЗУМНОЇ КОЛОНКИ З УКРАЇНСЬКИМ НАПРЯМОМ

Розумні пристрої все більше поширюються в нашому житті. Від акустичних помічників до систем розумного будинку, все це допомагає людині в повсякденному житті. Але є люди, яким це не лише допоможе, а й полегшить життя. Втрата зору сильно ускладнює життя людині, але не забирає його. Тому таким людям потрібна додаткова допомога, з чим можуть справитися сучасні технології. Метою роботи є розробка розумної колонки з українським спрямуванням, яка зможе в першу чергу допомогти людям з порушенням зору в повсякденному житті.

Порушення зору класифікуються на часткову втрату зору та повну сліпоту. Існують декілька проблем, з якими стикається людина з порушенням зору, особливо під час реабілітації: орієнтація в просторі та доступ до інформації. Враховуючи потреби таких людей розробляється розумна колонка. Основний функціонал включає: голосове керування, доступ до першочергової інформації (погода, час, новини, замітки, тощо) та пошук іншої інформації, за допомогою алгоритмів штучного інтелекту. Для вирішення потреб орієнтації в просторі заплановано інтеграцію із системою розумного будинку.

Аналіз подібних продуктів на ринку показує, що повністю україномовних смарт колонок немає, лише з певної доробкою. Тому вирішено збільшити кількість розумних україномовних пристроїв на ринку, щоб заповнити існуючу нішу.

З врахуванням проблем людини з порушенням зору, смарт акустична система повинна відповідати таким основним вимогам: гучність; невеликі розміри; наявність голосового керування; додаткове механічне керування, наприклад, кнопки гучності та живлення. Окрім цього пристрій повинен добре чути запит та перетворювати його в текст, з'єднуватися із штучним інтелектом для відправлення запитання та отримання відповіді, виконання базових запитів без з'єднання з ІІІ, озвучування запитів, додаткове сповіщення про запис голосового запиту. Перше вмикання пристрою

повинно запускати навчання смарт колонкою, в якому буде на практичних завданнях буде показано основи керування пристроєм. На рисунку 1 наведений приклад зовнішнього вигляду україномовної розумної колонки на прикладі G-90Q.

Для реалізації поставлених завдань доцільно розглянути використання мікроконтролерів ESP32 та Sipeed M0S на BL616. Обидва мікроконтролери мають гарні характеристики. На етапі тестування функціоналу було використано ESP32, через наявність обширної документації, незважаючи на дещо нижчі технічні параметри. Однак для фінального продукту планується застосування Sipeed завдяки його покращеним характеристикам, зокрема: підтримці Wi-Fi 6, Bluetooth 5.2 та Zigbee, компактнішим розмірам модуля та вищій тактовій частоті процесора [1].



Рисунок 1 - Портативний бездротовий Bluetooth-сумісний динамік G-90Q

У системах, що здійснюють передачу запитів за межі пристрою важливо враховувати ризики, пов'язані з передачею даних до зовнішніх серверів. Для розумних пристроїв виділяють наступні загрози: несанкціонований збір і використання даних, надійне управління даними, вразливість IoT-пристроїв до кібератак [2]. Усунення наведених загроз реалізується за допомогою активації колонки кодовою фразою, збереження запитів лише за згодою користувача, збереження особистих даних локально на пристрої, шифрування інформації переданої зовнішнім сервісам.

Автономність подібних пристроїв відіграє не останню роль, оскільки без додаткової інтеграції із системами розумного будинку вони не можуть охопити увесь житловий простір. Завдяки своїм компактним розмірам, пристрої можуть бути переносними, що допомагає розміщувати їх завжди

поблизу людини. Час роботи розумної колонки має бути достатнім для безперервного використання. Оптимальним рішенням для користувача є заряджання колонки за допомогою бездротової зарядної станції або зарядного пристрою з магнітним з'єднанням.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. M0S module [Електронний ресурс] – Режим доступу: <https://wiki.sipeed.com/hardware/en/maixzero/m0s/m0s.html>

2. Підлісний, Ю. І. Шляхи підвищення конфіденційності в мережах інтернету речей / Ю. І. Підлісний // Центральньоукраїнський науковий вісник. Технічні науки : зб. наук. пр. - Кропивницький : ЦНТУ, 2025. - Вип. 11(42). - Ч. 1. - С. 46-55.

УДК 004.94:681.5

Манько Д.В.¹, Шаптала С.В.²

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

² старш. викл. НУ «Запорізька політехніка»

РОЗРОБКА АЛГОРИТМІВ СИНХРОНІЗАЦІЇ 3D-МОДЕЛІ ЦИФРОВОГО ДВІЙНИКА РОБОТОТЕХНІЧНОГО ПРИСТРОЮ З ПОТОКОВИМИ ІОТ-ДАНИМИ

У сучасному світі технологія цифрових двійників набула все більшого значення, знаходячи застосування у різноманітних галузях, включаючи промисловість, логістику та робототехніку. Одним з ключових аспектів ефективності цифрових двійників є їх здатність до динамічної синхронізації з даними реальних об'єктів, що особливо актуально в контексті даної тематики.

Актуальність дослідження зумовлена зростаючою потребою у створенні гнучких та інтелектуальних систем моніторингу та управління, де віртуальні моделі в реальному часі відображають стан та поведінку фізичних об'єктів. Синхронізація 3D моделей цифрових двійників з поточними IoT-даними відкриває нові можливості для оптимізації процесів, прогнозування відмов та підвищення ефективності прийняття рішень.

Мета роботи полягала у розробці та дослідженні підходу до синхронізації 3D моделі цифрового двійника робототехнічного пристрою з поточними даними, що надходили від IoT-пристроїв.

Для досягнення поставленої мети було вирішено наступні задачі:

- досліджено існуючі підходи та технології створення та синхронізації цифрових двійників, зокрема у контексті використання іот-даних та середовища Webots;

- здійснено пошук та адаптацію готової 3D моделі робото технічного пристрою з відкритих джерел (рис. 1), виконано її модифікацію у середовищі Fusion 360 з урахуванням вимог симуляції у Webots. зокрема, було оптимізовано геометрію та налаштовано систему координат;



Рисунок 1 - Mecanum Wheel Robot

- розроблено віртуальне середовище для симуляції руху 3D моделі у Webots. Webots є потужним інструментом для моделювання та симуляції робото технічних систем. в рамках даної роботи було створено віртуальний світ, що включав 3D модель робото технічного пристрою та необхідне оточення для імітації його руху. особливу увагу було приділено налаштуванню фізичних параметрів моделі та інтеграції механізмів для керування рухом коліс. досліджено можливості Webots щодо імпорту зовнішніх 3D моделей та використання його API для динамічної зміни параметрів симуляції на основі зовнішніх даних;

- спроектовано та розроблено програмний інтерфейс для забезпечення обміну даними між IoT-пристроями (емуляцією IoT-пристроїв) та віртуальним середовищем Webots через базу даних (рис. 2);

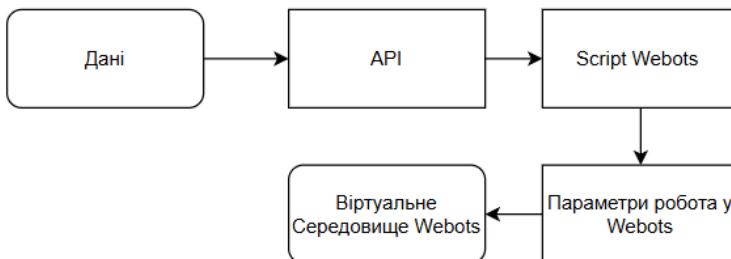


Рисунок 2 – Блок-схема програмного інтерфейсу для забезпечення обміну даними

- реалізовано механізм синхронізації параметрів 3D моделі у Webots на основі потокових даних, що надходили через розроблений API та зберігалися у базі даних. це включало розробку логіки, яка зчитувала дані з бази даних та в реальному часі оновлювала стан 3D моделі у Webots, відображаючи зміни, що відбувалися з віртуальними іот-датчиками, до 3D моделі передавалися потокові дані про швидкість обертання коліс та кут повороту осі;

- проведено експериментальну оцінку розробленої системи синхронізації, продемонструвавши відображення змін в ІоТ-даних на поведінці 3D моделі у віртуальному середовищі Webots.

Практичне значення отриманих результатів полягає у створенні прототипу системи, що демонструє можливість динамічної синхронізації віртуальної моделі з реальними або імітованими даними, що може бути використано для розробки систем моніторингу, управління та навчання для різноманітних рухомих об'єктів. Використання Webots як платформи для симуляції дозволило отримати наочне відображення поведінки об'єкта та протестувати різні сценарії без необхідності використання реального обладнання на початкових етапах розробки.

На основі проведених досліджень можна зробити висновок, що модифікація 3D моделі робототехнічного пристрою в середовищі Fusion 360 та розроблені алгоритми синхронізації забезпечили успішну реалізацію синхронізації 3D моделі цифрового двійника з потоковими ІоТ-даними у Webots.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Cyberbotics Ltd. Webots User Guide. – URL: <https://cyberbotics.com/doc/guide/index> (дата звернення: 12.04.2025)

УДК 623.4

Резниченко П.О.¹, Фурманова Н.І.², Яковенко В.В.³

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

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

³ д-р техн. наук, проф. НУ «Запорізька політехніка»

ПРОЄКТУВАННЯ БАГАТОФУНКЦІОНАЛЬНОЇ АВТОМАТИЗОВАНОЇ ПОВОРОТНОЇ ПЛАТФОРМИ

В умовах сучасних бойових дій зросла потреба в ефективних засобах виявлення, моніторингу та протидії ворожим дронам та піхоті. На даний момент відсутні серійні і доступні рішення, що дозволяють обертати корисне навантаження у потрібному напрямку з керуванням з захищеного місця.

Військові часто вимушені виготовляти їх самостійно з підручних компонентів, що зумовлює значні розбіжності у якості, функціональності та сумісності подібних пристроїв.

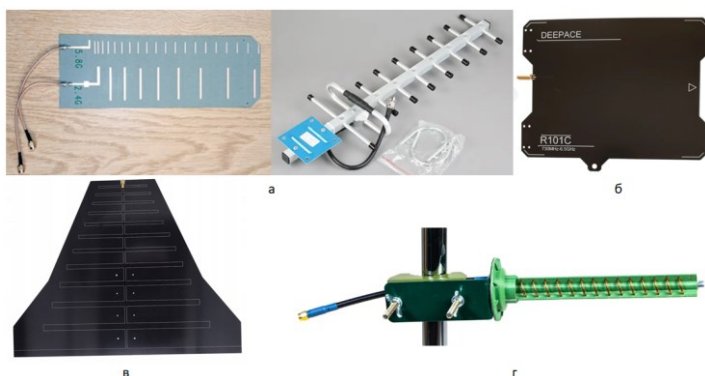
У межах роботи запропоновано концепцію універсальної автоматизованої поворотної турелі з можливістю дистанційного керування. Платформа дозволяє встановлення наступного корисного навантаження (приклади наведені на рисунках 1-2):

- денна FPV-камера Foxeer Cat;
- тепловізійна аналогова камера Caddx IRC-640CA;
- направлені антени (спіральна, логоперіодична, Вівальді або Yagi-типу)

для керування власними дронами;

- легкий саморобний однозарядний дробовик для фізичної протидії ворожій піхоті;

- антени у складі детекторів дронів на базі аналізаторів спектру Tiny SA ULTRA або SA6 для виявлення сигналів ворожих дронів.



а – YAGI антени; б – антена Вівальді;
в – логоперіодична антена; г – спіральна антена.

Рисунок 1 – Направлені антени.



а – тепловізійна камера; б – FPV камера; в – саморобний дробовик.

Рисунок 2 – Інші види навантаження.

Система умовно складається з трьох частин – пульту оператора, центрального вузлу живлення та поворотної платформи. Пульт оснащено джойстиком, кнопками і дисплеєм для зворотного зв'язку. Для передачі даних використовується стандарт RS-485 з відповідними перетворювачами інтерфейсів UART у RS-485, що забезпечує стабільність сигналу на відстанях до кілометра. Живлення системи забезпечується з єдиного джерела 12–24 В через стабілізатор напруги. У турелі використано невеликий кроковий двигун NEMA17 з планетарним редуктором, завдяки чому забезпечується високий момент утримання без втрати ККД — критичний для стабільної роботи в умовах непогоди.

На відміну від більшості наявних саморобок, запропонована конструкція спроектована з урахуванням серійного виготовлення. Вона легко масштабується, ремонтується та не вимагає дефіцитних компонентів.

УДК 621.396.67

Тарасов Є.П.¹, Поспеева І.Є.², Піроженко О.О.²

¹ студ. гр. БК-512сп НУ «Запорізька політехніка»

² старш. викл. НУ «Запорізька політехніка»

РОЗРОБКА КОНСТРУКЦІЇ ТА ПЛАТИ ОБРОБКИ СИГНАЛІВ ФАЗОВАНОЇ РЕШІТКИ

У контексті сучасних радіолокаційних та телекомунікаційних мереж виникає нагальна потреба в комплексних рішеннях для динамічного формування спрямованих променів із адаптивною зміною характеристик діаграми направленості, що здатні забезпечувати миттєвий перегляд простору без застосування механічних приводів. Фазовані антенні решітки, які здійснюють амплітудно фазове керування кожним елементом антенного розкриття, виступають ключовим активом у створенні багатофункціональних платформ, що поєднують в собі оперативність сканування, стабільність спрямованості та можливість програмного формування профілів випромінювання. З огляду на зростаючі вимоги до мобільності, мініатюризації та кросфункціонального використання апаратних засобів у складних середовищах, доцільність застосування цифрових фазовращачів із великою кількістю каналів стає критичною для підвищення гнучкості системи, зниження експлуатаційних затрат та забезпечення безперебійної роботи в умовах підвищених навантажень і загроз інформаційній безпеці.

Метою даної роботи є розробка інтегрованої архітектури антенної системи з тонкопрофільною конструкцією та створення плати обробки сигналів на основі мультиканального фазового комутатора ADAR1000, яка

забезпечить високоточне управління фазовими зрушеннями і коефіцієнтами підсилення до тридцяти двох каналів у широкому діапазоні частот. Новизна підходу полягає в уніфікації апаратних модулів та використанні єдиної платформи для реалізації адаптивного алгоритму формування променя без механічних елементів, що суттєво підвищує ефективність й економічність рішення.

Для реалізації адаптивного керування фазовими комутаторами та організації моніторингу ключових параметрів розроблено функціональну схему плати, що включає роз'єми для підключення антенної матриці, інтерфейс подачі гетеродинного сигналу гармонічних коливань, лінії керування й моніторингу стану системи, а також набір джамперів для вибору та конфігурації робочих режимів.

Плата обробки сигналів фазової решітки включає наступну конфігурацію основних елементів системи (рис. 1):

- фазовий комутатор ADAR1000;
- міксер LTC5548;
- малошумний підсилювач ADL8107;
- перемикач ADRF5019;
- синтезатор частоти ADF4159.

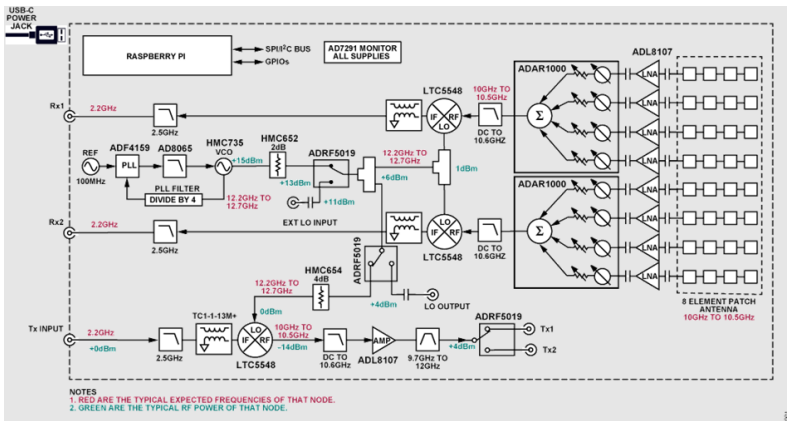


Рисунок 1— Блок-схема плати фазової решітки

Проведене дослідження підтверджує ефективність запропонованої архітектури фазової антенної решітки з інтегрованою платою обробки сигналів на базі ADAR1000, оскільки реалізовані цифрові інтерфейси та восьмишарова друкована плата забезпечують узгодженість імпедансів і мінімальні втрати, а адаптивні алгоритми керування фазовими зрушеннями

підтримують відношення сигнал/завада близько до теоретичного максимуму. Запропонована функціональна схема гарантує гнучкість експлуатації й оперативне коригування параметрів у реальному часі. Отримані результати свідчать про перспективність запропонованого рішення та відкривають можливості для його вдосконалення й адаптації до різних умов експлуатації

УДК 004.89 : 621.865

Пономарьов Є.А.¹, Фурманова Н.І.²

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

² доц. НУ «Запорізька політехніка»

ЕКОНОМІЧНА ЕФЕКТИВНІСТЬ ТА СТАЛИЙ РОЗВИТОК АВТОМАТИХОВАНИХ СИСТЕМ АДАПТИВНОГО ПАКУВАННЯ

Інтенсифікація вимог щодо екологічності виробництва, посилення конкурентної напруги на світових ринках та зростання вартості трудових ресурсів спричинили критичну необхідність технологічної модернізації пакувальних процесів. Упровадження адаптивних маніпуляторних систем у виробничих лініях – проблематика, актуальність котрої зумовлена не лише економічними, а й екологічними чинниками. Аналіз ґрунтується на статистичних відомостях, дослідженнях провідних галузевих експертів, практичному досвіді впровадження маніпуляторів на пакувальних лініях і розглядає технологічні, економічні та екологічні аспекти в контексті індустріальної трансформації пакувальної галузі, що розкриває шляхи досягнення комплексної ефективності виробництва з одночасним зменшенням техногенного навантаження на довкілля.

Для оцінки економічної ефективності зазвичай використовують показники ROI (повернення інвестицій) та TCO (загальні витрати володіння). Аналіз кейсів демонструє, що виробники упаковки досягають терміну окупності роботизованих рішень у межах 1–3 років завдяки суттєвому зниженню витрат на оплату праці (до 75% на лініях з високим рівнем ручних операцій) та підвищенню безперебійності виробничих ліній [1]. Дослідження показують, що розрахунок TCO для пакувальних ліній дозволяє виявити приховані витрати і скоротити загальні витрати протягом життєвого циклу обладнання на 20–30% [2]. Адаптивні маніпулятори з модульною архітектурою забезпечують швидку окупність завдяки можливості налаштування під різні типи продукції без суттєвих капіталовкладень, зменшуючи вартість переналадження на 40–60% порівняно з традиційними рішеннями [3].

Оптимізація енергоспоживання та мінімізація відходів дозволяють підвищити економічну ефективність виробництва. Інтеграція високоефективних серводвигунів з регенеративними гальмами дозволяє повертати до 25% кінетичної енергії під час гальмувальних циклів, що суттєво знижує загальні витрати на електроенергію [4]. Адаптивні маніпулятори з інтелектуальним керуванням оптимізують траєкторії руху та збалансовують навантаження на приводи, додатково зменшуючи енергоспоживання на 15-25% порівняно зі стандартними роботизованими системами [5]. Застосування цифрових двійників та IoT-сенсорів забезпечує економію близько 10-15% енергії за рахунок оптимізації режимів роботи [6].

Дослідження інженерних рішень демонструє, що пакувальні матеріали, дозовані із високою точністю завдяки комплексу "машинний зір-адаптивний захват", скорочують надмірне використання сировини на 15-25%; водночас, тактильні сенсори зворотного зв'язку в конструкції захватів оптимізують прикладене зусилля при взаємодії з тендітними виробами, зменшуючи пошкодження продукції у межах 30-45% [7]. Недостатньо оціненим залишається технологічний потенціал систем "box-on-demand", котрі уже зараз забезпечують зниження витрат картону під час складських операцій на рівні 20% через механізм виготовлення тари з урахуванням індивідуальних габаритів конкретного виробу [8].

Поширення колаборативних роботів із мінімізованою складністю програмування сприяє доступності автоматизації для підприємств малого й середнього сегментів, причому експлуатаційні показники свідчать про зниження витрат на інтеграцію на 40-60% у порівнянні з класичними індустріальними рішеннями [11]. Практика впровадження на виробництвах із обмеженими людськими ресурсами маніпуляторів з інтуїтивними інтерфейсами програмування показує зменшення витрат на підготовку персоналу на 50-70% — фактор, що має значний вплив на рішення стосовно технологічної модернізації в секторі МСП [11].

Ринкові тенденції демонструють зростання попиту на модульні технологічні платформи з реалізованими функціями швидкої заміни робочих інструментів, що, згідно з виробничою статистикою, забезпечують скорочення часових витрат на переналаштування ліній у діапазоні 65-80%, підвищуючи ефективність функціонування підприємств у секторі дрібносерійного виробництва [12]. У сфері фінансових моделей з'явилися інноваційні пропозиції «Robotics-as-a-Service», котрі надають змогу невеликим виробничим компаніям імплементувати автоматизовані процеси з мінімальними стартовими капіталовкладеннями на основі регулярних платежів, що визначаються фактичним використанням обладнання [13].

Технічний аналіз засвідчує ефективність впровадження реконфігурованих мультифункціональних систем, у межах яких один

маніпуляторний комплекс послідовно виконує низку технологічних операцій (захоплення, переорієнтування, переміщення, фіксацію, запечаткування), що фактично дає змогу оптимізувати використання виробничих площ до 40% з одночасним зниженням сукупних капітальних видатків на устаткування [14]. Неабиякий потенціал мають маніпулятори з інтегрованими механізмами машинного навчання, здатні до самоадаптації щодо варіацій геометричних характеристик об'єктів, завдяки чому відбувається зменшення потреби в додаткових інвестиціях при переході до нових виробів на 30-50% [15].

Комплексний аналіз функціонування адаптивних маніпуляторів у пакувальному сегменті виробництва свідчить про наявність трьох значимих аспектів: по-перше, це гарантоване фінансово-економічне зростання через швидку окупність інвестицій та значне скорочення сукупних експлуатаційних видатків; по-друге, забезпечення енергетичної оптимізації й мінімізації матеріальних відходів; по-третє, реалізація принципів циркуляторної економіки з одночасним підвищенням доступності передових технологій для широкого кола виробників за рахунок модульності та масштабованості системних рішень. Сумарно ці фактори підкреслюють визначальну роль маніпуляторних систем у наближенні вітчизняних пакувальних виробництв до стандартів Індустрії 4.0, що забезпечує збалансоване поєднання економічних показників, екологічної відповідальності й соціальної стабільності.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Sparck Technologies – What is the ROI of automated packaging? [Електронний ресурс]. – Режим доступу: <https://sparcktechnologies.com/what-is-the-roi-of-automated-packaging/>
2. BW Packaging – How to Calculate the Total Cost of Ownership (TCO) for Packaging Lines & Machinery [Електронний ресурс]. – Режим доступу: <https://www.bwpackaging.com/blog/post/blog/2022/01/21/tco-packaging-lines--machinery>
3. PwC – Building ROI for smart factory transformation [Електронний ресурс]. – Режим доступу: <https://www.pwc.com/us/en/library/case-studies/roi-smart-factory.html>
4. MEPC Engineering – Robots with regenerative braking help to reduce energy costs [Електронний ресурс]. – Режим доступу: <https://mepca-engineering.com/robots-with-regenerative-braking-help-to-reduce-energy-costs/>
5. ABB Robotics – Energy Efficiency Service press release [Електронний ресурс]. – Режим доступу: <https://new.abb.com/news/detail/119894/prsrl-abb-robotics-launches-energy-efficiency-service-to-help-customers-save-costs-and-enhance-sustainability>

6. Packaging World – Predictive Maintenance Rising Fast in Packaging and Processing [Электронный ресурс]. – Режим доступа: <https://www.packworld.com/trends/digital-transformation/article/22871046/predictive-maintenance-rising-fast-in-packaging-and-processing>

7. DHL Supply Chain – Packaging waste reduction and box-on-demand [Электронный ресурс]. – Режим доступа: <https://www.dhl.com/content/dam/dhl/global/csi/documents/pdf/glo-csi-sustainable-packaging-and-circularity.pdf>

8. DHL Supply Chain – Reducing environmental footprint through packaging [Электронный ресурс]. – Режим доступа: <https://www.dhl.com/content/dam/dhl/global/core/documents/pdf/dhl-sustainability-case-study-reducing-environmental-footprint-through-packaging.pdf>

9. ScienceDirect – Packaging design for the circular economy: A systematic review [Электронный ресурс]. – Режим доступа: <https://www.sciencedirect.com/science/article/pii/S235255092200152X>

10. Siemens – Maximising your ROI with scalable, predictive maintenance [Электронный ресурс]. – Режим доступа: https://assets.new.siemens.com/siemens/assets/api/uuid:854533af-0f63-46d2-8534-324cf0bbb161/ROI-Report_original.pdf

11. Food Industry Executive – 5 Ways Cobots Make Automation Accessible to SMEs [Электронный ресурс]. – Режим доступа: <https://foodindustryexecutive.com/2021/11/5-ways-cobots-make-automation-accessible-to-smes/>

12. Syntegon – Robotic Pick & Place (RPP) platform [Электронный ресурс]. – Режим доступа: <https://www.syntegon.com/solutions/food/robotic-packaging/>

13. SME News – Exploring the Importance of Supply Chain Automation in SMEs [Электронный ресурс]. – Режим доступа: <https://smenews.digital/exploring-the-importance-of-supply-chain-automation-in-smes/>

14. Flexlink – BRXXX® modular packaging automation [Электронный ресурс]. – Режим доступа: <https://www.flexlink.com/en/portfolio/cobots-and-robots/packing-automation>

15. Sustainability Packaging – Optimized Packaging Cost, Filling, and Sustainability [Электронный ресурс]. – Режим доступа: <https://www.sustainabilitypackaging.com/ai-driven-roi>

Наукове електронне видання
Можна використовувати в локальному та
мережному режимах

ТИЖДЕНЬ НАУКИ-2025
Факультет інформаційної безпеки та електронних комунікацій

Збірник тез доповідей щорічної
науково-практичної конференції серед студентів, викладачів, науковців,
молодих учених і аспірантів

14–18 квітня 2025 року

Один електронний оптичний диск (DVD-ROM); супровідна документація.
Тираж 100 прим. Зам. № 675.

Видавець і виготовлювач
Національний університет «Запорізька політехніка»
Україна, 69063, м. Запоріжжя, вул. Університетська, 64
Тел.: (061) 769–82–96, 220–12–14

Свідоцтво суб'єкта видавничої справи ДК № 6952 від 22.10.2019.