Міністерство освіти і науки України
Прикарпатський національний університет
імені Василя Стефаника

ISSN 3083-7618 eISSN 3083-7626

Information Technologies and Engineering Electronics

Інформаційні технології та інженерна електроніка

1/2024

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE

VASYL STEFANYK PRECARPATHIAN NATIONAL UNIVERSITY

INFORMATION TECHNOLOGIES AND ENGINEERING ELECTRONICS

Scientific journal

ISSN 3083-7618
eISSN 3083-7626

Founded in 2024

I S S U E 1

Ivano-Frankivsk
Vasyl Stefanyk Precarpathian
National University
2024

UDC 621.3 : 004

The scientific journal was founded by the Vasyl Stefanyk Precarpathian National University, by the decision of the Academic Council of the university, protocol No. 11 dated November 12, 2024, in the following specialties: F2 - Software Engineering; F3 - Computer Science; F7 - Computer Engineering; G5 - Electronics, Electronic Communications, Instrumentation and Radio Engineering.

Website: https://journals.pnu.edu.ua/index.php/itee/

Founder – Vasyl Stefanyk Precarpathian National University (EEDRPOU code 02125266 76018, Ivano-Frankivsk, Shevchenko St., 57 tel. (0342) 75-23-51 fax (0342) 53-15-74 e-mail: office@pnu.edu.ua).

Media identifier (National): R30-06174. Registered by the National Council of Ukraine for Television and Radio Broadcasting dated 29.05.2025 No. 1150.

The journal is published two times per year.

DOI prefix: 10.15330.

The authors are responsible for the content of the article.

Editorial Team

I.T. Kogut, *Dr. Sc. (Tech.), prof., Vasyl Stefanyk PNU, Ukraine (Chief Editor)*
I.V. Svyd, *PhD, Assoc. prof*., *Vasyl Stefanyk PNU*, *Ukraine (Deputy Chief Editor)*
M.V. Vistak, *Dr. Sc. (Tech.), prof*., *DNP "Danylo Halytsky Lviv National Medical University", Ukraine*
V.M. Hryha, *PhD, Assoc. prof., Vasyl Stefanyk PNU, Ukraine*
B.S. Dzundza, *PhD, Senior Researcher, Vasyl Stefanyk PNU*, *Ukraine*
A.O. Druzhini, *Dr. Sc. (Tech.), prof., Lviv Polytechnic National University, Ukraine*
Yu. Yu. Iliash, *PhD, Assoc. prof., Vasyl Stefanyk PNU, Ukraine*
V.H. Kobziev, *PhD, Senior Researcher, NURE, Ukraine*
M.I. Kozlenko, *PhD, Assoc. prof., Vasyl Stefanyk PNU, Ukraine*
M.V. Kuz, *Dr. Sc. (Tech.), prof*., *Vasyl Stefanyk PNU, Ukraine*
I.M. Lazarovych, *PhD, Assoc. prof., V. Stefanyk PNU, Ukraine*
V.I. Mandzyuk, *Dr. Sc. (Phys.-Math.)*, *prof., Vasyl Stefanyk PNU, Ukraine*
S.I. Nichkalo, *PhD, Assoc. prof., Lviv Polytechnic National University, Ukraine*
A.P. Oliinyk, *Dr. Sc. (Tech.)*, *prof., Vasyl Stefanyk PNU, Ukraine*

Editorial board members from foreign scientific and educational institutions

prof. Vahid Meghdadi (*France*), prof. Petryshyn Lyubomir (*Poland*),
prof. Haider Th. Salim ALRikabi (*Iraq*), prof. Larysa Titarenko (*Poland*), PhD Abdul Hadi M. Alaidi (*Iraq*).

Responsible for the issue: *I.T. Kogut, Dr. Sc. (Tech.), prof., I.V. Svyd, PhD, Assoc. prof.*

Recommended for publication by the editorial board of the scientific journal "Information Technologies and Engineering Electronics" on 27.12.2024.

Editorial Board address: Vasyl Stefanyk Precarpathian National University (Vasyl Stefanyk PNU), 76018, Ivano-Frankivsk, Shevchenko St., 57, office 210a, +38(0342) 59-60-07.

The materials are distributed under the terms of a Creative Commons Attribution 4.0 International License.
CC BY 4.0 https://creativecommons.org/licenses/by/4.0/

© Vasyl Stefanyk Precarpathian National University, 2024

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ПРИКАРПАТСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАСИЛЯ СТЕФАНИКА

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА ІНЖЕНЕРНА ЕЛЕКТРОНІКА

Науковий журнал

ISSN 3083-7618
eISSN 3083-7626

Засновано в 2024 р.

В И П У С К 1

Івано-Франківськ
Прикарпатський національний університет
імені Василя Стефаника
2024

УДК 621.3 : 004

Науковий журнал засновано Прикарпатським національним університетом імені Василя Стефаника, рішенням Вченої ради університету протокол № 11 від 12.11.2024 року, за спеціальностями: F2 – Інженерія програмного забезпечення; F3 – Комп'ютерні науки; F7 – Комп'ютерна інженерія; G5 – Електроніка, електронні комунікації, приладобудування та радіотехніка.

Сайт: https://journals.pnu.edu.ua/index.php/itee/

Засновник – Прикарпатський національний університет імені Василя Стефаника (код ЄДРПОУ 02125266 76018, м. Івано-Франківськ, вул. Шевченка, 57 тел. (0342) 75-23-51 факс (0342) 53-15-74 e-mail: office@pnu.edu.ua).

Ідентифікатор медіа: R30-06174. Зареєстровано Національною Радою України з питань телебачення і радіомовлення від 29.05.2025 № 1150.

Журнал видається два рази на рік.

Префікс DOI: 10.15330.

За зміст статей відповідальні автори.

Редакційна колегія

І.Т. Когут, *д.т.н., проф., ПНУ ім. В. Стефаника, Україна (головний редактор)*
І.В. Свид, *к.т.н., доц., ПНУ ім. В. Стефаника, Україна (заступник головного редактора)*
М.В. Вісьтак, *д.т.н., проф., ДНП "ЛНМУ імені Данила Галицького", Україна*
В.М. Грига, *к.т.н., доц., ПНУ ім. В. Стефаника, Україна*
Б.С. Дзундза, *к.т.н., с.н.с., ПНУ ім. В. Стефаника, Україна*
А.О. Дружинін, *д.т.н., проф., НУ «Львівська політехніка», Україна*
Ю.Ю. Іляш, *к.т.н., доц., ПНУ ім. В. Стефаника, Україна*
В.Г. Кобзєв, *к.т.н., с.н.с., ХНУРЕ, Україна*
М.І. Козленко, *к.т.н., доц., ПНУ ім. В. Стефаника, Україна*
М.В. Кузь, *д.т.н., проф., ПНУ ім. В. Стефаника, Україна*
І.М. Лазарович, *к.т.н., доц., ПНУ ім. В. Стефаника, Україна*
В.І. Мандзюк, *д.т.н., проф., ПНУ ім. В. Стефаника, Україна*
С.І. Нічкало, *к.т.н., доц., НУ «Львівська політехніка», Україна*
А.П. Олійник, *д.т.н., проф., ПНУ ім. В. Стефаника, Україна*

Члени редколегії з закордонних наукових установ та навчальних закладів

prof. Vahid Meghdadi (*Франція*), prof. Petryshyn Lyubomir (*Польща*),
prof. Haider Th. Salim ALRikabi (*Ірак*), prof. Larysa Titarenko (*Польща*), PhD Abdul Hadi M. Alaidi (*Ірак*).

Відповідальні за випуск: *І.Т. Когут, д-р техн. наук, проф., І.В. Свид, канд. техн. наук, доц.*

Рекомендовано до публікації редколегією наукового журналу «Інформаційні технології та інженерна електроніка» 27.12.2024.

Адреса редколегії: Прикарпатський національний університет імені Василя Стефаника (ПНУ ім. В. Стефаника), 76018, м. Івано-Франківськ, вул. Шевченка, 57, кабінет 210а, +38(0342) 59-60-07.

Матеріали поширюються на умовах ліцензії Creative Commons Attribution 4.0 International License.
CC BY 4.0 https://creativecommons.org/licenses/by/4.0/

© Прикарпатський національний університет імені Василя Стефаника, 2024.

CONTENT

ELECTRONICS, ELECTRONIC COMMUNICATIONS, INSTRUMENTATION AND RADIO ENGINEERING

V.Y. Fedenko, B.S. Dzundza, I.B. Hatala Application of a high-precision mppt controller for thin-film cadmium telluride photovoltaic devices 7

T.G. Benko Circuit engineering methods for reducing impulse interference in on-board electronic systems of un-manned aerial vehicles 11

COMPUTER SCIENCE

M.M. Pavliuk Analysis of network traffic as a means of cyber threat detection 17

COMPUTER ENGINEERING

V.I. Holota, V.O. Polinyayev, V.V. Martyniuk Methods of multilevel analysis of electrocardiographic signals using wavelet transforms 25

ABSTRACTS 30

ЗМІСТ

ЕЛЕКТРОНІКА, ЕЛЕКТРОННІ КОМУНІКАЦІЇ, ПРИЛАДОБУДУВАННЯ ТА РАДІОТЕХНІКА

В.Я. Феденько, Б.С. Дзундза, І.Б. Гатала Особливості застосування високоточного MPPT контролера для тонкоплівкових фотоперетворювачів телуриду кадмію (*англ.*) 7

Т.Г. Бенько Схемотехнічні методи зменшення імпульсних завад у бортових електронних системах безпілотних літальних апаратів 11

КОМП'ЮТЕРНІ НАУКИ

М.М. Павлюк Аналіз мережевого трафіку як засіб детектування кіберзагроз 17

КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

В.І. Голота, В.О. Поліняєв, В.В. Мартинюк Методи багаторівневого аналізу електрокардіографічних сигналів із застосуванням вейвлет-перетворень 25

РЕФЕРАТИ 30

УДК 621.383 **DOI:10.15330/itee.2024.1.01**

V. Y. FEDENKO, B. S. DZUNDZA, PhD, I. B. HATALA

APPLICATION OF A HIGH-PRECISION MPPT CONTROLLER FOR THIN-FILM CADMIUM TELLURIDE PHOTOVOLTAIC DEVICES

Introduction

The efficiency of modern photovoltaic systems is determined not only by the conversion efficiency of photovoltaic devices, but also by their ability to operate under dynamically changing weather conditions and partial shading while ensuring maximum power output [1]. Due to the nonlinear nature of the I-V and P-V characteristics, the MPP coordinates continuously shift, which leads to a mismatch between the equivalent resistance of the photovoltaic modules at the operating point and the equivalent load resistance; as a result, part of the output power is lost. The use of a maximum power point tracking (MPPT) controller enables dynamic adjustment of the system's input resistance, keeping the operating point continuously in the vicinity of the maximum power point. Modern MPPT controllers provide high MPPT tracking efficiency, typically in the range of 95-99% [2,3]. By using an MPPT controller, the overall system efficiency is improved; moreover, it can ensure an optimal battery-charging regime, which positively affects the operational stability of the photovoltaic system. When investigating the stability of laboratory-fabricated CdTe-based photovoltaic (PV) cell samples under real operating conditions, it is necessary to match the load resistance to the sample resistance. Consequently, research aimed at evaluating the effectiveness of MPPT algorithms for low-power PV cells remains highly relevant.

Materials and Methods

To obtain the performance characteristics of CdTe-based photovoltaic devices, numerical simulations were performed using the SCAPS software (Fig. 1) [4]. The parameters of the CdTe/CdS/ITO and CdTe/CdS/ZnO heterostructures on glass substrates (Table 1) were determined according to ref. [5-7]. The thickness of the CdTe absorber layer was set to 2,5 μm, which is generally regarded as an optimal value, as it provides strong light absorption while keeping recombination-related losses at a low level [5].

Table 1

SCAPS model parameters based on literature data [5-7]

Parameters	p-CdTe	n-CdS	ITO	ZnO
thickness, μm	2,5	0,01	0,01	0,01
bandgap (eV)	1,5	2,4	3,72	3,3
electron affinity (eV)	4	4,5	4,5	4,6
dielectric permittivity (relative)	9,4	10	9,4	9,0
CB effective density of states (1/cm3)	$8\cdot10^{17}$	$2{,}2\cdot10^{18}$	$4\cdot10^{19}$	$2{,}2\cdot10^{18}$
VB effective density of states (1/cm3)	$1{,}8\cdot10^{19}$	$1{,}8\cdot10^{19}$	$1\cdot10^{18}$	$1{,}8\cdot10^{19}$
electron thermal velocity (cm/s)	$1{,}0\cdot10^{7}$	$1{,}0\cdot10^{7}$	$2{,}0\cdot10^{7}$	$1{,}0\cdot10^{7}$
hole thermal velocity (cm/s)	$1{,}0\cdot10^{7}$	$1{,}0\cdot10^{7}$	$1{,}0\cdot10^{7}$	$1{,}0\cdot10^{7}$
electron mobility (cm²/Vs)	$3{,}2\cdot10^{2}$	50	30	$1{,}0\cdot10^{2}$
hole mobility (cm²/Vs)	$4\cdot10^{1}$	20	5	25
shallow uniform donor density N_D (1/cm3)	0	$1\cdot10^{18}$	$1\cdot10^{21}$	$1\cdot10^{18}$
shallow uniform acceptor density N_A (1/cm3)	$2\cdot10^{14}$	0	0	0

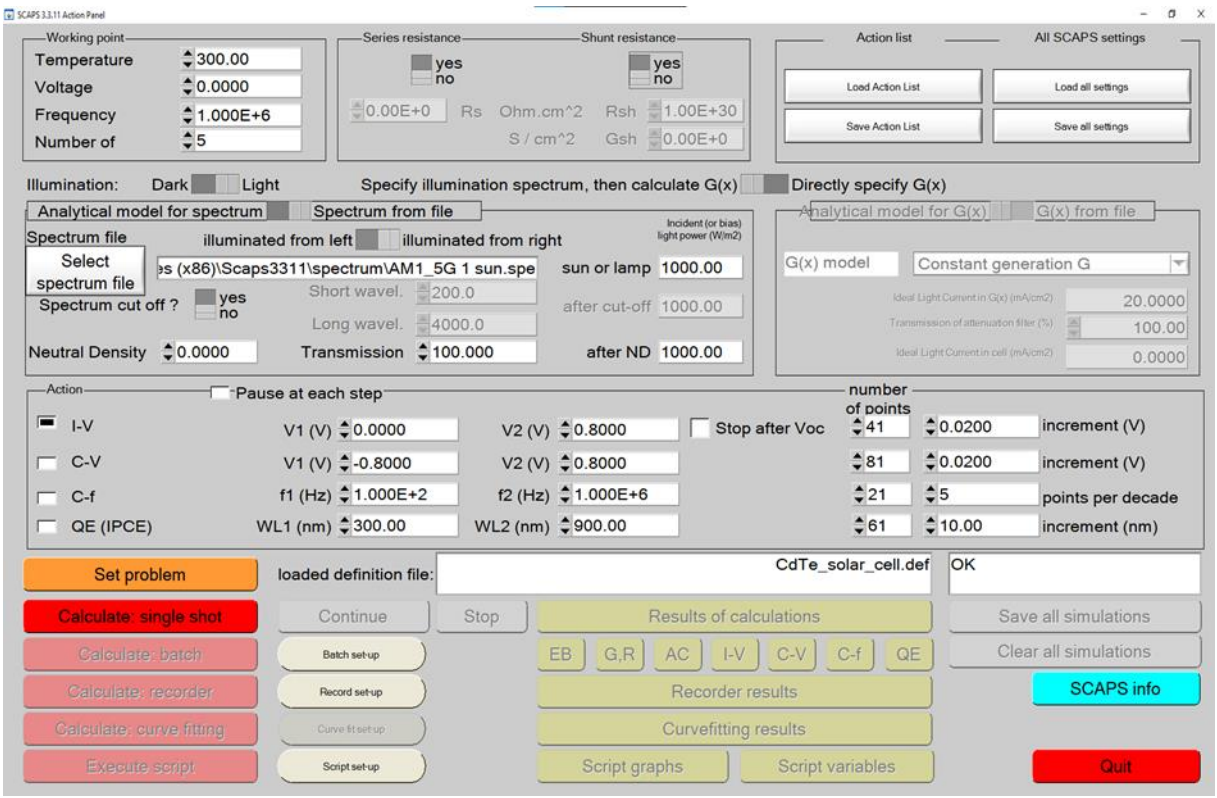

Fig. 1. SCAPS program window

For the practical implementation of the incremental conductance algorithm for thin-film CdTe/CdS heterostructures, an MPPT controller concept was developed based on a precision current regulator built around an operational amplifier (Fig. 2).

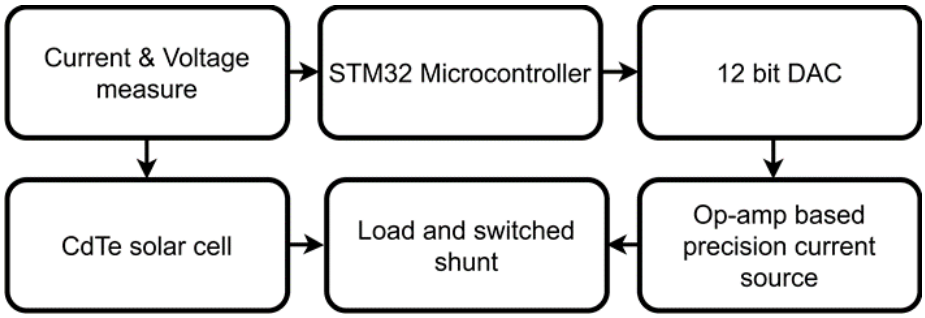

Fig. 2. Block diagram of the MPPT controller

The practical implementation of the proposed concept made it possible to develop a test setup adapted to laboratory samples of photovoltaic converters, enabling the characterization of devices with power ratings from several tens of milliwatts up to a few watts. The maximum sample voltage ranges from 0 to ~20 V and the current from 1 μA to 3 A, taking into account the maximum allowable power dissipation in the power transistor.

Results and Discussion

The results of SCAPS simulations for the CdTe/CdS/ITO and CdTe/CdS/ZnO semiconductor structures are presented in Table 2.

Based on the De Soto equations [9], a mathematical model of the incremental conductance MPPT algorithm operation over one year was developed using Python programming tools. The simulation results of the MPPT algorithm for the specified structures are shown in Fig. 3. It should

be noted that the heterostructure parameters obtained from SCAPS simulations differ only slightly; therefore, Fig. 3 presents result only for the CdTe/CdS/ITO structure.

Table 2.

Results of SCAPS simulations CdTe based solar cell

Structure	V_{oc}, V	J_{sc}, mA/cm2	FF, %	η, %
CdTe/CdS/ITO	0,93	28,58	69,9	18,74
CdTe/CdS/ZnO	0,92	28,58	70,15	18,5

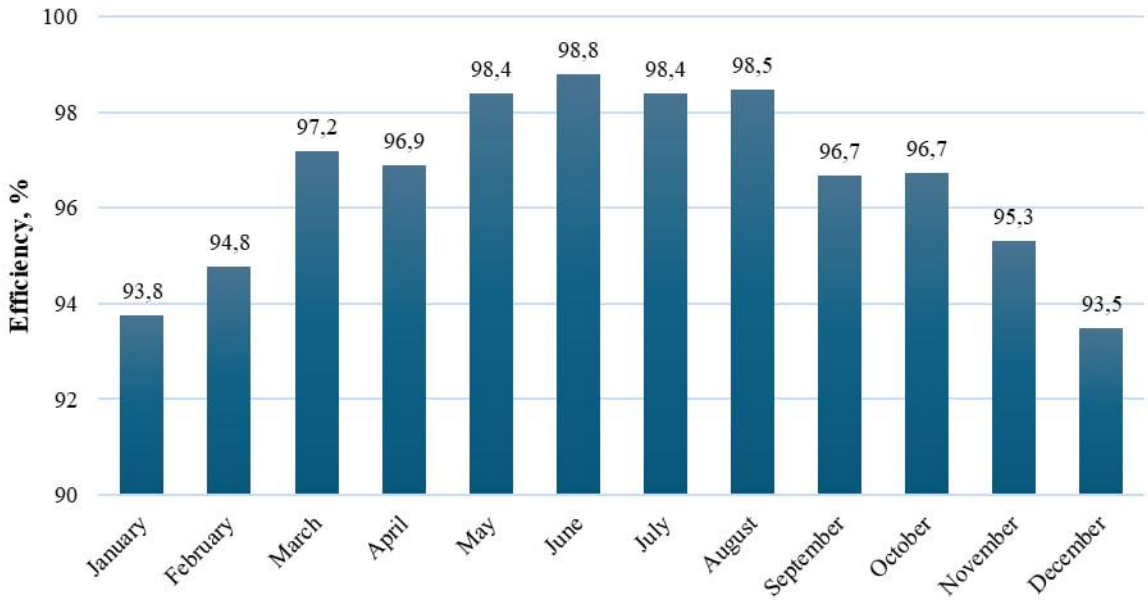

Fig. 3. Results of simulation of the incremental conductance MPPT algorithm for the CdTe/CdS/ITO structure over a one-year period

The monthly efficiency was evaluated using the following formula:

$$\eta_{mppt} = \frac{\sum\left(P_{op} \cdot \Delta t\right)}{\sum\left(P_{true_mppt} \cdot \Delta t\right)} 100\% \quad (1)$$

where: P_{op} is the actual power obtained by the system using the MPPT algorithm;

P_{true_mppt} is theoretical maximum power of the photovoltaic cell;

Δt is the time interval between measurements.

Overall, the simulation results indicate a high efficiency of the incremental conductance MPPT algorithm for the considered low-power laboratory samples of CdTe/CdS/ITO and CdTe/CdS/ZnO semiconductor structures. The short-circuit current of the model was calculated for a sample area of 25 mm², which corresponds to 7,1 mA under standard test conditions.

Conclusions

SCAPS modeling was performed and the operating parameters of cadmium telluride (CdTe) thin-film photovoltaic energy converters were determined. The short-circuit currents were calculated and normalized to the area of the actual sample. Based on the obtained data, a concept and a block/structural diagram of an MPPT controller were developed, which will ensure operation of the measurement setup within a sample voltage range of 0 to ~20 V and a current range of 1 μA to 3 A.

A year-long simulation of the Incremental Conductance MPPT algorithm was conducted, which demonstrated high efficiency of the applied algorithm when used with low-power photovoltaic converters. The average annual tracking efficiency was 96,6% of the theoretical maximum.

References:

1. A. Mohapatra, B. Nayak, P. Das, and K. B. Mohanty, "A review on MPPT techniques of PV system under partial shading condition," Renewable Sustain. Energy Rev., vol. 80, pp. 854–867, Dec. 2017. doi: https://doi.org/10.1016/j.rser.2017.05.083.
2. A. O. Salau and G. K. Alitasb, "MPPT efficiency enhancement of a grid connected solar PV system using Finite Control set model predictive controller," Heliyon, Mar. 2024. doi: https://doi.org/10.1016/j.heliyon.2024.e27663.
3. A. Chellakhi and S. E. Beid, "High-Efficiency MPPT Strategy for PV Systems: Ripple-Free Precision with Comprehensive Simulation and Experimental Validation," Results Eng., p. 103230, Oct. 2024 doi: https://doi.org/10.1016/j.rineng.2024.103230.
4. "Simulation programme SCAPS-1D for thin film solar cells developed at ELIS, University of Gent". SCAPS software. URL: https://scaps.elis.ugent.be/.
5. L. Hafaifa, M. Maache, Z. Allam, and A. Zebeir, "Simulation and performance analysis of CdTe thin film solar cell using different Cd-free zinc chalcogenide-based buffer layers," Results Opt., vol. 14, p. 100596, Feb. 2024. doi: https://doi.org/10.1016/j.rio.2023.100596.
6. G. Kartopu et al., "Enhancement of the photocurrent and efficiency of CdTe solar cells suppressing the front contact reflection using a highly-resistive ZnO buffer layer," Sol. Energy Mater. Sol. Cells, vol. 191, pp. 78–82, Mar. 2019. doi: https://doi.org/10.1016/j.solmat.2018.11.002.
7. Z. R. Zapukhlyak et al., "SCAPS modelling of ZnO/CdS/CdTe/CuO photovoltaic heterosystem," Phys. Chemistry Solid State, vol. 21, no. 4, pp. 660–668, Dec. 2020. doi: https://doi.org/10.15330/pcss.21.4.660-668.
8. W. De Soto, S. A. Klein, and W. A. Beckman, "Improvement and validation of a model for photovoltaic array performance," Sol. Energy, vol. 80, no. 1, pp. 78–88, Jan. 2006. doi: https://doi.org/10.1016/j.solener.2005.06.010.

Submitted to the editorial board 23.11.2024

Information about the authors:

Fedenko Vitalii – Ph.D student in the department of computer engineering and electronics, Vasyl Stefanyk Precarpathian National University / Прикарпатський національний університет імені Василя Стефаника, Ukraine; email: vitalii.fedenkoj@gmail.com; ORCID: https://orcid.org/0009-0009-8907-683X

Dzundza Bogdan – PhD, Senior Researcher, professor in the department of computer engineering and electronics, Vasyl Stefanyk Carpathian National University / Прикарпатський національний університет імені Василя Стефаника, Ukraine; email: bohdan.dzundza@pnu.edu.ua; ORCID: https://orcid.org/0000-0002-6657-5347

Hatala Iryna – Ph.D student in the Physics and Astronomy Department, Wayne State University / Університет штату Вейн, USA; email: iryna.hatala@gmail.com; ORCID: https://orcid.org/0009-0007-9361-2805

УДК 621.374 **DOI:10.15330/itee.2024.1.02**

Т.Г. БЕНЬКО

СХЕМОТЕХНІЧНІ МЕТОДИ ЗМЕНШЕННЯ ІМПУЛЬСНИХ ЗАВАД У БОРТОВИХ ЕЛЕКТРОННИХ СИСТЕМАХ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

Вступ

Безпілотні літальні апарати (БпЛА) набули широкого застосування у задачах спостереження, моніторингу, картографування, зв'язку та спеціальних операціях. Ефективність і надійність їх функціонування значною мірою визначаються якістю роботи бортових електронних систем, до складу яких входять навігаційні модулі, сенсорні підсистеми, системи керування та передачі даних. В умовах реального часу ці системи повинні забезпечувати високу точність, стабільність і завадостійкість за наявності жорстких обмежень за масою, енергоспоживанням та обчислювальними ресурсами.

Однією з ключових проблем бортової електроніки БпЛА є вплив імпульсних електромагнітних завад, що виникають у процесі роботи силових і комутаційних елементів. Основними джерелами таких завад є електродвигуни, регулятори обертів, імпульсні DC/DC-перетворювачі, системи стабілізації живлення та комутаційні процеси у бортовій мережі. Імпульсні завади характеризуються широким спектром частот і значною амплітудою, що може призводити до спотворення сигналів, зниження відношення сигнал/шум, збоїв у роботі сенсорів і порушення стабільності систем керування.

Для зменшення впливу завад у бортових системах БпЛА широко застосовуються методи цифрової обробки сигналів, зокрема програмна фільтрація та алгоритми компенсації шуму. Проте цифрові методи часто потребують додаткових обчислювальних ресурсів, збільшують затримки обробки сигналів і не завжди ефективні для придушення високочастотних імпульсних завад на ранніх етапах сигнального тракту. У зв'язку з цим особливої актуальності набувають схемотехнічні методи зменшення завад, реалізовані безпосередньо на рівні електронних кіл. Схемотехнічні методи придушення імпульсних завад включають використання пасивних і активних фільтрів, схем локального розв'язування живлення, демпфувальних ланцюгів та зворотних зв'язків. Перевагою таких методів є їх робота в реальному часі, відсутність обчислювальних затримок і можливість зменшення завад ще до етапу аналого-цифрового перетворення. Разом з тим ефективність схемотехнічних рішень значною мірою залежить від правильного вибору параметрів елементів і врахування реальних неідеальностей компонентів.

Незважаючи на наявність численних досліджень у галузі бортової електроніки та електромагнітної сумісності, питання системного аналізу схемотехнічних методів зменшення імпульсних завад у БпЛА залишається недостатньо опрацьованим. Багато робіт зосереджуються на експериментальних результатах або окремих схемних рішеннях без узагальненого підходу до моделювання завад та оцінки їх впливу на різні підсистеми [1].

У зв'язку з цим метою даної статті є дослідження та моделювання схемотехнічних методів зменшення імпульсних завад у бортових електронних системах безпілотних літальних апаратів. У роботі розглядаються основні джерела імпульсних завад, аналізуються пасивні та активні схеми їх придушення, а також оцінюється вплив параметрів електричних кіл на шумові характеристики та стабільність роботи бортових систем. Отримані результати можуть бути використані при проєктуванні надійних і завадостійких електронних систем БпЛА.

Схемотехнічні методи зменшення імпульсних завад

Для ефективного зменшення імпульсних завад у бортових електронних системах безпілотних літальних апаратів необхідно насамперед визначити основні джерела їх виникнення та шляхи проникнення в сигнальні кола. Імпульсні завади формуються внаслідок

комутаційних процесів у силових та керувальних підсистемах і поширюються через бортову мережу живлення, загальні шини заземлення та паразитні ємнісні й індуктивні зв'язки [2].

Після ідентифікації основних джерел імпульсних завад у бортових електронних системах безпілотних літальних апаратів доцільно розглянути схемотехнічні методи, спрямовані на зменшення їх рівня без істотного ускладнення конструкції та збільшення масогабаритних показників. Основна увага приділяється рішенням, які можуть бути реалізовані на рівні електричних схем і є сумісними з вимогами авіаційної електроніки.

Одним із найбільш ефективних методів зменшення імпульсних завад є застосування пасивних фільтрів у колах живлення чутливих електронних модулів. Типова схема фільтрації з використанням LC-ланцюга наведена на рис. 1. Така конфігурація забезпечує ослаблення високочастотних складових завад, що виникають унаслідок комутаційних процесів у силових перетворювачах. Правильний вибір індуктивності та ємності дозволяє узгодити фільтр зі спектром завад і зменшити рівень пульсацій напруги на вході навантаження без суттєвого падіння постійної складової.

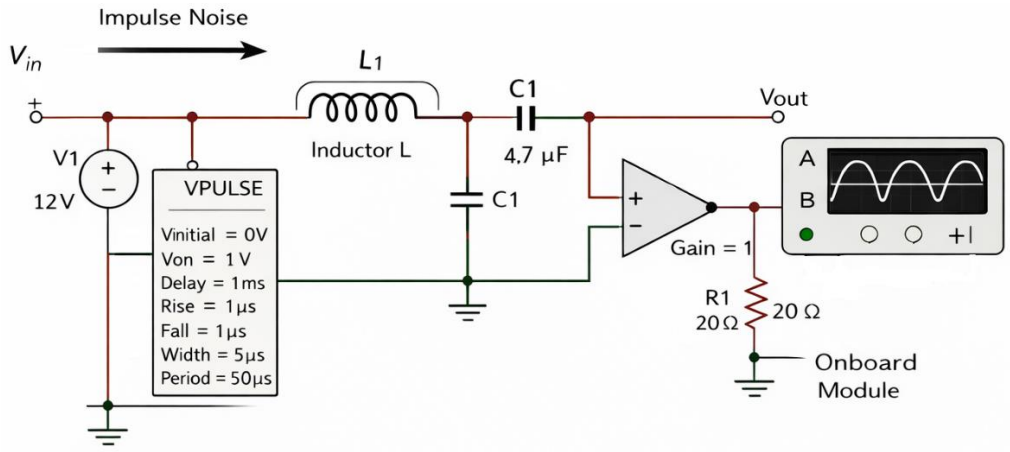

Рис. 1. Схемотехнічна реалізація LC-фільтра для зменшення імпульсних завад у колі живлення бортового електронного модуля

Для запобігання проникненню імпульсних завад у низькорівневі сигнальні кола застосовуються методи гальванічної та диференційної розв'язки [3]. Узагальнена схема використання диференційного підсилювача для підвищення завадостійкості наведена на рис. 2. Диференційна обробка сигналів дозволяє ефективно пригнічувати завади загального режиму, що є характерними для бортових систем із спільними шинами живлення та заземлення.

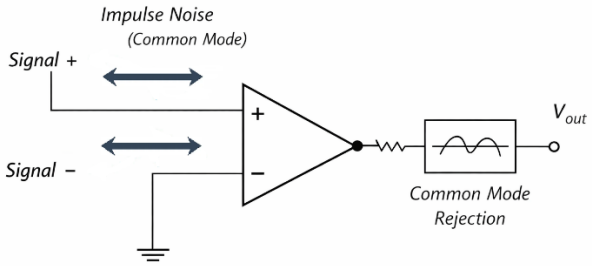

Рис. 2. Спрощена схема диференційного сигнального тракту з підвищеною стійкістю до імпульсних завад

Раціональна організація системи заземлення суттєво впливає на рівень імпульсних завад у бортових електронних системах БпЛА. Принцип «зіркоподібного» заземлення, показаний на рис. 3, дозволяє мінімізувати взаємний вплив силових і сигнальних контурів за рахунок усунення спільних струмових шляхів. Крім того, оптимізація топології друкованих плат,

зменшення площі струмових петель і використання суцільних заземлювальних площин сприяють зниженню паразитних індуктивностей і рівня наведень [4].

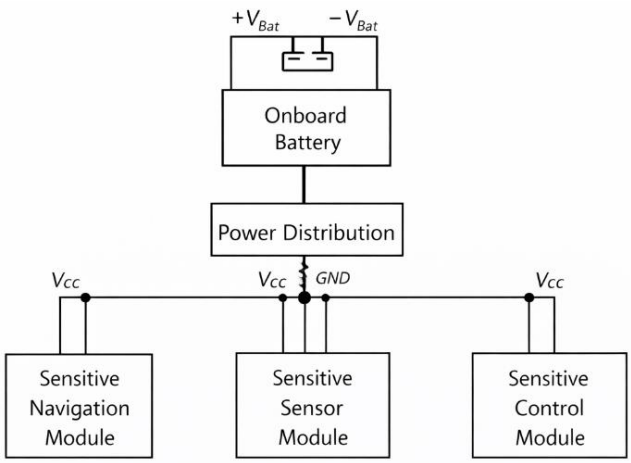

Рис. 3. Принципова схема організації зіркоподібного заземлення в бортовій електронній системі БпЛА

Для обмеження амплітуди імпульсних перенапруг і захисту чутливих електронних компонентів застосовуються демпфуючі та захисні елементи. Типова схема використання TVS-діода та RC-демпфера наведена на рис. 4.

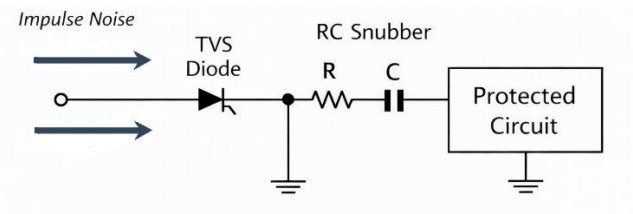

Рис. 4. Схема застосування TVS-діода та RC-ланцюга для захисту від імпульсних перенапруг у сигнальних і силових колах

Такі елементи забезпечують поглинання енергії короткочасних імпульсів і запобігають їх поширенню в суміжні функціональні блоки, що є особливо важливим для високощільних бортових систем.

Моделювання імпульсних завад та оцінка ефективності фільтрації

Моделювання виконувалося з метою оцінки ефективності пасивних і активних схем придушення завад, а також впливу топології заземлення на рівень наведень у чутливих електронних модулях. Імпульсні завади моделювалися у вигляді короткочасних перенапруг, що накладаються на шину живлення та виникають унаслідок комутаційних процесів силових перетворювачів і виконавчих механізмів [5]. Узагальнену модель поширення імпульсної завади в лініях живлення та сигналу наведено на рис. 5, де враховано паразитні опори та індуктивності провідників.

Ефективність пасивних фільтрувальних ланок досліджувалася на прикладі RC- та LC-фільтрів, включених у лінії живлення чутливих модулів (рис. 6). Результати моделювання показали, що RC-фільтри забезпечують зменшення амплітуди коротких імпульсів, проте їхня ефективність обмежується допустимим падінням напруги. LC-фільтри демонструють вищий рівень придушення високочастотних складових, однак за відсутності демпфування можуть спричиняти резонансні перехідні процеси. Моделювання активних схем подавлення завад запроваджувалося з використанням активних фільтрів другого порядку [6, 7].

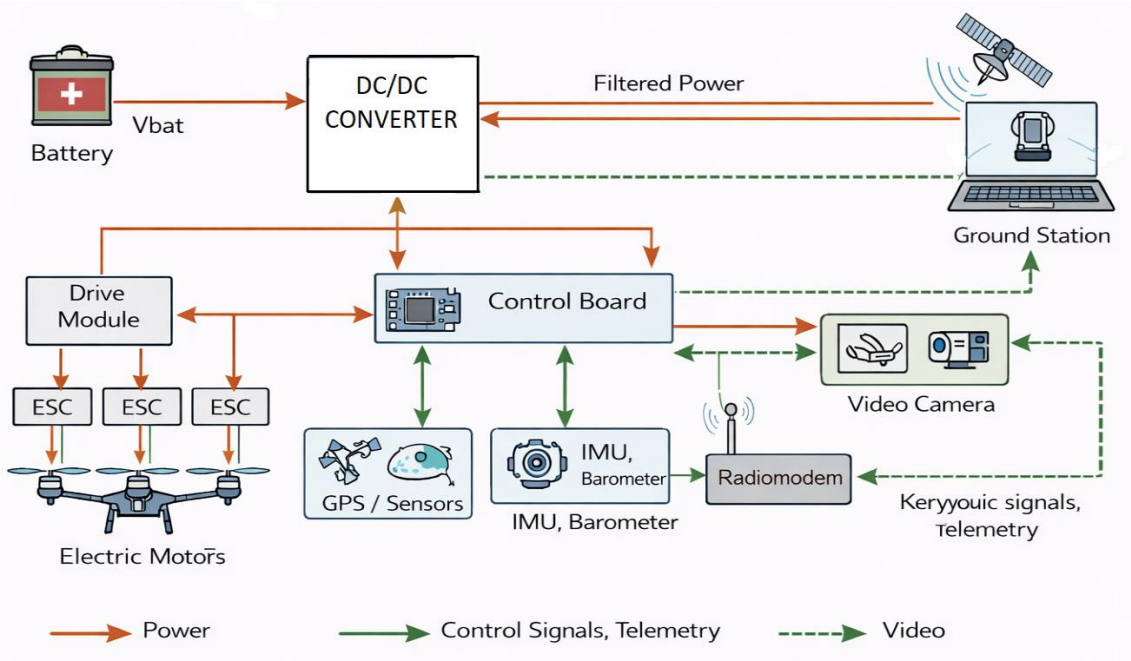

Рис. 5. Структурна схема розподілу живлення та сигналів бортової електроніки БпЛА

Встановлено, що такі схеми забезпечують суттєво більше ослаблення імпульсних перешкод у широкому частотному діапазоні, однак є чутливими до параметрів операційних підсилювачів і можуть впливати на стабільність системи в режимі реального часу [8, 9].

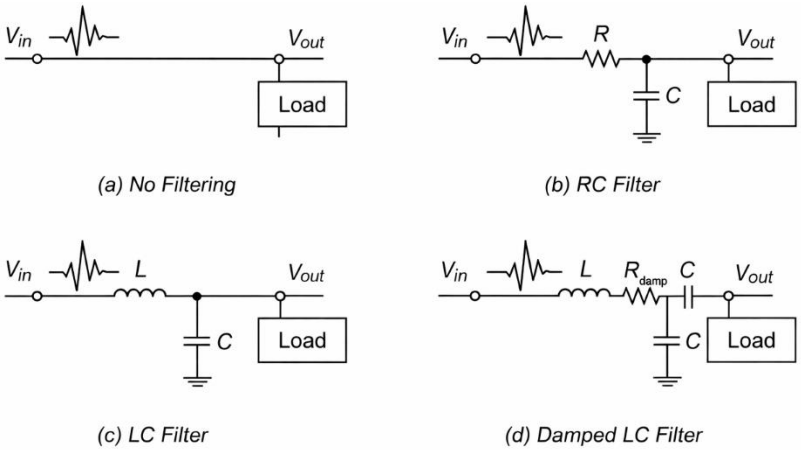

Рис. 6. Пасивні RC та LC-фільтри

Окремо досліджено вплив топології заземлення на рівень імпульсних наведень. Як показано на рис. 7, застосування зіркоподібної схеми заземлення дозволяє мінімізувати взаємний вплив між силовими та чутливими електронними модулями, зменшуючи рівень наведеної завади порівняно зі спільними заземлювальними шинами.

Захист від короткочасних перенапруг у сигнальних і силових колах моделювався з використанням TVS-діодів [10-12] та RC-ланцюгів демпфування (рис. 8). Результати підтвердили ефективність такого поєднання для обмеження амплітуди імпульсних перенапруг та зменшення швидкості фронтів завад.

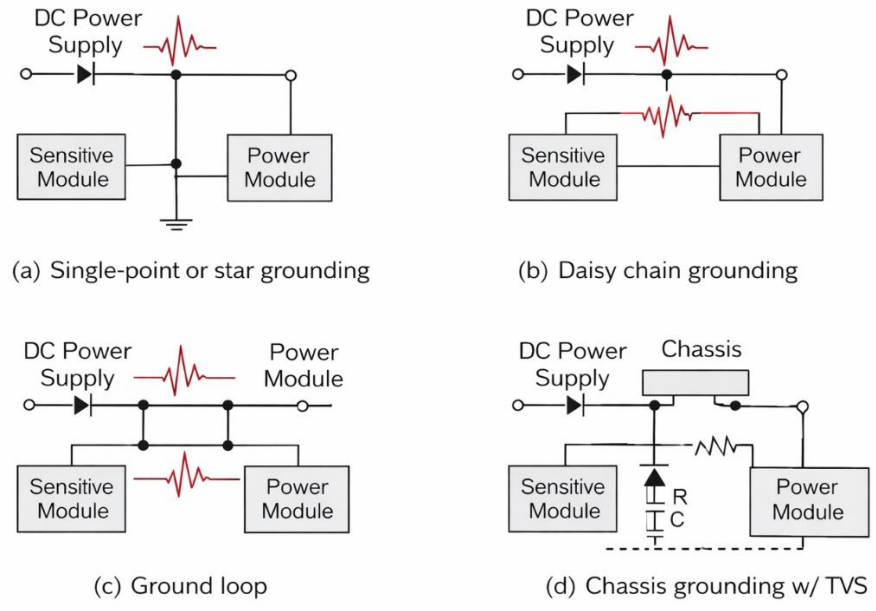

Рис. 7. Топології заземлення: (a) «зірка»; (b) «ланцюжок»;
(c) «земляна петля»; (d) шасі з TVS (плейсхолдер)

Як видно з рис. 8, у випадку відсутності фільтрації спостерігається максимальна амплітуда імпульсної завади. Перехідний процес супроводжується значними високочастотними коливаннями, що потенційно можуть призводити до порушення роботи чутливих електронних модулів.

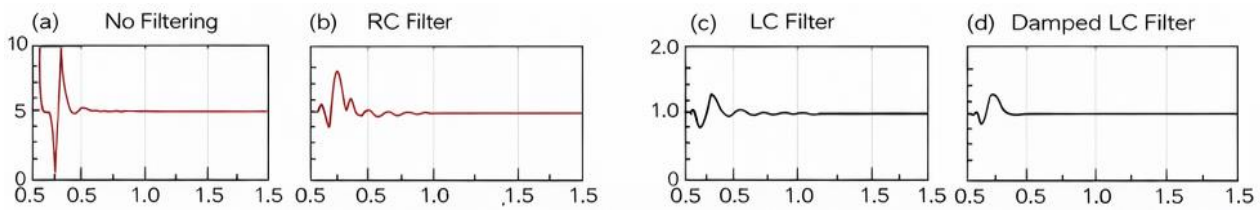

Рис. 8. Часові осцилограми сигналу:
(a) без фільтрації – максимальна амплітуда, високочастотні коливання;
(b) RC-фільтр – часткове згладжування фронтів;
(c) LC-фільтр – значне пригнічення високих частот, можливі резонансні коливання;
(d) демпфований LC – мінімальна амплітуда, скорочений час встановлення

Узагальнення результатів моделювання показує, що найбільш ефективне зменшення імпульсних завад у бортових електронних системах БпЛА досягається при комплексному застосуванні пасивної та активної фільтрації разом з оптимізованою топологією заземлення та елементами захисту від перенапруг.

Висновки

У роботі представлено підхід до схемотехнічного моделювання методів зменшення імпуль-сних завад у бортових електронних системах безпілотних літальних апаратів. За допомогою еквівалентних електричних моделей і часових симуляцій проаналізовано пасивні та активні методи придушення завад, а також вплив топології заземлення.

Результати моделювання показали, що пасивні RC-фільтри забезпечують обмежене ослаблення імпульсних завад при мінімальній складності схем, тоді як LC-фільтри демон-струють вищу ефективність, але можуть спричиняти резонансні перехідні процеси. Активні фільтри другого порядку забезпечують максимальний рівень ослаблення завад, проте потре-бують ретельного вибору параметрів для забезпечення стабільної роботи в режимі реального

часу. Також підтверджено, що застосування зіркоподібної топології заземлення суттєво зменшує взаємні наведення між силовими та чутливими електронними модулями.

Показано, що найбільш ефективне зменшення імпульсних завад у бортових електронних системах БпЛА досягається при комплексному застосуванні пасивної та активної фільтрації, оптимізованої системи заземлення та захисних елементів, таких як TVS-діоди й RC-демпфуючі ланцюги. Запропонований підхід до моделювання може бути використаний для обґрунтованого проєктування малошумних бортових електронних систем.

Список літератури:

1. X. Chang, W. Chen, Y. Yang, K. Wang and X. Yang, *Research and realization of a novel active common-mode EMI filter*, in Proc. IEEE Applied Power Electronics Conference and Exposition (APEC), 2015, pp. 1941–1945, doi: https://doi.org/10.1109/APEC.2015.7104612.

2. D. Hamza and P. K. Jain, *Conducted EMI noise mitigation in DC-DC converters using active filtering method*, in IEEE Annual Power Electronics Specialists Conference (PESC), 2008, doi: https://doi.org/10.1109/PESC.2008.4591923.

3. C.-Y. Zhuang and D.-B. Lin, *Design compact absorptive common-mode noise suppression filter with series unified circuit*, Sensors, vol. 23, no. 2, p. 957, Jan. 2023, doi: https://doi.org/10.3390/s23020957.

4. K. Mainali and R. Oruganti, *Conducted EMI mitigation techniques for switch-mode power converters: A survey*, IEEE Trans. Power Electronics, vol. 25, no. 9, pp. 2344–2356, 2010, doi: https://doi.org/10.1109/TPEL.2010.2047734.

5. Y. O. Onikienko, V. V. Pilinsky, P. V. Popovych, V. S. Lazebnyi, O. I. Smolenska and V. S. Baran, *Modelling of operation modes and electromagnetic interferences of GaN-transistor converters*, Electr. Eng. Electromech., no. 3, pp. 37–42, 2020, doi: https://doi.org/10.20998/2074-272X.2020.3.06.

6. . Sai Charishma Pathala and V. Y. Jayasree Pappu, "Elimination of CM Noise from SMPS Circuit using EMI Filter," *Int. j. elect. comput. eng. syst.*, vol. 14, no. 4, pp. 465–471, Apr. 2023. doi: https://doi.org/10.32985/ijeces.14.4.10.

7. Y. Ma, C. Feng, C. Li, L. Wang, Z. Jia, and J. Chen, "A Precise Design Method of EMI Filter Based on Compound Common-mode and Differential-mode Inductance," in *2017 2nd Int. Conf. Control, Automat. Artif. Intell. (CAAI 2017)*, Sanya, China, Jun. 25–26, 2017. Paris, France: Atlantis Press, 2017. doi: https://doi.org/10.2991/caai-17.2017.26.

8. S. Yu, N. Chen, L. Gao, H. Zhou, and Y. Huang, "Suppressing Conducted DM EMI in an Active Power Filter via Periodic Carrier Frequency Modulation," *Energies*, vol. 12, no. 10, p. 1903, May 2019. doi: https://doi.org/10.3390/en12101903.

9. G. Di Capua, N. Femia, and K. Stoyka, "Design of Differential-Mode Input Filters for DC-DC Switching Regulators," in *2019 16th Int. Conf. Synthesis, Model., Anal. Simul. Methods Appl. Circuit Des. (SMACD)*, Lausanne, Switzerland, Jul. 15–18, 2019. IEEE, 2019. doi: https://doi.org/10.1109/smacd.2019.8795273.

10. R. Goswami and S. Wang, "Modeling and Stability Analysis of Active Differential-Mode EMI Filters for AC/DC Power Converters," *IEEE Trans. Power Electron.*, vol. 33, no. 12, pp. 10277–10291, Dec. 2018. doi: https://doi.org/10.1109/tpel.2018.2806361.

11. W. Fan, Y. Shi, and Y. Chen, "A Method for CM EMI Suppression on PFC Converter Using Lossless Snubber with Chaotic Spread Spectrum," *Energies*, vol. 16, no. 8, p. 3583, Apr. 2023. doi: https://doi.org/10.3390/en16083583.

12. B. Narayanasamy and F. Luo, "Design and implementation of a novel differential mode active EMI filter with a twin circuit," in *2019 IEEE Int. Symp. Electromagn. Compat., Signal Power Integrity (EMC+SIPI)*, New Orleans, LA, USA, Jul. 22–26, 2019. IEEE, 2019. doi: https://doi.org/10.1109/isemc.2019.8825210.

Надійшла до редколегії 18.11.2024

Відомості про автора:

Бенько Тарас Григорович – асистент кафедри комп'ютерної інженерії та електроніки, Прикарпатський національний університет імені Василя Стефаника, Україна / Vasyl Stefanyk Precarpathian National University; email: taras.benko@pnu.edu.ua; ORCID: https://orcid.org/0000-0002-6310-8743

УДК 004.056.5 **DOI:10.15330/itee.2024.1.03**

М. М. ПАВЛЮК

АНАЛІЗ МЕРЕЖЕВОГО ТРАФІКУ ЯК ЗАСІБ ДЕТЕКТУВАННЯ КІБЕРЗАГРОЗ

Вступ

Розвиток широкосмугового інтернету та web-технологій спричинив значне зростання мережевого трафіку, в тому числі через активну роботу різних пристроїв, багато з яких не мають ефективного захисту від мережевих атак. Недостатній захист у мережевому просторі загрожує безпеці конфіденційної інформації, впливаючи на здоров'я, добробут та активи громадян.

Зростання кіберзагроз у зв'язку з поширенням Інтернету речей та збільшенням кількості інтернет-пристроїв зумовлює потребу в розробці ефективних програмних рішень для аналізу мережевого трафіку, здатних виявляти складні атаки та адаптуватися до нових загроз. Актуальність теми. Зростання кіберзагроз у зв'язку з поширенням Інтернету речей та збільшенням кількості інтернет-пристроїв зумовлює потребу в розробці ефективних програмних рішень для аналізу мережевого трафіку, здатних виявляти складні атаки та адаптуватися до нових загроз.

Мета роботи: дослідження сучасного стану методів виявлення кібератак через аналіз мережевого трафіку, оцінка ефективності статистичних методів та технологій машинного навчання, встановлення залежностей, що сприяють точності ідентифікації загроз у реальному часі, та розробка програмного забезпечення, що сприяє оптимізації витрат на кіберзахист.

Для досягнення мети роботи визначено наступні завдання:

- аналіз типів кіберзагроз та їх характеристик, огляд систем і алгоритмів безпеки для виявлення загроз через аналіз трафіку;
- вибір та застосування методів статистичного аналізу та машинного навчання для аналізу даних і розробка моделей виявлення кіберзагроз;
- розробка, валідація та тестування програмного забезпечення в реальному часі, включаючи оцінку якості та практичної застосовності.

Оцінка сучасного стану об'єкту дослідження. Кібербезпека активно еволюціонує з використанням штучного інтелекту та машинного навчання, включно з нейронними мережами, для ефективного аналізу мережевого трафіку та виявлення аномалій.

Світові тенденції розв'язання поставлених проблем. Глобальні методи кіберзахисту рухаються до створення гібридних систем, що інтегрують активні та пасивні методи безпеки для адаптивного реагування на кіберзагрози в реальному часі.

Дослідження базується на поєднанні статистичних методів та інструментів машинного навчання для аналізу мережевого трафіку та ідентифікації кіберзагроз. Застосовано аналіз аномалій з використанням Гаусових моделей та PCA, методи класифікації, а також рекурентні нейронні мережі та автокодувальники. Для ідентифікації складніших патернів використовуються згорткові нейронні мережі. Дослідження базується на аналізі історичних та синтетичних датасетів, зокрема UNSW-NB15 та CICIDS2017.

Системи та алгоритми безпеки, що використовують аналіз трафіку

Системи виявлення вторгнень (IDS) та системи запобігання вторгненням (IPS) є ключовими компонентами в архітектурі кібербезпеки [1].

IDS - система або програмне забезпечення, призначене для моніторингу мережі та систем на наявність зловмисних активностей чи порушень політик безпеки [1]. Вони ідентифікують підозрілі дії, відстежують мережевий трафік та системні журнали, порівнюючи їх з базою відомих атак або аномальних патернів. Після виявлення потенційного вторгнення IDS генерує сповіщення для адміністраторів мережі або безпеки.

IPS - є розширенням попереднього типу систем, яке не лише виявляє підозрілі активності, але й вживає заходів для їх блокування або запобіганнях [1]. IPS активно аналізує та фільтрує мережевий трафік на основі визначених політик безпеки та відомих підписів атак. Вони можуть автоматично відкидати пакети даних, блокувати IP-адреси атакувальної сторони або вживати інших заходів для запобігання виконання шкідливих дій у мережі.

Обидві системи є важливими для забезпечення превентивного захисту від різноманітних кіберзагроз, забезпечуючи раннє виявлення та реагування на потенційні вторгнення.

Наведемо деякі приклади статистичних моделей, моделей машинного навчання та штучних нейронних мереж, що використовуються для виконання класів задач з виявлення кіберзагроз.

Для виявлення аномалій у мережевому трафіку можна використовувати різні статистичні моделі, моделі машинного навчання та штучні нейронні мережі (рис. 1) [2, 3]. Кожен клас моделей має свої особливості та застосування.

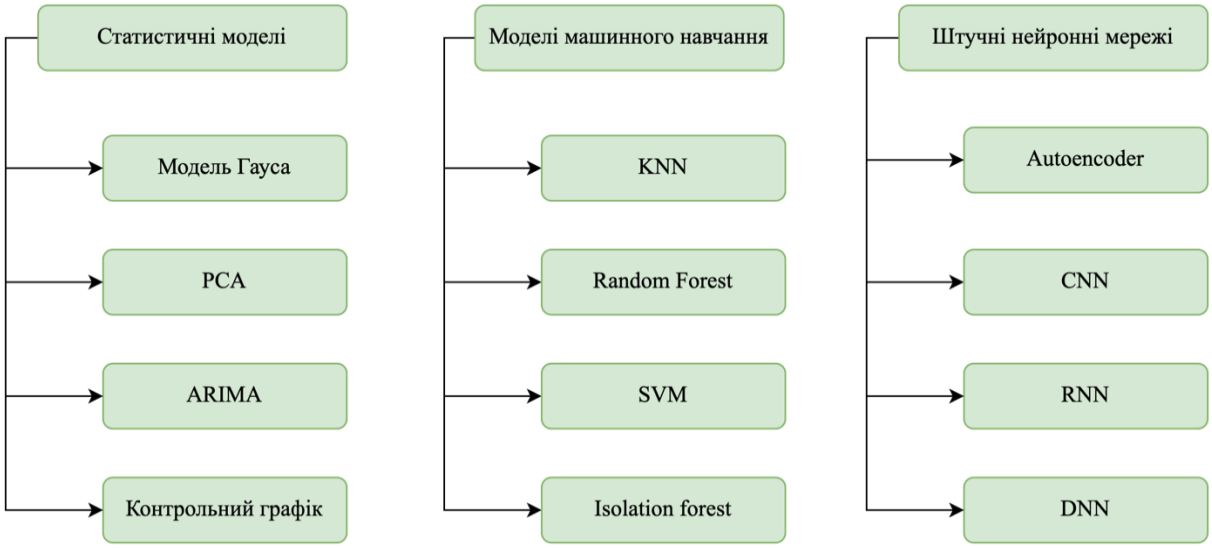

Рис. 1. Моделі аналізу трафіку (авторське опрацювання)

Кінцевою метою дослідження є створення сервісу, що інтегрується з системами фільтрації мережевих пакетів, наприклад, Iptables та Nftables, та дозволяє перейти від статичних налаштувань таких систем, до динамічних, що керуються моделями машинного навчання та штучним інтелектом. Реалізація модулів збору даних та аналізу даних з використанням ШІ доцільна у вигляді сервісів операційної системи Linux, як найбільш зручного для практичного використання варіанту. Виходячи з цього, основним завдання є створення концепції, алгоритмізація та програмна реалізація модуля штучного інтелекту, що виконує динамічні налаштування одного з UNIX-фаєрволів на базі аналізу трафіку.

Розглянуто більш детально послідовність робіт із розробки, проєктування, створення та тестування запропонованого модуля. З огляду на уже згадані статті, у яких здійснено дослідженням використання машинного навчання та штучних нейронних мереж в галузі аналізу трафіку, зроблено висновок, що дослідження проводяться в наступній послідовності (рис. 2):

а) Робота з наявними датасетами. На цьому початковому етапу використовуються доступні у відкритих джерелах датасети або такі, що надаються за запитом. Також у багатьох дослідженнях використовуються датасети, що вперше з'явились у різноманітних конкурсах науковців. Робота проводиться наступним чином:

1) проводиться попередній аналіз даних, вивчаються основні значущі ознаки та закономірності;

2) з використанням цих доступних даних будуються необхідні моделі, проводиться їх налаштування та порівняння, робляться висновки відносно доцільності та якості використання тієї чи іншої моделі;

3) проводиться більш точне налаштування та вивчення поведінки моделей, що показали найкращий результат на попередньому етапі;

б) робота з синтетичними датасетами. На цьому етапі дослідники переходять до генерування синтетичних датасетів з використанням спеціалізованого програмного забезпечення, що використовується для симуляції атак різних типів;

в) тестування створеного програмного забезпечення на тестових наборах даних та синтетичних джерелах даних про трафік, що дозволяє симулювати різноманітні типи атак ті виконувати коректність роботи програмного забезпечення у різних сценаріях використання;

г) тестування та вивчення поведінки програмного забезпечення при симулюванні атак в реальних мережах.

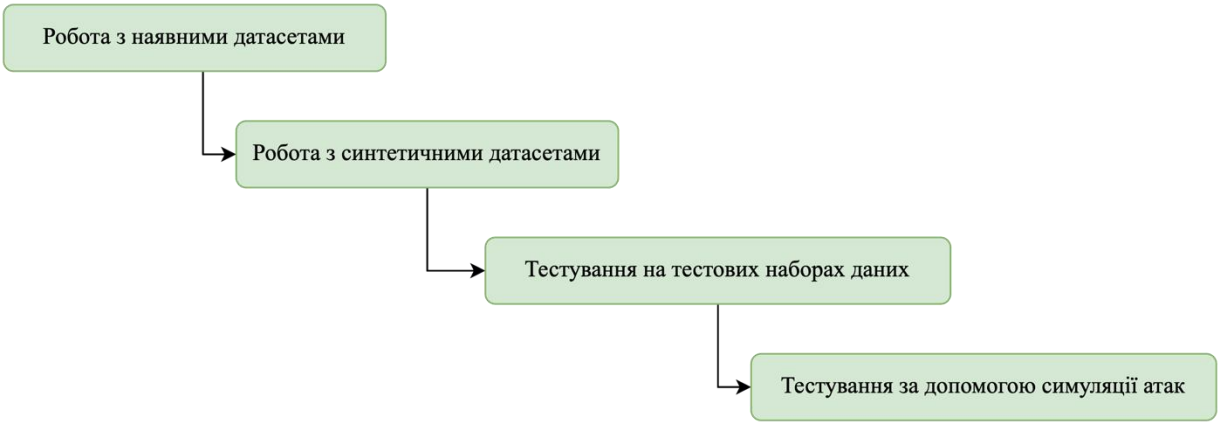

Рис. 2. Послідовність проведення дослідження (авторське опрацювання)

Проаналізовано, що численні дослідження закінчуються на етапі вивчення поведінки моделей у віртуальних середовищах чи на згенерованих датасетах, що пояснюється двома причинами:

1) спеціалізоване програмне забезпечення дозволяє створювати мережі різної топології та симулювати різні типи атак, створення яких в реальному середовищі пов'язано з чималими затратами;

2) наявні спеціалізовані датасети (історичні дані за великі періоди) містять більше патернів, змін, типів атак, аніж може симулювати дослідник у віртуальному чи реальному середовищі.

Базуючись на вище наведених міркуваннях, дослідження сплановано наступним чином:

- аналіз актуальних історичних датасетів, вибір актуального та найбільш доцільного в межах мети дослідження;
- аналіз обраного датасету з метою виділення залежностей, ранжування важливості характеристик трафіку;
- створення та тренування моделей машинного навчання та ШІ, тренування та оцінка побудованих моделей на обраному на попередніх кроках датасетові;
- тестування обраної моделі в реальному середовищі.

Дослідження наявних датасетів

Практичну частину роботи було організовано у вигляді трьох послідовних етапів: проаналізовано відкриті набори даних, здійснено моделювання атак із використанням спеціалізованого програмного забезпечення та проведено імітацію атаки в умовах реальної локальної мережі.

Опрацювання відкритих датасетів стало ключовим етапом дослідження з погляду формування та оцінювання поведінки моделей. Це дало змогу проаналізувати значні масиви зібраного мережевого трафіку, що відзначався достовірністю, різноманітністю та репрезентативністю. Завдяки цьому було виявлено особливості структури даних і закономірності, які необхідно враховувати під час побудови моделей. Використання лише спеціалізованого програмного забезпечення для симуляції атак або їх короткочасної імітації в реальному часі не дозволило б отримати настільки повний і різнорідний набір даних порівняно з інформацією, що накопичувалася дослідниками протягом тривалого часу та проходила попередню підготовку для подальшого аналізу.

Попри значний обсяг і різноманітність наявних наборів даних, було встановлено, що не всі з них відповідають цілям дослідження. Для застосування методів аналізу часових рядів будь-який датасет було попередньо трансформовано у відповідний формат. Для задач класифікації мережевого трафіку найбільш придатними було визначено KDD-99 (зокрема його модифікацію NSL-KDD), UNSW-NB15 та CAIDA DDoS Attack 2007. Для виявлення аномалій у протокольних характеристиках доцільними виявилися KDD-99 (NSL-KDD), UNSW-NB15 та CICIDS2017.

У результаті основну увагу було зосереджено на модифікованих версіях KDD-99, зокрема NSL-KDD, а також на датасеті UNSW-NB15. Додатково CAIDA DDoS Attack 2007 було використано для навчання моделей виявлення DDoS-атак, тоді як CICIDS2017 було залучено для дослідження методів пошуку аномалій.

Набір даних KDD Cup 1999 Data було розглянуто як один із базових стандартів для оцінювання систем комп’ютерної безпеки у задачах виявлення вторгнень та аналізу аномалій мережевого трафіку. Він містив широкий спектр змодельованих атак, зокрема переповнення буферів, несанкціонований доступ до даних та інші типи кібератак у контексті мережевої взаємодії. Вперше цей датасет було застосовано в межах змагання KDD Cup 1999, яке стало одним із перших масштабних заходів у галузі аналізу даних для задач кібербезпеки [4, 5].

Незважаючи на те, що контекст атак у цьому наборі даних частково втратив актуальність через розвиток сучасних методів здійснення атак, його аналіз не було проігноровано. Особливу увагу було приділено модифікованим версіям датасету, які було створено з метою усунення недоліків початкової вибірки та підвищення її збалансованості.

Датасет містив понад один мільйон унікальних записів і 42 ознаки. Цільовою змінною виступав тип атаки: було представлено 22 різновиди атак, об’єднані у чотири групи. Окремо було передбачено мітку normal, яка відповідала нормальному мережевому трафіку. Структурування атак за групами було наведено в таблиці 1.

Таблиця 1

Типи атак та їхні групи

DDoS Denial of Service	Відмова в обслуговуванні.	back, land, neptune, pod, smurf. teardrop
R2L Remote to Local	Несанкціонований доступ з віддаленого комп'ютера	ftp_write, guess_passwd, imap, multihop, phf, spy, warezclient, warezmaster
U2R User to Root	Несанкціонований доступ до привілеїв локального суперкористувача (root)	buffer_overflow, loadmodule, perl, rootkit
Probe	Спостереження та інші дослідження	ipsweep, nmap, portsweep, satan

Першими та наочними проблемами датасету є велика кількість ознак та незбалансованість класів [6, 7]. Остання ілюструється діаграмою на рис. 3.

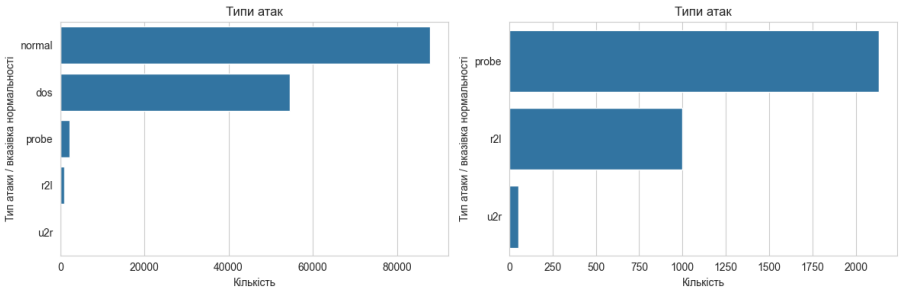

Рис. 3. Кількість атак за типами

Як модифіковану версію базового набору даних було розглянуто NSL-KDD - більш збалансовану повторну вибірку, сформовану на основі KDD-99. У цій версії було зменшено кількість дубльованих записів та приділено особливу увагу прикладам, які з високою ймовірністю могли бути неправильно класифіковані моделями, навченими на оригінальному KDD-99 [8, 9].

Разом із тим, головним обмеженням KDD-99 залишався його застарілий характер, що проявлявся у специфіці та типах атак, притаманних мережевому середовищу кінця 1990-х років. Попри це, датасет було визнано важливим етапом розвитку підходів до аналізу мережевого трафіку та оцінювання систем виявлення вторгнень.

У процесі експериментів було побудовано класифікаційні моделі на попередньо обробленому датасеті без зменшення кількості ознак. Отримані результати засвідчили високу точність роботи моделей. Порівняння основних метрик показало, що як у бінарній, так і в багатокласовій постановці задачі класифікатори продемонстрували високі значення F1-міри на тренувальних і тестових вибірках.

На підставі отриманих результатів було зроблено висновок, що подальше підвищення точності класифікації не є першочерговим завданням. В умовах обмежених обчислювальних ресурсів більш актуальною виявилася проблема забезпечення високої швидкодії алгоритмів.

У зв’язку з цим акцент у роботі було зміщено на оптимізацію використання ресурсів, зокрема на зменшення обчислювальної складності моделей за мінімальної втрати точності прогнозування. Одним із підходів до досягнення цієї мети було застосування методів зниження розмірності простору ознак.

Проведений аналіз головних компонент продемонстрував, що внесок окремих ознак у процес класифікації є нерівномірним. Результати застосування методу PCA представлено на рис. 4.

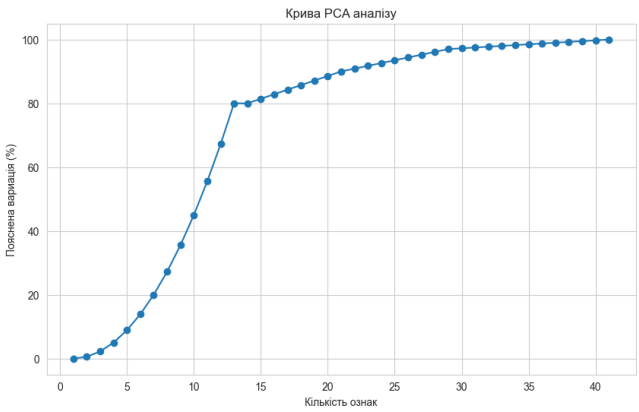

Рис. 4. Аналіз головних компонент

Зменшення кількості ознак дозволило підвищити швидкість обробки даних, що є критично важливим для систем, орієнтованих на функціонування в режимі реального часу.

Другим ключовим набором даних було визначено UNSW-NB15, розроблений Університетом Нового Південного Уельсу (Австралія) для задач виявлення вторгнень і аналізу мережевого трафіку. Цей датасет охоплював сучасніші типи атак і приклади нормального трафіку, що зробило його доцільним для побудови та тестування моделей детекції.

Водночас було враховано й певні обмеження UNSW-NB15, серед яких - відносно менша різноманітність атак, недостатня документованість окремих аспектів формування вибірки та проблеми зі збалансованістю класів. З огляду на це його не було використано як єдину основу для навчання моделей, а застосовано у поєднанні з іншими наборами даних, визначеними в межах цього розділу.

Проєктування архітектури системи та інфраструктури обробки даних

Під час розроблення системи було враховано суперечливі вимоги до обчислювальних ресурсів. З одного боку, алгоритми машинного навчання та нейронні мережі потребували значної обчислювальної потужності, особливо при роботі з великими таблицями даних, що містили сотні тисяч записів і десятки ознак. З іншого боку, практична придатність створеного програмного забезпечення безпосередньо залежала від його ресурсоємності: чим нижчими були вимоги до апаратного забезпечення, тим ширшими ставали можливості його застосування.

У зв’язку з цим було розмежовано три основні процеси:

1) збирання та підготовку даних для навчання моделей (включно з використанням великих відкритих датасетів);

2) безпосереднє навчання моделей;

3) експлуатацію вже навчених моделей у реальному середовищі.

Для організації потокового збору даних та опрацювання наявних датасетів було розгорнуто кластер на базі Apache Spark із використанням Spark Streaming та Hadoop. Навчання моделей і глибокий аналіз даних було виконано із залученням хмарних сервісів Google, що дозволило використовувати графічні процесори для обчислень у випадках, коли це було технічно доцільно. Зокрема, TensorFlow було орієнтовано на використання GPU, тоді як Scikit-learn та XGBoost переважно використовували ресурси центрального процесора.

Для тестування програмного забезпечення з інтегрованими навченими моделями було застосовано одноплатний комп’ютер Raspberry Pi 4 з 4 ГБ оперативної пам’яті та тактовою частотою процесора 1,5 ГГц, що дозволило оцінити можливість роботи системи на пристроях обмеженої потужності.

Реалізована система збору та обробки мережевого трафіку складалася з таких компонентів (рис. 5):

1) Filebeat і Fluentd - як агенти збору журналів подій із серверів, маршрутизаторів і міжмережевих екранів;

2) Apache Kafka - для централізованого приймання потокових даних від агентів;

3) Spark Streaming - для агрегації, попередньої обробки та фільтрації потоку даних;

4) Hadoop Distributed File System (HDFS) - для зберігання накопиченої інформації;

5) Apache Spark - для подальшого аналізу даних і формування вибірок для навчання математичних моделей та нейронних мереж;

6) Apache ZooKeeper - для координації та синхронізації роботи компонентів кластера.

Запропонована архітектура була доцільною у випадках збору власних даних або обслуговування локальної мережі, що включала понад 10 комп’ютерів і характеризувалася інтенсивним та різнорідним трафіком. Використання такого кластера забезпечувало не лише централізований моніторинг, а й можливість періодичного донавчання моделей на оновлених даних.

Як альтернативний сценарій було розглянуто використання програмного забезпечення з уже навченими моделями на малопотужних пристроях. Для цього варіанта було визначено мінімальний часовий інтервал аналізу (вікно спостереження), який становив приблизно 60 секунд. Було встановлено, що обсяг даних, накопичений за цей період, є достатнім для виявлення короткотривалих атак, зокрема DDoS-активності.

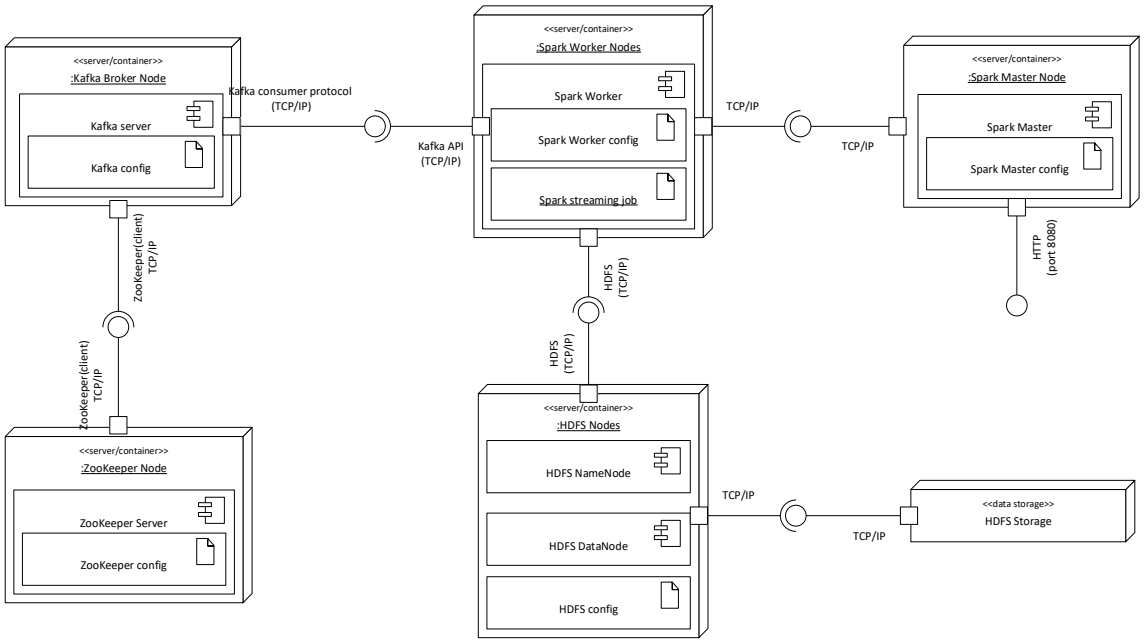

Рис. 5. Схема кластеру збору даних

Розроблене рішення відрізняється комплексним підходом, що інтегрує аналіз аномалій та класифікацію трафіку в одній системі, використовуючи машинне навчання для адаптації до нових загроз. Відмінність від традиційних IDS/IPS-систем полягає в поєднанні статистичних, поведінкових моделей та автокодувальників з CNN для виявлення як відомих, так і нових загроз. Рішення автоматично оновлює правила фаєрвола, адаптуючись до мережевих умов і знижуючи потребу в ручному налаштуванні, що робить його придатним для малих підприємств та IoT систем. Воно також стійке до загроз, орієнтованих на обхід стандартних захисних механізмів, забезпечуючи виявлення прихованих кіберзагроз.

Розроблене програмне рішення з відкритим кодом та низькими системними вимогами, що робить його доступним для малих підприємств та IoT систем, з можливістю спільноти вносити покращення завдяки MIT ліцензії. Програмне забезпечення пройшло тестування та дослідну експлуатацію в локальному тестовому середовищі та в тестовій локальній мережі. Розроблене рішення не потребує комерційних ліцензій та знижує витрати на відновлення після атак завдяки швидкому виявленню та блокуванню загроз, що робить його економічно привабливим. Запропоноване рішення для виявлення кіберзагроз надає ефективний та доступний інструмент захисту мережевого простору. Використання сучасних методів машинного навчання та аналізу аномалій сприяє зниженню хибнопозитивних спрацювань та стимулює спільноту спеціалістів до постійного вдосконалення системи.

Подальший розвиток передбачає вдосконалення алгоритмів класифікації, вдосконалення та збільшення різноманітності навчальних датасетів, що застосовуються в роботі, а також тестування в умовах реальних загроз. Можлива також інтеграції з системами інтелектуального аналізу поведінки.

Висновки

У ході дослідження було розроблено та апробовано методи й алгоритми виявлення кіберзагроз на основі аналізу мережевого трафіку із застосуванням підходів штучного інтелекту та машинного навчання. Отримані результати підтвердили їх високу ефективність у задачах детектування атак.

Проведені експерименти показали, що моделі забезпечували високі показники точності класифікації. Водночас в умовах обмежених обчислювальних ресурсів ключовим фактором стала не стільки подальша оптимізація точності, скільки підвищення швидкодії обробки даних. У зв'язку з цим акцент було зміщено на оптимізацію обчислювальних процесів із мінімальною втратою якості прогнозування.

Основним напрямом такої оптимізації визначено зменшення обчислювальної складності моделей, що дозволило забезпечити оперативну обробку значних обсягів трафіку та своєчасне реагування на потенційні загрози. З цією метою було застосовано методи зниження розмірності даних, зокрема аналіз головних компонент (PCA), що сприяло скороченню кількості ознак без істотного погіршення результатів класифікації.

Розроблене програмне забезпечення було орієнтовано на функціонування в режимі реального часу та адаптацію до змінних умов мережевого середовища. Такий підхід забезпечив можливість його використання для захисту як серверних систем, так і пристроїв із обмеженими ресурсами, підвищуючи загальний рівень стійкості мережі до кібератак

Список літератури:

1. D. Regalado, S. Harris, A. Harper, C. Eagle, J. Ness, B. Spasojevic, R. Linn та S. Sims, Gray Hat Hacking The Ethical Hacker's Handbook, Fourth Edition, McGraw Hill, 2022.
2. A. Divekar, M. Parekh, V. Savla, R. Mishra, and M. Shirole, "Benchmarking datasets for Anomaly-based Network Intrusion Detection: KDD CUP 99 alternatives," in *2018 IEEE 3rd Int. Conf. Comput., Communication Secur. (ICCCS)*, Kathmandu, Oct. 25–27, 2018. IEEE, 2018. doi: https://doi.org/10.1109/cccs.2018.8586840.
3. P. Singh, J. J. P, A. Pankaj, and R. Mitra, "Edge-Detect: Edge-Centric Network Intrusion Detection using Deep Neural Network," in *2021 IEEE 18th Annu. Consum. Commun. Netw. Conf. (CCNC)*, Las Vegas, NV, USA, Jan. 9–12, 2021. IEEE, 2021. doi: https://doi.org/10.1109/ccnc49032.2021.9369469.
4. T. Chen and C. Guestrin, "XGBoost," in *KDD '16: 22nd ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, San Francisco California USA. New York, NY, USA: ACM, 2016. doi: https://doi.org/10.1145/2939672.2939785.
5. T. Hu and T. Song, "Research on XGboost academic forecasting and analysis modelling," *J. Phys.: Conf. Ser.*, vol. 1324, p. 012091, Oct. 2019. doi: https://doi.org/10.1088/1742-6596/1324/1/012091.
6. M. R. Machado, S. Karray, and I. T. de Sousa, "LightGBM: an Effective Decision Tree Gradient Boosting Method to Predict Customer Loyalty in the Finance Industry," in *2019 14th Int. Conf. Comput. Sci. Educ. (ICCSE)*, Toronto, ON, Canada, Aug. 19–21, 2019. IEEE, 2019. doi: https://doi.org/10.1109/iccse.2019.8845529.
7. W. Richert та L. P. Coelho, Building Machine Learning Systems with Python, Packt, 2013.
8. T. T. Teoh and Z. Rong, *Artificial Intelligence with Python*. Singapore: Springer Singap., 2022. doi: https://doi.org/10.1007/978-981-16-8615-3.
9. H. Jones, An Essential Beginners Guide to Artificial Neural Networks and Their Role in Machine Learning and Artificial Intelligence, CreateSpace Independent Publishing Platform, 2018.

Надійшла до редколегії 26.11.2024

Відомості про автора:

Павлюк Михайло Михайлович – студент кафедри комп'ютерних наук та інформаційних систем, Прикарпатський національний університети імені Василя Стефаника / Vasyl Stefanyk Precarpathian National University, Україна, email: pavliuk.mykhailo.dev@gmail.com; ORCID: https://orcid.org/0009-0002-1072-1912

УДК 004.67 **DOI:10.15330/itee.2024.1.04**

В.І. ГОЛОТА, канд. техн. наук, В.О. ПОЛІНЯЄВ, В.В. МАРТИНЮК

МЕТОДИ БАГАТОРІВНЕВОГО АНАЛІЗУ ЕЛЕКТРОКАРДІОГРАФІЧНИХ СИГНАЛІВ ІЗ ЗАСТОСУВАННЯМ ВЕЙВЛЕТ-ПЕРЕТВОРЕНЬ

Вступ

У статті представлено розробку програмного комплексу для цифрової обробки та автоматизованої класифікації сигналів електрокардіограм (ЕКГ). Використано методи вейвлет-перетворення для формування спектрограм та згорткові нейронні мережі для класифікації сигналів. Розглянуто архітектуру системи, алгоритми обробки даних, інтерфейс користувача, а також методи оцінки ефективності програмного продукту [1-4]. Проведено порівняльний аналіз варіантів реалізації основних функцій із обґрунтуванням вибору оптимальних технічних рішень. Результати демонструють високий рівень точності та надійності системи, що підтверджує її готовність до використання в клінічній практиці.

Вимоги та функціональні можливості системи

Розроблена система передбачає виконання ключових функцій: завантаження даних ЕКГ конкретного пацієнта, відображення сигналу на екрані та автоматизовану класифікацію із відображенням результатів аналізу. Основні вимоги до програмного продукту включають здатність коректно обробляти сигнали ЕКГ різної тривалості та формату, відображати спектрограм, що дозволяє візуально оцінити динаміку серцевого циклу; надавати лікарю можливості записувати виявлений діагноз поряд із автоматично визначеним результатом та зберегти результатів обробки для подальшого аналізу та формування історії пацієнта.

Блок-схема роботи програми показана на рис. 1.

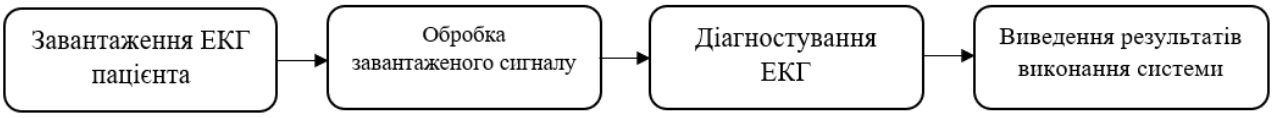

Рис. 1. Блок-схема робота системи

На схемі видно послідовність дій від завантаження ЕКГ до обробки сигналу та збереження результатів у базі даних. Така організація процесу дозволяє ефективно інтегрувати систему у клінічну практику та мінімізує ймовірність помилок при введенні даних. Архітектура системи продемонстрована на рис. 2.

Початковий сигнал ЕКГ є одновимірним часовим рядом. Для ефективного аналізу його необхідно перетворити у двовимірну частотно-часову форму [5]. У роботі використано неперервне вейвлет-перетворення, що дозволяє створювати спектрограми з характерними ознаками для здорових та патологічних станів серця (рис.3).

Для кожного пацієнта розглядаються три основні серцеві відведення, що дозволяє оцінити різні аспекти електричної активності серця. Три спектрограми накладаються в одне зображення з трьома каналами, яке подається на вхід згорткової нейронної мережі (рис.4).

Цей підхід дозволяє одночасно аналізувати всі основні відведення, що підвищує точність розпізнавання сигналів різних патологій [6].

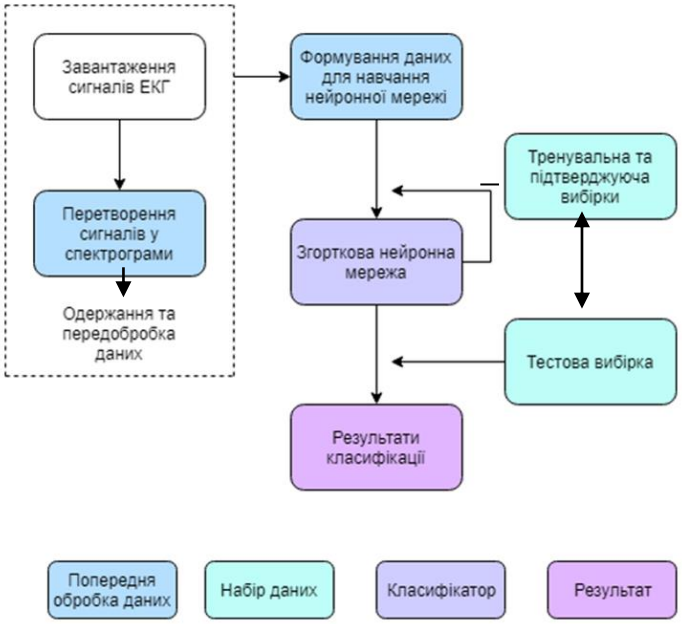

Рис. 2. Архітектура системи та алгоритми обробки сигналів

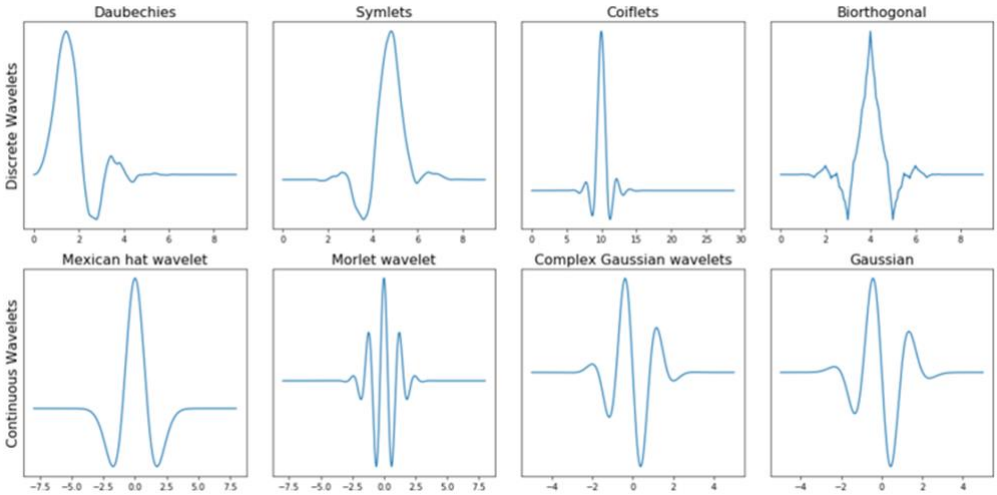

Рис. 3. Види сигналів ЕКГ вейлвлетів

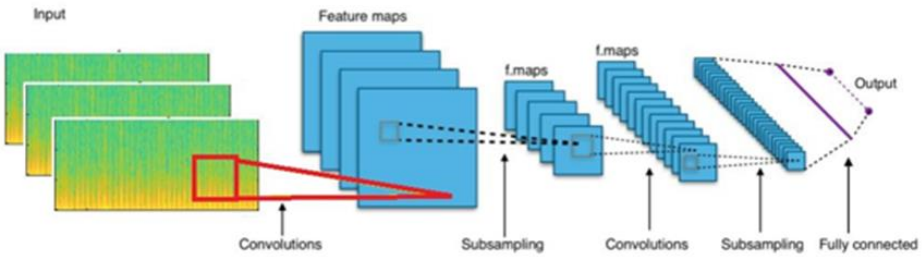

Рис. 4. Формування триканального зображення

Згорткова нейронна мережа складається з послідовних згорткових та підсумовуючих шарів, завершуючись повнозв'язним та вихідним шаром для класифікації сигналів (рис.5).

Така архітектура забезпечує здатність виділяти характерні ознаки сигналів та високий рівень точності класифікації.

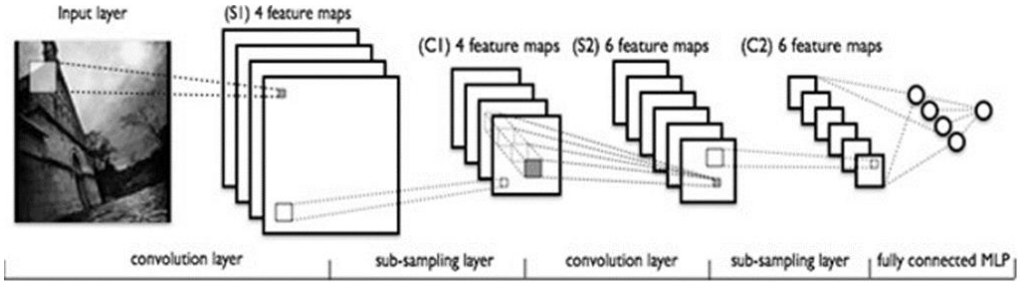

Рис. 5. Архітектура CNN

Оцінка роботи мережі показала високі результати: точність класифікації склала 92%, специфічність – 90%, чутливість – 94%. Це підтверджує правильність обраної архітектури та параметрів навчання.

Інтерфейс реалізовано із застосуванням бібліотеки Qt. Головне вікно програми містить кнопку «Завантажити ЕКГ», яка відкриває сигнал пацієнта з трьома основними відгалуженнями. Після завантаження відображаються дані пацієнта: ПІБ, вік та дата дослідження, що забезпечує зручність роботи з медичними даними.

Натискання кнопки «Обробити ЕКГ» активує алгоритм цифрової обробки сигналу та класифікації [7, 8]. На екрані з'являється ймовірний діагноз, який може бути доповнений власним висновком лікаря. Після підтвердження результатів користувач може зберегти їх у базі даних та обробити новий сигнал без перезапуску програми (рис.6).

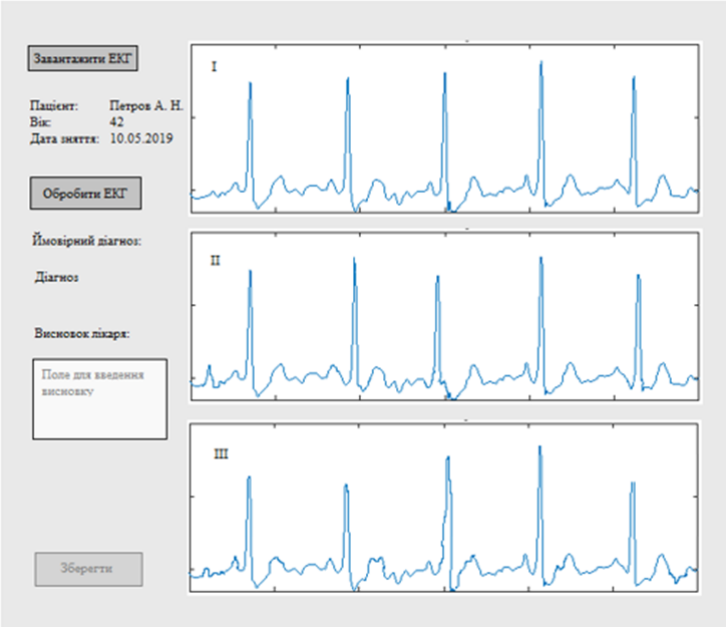

Рис. 6. Дані пацієнта та результат аналізу

Такий підхід забезпечує інтеграцію автоматизованого аналізу з професійною оцінкою лікаря, що підвищує надійність діагностики.

Для оцінки програмного продукту використано функціонально-вартісний аналіз (ФВА), що дозволяє визначити оптимальні технічні рішення та раціонально використовувати ресурси (рис.7). Основні функції системи включають вибір мови програмування, методу обробки сигналів, методу класифікації та технології інтерфейсу.

Рис. 7. Морфологічна карта програмного продукту

Аналіз варіантів реалізації функцій показав, що оптимальні комбінації включають Python для обчислень, перетворення Фур'є для обробки сигналів, CNN для класифікації та сучасний графічний інтерфейс (рис.8). Всі показники системи за швидкодією, обсягом пам'яті, часом обробки та обсягом коду відповідають вимогам [9, 10].

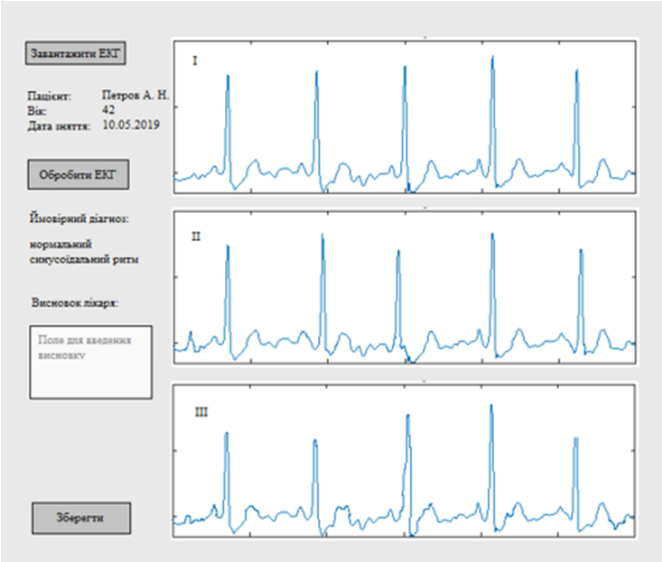

Рис. 8. Графічна оцінка параметрів

Експертне оцінювання параметрів проведено методом попарного порівняння, коефіцієнт узгодженості W=0,75 підтверджує достовірність результатів. Порівняльний аналіз показав, що обрана комбінація варіантів реалізації забезпечує максимальну якість та ефективність продукту.

Висновки

Розроблено програмний комплекс для цифрової обробки та автоматизованої класифікації сигналів ЕКГ із високою точністю. Використання вейвлет-перетворення та CNN дозволяє виділяти характерні ознаки сигналів, а зручний графічний інтерфейс забезпечує ефективність роботи користувачів. Економічне обґрунтування та експертна оцінка підтверджують раціональність обраної архітектури та технологій. Програмний продукт готовий до впровадження у клінічну практику для підтримки прийняття рішень при діагностиці серцево-судинних захворювань

Список літератури:

1. Mnevets, A.V., & Ivanushkina, N.G., "Neural Networks Detection of Low-Amplitude Components on ECG Using Modified Wavelet Transform," Visnyk NTUU KPI Seriia - Radiotekhnika Radioaparatobuduvannia, no. 97, pp. 46–57, 2024. doi: https://doi.org/10.20535/RADAP.2024.97.46-57
2. Software for Statistical Processing and Modeling of a Set of Synchronously Registered Cardio Signals of Different Physical Nature / S. Lupenko et al. Computer Modeling and Intelligent Systems. 2021. Vol. 2864. P. 194–205. doi: https://doi.org/10.32782/cmis/2864-17.
3. Dzundza, B.S., Kohut, I.T., Holota, V.I., Fedoriuk, V.V., & Nykyruy, L.I., "Principles of Construction of Hybrid Microsystems for Biomedical Applications," Physics and Chemistry of Solid State, vol. 23, no. 4, pp. 776–784, 2022. doi: https://doi.org/10.15330/pcss.23.4.776-784.
4. Electrocardiogram Classification Using Wavelet Transformations / I. Krak et al. 2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), Lviv-Slavske, Ukraine, 25–29 February 2020. 2020. doi: https://doi.org/10.1109/tcset49122.2020.235573.
5. Lee J.-A., Kwak K.-C. Heart Sound Classification Using Wavelet Analysis Approaches and Ensemble of Deep Learning Models. Applied Sciences. 2023. Vol. 13, no. 21. P. 11942. doi: https://doi.org/10.3390/app132111942.
6. Modeling of integrated signal converters for biomedical sensor microsystems / I. T. Kogut et al. Physics and Chemistry of Solid State. 2023. Vol. 24, no. 3. P. 515–519. doi: https://doi.org/10.15330/pcss.24.3.515-519.
7. Electrocardiographic signal analysis using wavelet transforms / G. S. Kumari et al. 2015 International Conference on Electrical, Electronics, Signals, Communication and Optimization (EESCO), Visakhapatnam, 24–25 January 2015. 2015. doi: https://doi.org/10.1109/eesco.2015.7253688.
8. Cyber-physical System for Monitoring and Analyzing Human Biomedical Data / I. Kogut et al. Advances in Cyber-Physical Systems. 2024. Vol. 9, no. 1. P. 32–38. doi: https://doi.org/10.23939/acps2024.01.032.
9. Darsana P., Kumar V. N. Extracting Fetal ECG Signals through a Hybrid Technique Utilizing Two Wavelet-Based Denoising Algorithms. IEEE Access. 2023. P. 1. doi: https://doi.org/10.1109/access.2023.3308409.
10. Mostovoy Y. M., Danilevych T. D. Predictors of heart rhythm disorders in the patients with severe COVID-infection. Reports of Vinnytsia National Medical University. 2020. Vol. 24, no. 4. P. 640–646. URL: https://doi.org/10.31393/reports-vnmedical-2020-24(4)-14.

Надійшла до редколегії 20.11.2024

Відомості про авторів:

Голота Віктор Іванович - кандидат технічних наук, доцент кафедри комп'ютерної інженерії та електроніки, Прикарпатський національний університети імені Василя Стефаника / Vasyl Stefanyk Precarpathian National University, Україна; email: viktor.holota@pnu.edu.ua, ORCID: https://orcid.org/0000-0003-4605-7507.

Поліняєв Владислав Олегович - магістрант кафедри комп'ютерної інженерії та електроніки, Прикарпатський національний університети імені Василя Стефаника / Vasyl Stefanyk Precarpathian National University, Україна; email: vladyslav.poliniaev.20@pnu.edu.ua ORCID: https://orcid.org/0009-0001-7413-0751.

Мартинюк Віталій Васильович – магістрант кафедри комп'ютерної інженерії та електроніки, Прикарпатський національний університети імені Василя Стефаника / Vasyl Stefanyk Precarpathian National University, Україна; email: vitalii.martyniuk.20@pnu.edu.ua, ORCID: https://orcid.org/0009-0001-4310-6302.

ABSTRACTS

РЕФЕРАТИ

ELECTRONICS, ELECTRONIC COMMUNICATIONS, INSTRUMENTATION AND RADIO ENGINEERING

ЕЛЕКТРОНІКА, ЕЛЕКТРОННІ КОМУНІКАЦІЇ, ПРИЛАДОБУДУВАННЯ ТА РАДІОТЕХНІКА

UDC 621.383

Application of a high-precision MPPT controller for thin-film cadmium telluride photovoltaic devices / *V.Y. Fedenko, B.S. Dzundza, I.B. Hatala* // Information Technologies and Engineering Electronics : Scientific journal, 2024, №1, P. 7-10.

The paper presents the concept of an MPPP controller capable of working with thin-film cadmium telluride photoconverters to study the stability of samples in real conditions. The parameters of photocells based on CdTe/CdS/ITO and CdTe/CdS/ZnO heterostructures were obtained during modeling in SCAPS 1D. To find the MPP, the well-known Incremental Conductance method was used, which is configured to work with low-power photoconverters.

Key words: computer simulation, CdTe, solar cell, renewable energy, MPPT algorithm.

2 tabl. 3 fig. Ref: 8 items.

УДК 621.383

Особливості застосування високоточного MPPT контролера для тонкоплівкових фотоперетворювачів телуриду кадмію / *В.Я. Феденько, Б.С. Дзундза, І.Б. Гатала* // Інформаційні технології та інженерна електроніка : Науковий журнал, 2024, №1, С. 7-10.

У роботі представлено концепцію MPPP контролера здатного працювати зі зразками тонкоплівкових фотоперетворювачів телуриду кадмію для дослідження стабільності зразків в реальних умовах. Параметри фотоелементів на основі гетероструктур CdTe/CdS/ITO та CdTe/CdS/ZnO отримано під час моделювання у SCAPS 1D. Для пошуку MPP застосовано відомий методом Incremental conductance, який налаштований для роботи з фотоперетворювачами низької вихідної потужності.

Ключові слова: комп'ютерне моделювання, CdTe, сонячний елемент, відновлювана енергетика, алгоритм MPPT.

Табл. 2. Іл. 3. Бібліогр.: 8 назв.

UDC 621.374

Circuit engineering methods for reducing impulse interference in on-board electronic systems of unmanned aerial vehicles / *T.G. Benko* // Information Technologies and Engineering Electronics : Scientific journal, 2024, №1, P. 11-16.

In the onboard electronic systems of unmanned aerial vehicles, pulsed electromagnetic interference is one of the main factors limiting the reliability and accuracy of the operation of navigation, sensor and control subsystems. The sources of such interference are power electronic converters, electric motors, pulsed voltage regulators and switching processes in the on-board power supply network. Pulsed interference can lead to signal distortion, a decrease in the signal-to-noise ratio and a violation of the stability of the operation of electronic modules, especially in real-time conditions.

This paper considers circuit engineering methods for reducing pulsed interference in the onboard electronic systems of unmanned aerial vehicles. An approach to modeling the main sources of pulsed interference and their propagation in electronic circuits is proposed, taking into account the real parameters of the components. The effectiveness of passive and active interference suppression schemes, in particular RC and LC filters, active filters on operational amplifiers, as well as local resolution and power stabilization schemes, is analyzed.

The study was performed using circuit modeling, which allowed us to assess the influence of circuit parameters on the level of impulse interference, spectral characteristics of noise and stability of electronic systems. The results obtained demonstrate the possibility of significantly reducing the amplitude of impulse interference and improving the noise characteristics of UAV onboard electronics without increasing delays and computational complexity. The proposed methods can be used in the design of reliable and low-noise electronic systems of unmanned aerial vehicles.

Key words: unmanned aerial vehicles, onboard electronics, impulsive interference, circuit-level methods, noise suppression, interference filtering, real-time systems.

8 fig. Ref: 12 items.

УДК 621.374

Схемотехнічні методи зменшення імпульсних завад у бортових електронних системах безпілотних літальних апаратів / *Т.Г. Бенько* // Інформаційні технології та інженерна електроніка : Науковий журнал, 2024, №1, С. 11-16.

У бортових електронних системах безпілотних літальних апаратів імпульсні електромагнітні завади є одним з основних чинників, що обмежують надійність і точність роботи навігаційних, сенсорних та керувальних підсистем. Джерелами таких завад є силові електронні перетворювачі, електродвигуни, імпульсні регулятори напруги та комутаційні процеси у бортовій мережі живлення. Імпульсні завади можуть призводити до спотворення сигналів, зниження відношення сигнал/шум та порушення стабільності роботи електронних модулів, особливо в умовах реального часу.

У даній роботі розглянуто схемотехнічні методи зменшення імпульсних завад у бортових електронних системах безпілотних літальних апаратів. Запропоновано підхід до моделювання основних джерел імпульсних завад та їх поширення в електронних колах з урахуванням реальних параметрів компонентів. Проаналізовано ефективність пасивних та активних схем придушення завад, зокрема RC- та LC-фільтрів, активних фільтрів на операційних підсилювачах, а також схем локального розв’язування та стабілізації живлення.

Дослідження виконано з використанням схемотехнічного моделювання, що дозволило оцінити вплив параметрів схем на рівень імпульсних завад, спектральні характеристики шуму та стабільність роботи електронних систем. Отримані результати демонструють можливість суттєвого зменшення амплітуди імпульсних завад і покращення шумових характеристик бортової електроніки БпЛА без збільшення затримок та обчислювальної складності. Запропоновані методи можуть бути використані при проєктуванні надійних і малошумних електронних систем безпілотних літальних апаратів.

Ключові слова: безпілотні літальні апарати, бортова електроніка, імпульсні завади, схемотехнічні методи, придушення шуму, фільтрація завад; системи реального часу.

Іл. 8. Бібліогр.: 12 назв.

COMPUTER SCIENCE

КОМП’ЮТЕРНІ НАУКИ

UDC 004.056.5

Analysis of network traffic as a means of cyber threat detection / *M.M. Pavliuk* // Information Technologies and Engineering Electronics : Scientific journal, 2024, №1, P. 17-24.

The work presents methods and algorithms for detecting cyber threats based on network traffic analysis using machine learning and artificial intelligence techniques. The study evaluates statistical analysis, ensemble models, and neural networks for identifying anomalies and unusual behavior patterns. Emphasis is placed on optimizing computational efficiency while maintaining prediction accuracy. A real-time system architecture for data collection and analysis is proposed.

Key words: cybersecurity, network traffic, intrusion detection; machine learning, neural networks, anomaly detection, PCA, dimensionality reduction, real-time processing, IoT.

5 fig. Ref: 9 items.

УДК 004.056.5

Аналіз мережевого трафіку як засіб детектування кіберзагроз / *М.М. Павлюк* // Інформаційні технології та інженерна електроніка : Науковий журнал, 2024, №1, С. 17-24.

У роботі розглянуто методи та алгоритми виявлення кіберзагроз на основі аналізу мережевого трафіку з використанням машинного навчання та штучного інтелекту. Проведено оцінку ефективності статистичних методів, ансамблевих моделей і нейронних мереж для ідентифікації аномалій та нестандартних поведінкових патернів. Основну увагу приділено оптимізації обчислювальних процесів при збереженні точності прогнозування. Запропоновано архітектуру системи збору та обробки даних у режимі реального часу.

Ключові слова: кібербезпека, мережевий трафік, виявлення вторгнень, машинне навчання, нейронні мережі, аномалії, PCA, зниження розмірності, обробка даних у реальному часі, IoT.

Іл. 5. Бібліогр.: 9 назв.

COMPUTER ENGINEERING

КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

UDC 004.67

Methods of multilevel analysis of electrocardiographic signals using wavelet transforms / *V.I. Holota, V.O. Polinyayev, V.V. Martyniuk* // Information Technologies and Engineering Electronics : Scientific journal, 2024, №1, P. 25-29.

The article presents the analyze and development of a software system for digital processing and automated classification of electrocardiogram (ECG) signals using artificial intelligence methods. It demonstrates the creation of ECG spectrograms with wavelet transforms and the application of a three-channel convolutional neural network for accurate pathology recognition. The system architecture, user interface, and workflow are described. Performance evaluation and comparative analysis of technical solutions confirm the reliability, efficiency, and practical applicability of the developed system for clinical use.

Key words: electrocardiogram, ECG, digital signal processing, convolutionary neural networks, machine learning, deep neural models.

8 fig. Ref: 10 items.

УДК 004.67

Методи багаторівневого аналізу електрокардіографічних сигналів із застосуванням вейвлет-перетворень / *В.І. Голота, В.О. Поліняєв, В.В. Мартинюк* // Інформаційні технології та інженерна електроніка : Науковий журнал, 2024, №1, С. 25-29.

У статті представлено аналіз та розробку програмного комплексу для цифрової обробки та автоматизованої класифікації сигналів електрокардіограм (ЕКГ) із застосуванням методів штучного інтелекту. Показано створення спектрограм ЕКГ за допомогою вейвлет-перетворення та застосування триканальної згорткової нейронної мережі для точного розпізнавання патологій. Описано архітектуру системи, інтерфейс користувача та робочий процес. Оцінка продуктивності та порівняльний аналіз технічних рішень підтверджують надійність, ефективність та практичну придатність розробленої системи для клінічного використання.

Ключові слова: електрокардіограма, ЕКГ, методи цифрової обробки сигналів, згорткові нейронні мережі, машинне навчання, глибинні нейронні моделі.

Іл. 8. Бібліогр.: 10 назв.

SCIENTIFIC JOURNAL
INFORMATION TECHNOLOGIES AND ENGINEERING ELECTRONICS
ISSN 3083-7618
eISSN 3083-7626
Issue 1
In English and Ukrainian

НАУКОВИЙ ЖУРНАЛ
ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА ІНЖЕНЕРНА ЕЛЕКТРОНІКА
ISSN 3083-7618
eISSN 3083-7626
Випуск 1
Англійською та українською мовами

Комп'ютерна верстка І.В. Свид

Підп. до друку 27.12.2024. Формат 60х90/8. Папір офсет. Гарнітура Таймс. Друк. ризограф.
Ум. друк. арк. 3,85. Тираж 100 прим. Ціна договір.

Прикарпатський національний університет імені Василя Стефаника (ПНУ ім. Василя Стефаника)
м. Івано-Франківськ, вул. Шевченка, 57 тел. +38 (0342) 75-23-51, факс +38 (0342) 53-15-74,
e-mail: office@pnu.edu.ua.

Друк: підприємець Голіней О.М.
вул. Галицька, 128, м. Івано-Франківськ, 76008
Тел. +38(0342) 58-04-32