

Національний університет «Одеська політехніка»

**РОЗВИТКИ
ІНФОРМАЦІЙНО-КЕРУЮЧИХ СИСТЕМ ТА
ТЕХНОЛОГІЙ**

МОНОГРАФІЯ



Львів-Торунь
2024

УДК 004:37:001:62

P64

Авторський колектив:

Д. Антонов, Н. Аксак, О. Базей, О. Беспалов, Ю. Бондар, Р. Віт, В. Вичужанін, О. Вичужанін, В. Власенко, О. Гузун, А. Давиденко, О. Задорожний, М. Корабльов, А. Король, Ю. Котух, М. Кушнар'єв, Л. Ковальчук, С. Маїталір, О. Мазурець, М. Молчанова, П. Михайловський, С. Науменко, Ю. Нетребін, О. Ніколенко, Г. Охотько, О. Орехов, С. Орлов, Т. Отрадська, І. Петров, О. Поліщук, І. Розломій, М. Рудніченко, В. Саваневич, О. Собко, А. Татарніков, О. Ткачук, В. Троянський, Т. Трунова, Є. Хаджисєв, Г. Халімов, С. Хламов, Д. Шведов, Н. Шибасєва, І. Шпінарева, А. Ярмілко

Рекомендовано до друку вченою порадою
Національного університету «Одеська політехніка»
(протокол №1 від 25.09.2024 р.)

Рецензенти:

Професор **Є Чженмао**, Південний університет (США);
Професор **С. Овермайєр**, Університет Південного Нью-Гемпширу (США);
Професор **А. Тріпаті**, Індійський технологічний інститут (ВНУ) (Індія)

P64 **Розвитки** інформаційно-керуючих систем та технологій : монографія / Н. Аксак, Д. Антонов та ін.; під наук. ред. проф. В.Вичужаніна. – Львів-Торунь : Liha-Pres, 2024 – 380 с.
Укр., англ. мовами.

ISBN 978-966-397-422-4

DOI 10.36059/978-966-397-422-4

У монографії відображені результати наукових досліджень у галузі інформаційних, інтелектуальних систем та аналізу даних, моделювання. Матеріали монографії будуть корисними для аспірантів, магістрантів, викладачів вищих навчальних закладів, що спеціалізуються на галузі ІТ-технологій.

УДК 004:37:001:62

ISBN 978-966-397-422-4

© Національний університет
"Одеська політехніка", 2024
© Колектив авторів, 2024

**ADVANCES
IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES**

CONTENTS

Preface	7
SECTION 1. INTELLIGENT CONTROL OF SYSTEMS AND TECHNOLOGIES	
ПОКРАЩЕНЕ ШИФРУВАННЯ НА ОСНОВІ НЕАБЕЛЕВИХ МАЛИХ ГРУП P1	
Dr.Sci. С. Котух <i>НТУ «Дніпровська політехніка», Україна</i>	
Dr.Sci. Г. Халімов <i>Харківський національний університет радіоелектроніки, Україна</i>	8
MODERN ENCRYPTION METHODS IN IOT: HARDWARE SOLUTIONS AND CRYPTOGRAPHIC LIBRARIES FOR DATA PROTECTION	
Ph.D. I. Rozlomii <i>Cherkasy State Technological University, Ukraine</i>	
Ph.D. A. Yarmilko <i>Bohdan Khmelnytsky National University of Cherkasy, Ukraine</i>	
S. Naumenko <i>Bohdan Khmelnytsky National University of Cherkasy, Ukraine</i>	
P. Mykhailovskyi <i>Bohdan Khmelnytsky National University of Cherkasy, Ukraine</i>	28
AGENT-DRIVEN APPROACH TO ENHANCING E-LEARNING EFFICIENCY	
Dr.Sci. N. Axak <i>Kharkiv National University of Radio Electronics, Ukraine</i>	
Ph.D. M. Kushnaryov <i>Kharkiv National University of Radio Electronics, Ukraine</i>	
A. Tatarnykov <i>Kharkiv National University of Radio Electronics, Ukraine</i>	46
SECTION 2. INTELLIGENT SYSTEMS AND DATA ANALYSIS	
METHOD OF ASSESSING AND FORECASTING THE TECHNICAL STATE OF COMPLEX SYSTEMS OF CRITICAL APPLICATION BASED ON PRECEDENTS	
Ph.D. O. Vychuzhanin <i>Odesa Polytechnic National University, Ukraine</i>	
Dr.Sci. V. Vychuzhanin <i>Odesa Polytechnic National University, Ukraine</i>	71

**ADVANCES
IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES**

**ПРОГНОЗУВАННЯ ФІНАНСОВОГО РИНКУ НА ОСНОВІ
МОДЕЛІ АНАЛІЗУ АКЦІЙ, ЯКА ВРАХОВУЄ ЇХ ЗВ'ЯЗКИ**

Dr.Sci. М. Корабльов,

Д. Антонов,

О. Ткачук

Харківський національний університет радіоелектроніки, Україна...99

**AUTOMATED DATA MINING OF THE SINGLE ASTRONOMICAL
OBJECTS FROM THE BLURRED CCD-FRAMES**

Ph.D. S. Khlamov

Kharkiv National University of Radio Electronics, Ukraine

Dr.Sci. V. Savanevych

Kharkiv National University of Radio Electronics, Ukraine

Ph.D. V. Vlasenko

National Space Facilities Control and Test Center, Ukraine,

E. Hadzhyiev

Kharkiv National University of Radio Electronics, Ukraine.....117

**DISTRIBUTED MICROSERVICES-ORIENTED INFORMATION
SYSTEM FOR ASTRONOMICAL DATA PROCESSING USING
OPENAPI SPECIFICATION**

Ph.D. S. Khlamov

Kharkiv National University of Radio Electronics, Ukraine

S. Orlov

National Aerospace University – Kharkiv Aviation Institute, Ukraine,

T. Trunova

Kharkiv National University of Radio Electronics, Ukraine

Y. Bondar

Kharkiv National University of Radio Electronics, Ukraine

Y. Netrebin

INTIVE Limited, O'Connell Bridge House, Ireland.....136

**DATA MINING OF THE PRIMARY ORBITS OF THE SOLAR
SYSTEM OBJECTS USING THE COLITEC SOFTWARE AND THE
VÄISÄLÄ METHOD**

Ph.D. V. Troianskyi

Odesa I. I. Mechnikov National University, Ukraine

Dr.Sci. O. Bazyey

Odesa I. I. Mechnikov National University, Ukraine

Ph.D. H. Okhotko

Odesa I. I. Mechnikov National University, Ukraine

Ph.D. S. Khlamov

Kharkiv National University of Radio Electronics, Ukraine.....156

**ADVANCES
IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES**

**ARTIFICIAL INTELLIGENCE IN THE DIAGNOSIS, PROGNOSIS
AND TREATMENT OF DIABETIC NEOVASCULAR GLAUCOMA**

Dr.Sci. V. Vychuzhanin

Odessa Polytechnic National University, Ukraine

Ph.D. O. Guzun

*ISI "The Filatov Institute of Eye Diseases and Tissue Therapy of the
National Academy of Medical Sciences of Ukraine", Ukraine*

Ph.D. M. Rudnichenko

Odessa Polytechnic National University, Ukraine

Ph.D. O. Zadorozhnyy

*ISI "The Filatov Institute of Eye Diseases and Tissue Therapy of the
National Academy of Medical Sciences of Ukraine", Ukraine*

Ph.D. A. Korol

*ISI "The Filatov Institute of Eye Diseases and Tissue Therapy of the
National Academy of Medical Sciences of Ukraine", Ukraine.....176*

**ІНТЕЛЕКТУАЛЬНА СИСТЕМА АНАЛІЗУ ТА ДЕТЕКЦІЇ
ТЕКСТОВОГО БОТ-КОНТЕНТУ ВЕЛИКОГО ОБСЯГУ У
СОЦІАЛЬНИХ МЕРЕЖАХ**

Ph.D. M. Рудніченко

Національний університет «Одеська Політехніка», Україна

Ph.D. H. Шибяєва

Національний університет «Одеська Політехніка», Україна

Ph.D. T. Отрадська

Одеський коледж комп'ютерних технологій «СЕРВЕР», Україна

Д. Шведов

Національний університет «Одеська Політехніка», Україна

Ph.D. I. Шпінарева

Національний університет «Одеська Політехніка», Україна

Dr.Sci. I. Петров

Національний університет «Одеська Політехніка», Україна.....197

**ІНТЕЛЕКТУАЛЬНИЙ МЕТОД ВИЯВЛЕННЯ ЦІЛЮВИХ
ОБ'ЄКТІВ ПРЕДМЕТНОЇ ОБЛАСТІ ЗА ПОКАЗНИКАМИ
СЕМАНТИЧНОЇ ЗВ'ЯЗНОСТІ ДЛЯ КЛАСИФІКАЦІЇ
ТЕКСТОВОЇ ІНФОРМАЦІЇ**

Ph.D. O. Мазурець

Хмельницький національний університет, Україна

P. Віт

Хмельницький національний університет, Україна.....223

**ADVANCES
IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES**

**МЕТОД ВИЯВЛЕННЯ ТА КЛАСИФІКАЦІЇ ТЕХНІК
ПРОПАГАНДИ У ТЕКСТОВОМУ КОНТЕНТІ ЗАСОБАМИ
ШТУЧНОГО ІНТЕЛЕКТУ**

М. Молчанова

Хмельницький національний університет, Україна.....245

**МЕТОД ІНТЕЛЕКТУАЛЬНОГО ВИЯВЛЕННЯ
КІБЕРЗАЛЯКУВАНЬ У ТЕКСТОВОМУ КОНТЕНТІ**

О. Собко

Хмельницький національний університет, Україна.....267

**HIERARCHICAL CLASSIFICATION OF UKRAINIAN
TECHNICAL TEXTS USING TREE-BASED MODELS:
APPLICATIONS IN THE AUTOMOTIVE INDUSTRY**

S. Mashtalir

Kharkiv National University of Radio Electronics

О. Nikolenko

Uzhhorod National University.....288

**SECTION 3. MODELING AND SOFTWARE ENGINEERING
PROTECTION OF MULTILAYER NETWORK SYSTEMS FROM
SUCCESSIVE, GROUP AND SYSTEM-WIDE TARGETED
ATTACKS**

Dr.Sci. O. Polishchuk

*Pidstryhach Institute for Applied Problems of Mechanics and Mathematics,
National Academy of Sciences of Ukraine, Ukraine.....315*

**NEW STATISTICAL CRITERIA FOR CHECKING
INDEPENDENCE OF BIT RANDOM VARIABLES AND
SEQUENCES**

Dr.Sci. L. Kovalchuk

G.E. Pukhov Institute for Modelling in Energy Engineering, Ukraine

Dr.Sci. A. Davydenko

G.E. Pukhov Institute for Modelling in Energy Engineering, Ukraine

О. Bespalov

G.E. Pukhov Institute for Modelling in Energy Engineering, Ukraine.....341

**SECTION 4. MATHEMATICAL AND SIMULATION
MODELING**

**Т ЧОТИРЬОХФАКТОРНА НЕЛІНІЙНА РЕГРЕСІЙНА МОДЕЛЬ
ДЛЯ ОЦІНЮВАННЯ РОЗМІРУ JAVA-ЗАСТОСУНКІВ НА
РАННІХ СТАДІЯХ РОЗРОБКИ**

О. Орехов

*Національний університет кораблебудування імені адмірала Макарова,
Україна.....360*

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

PREFACE

The monograph contains materials from articles received from the Council of articles sent to the XII International Scientific and Practical Conference "Information Control Systems & Technologies (ICST-Odesa-2024)"

The collective monograph presents the results of scientific research in the field of information systems and technologies, intelligent systems, data analysis, modeling and software development.

The monograph is compiled in the form of scientific articles- sections corresponding to thematic areas, which comprehensively reflect the results of research in the following areas: intelligent control technologies; intelligent systems and data analysis, modeling and software engineering, mathematical and simulation modeling.

In the monograph, the authors pay attention to solving problems in the field of information systems and technologies using improved encryption based on non-abelian small groups r_i , the method of assessment and forecasting the technical state of complex systems of critical application based on precedents, protection of multilayer network systems from sequential, group and system-wide targeted attacks, new statistical criteria for checking the independence of bit random variables and sequences. Considerable attention is paid to the agent-controlled approach to increasing the efficiency of e-learning, automated data extraction of individual astronomical objects from blurry ccd images, artificial intelligence in diagnostics, prognosis and treatment of diabetic neovascular glaucoma.

Thanks to the presented research results, readers will receive a useful amount of knowledge necessary for a better understanding problems and solutions in the field of information systems and technologies.

The articles presented in the monograph correspond to the original author's variants. The authors alone are responsible for the content of the articles.

The materials of the monograph will be useful for postgraduate students, master's students, and teachers of higher educational institutions specializing in the field of information systems and technologies. Scientists including 11 doctors of science, 15 candidates of science and 17 applicants took part in the work on the collective monograph.

Section 1. Information control systems

UDC 004.056: 004.9

ПОКРАЩЕНЕ ШИФРУВАННЯ НА ОСНОВІ НЕАБЕЛЕВИХ МАЛИХ ГРУП P_i

Dr.Sci. Є. Котух ORCID: 0000-0003-4997-620X

НТУ «Дніпровська політехніка», Україна

E-mail: yevgenkotukh@gmail.com

Dr.Sci. Г. Халімов ORCID: 0000-0002-2054-9186

Харківський національний університет радіоелектроніки, Україна,

E-mail: hennadii.khalimov@nure.ua

***Анотація.** У статті описано нову реалізацію схеми шифрування на основі малих груп Ree . Наша пропозиція полягає в тому, щоб використовувати невеликі групи P_i для шифрування повної групи з пов'язаними ключами та складністю атаки грубою силою. Ми поширили логарифмічний підпис на всю групу Ree і змінили алгоритм шифрування, щоб зв'язати ключі логарифмічного підпису та захистити від атаки послідовного відновлення.*

***Ключові слова:** криптосистема MST , логарифмічний підпис, випадкове покриття, малі групи P_i .*

1. Постановка проблеми

Поява квантових комп'ютерів, здатних вирішувати будь-які складні проблеми, ставить під сумнів існування криптографії в тому вигляді, в якому вона є сьогодні. Класичні криптографічні протоколи з відкритим ключем, які використовують ідею складності вирішення проблеми факторизації великих чисел, стануть небезпечними. Актуальним стає впровадження криптосистем на некомутативних алгебрах груп, які на даний момент належать до класу важкорозв'язних задач для квантових обчислень.

2. Аналіз досліджень та публікацій

Некомутативна криптографія, заснована на складних для вирішення математичних задачах, була запропонована в 1980-х роках. Вагнер і Маджарик [1] запропонували концепцію криптосистеми, засновану на нерозв'язній проблемі слів у групах і напівгрупах. Бірбет та ін. [2] спроектував цю ідею на криптосистему з відкритим ключем у кінцевих згенерованих групах. Швидко розвивався тип криптосистем, заснований на груповій факторизації [3-7].

У 1986 році Магліверас [5] запропонував симетричну криптосистему, засновану на факторизації в кінцевих групах перестановок, яка називається логарифмічною сигнатурою (LS). У 2009 році Lempken та ін. [4] розробили нову криптографічну систему з відкритим ключем - $MST3$, засновану на

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

випадкових покриттях і 2-групі Suzuki. У 2008 році Magliveras et al. [8] представили комплексний аналіз криптосистеми MST3 і заявили, що транзитивний логарифмічний підпис не підходить для криптосистеми MST3. У 2010 році Сваба та ін. [6] проаналізували всі опубліковані посилання на атаки на криптографію MST і створили більш безпечну криптосистему eMST3, додавши секретне гомоморфне покриття. У 2018 році ван Трунг [9] запропонував загальний метод побудови сильних аперіодичних логарифмічних сигнатур для абелевих р-груп і зробив внесок у практичне застосування криптосистем MST. Подальший розвиток криптосистем MST3 запропоновано в [10–13]. Тут вперше розглядаються реалізації на багатопараметричних групах. Основна ідея лежить у площині вирішення проблеми оптимізації накладних витрат - зменшення великого розміру ключів і підвищення ефективності алгоритму шифрування (дешифрування). Показано, що на групах великого порядку можна побудувати криптосистеми з обчисленнями логарифмічної сигнатури поза центром групи над скінченними полями малої розмірності.

Цілями статті є: реалізація алгоритму шифрування з логарифмічними підписами на основі малої групи P_i , що дозволить збільшити розмір зашифрованого тексту та зменшити вимоги до розміру логарифмічних підписів; розглянути напрями покращення характеристик безпеки запропонованої конструкції та запропонувати новий алгоритм шифрування з пов'язаними ключами; проаналізувати атаки грубої сили на відновлення ключа для криптосистеми з групами P_i .

3. Виклад основного матеріалу дослідження

Концепція побудови MST криптосистема міститься в застосуванні некоммутативної групової алгебри для покриття логарифмічного підписи. Логарифмічний підпис, як відображення задається наступним визначенням [14].

Визначення (відображення покриття (логарифмічний підпис)). Нехай G буде кінцевою абстрактною групою і $\alpha = [A_1, \dots, A_s]$ буде покриттям типу (r_1, r_2, \dots, r_s) для G з $A_i = [a_{i,1}, a_{i,2}, \dots, a_{i,r_i}]$, де $m = \prod_{i=1}^s r_i$. Нехай $m_1 = 1$; $m_i = \prod_{j=1}^{i-1} r_j$ для $i = 2, \dots, s$. Послідовності A_i називаються блоками; вектор (r_1, r_2, \dots, r_s) із $r_i = |A_i|$ типом, а довжина визначена як $l(\alpha) = \sum_{i=1}^s r_i$. Позначимо τ канонічну бієкцію

$$\tau : \square_{r_1} \times \square_{r_2} \times \dots \times \square_{r_s} \rightarrow \square_m, \quad \tau(j_1, j_2, \dots, j_s) = \sum_{i=1}^s j_i \cdot m_i$$

Тоді сюр'єктивне (бієкційне) відображення $\alpha' : \square_m \rightarrow G$ є індукованим

$$\alpha'(x) = a_{1j_1} \cdot a_{2j_2} \cdots a_{sj_s}$$

**ADVANCES
IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES**

де $(j_1, j_2, \dots, j_s) = \tau^{-1}(x)$.

Нехай G кінцева неабелева група з нетривіальним центром Z , така що G не розкладається над Z . Припустимо, він Z досить великий, так що пошук закінчено Z є обчислювально непрактичним. У більш загальному випадку, якщо $\alpha = [A_1, \dots, A_s]$ є логарифмічним підписом, то кожен елемент $g \in G \in$ може бути виражений однозначно (принаймні одним способом) як добуток форми $g = a_1 \cdot a_2 \cdots a_s$, для $a_i \in A_i$. $\alpha = [A_1, \dots, A_s]$ називається простим (таким, що розкладається на множники), якщо наведену вище розкладку можна досягти в поліномі ширину $w [G \ 1 \ 0]$.

Криптографічна гіпотеза, яка є основою для криптосистеми, полягає в тому, що якщо $\alpha = [A_1, A_2, \dots, A_s] := (a_{i,j})$ – випадкове покриття на «велике» відображення S на G , то знайти прообраз $g = a_{1j_1} a_{2j_2} \cdots a_{sj_s}$ для будь-якого елемента $g \in G$ відносно α є нерозв'язною проблемою.

Одна з концепцій секретності лежить у площині застосування аперіодичних логарифмічних підписів. Конструкції аперіодичних логарифмічних підписів широко представлені [9]. Дослідження та оцінки виконані в [9] є досить оптимістичними. Існують також питання до криптоаналізу MST пов'язані з груповою алгеброю. Ми тут опускаємо тонкі питання аналізу основних атак, хоча деталі часто є суттєвими.

Реалізація криптосистеми MST на малій групі P_i експлуатують ідею, що на багатопараметричній групі великого порядку можна отримати хороші характеристики реалізації та секретності. Мала група P_i визначена над

кінцевим полем F_q , $q = 3^{2m+1}$ для деяких $m > 0$; $t = 3^m$ як [15]

$$\text{Ree}(q) = \langle \alpha(x), \beta(x), \gamma(x), h(\lambda), I^- \mid x \in F_q, \lambda \in F_q^\times \rangle.$$

Підгрупа $U(q)$ для групи $\text{Ree}(q)$ верхніх трикутних матриць має представлення

$$U(q) = \langle \alpha(x), \beta(x), \gamma(x) \mid x \in F_q \rangle.$$

Кожен елемент $U(q)$ може бути виражений унікальним чином

$$S(a, b, c) = \alpha(a)\beta(b)\gamma(c)$$

отже $U(q) = \{S(a, b, c) \mid a, b, c \in F_q\}$, і з цього випливає, що $|U(q)| = q^3$. Крім того,

$U(q)$ є силовською 3-підгрупою $\text{Ree}(q)$, і це показують прямі обчислення

$$S(a_1, b_1, c_1)S(a_2, b_2, c_2) = S(a_1 + a_2, b_1 + b_2 - a_1 a_2^{3t}, c_1 + c_2 - a_2 b_1 + a_1 a_2^{3t+1} - a_1^2 a_2^{3t}),$$

$$S(a, b, c)^{-1} = S(-a, -b - a^{3t+1}, -c - ab + a^{3t+2}).$$

**ADVANCES
IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES**

Центр $Z(U(q)) = \{S(0,0,c) \mid c \in F_q\}$.

Підгрупа $U(q)$ для малої групи $\text{Ree}(q)$ має більший порядок $\text{ord}U(q) = q^3$ ніж порядок групи Сузукі. Групи Сузукі, які також використовуються в криптосистемах MST3, ізоморфні проєктивній лінійній групі $PGL(3, F_q)$, де $q = 2q_0^2$, $q_0 = 2^n$ і має порядок q^2 .

Пропозиція для схеми шифрування на основі малої групи $\text{Pi Ree}(q)$ має наступне відображення [13]. Далі продемонструємо основні кроки алгоритму шифрування.

Крок 1. Генерація ключів

Вхід : велика група $U(q) = \{S(a,b,c) \mid a,b,c \in F_q\}$, $q = 3^{2m+1}$, $m > 0$, $t = 3^m$.

Вихід : відкритий ключ $[\alpha, \gamma, f]$ із відповідним закритим ключем $[\beta, (t_0, \dots, t_s)]$.

Побудуємо два простих логарифмічних підпис:

$$\beta_{(1)} = [B_{1(1)}, \dots, B_{s(1)}] = (b_{ij})_{(1)} = S(0, b_{ij(1)}, 0), \quad \beta_{(2)} = [B_{1(2)}, \dots, B_{s(2)}] = (b_{ij})_{(2)} = S(0, 0, b_{ij(2)})$$

типів $(r_{1(k)}, \dots, r_{s(k)})$, $i = \overline{1, s(k)}$, $j = \overline{1, r_{i(k)}}$, $b_{ij(k)} \in F_q$, $k = 1, 2$ для координат b_{ij} і c .

Побудуємо два випадкові накриття

$$\alpha_{(1)} = [A_{1(1)}, \dots, A_{s(1)}] = (a_{ij})_{(1)} = S(a_{ij(1)_a}, a_{ij(1)_b}, a_{ij(1)_c}), \quad \alpha_{(2)} = [A_{1(2)}, \dots, A_{s(2)}] = (a_{ij})_{(2)} = S(0, a_{ij(2)_b}, a_{ij(2)_c})$$

того самого типу, що й $\beta_{(k)}$, $k = 1, 2$ соответственно, $a_{ij} \in U(q)$, $a_{ij(k)_a}, a_{ij(k)_b}, a_{ij(k)_c} \in F_q \setminus \{0\}$.

Беремо $t_{0(k)}, t_{1(k)}, \dots, t_{s(k)} \in U \setminus Z$, $t_{i(k)} = S(t_{i(k)_a}, t_{i(k)_b}, t_{i(k)_c})$, $t_{i(k)_j} \in F_q \setminus \{0\}$, $i = \overline{0, s(k)}$, $j = \overline{1, 3}$, $k = \overline{1, 2}$; $t_{s(1)} = t_{0(2)}$ та обчислимо

$$\gamma_{(k)} = [h_{1(k)}, \dots, h_{s(k)}] = (h_{ij})_{(k)} = t_{(i-1)(k)}^{-1} f((a_{ij})_{(k)})(b_{ij})_{(k)} t_{i(k)}, \quad i = \overline{1, s(k)}, \quad j = \overline{1, r_{i(k)}}$$

де f є гомоморфізм $f(S(a,b,c)) = S(0, a, b)$, $k = \overline{1, 2}$.

Вихідний відкритий ключ $[f, (\alpha_k, \gamma_k)]_i$ закритий ключ $[\beta_{(k)}, (t_{0(k)}, \dots, t_{s(k)})]$, $k = \overline{1, 2}$.

Крок 2. Шифрування

Вхідні дані : повідомлення $m = S(0, m_2, m_3)$ та відкритий ключ $[f, (\alpha_k, \gamma_k)]$, $k = \overline{1, 2}$.

Вихід : зашифрований текст (y_1, y_2, y_3) повідомлення m .

Беремо випадковий $R = (R_1, R_2)$, $R_1, R_2 \in Z_{|Z|}$.

Обчислимо

**ADVANCES
IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES**

$$y_1 = \alpha'(R) \cdot m = \alpha_1'(R_1) \cdot \alpha_2'(R_2) \cdot m, \quad y_2 = \gamma'(R) = \gamma_1'(R_1) \cdot \gamma_2'(R_2), \quad y_3 = f(\alpha_2'(R_2)).$$

Вихід (y_1, y_2, y_3) .

Крок 3. Дешифрування

Вхідні дані : зашифрований текст (y_1, y_2, y_3) ; особистий ключ $[\beta_{(k)}, (t_{0(k)}, \dots, t_{s(k)})]$, $k = \overline{1, 2}$.

Вихід : повідомлення, $m \in A(P_\infty)$ що відповідає зашифрованому тексту (y_1, y_2, y_3) .

Щоб розшифрувати повідомлення m , нам потрібно відновити випадкові числа $R = (R_1, R_2)$. Параметр $a_{(1)}(R_1)$ відомо з y_1 і він входить до складу другого компонента з y_2 .

Обчислимо

$$D^{(1)}(R_1, R_2) = t_{0(1)} \cdot y_2 t_{s(2)}^{-1}, \quad D^*(R) = f(y_1)^{-1} D^{(1)}(R_1, R_2).$$

Відновимо R_1 з $\beta_{(1)}(R_1)$ використовуючи $\beta_{(1)}(R_1)^{-1}$. Заберемо $\gamma_1'(R_1)$ із y_2 $y_2^{(1)} = \gamma_1'(R_1)^{-1} y_2 = \gamma_2'(R_2)$.

Обчислимо

$$D^{(2)}(R_2) = t_{0(2)} \cdot y_2 t_{s(2)}^{-1}, \quad D^*(R) = D^{(2)}(R_2) y_3^{-1} = D^{(2)}(R_2)$$

і відновимо R_2 з $\beta_{(2)}(R_2)$ використовуючи $\beta_{(2)}(R_2)^{-1}$.

Відновимо $R = (R_1, R_2)$ та отримаємо повідомлення m від y_1 $m = \alpha'(R_1, R_2)^{-1} \cdot y_1$.

Коректність такої реалізації показано в [13]. Розглянуте шифрування має кілька суттєвих недоліків.

По-перше, в алгоритмі шифрування ключі R_1 та R_2 є слабо пов'язаними і допускають атаку послідовного відновлення ключів. Відновлення ключа R_1 через атаку грубої сили на основі перебору R_1' можна виконати на основі

обчислення $\alpha_1'(R_1')$ з наступним порівнянням значення y_1 у координаті a тому що:

$$y_1 = \alpha'(R') \cdot m = S(a_{(1)_a}(R_1'), a_{(1)_b}(R_1') + a_{(2)_b}(R_2') + m_b, *)$$

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

Перебір та знаходження R_1' не залежить від значення R_2 . Відновлення ключа R_2 можливо через обчислення $\alpha_2'(R_2')$ та порівняння з y_3 у координаті c $y_3 = f(\alpha_2'(R_2')) = S(0, 0, a_{(2)_b}(R_2'))$.

У цьому випадку складність атаки на ключі $R = (R_1, R_2)$ складає $2q$. По-друге, алгоритм шифрування не використовує всю область визначення групи P_i , а тільки похідну групу $U_1(q) = \{S(0, b, c) | b, c \in F_q\}$, яка має $|U_1(q)| = q^2$, що визначає розмір повідомлення під час шифрування $|m| = q^2$.

4. Новий покращений алгоритм

У новій реалізації криптосистеми ми усуваємо ці недоліки. Ми розширили логарифмічний підпис на всю групу P_i $U(q) = \{S(a, b, c) | a, b, c \in F_q\}$, $|U(q)| = q^3$ та змінили алгоритм шифрування таким чином щоб зв'язати ключі логарифмічних підписів та захистити від атаки послідовного відновлення. Наша пропозиція полягає в використанні малої групи P_i для шифрування на повній групі $U(q) = \{S(a, b, c) | a, b, c \in F_q\}$ зі пов'язаними ключами $R = (R_1, R_2, R_3)$ та складністю атаки грубої сили q^3 . Пропонуємо опис схеми з послідовним кривими відтворення.

Крок 1. Генерація ключів

Вхід : велика група $U(q) = \{S(a, b, c) | a, b, c \in F_q\}$, $q = 3^{2m+1}$, $m > 0$, $t = 3^m$.

Вихід : відкритий ключ $[\alpha, \gamma, f]$ із відповідним закритим ключем $[\beta, (t_0, \dots, t_s)]$.

Вибираємо прості логарифмічні підписи $\beta_{(k)} = [B_{1(k)}, \dots, B_{s(k)}] = (b_{ij})_{(k)}$, де $(b_{ij})_{(k)} \in U(q)$ типу $(r_{1(k)}, \dots, r_{s(k)})$, $i = \overline{1, s(k)}$, $j = \overline{1, r_{i(k)}}$, $b_{ij(k)} \in F_q$, $k = \overline{1, 3}$.

Груповий елемент $(b_{ij})_{(k)}$ має значення лише в одній координаті a , b , або c відповідно. Наприклад $(b_{ij})_{(1)} = S(b_{ij(a)}, 0, 0)$.

**ADVANCES
IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES**

Вибираємо випадкові накриття $\alpha_{(k)} = [A_{1(k)}, \dots, A_{s(k)}] = (a_{ij})_{(k)} = S(a_{ij(k)_a}, a_{ij(k)_b}, a_{ij(k)_c})$ тих самих типів, що й $\beta_{(k)}$, де $a_{ij} \in U(q)$, $a_{ij(k)_a}, a_{ij(k)_b}, a_{ij(k)_c} \in F_q \setminus \{0\}$, $i = \overline{0, s(k)}$, $j = \overline{1, r_{i(k)}}$, $k = \overline{1, 3}$.

Вибираємо $t_{0(k)}, t_{1(k)}, \dots, t_{s(k)} \in U \setminus Z$, $t_{i(k)} = S(t_{i(k)_a}, t_{i(k)_b}, t_{i(k)_c})$, $t_{i(k)_a}, t_{i(k)_b}, t_{i(k)_c} \in F_q \setminus \{0\}$, $i = \overline{0, s(k)}$, $k = \overline{1, 3}$. Такі, що $t_{s(k-1)} = t_{0(k)}$, $k = \overline{1, 3}$.

Побудуємо гомоморфізм, визначений наступним чином

$$f_1(S(a, b, c)) = S(0, b, c), \quad f_2(S(a, b, c)) = S(0, 0, c).$$

Проведемо наступні розрахунки

$$\begin{aligned} \gamma_{(1)} &= [h_{1(1)}, \dots, h_{s(1)}] = (h_{ij})_{(1)} = t_{(i-1)(1)}^{-1} (a_{ij})_{(1)} (b_{ij})_{(1)} t_{i(1)}, \quad i = \overline{1, s(1)}, \quad j = \overline{1, r_{i(1)}}, \\ \gamma_{(2)} &= [h_{1(2)}, \dots, h_{s(2)}] = (h_{ij})_{(2)} = t_{(i-1)(2)}^{-1} f_1((a_{ij})_{(2)}) (b_{ij})_{(2)} t_{i(2)}, \quad i = \overline{1, s(2)}, \quad j = \overline{1, r_{i(2)}}, \\ \gamma_{(3)} &= [h_{1(3)}, \dots, h_{s(3)}] = (h_{ij})_{(3)} = t_{(i-1)(3)}^{-1} f_2((a_{ij})_{(3)}) (b_{ij})_{(3)} t_{i(3)}, \quad i = \overline{1, s(3)}, \quad j = \overline{1, r_{i(3)}}. \end{aligned}$$

де $a_{ij(1)} b_{ij(1)} = S(a_{ij(1)_a}, a_{ij(1)_b}, a_{ij(1)_c}) S(b_{ij(1)_a}, 0, 0) = S(a_{ij(1)_a} + b_{ij(1)_a}, *, *)$

$$f_1(a_{ij(2)}) b_{ij(2)} = S(0, a_{ij(2)_b}, a_{ij(2)_c}) S(0, b_{ij(2)_b}, 0) = S(0, a_{ij(2)_b} + b_{ij(2)_b}, a_{ij(2)_c}),$$

$$f_2(a_{ij(3)}) b_{ij(3)} = S(0, 0, a_{ij(3)_c}) S(0, 0, b_{ij(3)_c}) = S(0, 0, a_{ij(3)_c} + b_{ij(3)_c}).$$

Вихідний відкритий ключ $[f_1, f_2, (\alpha_k, \gamma_k)]_i$ закритий ключ $[\beta_{(k)}(t_{0(k)}, \dots, t_{s(k)})]_i$, $k = \overline{1, 3}$.

Крок 2. Шифрування

Вхідні дані : повідомлення $m \in U(q)$ та $m = S(m_a, m_b, m_c)$ відкритий ключ $[f_1, f_2, (\alpha_k, \gamma_k)]_i$, $k = \overline{1, 3}$.

Вихід : зашифрований текст (y_1, y_2, y_3) повідомлення m .

Вибираємо випадковий $R = (R_1, R_2, R_3)$, $R_k \in Z_{|Z|}$, $k = \overline{1, 3}$. Обчислимо ключ шифрування через відображення

$$R' = \pi(R_1, R_2, R_3) = (R_1', R_2', R_3')$$

Обчислимо

$$y_1 = \alpha'(R') \cdot m = \alpha_1'(R_1') \cdot \alpha_2'(R_2') \cdot \alpha_3'(R_3') \cdot m.$$

Обчислювальний компонент y_2 .

$$\gamma(R) = \gamma_1'(R_1) \cdot \gamma_2'(R_2) \cdot \gamma_3'(R_3),$$

**ADVANCES
IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES**

$$\gamma(R) = S \left(t_{0(1)}^{-1} + \sum_{i=1, j=R_{i(1)}}^{s(1)} (a_{ij(1)_a} + \beta_{ij(1)_a}) + t_{s(3)}, \sum_{i=1, j=R_{i(2)}}^{s(2)} (a_{ij(2)_b} + \beta_{ij(2)_b}) + *, \sum_{i=1, j=R_{i(3)}}^{s(3)} (a_{ij(3)_c} + \beta_{ij(3)_c}) + * \right)$$

$$y_2 = \gamma(R) \cdot f_2(\alpha_3'(R_3)) \cdot f_1(\alpha_3'(R_3)) \cdot f_1(\alpha_2'(R_2)),$$

де

$$f_1(\alpha_k'(R_k)) = \prod_{i=1, j=R_{i(k)}}^{s(k)} S(a_{ij(k)_a}, 0, 0) = S \left(\sum_{i=1, j=R_{i(k)}}^{s(k)} a_{ij(k)_a}, *, * \right), k = 2, 3$$

$$f_2(\alpha_k'(R_k)) = \prod_{i=1, j=R_{i(k)}}^{s(k)} S(0, a_{ij(k)_b}, 0) = S \left(0, \sum_{i=1, j=R_{i(k)}}^{s(k)} a_{ij(k)_b}, 0 \right), k = 3$$

$$y_2 = S \left(t_{0(1)}^{-1} + \sum_{k=1}^3 \sum_{i=1, j=R_{i(k)}}^{s(1)} a_{ij(k)_a} + \sum_{i=1, j=R_{i(1)}}^{s(1)} \beta_{ij(1)_a} + t_{s(3)}, \sum_{i=1, j=R_{i(2)}}^{s(2)} (a_{ij(2)_b} + \beta_{ij(2)_b}) + \sum_{i=1, j=R_{i(3)}}^{s(3)} a_{ij(3)_b} + *, \sum_{i=1, j=R_{i(3)}}^{s(3)} (a_{ij(3)_c} + \beta_{ij(3)_c}) + * \right)$$

Обчислювальний компонент Y_3 .

$$\lambda(R) = \alpha_1'(R_1) \cdot f_1(\alpha_2'(R_2)) \cdot f_1(\alpha_3'(R_3)), y_3 = \lambda(R) f_1(\alpha_3'(R_3)) \cdot f_1(\alpha_2'(R_2)),$$

де

$$f_1(\alpha_k'(R_k)) = \prod_{i=1, j=R_{i(k)}}^{s(k)} S(0, a_{ij(k)_b}, a_{ij(k)_c}) = S \left(0, \sum_{i=1, j=R_{i(k)}}^{s(k)} a_{ij(k)_b}, \sum_{i=1, j=R_{i(k)}}^{s(k)} a_{ij(k)_c} \right)$$

для $k = 2, 3$ і

$$y_3 = S \left(\sum_{k=1}^3 \sum_{i=1, j=R_{i(k)}}^{s(k)} a_{ij(k)_a}, \sum_{k=2}^3 \sum_{i=1, j=R_{i(k)}}^{s(k)} a_{ij(k)_b} + *, \sum_{k=2}^3 \sum_{i=1, j=R_{i(k)}}^{s(k)} a_{ij(k)_c} + * \right).$$

Вихід (y_1, y_2, y_3) .

Крок 3. Дешифрування

Вхідні дані : зашифрований текст $(y_1, y_2, y_3)_i$ особистий ключ $[\beta_{(k)}, (t_{0(k)}, \dots, t_{s(k)})]$, $k = \overline{1, 3}$.

Вихід : повідомлення, $m \in A(P_\infty)$ що відповідає зашифрованому тексту (y_1, y_2, y_3) .

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

Щоб розшифрувати повідомлення m , нам потрібно відновити випадкові числа $R = (R_1, R_2, R_3)$.

Обчислимо

$$D(R_1, R_2, R_3) = t_{0(1)} y_2 y_3^{-1} t_{s(3)}^{-1}$$

$$D(R_1, R_2, R_3) = t_{0(1)} S \left(t_{0(1)}^{-1} + \sum_{k=1}^3 \sum_{i=1, j=R_{(1)}}^{s(1)} a_{ij(k)_a} + \sum_{i=1, j=R_{(1)}}^{s(1)} \beta_{ij(1)_a} + t_{s(3)}, *, * \right)$$

$$S \left(\sum_{k=1}^3 \sum_{i=1, j=R_{(k)}}^{s(k)} a_{ij(k)_a}, \sum_{k=2}^3 \sum_{i=1, j=R_{(k)}}^{s(k)} a_{ij(k)_b} + *, \sum_{k=2}^3 \sum_{i=1, j=R_{(k)}}^{s(k)} a_{ij(k)_c} + * \right)^{-1} t_{s(3)}^{-1} = S \left(\sum_{i=1, j=R_{(1)}}^{s(1)} \beta_{ij(1)_a} + t_{s(3)}, *, * \right)$$

Відновимо R_1 з $\beta_{(1)}(R_1) = \sum_{i=1, j=R_{(1)}}^{s(1)} \beta_{ij(1)_a}$ використовуючи $\beta_{(1)}(R_1)^{-1}$, тому що β_1 є простим. Для подальшого розрахунку необхідно видалити компонент $\gamma_1'(R_1)$ від y_2 ; $\alpha_1'(R_1)$ від y_3 .

Обчислимо

$$y_2^{(1)} = \gamma_1'(R_1)^{-1} y_2 = \gamma_2'(R_2) \gamma_3'(R_3) \cdot f_2(\alpha_3'(R_3)) \cdot f_1(\alpha_3'(R_3)) \cdot f_1(\alpha_2'(R_2)) =$$

$$S \left(t_{0(2)}^{-1} + \sum_{k=2}^3 \sum_{i=1, j=R_{(1)}}^{s(1)} a_{ij(k)_a} + t_{s(3)}, \sum_{i=1, j=R_{(2)}}^{s(2)} (a_{ij(2)_b} + \beta_{ij(2)_b}) + \sum_{i=1, j=R_{(3)}}^{s(3)} a_{ij(3)_c} + *, \sum_{i=1, j=R_{(3)}}^{s(3)} (a_{ij(3)_c} + \beta_{ij(3)_c}) + * \right).$$

і

$$y_3^{(1)} = \alpha_1'(R_1)^{-1} y_3 = f_1(\alpha_2'(R_2)) \cdot f_1(\alpha_3'(R_3)) f_1(\alpha_3'(R_3)) \cdot f_1(\alpha_2'(R_2)) =$$

$$S \left(\sum_{k=2}^3 \sum_{i=1, j=R_{(k)}}^{s(k)} a_{ij(k)_a}, \sum_{k=2}^3 \sum_{i=1, j=R_{(k)}}^{s(k)} a_{ij(k)_b} + *, \sum_{k=2}^3 \sum_{i=1, j=R_{(k)}}^{s(k)} a_{ij(k)_c} + * \right)$$

Повторимо обчислення для $D(R_2, R_3)$

$$D(R_2, R_3) = t_{0(2)} y_2^{(1)} (y_3^{(1)})^{-1} t_{s(3)}^{-1} = t_{0(2)} y_2'(R_2) \gamma_3'(R_3) \cdot f_2(\alpha_3'(R_3)) \cdot f_1(\alpha_3'(R_3)) \cdot f_1(\alpha_2'(R_2))$$

$$\left(f_1(\alpha_2'(R_2)) \cdot f_1(\alpha_3'(R_3)) f_1(\alpha_3'(R_3)) \cdot f_1(\alpha_2'(R_2)) \right)^{-1} t_{s(3)}^{-1} =$$

$$t_{0(2)} y_2'(R_2) \gamma_3'(R_3) \cdot f_2(\alpha_3'(R_3)) f_1(\alpha_3'(R_3))^{-1} f_1(\alpha_2'(R_2))^{-1} t_{s(3)}^{-1} = S \left(0, \sum_{i=1, j=R_{(2)}}^{s(2)} \beta_{ij(2)_b}, \sum_{i=1, j=R_{(3)}}^{s(3)} (a_{ij(3)_c} + \beta_{ij(3)_c}) + * \right).$$

Відновимо R_2 з $\beta_{(2)}(R_2) = \sum_{i=1, j=R_{(1)}}^{s(2)} \beta_{ij(1)_a}$ використовуючи $\beta_{(2)}(R_2)^{-1}$, тому що β_2 є простим.

**ADVANCES
IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES**

Видалимо компонент $\gamma_2'(R_2)$ від $y_2^{(1)}$; $f_1(\alpha_2'(R_2))$ від $y_3^{(1)}$.

$$y_2^{(2)} = \gamma_2'(R_2)^{-1} y_2^{(1)} = \gamma_3'(R_3) \cdot f_2(\alpha_3'(R_3)) \cdot f_1(\alpha_3'(R_3)) \cdot f_1(\alpha_2'(R_2)) =$$

$$S \left(t_{0(3)}^{-1} + \sum_{k=2}^3 \sum_{i=1, J=R_{i(3)}}^{s(1)} a_{ij(k)_a} + t_{s(3)}, \sum_{i=1, J=R_{i(3)}}^{s(3)} a_{ij(3)_b} + *, \sum_{i=1, J=R_{i(3)}}^{s(3)} (a_{ij(3)_c} + \beta_{ij(3)_c}) + * \right)$$

i

$$y_3^{(2)} = f_1(\alpha_2'(R_2))^{-1} y_3^{(1)} = f_1(\alpha_3'(R_3)) f_1(\alpha_3'(R_3)) \cdot f_1(\alpha_2'(R_2)) =$$

$$S \left(\sum_{k=2}^3 \sum_{i=1, J=R_{i(3)}}^{s(1)} a_{ij(k)_a}, \sum_{i=1, J=R_{i(3)}}^{s(3)} a_{ij(3)_b} + *, \sum_{i=1, J=R_{i(3)}}^{s(3)} (a_{ij(3)_c} + \beta_{ij(3)_c}) + * \right)$$

Обчислимо $D(R_3) = t_{0(3)} y_2^{(2)} (y_3^{(2)})^{-1} t_{s(3)}^{-1}$,

$$D(R_3) = t_{0(3)} y_2^{(2)} (y_3^{(2)})^{-1} t_{s(3)}^{-1} = t_{0(3)} \gamma_3'(R_3) f_2(\alpha_3'(R_3)) \cdot f_1(\alpha_3'(R_3)) \cdot f_1(\alpha_2'(R_2))$$

$$(f_1(\alpha_3'(R_3)) f_1(\alpha_3'(R_3)) \cdot f_1(\alpha_2'(R_2)))^{-1} t_{s(3)}^{-1} = \gamma_3'(R_3) f_2(\alpha_3'(R_3)) \cdot f_1(\alpha_3'(R_3))^{-1} = S \left(0, 0, \sum_{i=1, J=R_{i(3)}}^{s(3)} \beta_{ij(3)_c} \right)$$

Відновимо R_3 з $\beta_{ij(3)}(R_3)$ використовуючи $\beta_{ij(3)}(R_3)^{-1}$.

Ми отримуємо $R' = \pi(R_1, R_2, R_3) = (R_1', R_2', R_3')$ і відновимо повідомлення m від y_1

$$m = \alpha'(R_1', R_2', R_3')^{-1} \cdot y_1$$

5. Обґрунтування коректності отриманих результатів

Наступний приклад демонструє коректність отриманих виразів.

Візьмемо підгрупу $U(q) = \{S(a, b, c) \mid a, b, c \in F_q\}$ для групи $\text{Ree}(q)$ над F_q ,
 $q = 3^5$, $g(x) = x^5 + 2x + 1$, $t = 3^2$.

Логарифмічні підписи β_k , $k = \overline{1, 3}$ в групі відображень визначають $b_{ij(k)}$ координати a, b, c . Типи $(r_{1(k)}, \dots, r_{s(k)})$ та логарифмічні підписи β_k вибираються самостійно. Визначимо логарифмічні підписи β_k , $k = \overline{1, 3}$ м, що мають типи $(r_{1(1)}, r_{2(1)}, r_{3(1)}, r_{4(1)}) = (3, 3, 3^2, 3)$,
 $(r_{1(2)}, r_{2(2)}, r_{3(2)}) = (3, 3^2, 3^2)$; $(r_{1(3)}, r_{2(3)}, r_{3(3)}, r_{4(3)}) = (3^2, 3, 3, 3)$. Масив $b_{ij(k)}$ складається з підмасивів з кількістю рядків, що дорівнює $r_{i(k)}$. Ви можете

**ADVANCES
IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES**

вибрати будь-яку фрагментацію масивів з умовою $\prod_{i=1}^s r_i = q$. У нашому випадку ми маємо $\prod_{i=1}^s r_i = 3^5$. Кожен рядок b_{ij} є елементом поля F_q . Вимоги до побудови масивів логарифмічних підписів описані в [16]. Для нашого прикладу ми використовуємо конструкцію з простими логарифмічними підписами. Ми побудуємо $\beta_k = [B_{1(k)}, B_{2(k)}, B_{3(k)}]$, $k = \overline{1, 3}$, які мають наступні відображення у вигляді рядків та елементів групи

Таблиця 1

$\beta_k = [B_{1(k)}, B_{2(k)}, B_{3(k)}] = (b_{ij})_{(k)}, (b_{ij})_{(k)} \in U(q), k = \overline{1, 3}$					
$B_{1(1)}$	$(b_{ij})_{(1)}$	$B_{1(2)}$	$(b_{ij})_{(2)}$	$B_{1(3)}$	$(b_{ij})_{(3)}$
00000	0,0,0	00000	0,0,0	00000	0,0,0
10000	$\alpha^0, 0, 0$	10000	$0, \alpha^0, 0$	10000	$0, 0, \alpha^0$
20000	$\alpha^{121}, 0, 0$	20000	$0, \alpha^{121}, 0$	20000	$0, 0, \alpha^{121}$
$B_{2(1)}$		$B_{2(2)}$		01000	$0, 0, \alpha^1$
10000	$\alpha^0, 0, 0$	20000	$0, \alpha^{121}, 0$	11000	$0, 0, \alpha^{69}$
01000	$\alpha^1, 0, 0$	01000	$0, \alpha^1, 0$	21000	$0, 0, \alpha^5$
12000	$\alpha^{126}, 0, 0$	12000	$0, \alpha^{126}, 0$	02000	$0, 0, \alpha^{122}$
$B_{3(1)}$		00100	$0, \alpha^2, 0$	12000	$0, 0, \alpha^{126}$
10000	$\alpha^0, 0, 0$	01100	$0, \alpha^{70}, 0$	22000	$0, 0, \alpha^{190}$
10100	$\alpha^{46}, 0, 0$	02100	$0, \alpha^0, 0$	$B_{2(3)}$	
22200	$\alpha^{131}, 0, 0$	00200	$0, \alpha^{123}, 0$	10000	$0, 0, \alpha^0$
00010	$\alpha^2, 0, 0$	21200	$0, \alpha^{17}, 0$	01100	$0, 0, \alpha^{70}$
01110	$\alpha^{11}, 0, 0$	12200	$0, \alpha^{88}, 0$	00200	$0, 0, \alpha^{123}$
11210	$\alpha^{61}, 0, 0$	$B_{3(2)}$		$B_{3(3)}$	
22020	$\alpha^{93}, 0, 0$	02200	$0, \alpha^{191}, 0$	21200	$0, 0, \alpha^{17}$
01120	$\alpha^{102}, 0, 0$	02210	$0, \alpha^{223}, 0$	20010	$0, 0, \alpha^{15}$
22220	$\alpha^{236}, 0, 0$	01020	$0, \alpha^{196}, 0$	11020	$0, 0, \alpha^{28}$
$B_{4(1)}$		02001	$0, \alpha^{16}, 0$	$B_{4(3)}$	
20120	$\alpha^{233}, 0, 0$	02111	$0, \alpha^{217}, 0$	02000	$0, 0, \alpha^{122}$
20221	$\alpha^{43}, 0, 0$	22221	$0, \alpha^{203}, 0$	21001	$0, 0, \alpha^{73}$
21122	$\alpha^{81}, 0, 0$	20002	$0, \alpha^{68}, 0$	00002	$0, 0, \alpha^{125}$
		12112	$0, \alpha^{24}, 0$		
		21122	$0, \alpha^{81}, 0$		

На наступному кроці генеруємо випадкові обкладинки α_k для того самого типу, що й β_k , $k = \overline{1, 3}$

$$\alpha_k = [A_{1(k)}, \dots, A_{s(k)}] = (a_{ij})_{(k)} = S(a_{ij(k)_a}, a_{ij(k)_b}, a_{ij(k)_c})$$

де $a_{ij} \in U(q)$, $a_{ij(k)_a}, a_{ij(k)_b}, a_{ij(k)_c} \in F_q \setminus \{0\}$, $i = \overline{1, s(k)}$, $j = \overline{1, r_i(k)}$, $k = \overline{1, 3}$.

У полі відображення $\alpha_k = S(a_{ij(k)_a}, a_{ij(k)_b}, a_{ij(k)_c})$ має наступний вигляд

**ADVANCES
IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES**

Таблица 2

$$\alpha_k = [A_{1(k)}, \dots, A_{s(k)}] = S(a_{ij(k)_a}, a_{ij(k)_b}, a_{ij(k)_c})$$

$k = 1$	$k = 2$	$k = 3$
$A_{1(1)}$	$A_{1(2)}$	$A_{1(3)}$
$\alpha^{92}, \alpha^{114}, \alpha^{205}$	$\alpha^{66}, \alpha^{128}, \alpha^{44}$	$\alpha^{121}, \alpha^3, \alpha^{105}$
$\alpha^{172}, \alpha^{116}, \alpha^{227}$	$\alpha^{41}, \alpha^{183}, \alpha^{126}$	$\alpha^{96}, \alpha^{69}, \alpha^{39}$
$\alpha^{210}, \alpha^{111}, \alpha^{193}$	$\alpha^{12}, \alpha^3, \alpha^{156}$	$\alpha^{195}, \alpha^{180}, \alpha^{34}$
$A_{2(1)}$	$A_{2(2)}$	$\alpha^{113}, \alpha^{68}, \alpha^{109}$
$\alpha^{20}, \alpha^{91}, \alpha^{168}$	$\alpha^{75}, \alpha^{158}, \alpha^{31}$	$\alpha^{119}, \alpha^{175}, \alpha^{207}$
$\alpha^{228}, \alpha^{106}, \alpha^{39}$	$\alpha^{20}, \alpha^{238}, \alpha^{197}$	$\alpha^{189}, \alpha^{212}, \alpha^{224}$
$\alpha^{100}, \alpha^{45}, \alpha^{156}$	$\alpha^{49}, \alpha^{111}, \alpha^{27}$	$\alpha^{211}, \alpha^{171}, \alpha^{40}$
$A_{3(1)}$	$\alpha^{176}, \alpha^{136}, \alpha^{61}$	$\alpha^{215}, \alpha^{157}, \alpha^7$
$\alpha^{164}, \alpha^{52}, \alpha^{207}$	$\alpha^{138}, \alpha^{21}, \alpha^{164}$	$\alpha^{230}, \alpha^{14}, \alpha^{44}$
$\alpha^{17}, \alpha^{226}, \alpha^{65}$	$\alpha^{15}, \alpha^{90}, \alpha^2$	$A_{2(3)}$
$\alpha^{38}, \alpha^{65}, \alpha^{38}$	$\alpha^{154}, \alpha^{176}, \alpha^{159}$	$\alpha^{36}, \alpha^{126}, \alpha^8$
$\alpha^{106}, \alpha^{26}, \alpha^{12}$	$\alpha^{163}, \alpha^{172}, \alpha^{206}$	$\alpha^{167}, \alpha^{25}, \alpha^{100}$
$\alpha^{96}, \alpha^{160}, \alpha^{42}$	$\alpha^1, \alpha^{190}, \alpha^{184}$	$\alpha^{210}, \alpha^{11}, \alpha^{135}$
$\alpha^{241}, \alpha^{190}, \alpha^{100}$	$A_{3(2)}$	$A_{3(3)}$
$\alpha^{11}, \alpha^{163}, \alpha^{110}$	$\alpha^{66}, \alpha^{118}, \alpha^{179}$	$\alpha^{32}, \alpha^{142}, \alpha^{94}$
$\alpha^{110}, \alpha^{128}, \alpha^{152}$	$\alpha^{121}, \alpha^{221}, \alpha^{169}$	$\alpha^{224}, \alpha^{166}, \alpha^{43}$
$\alpha^{199}, \alpha^{134}, \alpha^{81}$	$\alpha^{63}, \alpha^{45}, \alpha^{226}$	$\alpha^{218}, \alpha^{128}, \alpha^{164}$
$A_{4(1)}$	$\alpha^{89}, \alpha^{131}, \alpha^{209}$	$A_{4(3)}$
$\alpha^{157}, \alpha^{39}, \alpha^{169}$	$\alpha^{191}, \alpha^{124}, \alpha^{49}$	$\alpha^{156}, \alpha^{58}, \alpha^{147}$
$\alpha^{156}, \alpha^{79}, \alpha^{102}$	$\alpha^{32}, \alpha^{204}, \alpha^{139}$	$\alpha^{153}, \alpha^{10}, \alpha^{54}$
$\alpha^{126}, \alpha^{110}, \alpha^{238}$	$\alpha^{20}, \alpha^{93}, \alpha^{48}$	$\alpha^{22}, \alpha^8, \alpha^{49}$
	$\alpha^{56}, \alpha^{123}, \alpha^{125}$	
	$\alpha^{34}, \alpha^{89}, \alpha^{91}$	

Вибираємо $t_{0(k)}, t_{1(k)}, \dots, t_{s(k)} \in U(q) \setminus Z$ випадковим і $k = \overline{1, 3}$, нехай $t_{3(j)} = t_{0(j+1)}$

Таблица 3

$$t_{0(k)}, t_{1(k)}, \dots, t_{s(k)} \in U(q) \setminus Z, s(k), k = \overline{1, 3}$$

$k = 1$	$k = 2$	$k = 3$
$(\alpha^{14}, \alpha^{16}, \alpha^{59})$	$(\alpha^{109}, \alpha^{229}, \alpha^{106})$	$(\alpha^{52}, \alpha^{125}, \alpha^{228})$
$(\alpha^{14}, \alpha^{206}, \alpha^{63})$	$(\alpha^{21}, \alpha^{66}, \alpha^{44})$	$(\alpha^{117}, \alpha^{143}, \alpha^{78})$
$(\alpha^{154}, \alpha^{69}, \alpha^{38})$	$(\alpha^{43}, \alpha^{54}, \alpha^{29})$	$(\alpha^{159}, \alpha^{207}, \alpha^{74})$
$(\alpha^{53}, \alpha^{180}, \alpha^{77})$	$(\alpha^{52}, \alpha^{125}, \alpha^{228})$	$(\alpha^{228}, \alpha^{111}, \alpha^{225})$
$(\alpha^{109}, \alpha^{229}, \alpha^{106})$		$(\alpha^{196}, \alpha^{164}, \alpha^2)$
$t_{0(k)}^{-1}, t_{1(k)}^{-1}, \dots, t_{s(k)}^{-1} \in U(q) \setminus Z, s = 3, k = \overline{1, 3}$		
$(\alpha^{135}, \alpha^{127}, \alpha^{19})$	$(\alpha^{230}, \alpha^{50}, \alpha^{150})$	$(\alpha^{173}, 0, \alpha^{117})$
$(\alpha^{135}, \alpha^5, \alpha^{37})$	$(\alpha^{142}, \alpha^{116}, \alpha^{34})$	$(\alpha^{238}, \alpha^{237}, \alpha^{118})$
$(\alpha^{33}, \alpha^{136}, \alpha^{61})$	$(\alpha^{164}, \alpha^{193}, \alpha^{222})$	$(\alpha^{38}, \alpha^{35}, \alpha^{80})$
$(\alpha^{174}, \alpha^{167}, \alpha^{174})$	$(\alpha^{173}, 0, \alpha^{117})$	$(\alpha^{107}, \alpha^{69}, \alpha^{37})$
$(\alpha^{230}, \alpha^{50}, \alpha^{150})$		$(\alpha^{75}, \alpha^{164}, \alpha^{123})$

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

Наступним кроком є обчислення масивів γ_k , $k = \overline{1,3}$. За умовою прикладу отримуємо

$$\gamma_{(1)} = [h_{1(1)}, \dots, h_{s(1)}] = (h_{ij})_{(1)} = t_{(i-1)(1)}^{-1} (a_{ij})_{(1)} (b_{ij})_{(1)} t_{i(1)}, \quad i = \overline{1,4}, \quad j = \overline{1, r_{i(1)}},$$

$$\gamma_{(2)} = [h_{1(2)}, \dots, h_{s(2)}] = (h_{ij})_{(2)} = t_{(i-1)(2)}^{-1} f_1((a_{ij})_{(2)}) (b_{ij})_{(2)} t_{i(2)}, \quad i = \overline{1,3}, \quad j = \overline{1, r_{i(2)}},$$

$$\gamma_{(3)} = [h_{1(3)}, \dots, h_{s(3)}] = (h_{ij})_{(3)} = t_{(i-1)(3)}^{-1} f_2((a_{ij})_{(3)}) (b_{ij})_{(3)} t_{i(3)}, \quad i = \overline{1,4}, \quad j = \overline{1, r_{i(3)}}.$$

У полі відображення $\gamma_k = S(h_{ij(k)a}, h_{ij(k)b}, h_{ij(k)c})$, $k = \overline{1,3}$ має наступний вигляд

Таблиця 4

$\gamma_k = S(h_{ij(k)a}, h_{ij(k)b}, h_{ij(k)c}), \quad k = \overline{1,3}$		
$h_{1(1)}$	$h_{1(2)}$	$h_{1(3)}$
$\alpha^{92}, \alpha^{18}, \alpha^{72}$	$\alpha^{91}, \alpha^{155}, \alpha^{100}$	$\alpha^{93}, \alpha^{176}, \alpha^{223}$
$\alpha^{182}, \alpha^{22}, \alpha^{90}$	$\alpha^{91}, \alpha^{116}, \alpha^{38}$	$\alpha^{93}, \alpha^{176}, \alpha^{29}$
$\alpha^{143}, \alpha^{35}, \alpha^{128}$	$\alpha^{91}, \alpha^{153}, \alpha^{91}$	$\alpha^{93}, \alpha^{176}, \alpha^{28}$
$h_{2(1)}$	$h_{2(2)}$	$\alpha^{93}, \alpha^{176}, \alpha^{38}$
$\alpha^{41}, \alpha^{130}, \alpha^{59}$	$\alpha^{110}, \alpha^{176}, \alpha^{219}$	$\alpha^{93}, \alpha^{176}, \alpha^{110}$
$\alpha^{35}, \alpha^{140}, \alpha^{49}$	$\alpha^{110}, \alpha^{48}, \alpha^{140}$	$\alpha^{93}, \alpha^{176}, \alpha^{127}$
$\alpha^{81}, \alpha^{205}, \alpha^{86}$	$\alpha^{110}, \alpha^{34}, \alpha^{61}$	$\alpha^{93}, \alpha^{176}, \alpha^{179}$
$\chi_{3(1)}$	$\alpha^{110}, \alpha^{125}, \alpha^{145}$	$\alpha^{93}, \alpha^{176}, \alpha^{185}$
$\alpha^{70}, \alpha^{24}, \alpha^{216}$	$\alpha^{110}, \alpha^{25}, \alpha^{217}$	$\alpha^{93}, \alpha^{176}, \alpha^{166}$
$\alpha^{20}, \alpha^{64}, \alpha^{183}$	$\alpha^{110}, \alpha^{35}, \alpha^{241}$	$h_{2(3)}$
$\alpha^{200}, \alpha^{162}, \alpha^{124}$	$\alpha^{110}, \alpha^1, \alpha^{11}$	$\alpha^{77}, \alpha^{86}, \alpha^{149}$
$\alpha^{80}, \alpha^{164}, \alpha^{140}$	$\alpha^{110}, \alpha^{27}, \alpha^5$	$\alpha^{77}, \alpha^{86}, \alpha^{52}$
$\alpha^{136}, \alpha^{118}, \alpha^{149}$	$\alpha^{110}, \alpha^{63}, \alpha^{137}$	$\alpha^{77}, \alpha^{86}, \alpha^{57}$
$\alpha^{191}, \alpha^{77}, \alpha^5$	$h_{3(2)}$	$\chi_{3(3)}$
$\alpha^{62}, \alpha^{174}, \alpha^{10}$	$\alpha^{88}, \alpha^{145}, \alpha^{196}$	$\alpha^{160}, \alpha^{107}, \alpha^{99}$
$\alpha^{46}, \alpha^{229}, \alpha^{156}$	$\alpha^{88}, \alpha^{174}, \alpha^{148}$	$\alpha^{160}, \alpha^{107}, \alpha^{128}$
$\alpha^{40}, \alpha^{63}, \alpha^{237}$	$\alpha^{88}, \alpha^{156}, \alpha^{29}$	$\alpha^{160}, \alpha^{107}, \alpha^{59}$
$h_{4(1)}$	$\alpha^{88}, \alpha^{118}, \alpha^{12}$	$\chi_{3(3)}$
$\alpha^{203}, \alpha^{77}, \alpha^{16}$	$\alpha^{88}, \alpha^{228}, \alpha^{63}$	$\alpha^{129}, \alpha^{60}, \alpha^{86}$
$\alpha^{14}, \alpha^{137}, \alpha^{162}$	$\alpha^{88}, \alpha^{28}, \alpha^{77}$	$\alpha^{129}, \alpha^{60}, \alpha^{138}$
$\alpha^{222}, \alpha^{90}, \alpha^{128}$	$\alpha^{88}, \alpha^{156}, \alpha^{14}$	$\alpha^{129}, \alpha^{60}, \alpha^{196}$
	$\alpha^{88}, \alpha^{186}, \alpha^{41}$	
	$\alpha^{88}, \alpha^{162}, \alpha^{190}$	

Наприклад, нехай $R_1 = 209$. Ми отримуємо наступну базову факторизацію для заданого типу $(r_{1(1)}, r_{2(1)}, r_{3(1)}, r_{4(1)}) = (3, 3, 3^2, 3)$ у формі $R_1 = (R_{1(1)}, R_{2(1)}, R_{3(1)}, R_{4(1)}) = (2, 0, 5, 2)$, де $R_{1(1)} + R_{2(1)} 3 + R_{3(1)} 3^2 + R_{4(1)} 3^4 = 209$.

Обчислимо γ_1

**ADVANCES
IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES**

$$\gamma_1(209) = h_{(1)}(2)h_{(2)}(0)h_{(3)}(5)h_{(4)}(2) = S(\alpha^{143}, \alpha^{35}, \alpha^{128})S(\alpha^{41}, \alpha^{130}, \alpha^{59})S(\alpha^{191}, \alpha^{77}, \alpha^5)S(\alpha^{222}, \alpha^{90}, \alpha^{128}) = S(\alpha^5, \alpha^{123}, \alpha^{41}).$$

Виберемо $R_2 = 81$. ми отримати для а типу $(r_{1(2)}, r_{2(2)}, r_{3(2)}) = (3, 3^2, 3^2)$ наступну факторизацію

$$R_2 = (R_{1(2)}, R_{2(2)}, R_{3(2)}) = (0, 0, 3) = 81$$

і значення γ_2

$$\gamma_2(81) = h_{1(2)}(0)h_{2(2)}(0)h_{3(2)}(3) = S(\alpha^{105}, \alpha^{149}, \alpha^{27}).$$

Нехай $R_3 = 129$, ми маємо $R_3 = (R_{1(3)}, R_{2(3)}, R_{3(3)}, R_{4(3)}) = (3, 2, 1, 1) = 129$ для типу $(r_{1(3)}, r_{2(3)}, r_{3(3)}, r_{4(3)}) = (3^2, 3, 3, 3)$ та значення γ_3

$$\gamma_3(129) = h_{1(3)}(3)h_{2(3)}(2)h_{3(3)}(1)h_{4(3)}(1) = S(\alpha^{94}, \alpha^{222}, \alpha^{30}).$$

Перейдем до кроків шифрування і дешифрування.

Крок 1. Шифрування

Вхідні дані : повідомлення $m \in U(q)$, $m = S(m_a, m_b, m_c)$ та відкритий ключ $[f_1, f_2, (\alpha_k, \gamma_k)]$, $k = \overline{1, 3}$

Вихід : зашифрований текст (y_1, y_2, y_3) повідомлення m .

Нехай $m = (a^{10}, a^{20}, a^{30}) = S(a^{10}, a^{20}, a^{30})$.

Виберемо випадковий $R = (R_1, R_2, R_3) = (209, 81, 129)$. Визначимо відображення для шифрування ключів у відео

$$R' = \pi(R_1, R_2, R_3) = (R_3, R_2, R_1) = (129, 81, 209)$$

Обчислимо зашифрований текст

Для $R_3 = 129$ ми отримуємо наступну базову факторизацію для заданого типу $(r_{1(3)}, r_{2(3)}, r_{3(3)}) = (3, 3, 3^2, 3)$ у формі $R_1 = (R_{1(1)}, R_{2(1)}, R_{3(1)}, R_{4(1)}) = (0, 1, 5, 1)$, де $R_1 + R_2 \cdot 3 + R_3 \cdot 3^2 + R_4 \cdot 3^4 = 129$.

Для $R_2 = 81$ ми отримуємо наступну базову факторизацію для заданого типу $(r_{1(2)}, r_{2(2)}, r_{3(2)}) = (3^2, 3, 3, 3)$ у формі

$R_2 = (R_{1(2)}, R_{2(2)}, R_{3(2)}, R_{4(2)}) = (2, 2, 1, 2)$, де $R_1 + R_2 \cdot 3^2 + R_3 \cdot 3^3 + R_4 \cdot 3^4 = 209$.

$$y_1 = \alpha'(R) \cdot m = \alpha_1'(R_3) \cdot \alpha_2'(R_2) \cdot \alpha_3'(R_1) \cdot m = S(\alpha^{118}, \alpha^{102}, \alpha^{224})$$

Обчислимо

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

$$\gamma(R) = \gamma_1'(R_1) \cdot \gamma_2'(R_2) \cdot \gamma_3'(R_3) = S(\alpha^5, \alpha^{123}, \alpha^{41}) S(\alpha^{105}, \alpha^{149}, \alpha^{27}) S(\alpha^{94}, \alpha^{222}, \alpha^{30}) = S(\alpha^{138}, \alpha^{113}, \alpha^{45});$$

другий компонент шифрованого тексту

$$y_2 = \gamma(R) \cdot f_2(\alpha_3'(R_3)) \cdot f_1(\alpha_3'(R_3)) \cdot f_1(\alpha_2'(R_2)) = S(\alpha^{138}, \alpha^{113}, \alpha^{45}) S(0, \alpha^{41}, 0) S(\alpha^{219}, \alpha^{227}, \alpha^{162}) S(\alpha^{100}, \alpha^{204}, \alpha^{27}) = S(\alpha^{94}, \alpha^{222}, \alpha^{30}).$$

Обчислювальний компонент y_3 .

$$\lambda(R) = \alpha_1'(R_1) \cdot f_1(\alpha_2'(R_2)) \cdot f_1(\alpha_3'(R_3)) = S(\alpha^{210}, \alpha^{21}, \alpha^{103}) S(0, \alpha^{68}, \alpha^{126}) S(0, \alpha^{41}, \alpha^{217}) = S(\alpha^{210}, \alpha^{141}, \alpha^{22})$$

$$y_3 = \lambda(R) f_1(\alpha_3'(R_3)) \cdot f_1(\alpha_2'(R_2)) = S(\alpha^{210}, \alpha^{141}, \alpha^{22}) S(0, \alpha^{41}, \alpha^{217}) S(0, \alpha^{68}, \alpha^{126}) = S(\alpha^{91}, \alpha^{155}, \alpha^{213}).$$

Ми отримали вихід $y_1 = (\alpha^{118}, \alpha^{102}, \alpha^{224})$, $y_2 = (\alpha^{100}, \alpha^{204}, \alpha^{27})$, $y_3 = (\alpha^{91}, \alpha^{155}, \alpha^{213})$.

Крок 2. Дешифрування

Вхідні дані : зашифрований текст $(y_1, y_2, y_3)_i$ особистий ключ $[\beta_k, (t_{0(k)}, \dots, t_{s(k)})]$, $k = \overline{1, 3}$.

Вихід : повідомлення, $m \in U(q)$ що відповідає зашифрованому тексту (y_1, y_2, y_3) .

Щоб розшифрувати повідомлення m , нам потрібно відновити випадкові числа $R = (R_1, R_2, R_3)$.

Обчислимо

$$D(R_1, R_2, R_3) = t_{0(1)} y_2 y_3^{-1} t_{s(3)}^{-1} = S(\alpha^{14}, \alpha^{169}, \alpha^{59}) S(\alpha^{100}, \alpha^{204}, \alpha^{27}) S(\alpha^{91}, \alpha^{155}, \alpha^{213})^{-1} S(\alpha^{196}, \alpha^{164}, \alpha^2)^{-1} = S(\alpha^{50}, \alpha^{83}, \alpha^{56})$$

Ми отримуємо $\beta_1(R_1) = \alpha^{50} = (02101)$.

Відновлення R_1 було зроблено раніше $R_1 = (R_{1(1)}, R_{2(1)}, R_{3(1)}, R_{4(1)}) = (0, 1, 5, 1)$.

0|2|10| 1

2|0|22| 1

0|2|10| 1-2|0|22| 1=1|2|21| 0 $R_1 = (*, *, 5, 1)$

1|1| 2|1|0

1|2| 2|1|0-1|1| 2|1|0=0| 1| 0|0|0 $R_1 = (*, 1, 5, 1)$

0| 1 | 0|0|0

0| 1 | 0|0|0-0| 1 | 0|0|0=0| 0 | 0|0|0 $R_1 = (0, 1, 5, 1)$

Для подальших обчислень необхідно видалити компоненти s і $\alpha_1'(R_1)$ із $\gamma_1'(R_1)$ зашифрованого тексту (y_2, y_3) .

**ADVANCES
IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES**

Обчислимо

$$y_2^{(1)} = \gamma_1 '(R_1)^{-1} y_2 = S(\alpha^5, \alpha^{123}, \alpha^{41})^{-1} S(\alpha^{100}, \alpha^{204}, \alpha^{27}) = S(\alpha^{137}, \alpha^{187}, \alpha^{160})$$

i

$$y_3^{(1)} = \alpha_1 '(R_1)^{-1} y_3 = S(\alpha^{210}, \alpha^{21}, \alpha^{103})^{-1} S(\alpha^{91}, \alpha^{155}, \alpha^{213}) = S(0, \alpha^{166}, \alpha^{107})$$

Обчислимо

$$D(R_2, R_3) = t_{0(2), y_2^{(1)}}(y_3^{(1)})^{-1} t_{s(3)}^{-1} = S(\alpha^{109}, \alpha^{229}, \alpha^{106}) S(\alpha^{137}, \alpha^{187}, \alpha^{160}) S(\alpha^{135}, \alpha^{63}, \alpha^{10})^{-1} S(\alpha^{196}, \alpha^{164}, \alpha^2)^{-1} = S(0, \alpha^{166}, \alpha^{107})$$

Ми отримуємо $\beta_2(R_2) = \alpha^{166} = (22001)$.

Відновимо R_2 за допомогою $\beta_2(R_2) = \alpha^{166} = (22001)$.

Виконаємо обернені обчислення $\beta_2(R_2)^{-1}$. Виберемо групи бітів у векторі $\beta(R)$ відповідно до типу $(r_{1(2)}, \dots, r_{s(2)}) = (3, 3^2, 3^2)$. Використовуємо ті ж

обчислення, що й у прикладі для $\beta_1(R_1)^{-1}$, і отримуємо

$$2|20| \underline{01}$$

$$0|20|01$$

$$2|20| \underline{01} - 0|20|01 = 2|00| \underline{00} R_2 = (*, 0, 3)$$

$$2| \underline{00|00}$$

$$2| \underline{00|00} - 2| \underline{00|00} = 0| \underline{00|00} R_2 = (0, 0, 3)$$

$$\beta_2(R)^{-1} = 2|20|01 = (R_{1(2)}, R_{2(2)}, R_{3(2)}) = (0, 0, 3) \quad R_2 = (R_{1(2)}, R_{2(2)}, R_{3(2)}) = (0, 0, 3) = 81$$

Видалимо компонент $\gamma_2 '(R_2)$ від $y_2^{(1)}$; $f_1(\alpha_2 '(R_2))$ від $y_3^{(1)}$.

$$y_2^{(2)} = \gamma_2 '(R_2)^{-1} y_2^{(1)} = S(\alpha^{105}, \alpha^{149}, \alpha^{27})^{-1} S(\alpha^{137}, \alpha^{187}, \alpha^{160}) = S(\alpha^{159}, \alpha^{136}, \alpha^{23})$$

i

$$y_3^{(2)} = f_1(\alpha_2 '(R_2))^{-1} y_3^{(1)} = S(0, \alpha^{68}, \alpha^{126})^{-1} S(\alpha^{135}, \alpha^{63}, \alpha^{10}) = S(\alpha^{135}, \alpha^{11}, \alpha^{212})$$

Обчислимо

$$D(R_3) = t_{0(3), y_2^{(2)}}(y_3^{(2)})^{-1} t_{s(3)}^{-1} = S(\alpha^{52}, \alpha^{125}, \alpha^{228}) S(\alpha^{159}, \alpha^{136}, \alpha^{23}) S(\alpha^{135}, \alpha^{11}, \alpha^{212})^{-1} S(\alpha^{196}, \alpha^{164}, \alpha^2)^{-1} = S(0, 0, \alpha^{98})$$

Ми отримуємо $\beta_3(R_3) = \alpha^{98} = (10212)$.

Відновимо R_3 за допомогою $\beta_3(R_3) = \alpha^{98} = (10212)$.

Виконаємо обернені обчислення $\beta_3(R_3)^{-1}$. Виберемо групи бітів у векторі

$\beta(R)$ відповідно до типу $(r_{1(3)}, r_{2(3)}, r_{3(3)}, r_{4(3)}) = (3^2, 3, 3, 3)$. Ми отримуємо

$$10|2|1| \underline{2}$$

$$00|0|0| \underline{2}$$

**ADVANCES
IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES**

$$10|2|1| \underline{2} - 00 | 0 | 0 | \underline{2} = 10|2 | 1 | \underline{0} R_3 = (*, *, 1, 2)$$

$$20|0| \underline{1} | \underline{0}$$

$$10|2 | 1 | \underline{0} - 20|0 | \underline{1} | \underline{0} = 20|2 | 0 | \underline{0} R_3 = (*, 2, 1, 2)$$

$$00| \underline{2} | \underline{0} | \underline{0}$$

$$20| \underline{2} | \underline{0} | \underline{0} - 00| \underline{2} | \underline{0} | \underline{0} = 20| \underline{0} | \underline{0} | \underline{0} R_3 = (2, 2, 1, 2)$$

$$\beta_3 (R')^{-1} = 10|2|1|2| = (R_{1(3)}, R_{2(3)}, R_{3(3)}, R_{4(3)}) = (2, 2, 1, 2)$$

$$R_3 = (R_{1(3)}, R_{2(3)}, R_{3(3)}, R_{4(3)}) = (2, 2, 1, 2) = 209$$

Отримасмо повідомлення

$$\begin{aligned} m &= \alpha'(R)^{-1} y_1 = \alpha_3'(R_3)^{-1} \alpha_2'(R_2)^{-1} \cdot \alpha_1'(R_1)^{-1} \cdot y_1 \\ &= S(\alpha^{49}, \alpha^{184}, \alpha^{211})^{-1} S(\alpha^{200}, \alpha^{50}, \alpha^{124})^{-1} \\ &S(\alpha^{144}, \alpha^{65}, \alpha^{173})^{-1} S(\alpha^{13}, \alpha^{135}, \alpha^{203}) \\ &= S(\alpha^0, \alpha^1, \alpha^2). \end{aligned}$$

Вихід : повідомлення $m = (a^0, a^1, a^2)$.

6. Аналіз безпеки конструкції

Розглянемо атаку грубою сили на відновлення ключа $R = (R_1, R_2, R_3)$.

Можливі три реалізації такої атаки.

Атака на шифротекст. Вибираючи $R = (R_1, R_2, R_3)$ ми спробуємо розшифрувати текст $y_1' = \alpha'(R') \cdot m = \alpha_1'(R_1') \cdot \alpha_2'(R_2') \cdot \alpha_3'(R_3') \cdot m$.

Накриття $\alpha_{(k)} = [A_{1(k)}, \dots, A_{s(k)}] = (a_{ij})_{(k)} = S(a_{ij(k)_a}, a_{ij(k)_b}, a_{ij(k)_c})$ вибрано

випадково та значення $\alpha'(R')$ обрано множенням у групі без координатних

обмежень. Результативний вектор $\alpha'(R')$ залежить від усіх компонентів

$\alpha_1'(R_1'), \alpha_2'(R_2'), \alpha_3'(R_3')$. Перебір значень ключа $R = (R_1, R_2, R_3)$ має

оцінку складності q^3 . Для практичної атаки повідомлення m так само не

відомо і має невизначеність для вибору q^3 . Це робить атаку на ключ

неможливою. Якщо взяти модель атаки з відомим текстом тоді складність

атаки все одно є рівною q^3 .

Атака на шифротекст y_2 . Виберемо $R = (R_1, R_2, R_3)$ що співпадає з

$y_2 = \gamma(R) \cdot f_2(\alpha_3'(R_3)) \cdot f_1(\alpha_3'(R_3)) \cdot f_1(\alpha_2'(R_2))$. Уявимо y_2 через компоненти

$$\alpha_i'(R_i)$$

**ADVANCES
IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES**

$$y_2 = S \left(t_{0(1)}^{-1} + \sum_{k=1}^3 \sum_{i=1, j=R_{(1)}}^{s(1)} a_{ij(k)_a} + \sum_{i=1, j=R_{(1)}}^{s(1)} \beta_{ij(1)_a} + t_{s(3)}, \sum_{i=1, j=R_{(2)}}^{s(2)} (a_{ij(2)_b} + \beta_{ij(2)_b}) + \sum_{i=1, j=R_{(3)}}^{s(3)} a_{ij(3)_b} + *, \sum_{i=1, j=R_{(3)}}^{s(3)} (a_{ij(3)_c} + \beta_{ij(3)_c}) + * \right).$$

Тут, (*) компоненти визначаються за допомогою перехресних розрахунків в груповій операції добутку $t_{0(k)}, \dots, t_{s(k)}$ і добутку $\alpha_{1_a}(R_1), \beta_{1_b}(R_1)$ для координати b та добутку $\alpha_{1_a}(R_1), \beta_{1_b}(R_1), \alpha_{2_b}(R_2), \beta_{2_c}(R_2)$ для координати c .

Значення координат Y_2 отримаємо обчисленнями над векторами $\alpha_1'(R_1), \alpha_2'(R_2), \alpha_3'(R_3)$. Ключі R_1, R_2, R_3 є пов'язаними зміна будь-якого з них причини до змін Y_2 . Перебірна атака на ключ $R = (R_1, R_2, R_3)$ має оцінку складності q^3 .

Атака на шифротекст Y_3 . Виберемо $R = (R_1, R_2, R_3)$ що співпадає з $y_3 = \lambda(R) f_1(\alpha_3'(R_3)) \cdot f_1(\alpha_2'(R_2))$. Визначимо Y_3 через компоненти $\alpha_i'(R_i)$. Ми отримаємо

$$y_3 = S \left(\sum_{k=1}^3 \sum_{i=1, j=R_{(k)}}^{s(k)} a_{ij(k)_a}, \sum_{k=2}^3 \sum_{i=1, j=R_{(k)}}^{s(k)} a_{ij(k)_b} + *, \sum_{k=2}^3 \sum_{i=1, j=R_{(k)}}^{s(k)} a_{ij(k)_c} + * \right)$$

Значення координат Y_3 ознайомитися обчисленнями над векторами $\alpha_1'(R_1), \alpha_2'(R_2), \alpha_3'(R_3)$. Ключі R_1, R_2, R_3 є також пов'язаними зміна будь-якого з них причини до змін Y_3 . Перебірна атака на ключ $R = (R_1, R_2, R_3)$ також має оцінку складності q^3 .

Атака на вектори $(t_{0(k)}, \dots, t_{s(k)})$. Перебірна атака $(t_{0(k)}, \dots, t_{s(k)}) \in F^q$ загальною для MST криптосистем і для обчислення у полі над центром групи $Z(G)$ має оцінку складності q . Для нашого алгоритму шифрування обчислення підтримується на всій групі $|G| = q^3$ та складність атаки грубої сили на $(t_{0(k)}, \dots, t_{s(k)})$ буде мати складність q^3 .

Атака на алгоритм. Оцінка такої атаки буде справедлива для реалізації MST на будь-якій некомутативній групі та вимагає окремого аналізу. Ця атака має багато деталей, які пов'язані з уразливістю логарифмічного підпису та можливо з груповими операціями.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

7. Висновки дослідження та подальші напрями

Наша пропозиція полягає у використанні малих груп P_i для шифрування на повній групі $U(q) = \{S(a,b,c) \mid a,b,c \in F_q\}$ з пов'язаними ключами $R = (R_1, R_2, R_3)$ та складністю атаки грубої сили q^3 . Ми розширили логарифмічний підпис на всю групу P_i $U(q) = \{S(a,b,c) \mid a,b,c \in F_q\}$, з $|U(q)| = q^3$ та змінили алгоритм шифрування таким чином, щоб зв'язати ключі логарифмічних підписів та захистити від атаки послідовного відновлення ключа.

В подальшому пропонується провести більш змістовний аналіз безпеки використання некомутативних груп для побудови криптосистем на основі запропонованого алгоритму, розглянути можливість реалізації атак з використанням алгоритмів, що реалізовано за допомогою квантових обчислень та визначити напрями забезпечення стійкості щодо методів квантового криптоаналізу.

8. Література

- [1] N.R. Wagner and M.R. Magyarik, "A public-key cryptosystem based on the word problem", Proc. Advances in Cryptology – CRYPTO 1984, LNCS 196, Springer-Verlag (1985), 19–36.
- [2] J. Birget, S. S. Magliveras, and M. Sramka, "On public-key Cryptosystems based on combinatorial group theory," Tatra Mt. Math. Publ., vol. 33, pp. 137-148, Jan. 2006.
- [3] A. Caranti and F. D. Volta, "The round functions of cryptosystem PGM generate the symmetric group," Des. Codes Cryptogr., vol. 38, no. 1, pp. 147-155, 2006.
- [4] W. Lempken, S.S. Magliveras, Tran van Trung and W. Wei, "A public key cryptosystem based on non-abelian finite groups", J. of Cryptology, 22 (2009), 62–74.
- [5] S. S. Magliveras, "A cryptosystem from logarithmic signatures of finite groups," in Proceedings of the 29th Midwest Symposium on Circuits and Systems, pp. 972–975, Elsevier Publishing, Amsterdam, The Netherlands, 1986.
- [6] P. Svaba and T. van Trung, "Public key cryptosystem MST3 cryptanalysis and realization", Journal of Mathematical Cryptology, vol.4, no.3, pp.271–315, 2010.
- [7] T. van Trung, "New approaches to designing public key cryptosystems using one-way functions and trapdoors in finite groups," J. Cryptol., vol. 15, no. 4, pp. 285-297, 2002.
- [8] Magliveras S S, Svaba P, van Trung T, et al. On the security of a realization of cryptosystem MST3. Tatra Mt Math Publ, 2008, 41: 1–13
- [9] T. van Trung, "Construction of strongly aperiodic logarithmic signatures," J. Math. Cryptol., vol. 12, no. 1, pp. 23-35, 2018.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

- [10] G. Khalimov, Y. Kotukh, S.Khalimova “MST3 cryptosystem based on the automorphism group of the hermitian function field” // IEEE International Scientific-Practical Conference: Problems of Infocommunications Science and Technology, PIC S and T 2019 - Proceedings, 2019, pp. 865–868.
- [11] G. Khalimov, Y. Kotukh, S.Khalimova “MST3 cryptosystem based on a generalized Suzuki 2 - Groups” // CEUR Workshop Proceedings, 2020, 2711, pp. 1–15.
- [12] G. Khalimov, Y. Kotukh, S.Khalimova “Encryption scheme based on the automorphism group of the Ree function field” The 7th International Conference on Internet of Things: Systems, Management and Security (IOTSMS 2020) Paris, France. December 14-16, 2020 Date Added to IEEE Xplore: 02 February 2021 ISBN Information: DOI: 10.1109/IOTSMS52051.2020.9340192
- [13] G. Khalimov, Y. Kotukh, I. Didmanidze, S.Khalimova “Encryption scheme based on small Ree groups” The 7th International Conference on Internet of Things: Systems, Management and Security (IOTSMS 2020) Paris, France. December 14-16, 2020 Date Added to IEEE Xplore: 02 February 2021 ISBN Information: DOI: 10.1109/IOTSMS52051.2020.9340192
- [14] W. Lempken and T. van Trung, “On minimal logarithmic signatures of finite groups,” *Experimental Mathematics*, vol.14, no. 3, pp. 257–269, 2005.
- [15] Gregor Kemper, Frank L’ubeck, and Kay Magaard, Matrix generators for the Ree groups $2G_2(q)$, *Comm. Algebra* 29 (2001), no. 1, 407–413. MR MR1842506 (2002e:20025)
- [16] P. Svaba, “Covers and logarithmic signatures of finite groups in cryptography”, Dissertation, <https://bit.ly/2Ws2D24>

IMPROVED ENCRYPTION BASED ON NON-BELEAR SMALL RI GROUPS

Dr.Sci. E. Kotukh ORCID: 0000-0003-4997-620X

NTU "Dniprovska Polytechnic", Ukraine

E-mail: yevgenkotukh@gmail.com

Dr.Sci. G. Khalimov ORCID: 0000-0002-2054-9186

Kharkiv National University of Radio Electronics, Ukraine,

E-mail: hennadii.khalimov@nure.ua

Annotation. *The paper describes a new implementation of an encryption scheme based on Ree small groups. Our proposal is to use small groups of Ri to encrypt the full group with associated keys and brute-force attack complexity. We extended the logarithmic signature to the entire Ree group and modified the encryption algorithm to link the logarithmic signature keys and protect against a sequential recovery attack.*

Keywords: *MST cryptosystem, logarithmic signature, random coverage, small groups of Ri.*

**MODERN ENCRYPTION METHODS IN IOT: HARDWARE
SOLUTIONS AND CRYPTOGRAPHIC LIBRARIES FOR DATA
PROTECTION**

Ph.D. I. Rozlomii ORCID: 0000-0001-5065-9004

Cherkasy State Technological University, Ukraine

E-mail: inna-roz@ukr.net

Ph.D. A. Yarmilko ORCID: 0000-0003-2062-2694

Bohdan Khmelnytsky National University of Cherkasy, Ukraine

E-mail: a-ja@ukr.net

S. Naumenko ORCID: 0000-0002-6337-1605

Bohdan Khmelnytsky National University of Cherkasy, Ukraine

E-mail: naumenko.serhii1122@vu.edu.ua

P. Mykhailovskiy ORCID: 0009-0008-4324-1724

Bohdan Khmelnytsky National University of Cherkasy, Ukraine

E-mail: mykhailovskiy.pavlo1123@vu.edu.ua

Abstract. *This article presents a detailed analysis of hardware encryptors and cryptographic libraries for ensuring security in IoT systems. The Internet of Things (IoT) is currently one of the most dynamic fields, where data security is becoming critically important. The study examines how various microcontrollers use hardware and software encryption methods to protect data and provides a comparative analysis of the effectiveness of these methods. Microcontrollers, which form the backbone of many IoT devices, perform tasks ranging from sensor reading to controlling various devices. To ensure the security of data transmitted through IoT systems, it is essential to use reliable encryption methods. Hardware encryptors embedded in microcontrollers provide high performance and energy efficiency. Software cryptographic libraries, such as mbed TLS, AESLib, TinyAES, and others, offer flexibility and can be used on various platforms. The article examines encryption methods, both hardware and software, using popular microcontrollers such as the STM32F407VG and ESP32-WROOM-32 as examples. Performance, energy consumption, and security levels were measured. Performance was assessed by determining the number of encryption operations per second, which allows evaluating the real-time encryption speed. Energy consumption was measured using a precision multimeter to determine the amount of energy consumed during encryption. Security level was assessed through an analysis of the physical security of keys and resistance to various types of attacks, including brute force and side-channel attacks. The results of the study showed that hardware encryption on the STM32F407VG microcontroller provides significantly higher performance, lower energy consumption, and higher security compared to software encryption on the ESP32-WROOM-32. This confirms the high efficiency of hardware encryption for use in IoT systems that require reliable data protection.*

Keywords. *Hardware encryptor; cryptographic libraries; STM32; ESP32; data security; energy consumption; performance*

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

1. Introduction

In today's technological landscape, the Internet of Things (IoT) is becoming an increasingly significant part of our daily lives [1]. With the growing number of devices connected to the IoT network, the risk of data security also increases, which is one of the most pressing issues today. IoT devices, including microcontrollers, are becoming potential targets for cybercriminals who use various attack methods to gain unauthorized access to confidential information [2]. Data encryption is one of the most effective methods for protecting information in IoT. It allows data to be transformed into a format that cannot be read without a special key, thus ensuring its confidentiality even if intercepted [3]. Furthermore, encryption helps maintain data integrity and device authentication, which is particularly important in large and complex IoT systems [4].

Microcontrollers, which are the backbone of many IoT devices, use both hardware and software encryption [5]. Hardware encryptors, integrated directly into microcontrollers, provide high performance and energy efficiency [6]. At the same time, software encryption libraries offer flexibility and ease of integration into various systems.

Hardware encryptors, such as AES-encryptors and other specialized modules, are designed to accelerate the encryption and decryption processes on microcontrollers, which allows to reduce energy consumption and increase the speed of the system. They are particularly effective in resource-constrained environments, where every processor cycle and millijoule of energy matter [7]. However, hardware solutions have their limitations, including complexity in updating and maintenance, as well as possible problems with compatibility with different platforms [8].

On the other hand, software cryptographic libraries provide greater flexibility and adaptability to different conditions and security requirements. They enable the rapid integration of encryption algorithms into various IoT applications and provide a wider choice of algorithms for developers, which can be useful for adapting to new threats and security requirements [9]. At the same time, software solutions may have lower performance compared to hardware solutions due to dependence on the computing resources of the microcontroller [10]. The integration of hardware and software solutions to ensure cryptographic protection is a promising direction for the development of IoT security. Combined approaches allow you to balance performance, energy efficiency, flexibility and ease of system deployment. Research in this direction helps developers create complex solutions that can meet the specific requirements of various IoT applications [11].

The purpose of this study is to evaluate the effectiveness of hardware and software encryption on microcontrollers in the context of IoT systems. The research aims to determine the performance, energy consumption, and security level of the two encryption approaches: hardware encryption on the STM32F407VG microcontroller and software encryption on the ESP32-WROOM-32 microcontroller using the mbed TLS cryptographic library.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

2. Related works

The analysis of existing works allows identifying the trends and challenges faced by IoT device developers, as well as approaches that can be used to optimize security [12], which arise in IoT systems due to shortcomings in the implementation of cryptographic algorithms and protocols. Several publications are dedicated to data protection tasks in IoT networks, with some studies focusing on improving encryption methods [13]. In addition, considerable attention in the literature is devoted to the problems of authentication and authorization in IoT environments. Given the limited resources of IoT devices, traditional authentication approaches such as public key-based protocols are too costly in terms of power consumption and computing power. To solve this problem, light protocols based on cryptography with symmetric keys or algorithms based on hash functions are proposed, which significantly reduces resource requirements and provides a sufficient level of security [14, 15]. New encryption algorithms are adapted for resource-constrained microcontrollers, enabling reliable information protection with minimal consumption [16]. Specifically, in [17], a new lightweight hybrid encryption algorithm with a novel design approach for IoT is discussed, while [18] presents a compact implementation of the CHAM block cipher on lower-class microcontrollers.

Regarding the libraries for implementing these ciphers on microcontrollers, several researchers [19] have developed their own libraries to facilitate the encryption implementation process. For example, the study [20] presented a multiprecision ANSI C library, which ensures efficient execution of cryptographic algorithms across various platforms. This library is optimized for resource-constrained microcontrollers and allows for high-performance execution of basic encryption operations. Another study describes Seal-embedded, a homomorphic encryption library for IoT [21]. However, it is important to note that not all libraries are equally efficient in terms of resource consumption and resistance to attacks [22].

Many studies also address the optimization of microcontroller resources when applying encryption, particularly ways to reduce computational costs and memory requirements for implementing encryption algorithms [1]. Other authors compare the encryption efficiency on different devices to ensure IoT security [23] and evaluate the performance of IoT encryption algorithms in the context of memory and energy consumption [24].

Research also considers the use of adaptive encryption methods that allow devices to dynamically change the level of protection depending on the current state of resources and the level of threat, which increases the efficiency of IoT systems in conditions of variable load. An important trend is the integration of machine learning technologies to analyze threats and automatically optimize security measures, allowing IoT devices to respond to attacks in real time. Despite some research in this area, there are certain unresolved issues and tasks that require further investigation. One of the main challenges is ensuring maximum data security with the limited resources of microcontrollers. Additionally, research on the effectiveness of

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

encryption optimization methods to ensure low energy consumption and high data processing speed in IoT networks remains relevant.

3. Microcontrollers in IoT

Microcontrollers are the foundation of most IoT devices, providing data processing, communication, and device management. Their typically rich functional capabilities make them suitable for a variety of applications. Microcontrollers play a key role in IoT, as they are used to control and monitor connected devices and collect data from them.

The role of microcontrollers in an IoT system usually depends on their functionality and the tasks they are assigned. The use of microcontrollers in IoT has several typical directions, including:

Sensors and Data Collection. Microcontrollers play an important role in connecting to a variety of sensors that collect information about the environment, such as temperature, humidity, light level, or motion. This data is then processed and can be used for decision making or further processing. For example, the STM32F103C8 microcontroller from STMicroelectronics' STM32 series has built-in capabilities to connect to sensors via I2C, SPI, UART interfaces, making it ideal for data acquisition projects. Thanks to its performance and low power consumption, this microcontroller can process large amounts of data in real time, ensuring efficient operation in resource-constrained environments.

Device Control. Microcontrollers can control various devices, including relays, LEDs, motors, and other actuators. This allows them to respond to changes in the environment by executing commands, such as turning on lights when motion is detected or adjusting the temperature in the HVAC system [25]. Popular microcontrollers such as the STM32 offer high performance and reliability in controlling devices, making them the choice for many IoT applications.

Communication with the Cloud or Network. Microcontrollers with built-in communication modules such as Wi-Fi, Bluetooth or Zigbee allow easy integration of IoT devices into the global network. They can transfer data to cloud service servers, providing access to information at any time and from anywhere in the world. For example, Espressif's ESP8266 offers built-in Wi-Fi support, allowing data transfer to popular platforms such as AWS, Google Cloud or Microsoft Azure without additional communication modules [26].

On-site Data Processing. Some modern microcontrollers have enough power to process data on the device before sending it to the cloud. This allows you to reduce delays, improve the efficiency of the use of network resources and increase the overall level of security, since data does not leave the boundaries of the local network. For example, the Nordic nRF52840 has a powerful ARM Cortex-M4 processor, which allows processing data received from sensors without the need to transfer them to an external server. Overall, microcontrollers are a fundamental component of IoT systems, as they perform critical tasks related to sensors, device control, communication, and data

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

processing. In the context of these functions, ensuring data security becomes extremely important.

The requirements for protecting the confidentiality, integrity, and availability of data are the main reasons why encryption plays a crucial role in IoT. Microcontrollers collect and process a lot of sensitive information, and without proper protection, this data can become a target for cybercriminals. The use of modern cryptographic methods, such as hardware and software encryption, helps ensure reliable data protection at all levels of the IoT system.

4. Encryption on microcontrollers

Encryption on microcontrollers plays a critical role in ensuring data security in embedded systems, particularly in the context of IoT [27]. The primary objective of this process is to prevent unauthorized access to data and devices or alteration of information by transforming it into a cryptographically unintelligible form using specialized algorithms. Implementing encryption on a microcontroller involves a complex sequence of operations aimed at ensuring data confidentiality, integrity, and authenticity [28]. Many modern microcontrollers are equipped with built-in hardware modules for encryption. These hardware encryptors allow cryptographic operations to be performed at the hardware level, ensuring high data processing speed and low power consumption. Hardware encryption significantly reduces the load on the microcontroller's central processor, freeing it to perform other important tasks.

For microcontrollers that do not have built-in hardware encryption modules, software cryptographic libraries are used. These libraries provide necessary functions for encryption, decryption, and key management, implementing cryptographic algorithms at the software level.

The features of hardware encryption and the use of cryptographic libraries will be discussed in the following sections, where we will analyze their advantages, disadvantages, and compare their effectiveness in various usage scenarios in IoT systems.

4.1. Hardware encryption

Hardware encryption is an essential component of the functionality of modern microcontrollers, providing high performance and low power consumption during cryptographic operations. Hardware encryptors are integrated directly into microcontrollers and allow encryption and decryption of data at the hardware level. Figure 1 illustrates the block diagram showing the main components of the hardware encryptor and their interaction. From Figure 1, it can be seen that the input data is fed into the Encryption Processor, which performs the core cryptographic operations (Table 1) to transform Plaintext into Ciphertext.

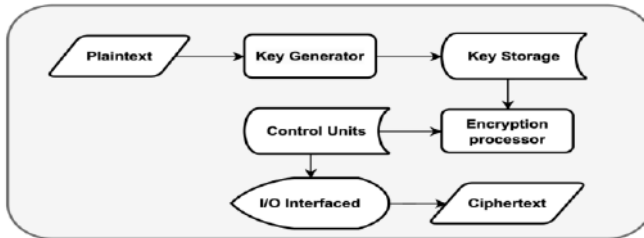


Figure 1. Block diagram of hardware encryption process

The Key Generator block denotes the generation of cryptographic keys using a Pseudo-Random Number Generator (PRNG) to create reliable keys. These keys are stored in the key memory and passed to the encryption processor and control blocks. Keys are stored in **The Key Storage** and are only accessible to the encryption processor through the control blocks. **Control Units** manage the encryption process, provide operation synchronization, and control access to keys and data. Input/Output (**I/O Interfaces**) Interfaces facilitate data exchange between the hardware encryptor and other parts of the microcontroller or external devices. They transmit encrypted data to the next processing or storage stages. Encrypted data (Ciphertext) emerges at the output of the encryption processor, which can be safely transmitted or stored. Upon completion of the encryption process, the data will be protected from unauthorized access.

Let's consider the properties of popular microcontrollers and SoCs that have built-in hardware capabilities for encryption.

1. **STM32.** STM32 microcontrollers typically feature built-in AES (Advanced Encryption Standard) hardware encryption, providing efficient and secure data encryption [29]. Using this hardware encryption allows encryption operations to be performed without significant CPU resource consumption [30].

2. **ESP8266 and ESP32.** These microcontrollers from Espressif also support hardware encryption [31]. For example, ESP8266 has a built-in AES hardware encryptor, while ESP32 additionally supports hardware encryption using SHA (Secure Hash Algorithm) hash functions.

3. **Raspberry Pi and BeagleBone.** These single-board computers can also utilize hardware encryption. For instance, Raspberry Pi can employ a built-in AES hardware encryptor available through the processor's advanced capabilities [32].

4. **PIC.** Microcontrollers from Microchip, such as PIC, may also feature hardware encryption [33]. For example, some PIC models have built-in AES hardware encryptor.

5. **Nordic nRF52.** This microcontroller has built-in AES hardware encryption support, ensuring efficient data encryption with minimal energy consumption, which is particularly crucial for battery-operated IoT devices.

6. **TI CC3200.** Texas Instruments' microcontroller supports AES hardware encryption, making it ideal for IoT connected devices due to its built-in Wi-Fi and low power consumption.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

7. NXP LPC. Some LPC microcontroller models feature a built-in AES hardware encryptor, enabling cryptographic operations to be performed more efficiently with less strain on the processor, ensuring high computational power and flexibility.

Table 1

Encryption processor operations

Operation Description	Formula
Non-linear substitution of each byte of the plaintext using a substitution table (S-box)	$SubBytes(a) = S(a)$
Cyclic shift of bytes in each row of the state matrix	$ShiftRows(s) = s'$
Linear transformation of each column of the state matrix	$MixColumns(s) = s''$
Bitwise XOR between the state matrix and the round key	$AddRoundKey(s, k) = s \oplus k$

Hardware encryption not only increases the performance and efficiency of IoT devices, but also provides flexibility in choosing an approach to data protection. Depending on the needs of a specific system, developers can choose between different options of microcontrollers and SoCs with integrated hardware encryption tools, optimizing the relationship between performance, power consumption and level of security. The use of hardware encryption becomes especially important in resource-constrained environments where microcontrollers run on batteries or have other power constraints. Built-in cryptographic accelerators allow you to perform cryptographic operations quickly and with minimal impact on the performance of the main processor, which extends the life of devices and ensures constant security. In addition, the integration of hardware encoders into microcontrollers makes it possible to implement multi-level protection strategies. For example, hardware data encryption can be combined with additional security measures, such as cryptography based on symmetric and asymmetric keys or the use of hashing algorithms for data integrity. Such a combined approach makes it possible to significantly increase the level of security of the IoT system against various types of attacks, in particular brute force attacks or physical attacks. The use of microcontrollers with built-in cryptographic accelerators allows you to create modern IoT solutions that meet the requirements for protecting information in conditions of real threats and limited resources.

4.2. Cryptographic libraries for microcontrollers

Hardware encryption provides significant advantages in performance and security, as encryption is performed by specialized components of the

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

microcontroller. However, not all microcontrollers have built-in cryptographic accelerators. In such cases, software cryptographic libraries come to the rescue, implementing the necessary cryptographic algorithms and functions at the software level. Cryptographic libraries play an important role in ensuring data security in microcontroller-based systems, especially when hardware encryptors are unavailable or insufficient to perform all necessary cryptographic operations. These libraries implement various cryptographic algorithms and functions at the software level, providing flexibility and a wide range of capabilities for developers.

The first step in implementing encryption is initializing the necessary cryptographic libraries on the microcontroller. This stage involves selecting the cryptographic algorithm, generating keys, and configuring operating modes (encryption or decryption). Subsequent procedures involve data preparation, including dividing it into blocks if the algorithm requires working with data blocks, and adding additional information, such as an initialization vector, to enhance encryption security. Data encryption is performed according to the selected cryptographic algorithm and key, including adding data for authentication (if necessary), key expansion, and performing mathematical encryption operations on data blocks. Upon completion of the encryption operations, encrypted data is obtained, which can be used for transmission or storage in a secure location.

The list of popular cryptographic libraries relevant for microcontroller-based projects is quite extensive:

1. **Crypto** – a cryptographic function library for Arduino and other microcontrollers [34]. It contains implementations of various encryption algorithms, such as AES (Advanced Encryption Standard) and DES (Data Encryption Standard), as well as hash functions like MD5 and SHA. However, it may require more resources than some other libraries.

2. **AESLib** – a library specializing in the implementation of the AES algorithm, widely used for data encryption. It allows the use of different keys and AES modes of operation to protect information. It works on most Arduino boards, including Arduino Uno, although the operation speed may be limited due to resource constraints [35].

3. **TinyAES** – a library for implementing AES on Arduino microcontrollers. It is known for its efficiency and small size, making it an ideal choice for resource-constrained embedded systems. This library offers AES implementation on AVR microcontrollers (on which Arduino Uno is based) and is optimized for the limited resources of these devices. It can be particularly useful for projects where code size and speed are crucial [36].

4. **uECC** – a library used to implement elliptic curve cryptography on microcontrollers [37]. It provides the ability to use elliptic curves for key generation and data signing.

5. **Mbedtls** – a library offering implementations of a wide range of cryptographic algorithms, but may be somewhat heavy for use on Arduino Uno platforms due to its large amount of code and resource requirements [38].

In addition to the mentioned libraries, it is important to pay attention to new developments in cryptography for embedded systems that offer improved

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

performance and security. For example, libraries focused on post-quantum cryptography are becoming increasingly relevant due to the threat of future quantum computing that could potentially break traditional cryptographic algorithms. Such libraries can use lightweight algorithms designed to run on devices with limited computing resources and power consumption. In particular, the wolfSSL library is one of such modern cryptographic libraries developed for resource-dependent devices [39]. It supports a large set of algorithms such as RSA, ECC, AES, and post-quantum cryptography algorithms. Thanks to its modular architecture and low resource requirements, it is ideal for IoT devices that require a high level of security with minimal energy consumption. wolfSSL is actively used in projects with high security requirements, such as financial and medical applications.

Another library worth noting is BearSSL, which is designed with a focus on small code size and high performance. It supports major cryptographic algorithms and protocols, such as TLS, and can be easily integrated into existing systems [40]. Its feature is low power consumption and light weight, which allows it to be used in projects with strict limitations on memory and computing power. Choosing a cryptographic library for a microcontroller depends on specific security requirements, performance, hardware compatibility, and resource constraints.

The combination of hardware and software solutions, such as the use of hardware accelerators together with lightweight cryptographic libraries, provides effective data protection and allows you to create secure and reliable IoT systems ready for today's and future cyber security challenges.

4.3. Library compatibility with microcontrollers

Compatibility of encryption libraries with different microcontroller modifications is a crucial aspect in the development of security systems for embedded devices. The choice of an appropriate library depends on several factors, including the computational power of the microcontroller, the amount of available memory, energy consumption requirements, and support for specific cryptographic algorithms. Let's consider the main aspects of compatibility:

1. **Computational Power.** Microcontrollers with higher computational power (e.g., ARM Cortex-M series) can support more complex cryptographic algorithms and libraries, such as mbed TLS or WolfSSL. Less powerful microcontrollers (e.g., AVR or PIC) may require libraries optimized for them, such as TinyCrypt.

2. **Memory.** The amount of available RAM and Flash memory also affects the choice of library. Some encryption libraries require significant memory to store keys and perform algorithms, which can be an issue for microcontrollers with limited resources. For such cases, there are optimized libraries like micro-ecc for ECC cryptography.

3. **Energy Consumption.** For battery-powered devices, it is important to choose libraries optimized for low energy consumption. This might include the use of specific algorithms or hardware cryptography accelerators if they are available in the microcontroller.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

4. **Support for Cryptographic Algorithms.** Different applications may require different cryptographic algorithms (AES, RSA, ECC, etc.). It is important to ensure that the library supports the necessary algorithms and that they are optimized for the specific microcontroller.

Comparison of the properties of cryptographic libraries for microcontrollers is presented in Table 2. In addition to technical aspects, it is important to consider the factors of support and updating of libraries. For example, some libraries, such as Mbed TLS or wolfSSL, are actively supported by the community and have regular updates that provide protection against new threats and improve performance. This can be critical for projects that require a high level of security and flexibility in adapting to new requirements. Another important aspect is the possibility of optimizing libraries for the specific needs of the project. For example, TinyAES or micro-ecc can be modified to reduce code size or increase speed, which is important for applications that operate under resource-constrained conditions or have specific power consumption requirements. Such optimization may include the use of special processor instructions or hardware accelerators, which significantly improve overall performance and security. The choice of the appropriate library also depends on the possibility of integration with other system components. For example, libraries that support SSL/TLS protocols, such as Mbed TLS or wolfSSL, may be necessary for secure communication in Internet applications. At the same time, libraries with less functionality, such as AESLib or TinyAES, may be better suited for simple applications where data encryption is the main concern.

Table 2

Comparison of encryption libraries for microcontrollers

Library	Supported Algorithms	Advantages	Compatibility
Crypto	AES, RSA, SHA, others	Wide range of functions, flexibility	All well-known microcontrollers
AESLib	AES	Low resource consumption, simplicity	AVR, ESP8266
TinyAES	AES	Low memory usage, high speed	AVR, ARM Cortex-M, ESP8266, ESP32
uECC	ECC	Low memory usage, high security	STM32, AVR, ESP32
Mbedtls	AES, RSA, ECC, SSL/TLS	Easy integration, high performance	STM32, ESP32, ARM Cortex-M
mbed TLS	AES, RSA, ECC, others	High performance, flexibility	STM32, ESP32, NXP LPC

5. Results

The study used two types of microcontrollers: one with hardware encryption (STM32F407VG) and one with software encryption (ESP32-WROOM-32). To

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

evaluate the efficiency of hardware and software encryption, the performance, energy consumption and security metrics were used

5.1. Performance

The number of encryption operations per second was measured to assess how quickly encryption can be performed in real-time.

Encryption performance was measured by determining the number of encryption operations executed per second.

This allows for evaluating the real-time encryption speed and comparing the efficiency of different encryption approaches. For software encryption on the ESP32-WROOM-32, the mbed TLS cryptographic library was used. Each microcontroller was set up to perform encryption on a fixed-size data block (16 bytes) using the AES algorithm.

Specific programs were developed to execute encryption in a loop for this purpose. The testing procedure involved running the encryption program on the microcontroller and measuring the time required to perform a certain number of encryption operations (1000 operations).

The number of encryption operations per second was then calculated by dividing the total number of operations by the total execution time. Data was collected for each type of encryption (hardware and software).

The test results were recorded and analyzed to determine the average performance value, after which graphs were created to visualize the performance comparison between hardware and software encryption.

The measurements showed that hardware encryption on the STM32F407VG significantly outperformed software encryption on the ESP32-WROOM-32 in terms of the number of encryption operations per second (Figure 2).

This confirms the high efficiency of hardware encryption for use in systems requiring fast and reliable data encryption.

5.2. Energy consumption

Energy consumption was measured during the execution of encryption operations. This is crucial for devices with limited power resources, such as battery-powered devices. Software encryption on the ESP32-WROOM-32 was performed using the mbed TLS cryptographic library.

Each microcontroller was configured to encrypt a fixed-size data block (e.g., 16 bytes) using the AES algorithm. Corresponding programs were developed to perform encryption in a loop.

Energy consumption was measured using a precision multimeter or similar equipment that can accurately measure the current and voltage consumed by the microcontroller.

After starting the encryption program on the microcontroller, the current and voltage were measured during the encryption operations. Power was calculated, and

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

the time required to perform a certain number of encryption operations (1000 operations) was measured.

Data was collected for each type of encryption (hardware and software), and the measurement results were recorded and analyzed to determine the average energy consumption during the encryption operations.

Graphs were then created to visualize the comparison of energy consumption between hardware and software encryption.

Measurements showed that hardware encryption on the STM32F407VG had significantly lower energy consumption compared to software encryption on the ESP32-WROOM-32 (Figure 2).

This confirms the high efficiency of hardware encryption for use in energy-constrained systems that require effective encryption with minimal energy consumption.

5.3. Security

The level of protection was assessed, including the physical protection of keys and resistance to attacks. Evaluating the security level of encryption involved analyzing the physical protection of keys and resistance to various types of attacks. This stage is critically important for ensuring reliable data protection, especially in the face of increasing threats in the field of information security. Hardware encryption provides a higher level of security because keys are stored in specialized memory of the microcontroller, making unauthorized access more difficult. Software encryption was supported by the mbed TLS cryptographic library, which stores keys in the microcontroller's general memory, making them more vulnerable to attacks.

Resistance to attacks was assessed by conducting simulations of various types of attacks, including brute-force attacks, side-channel attacks, and differential attacks. Tests were conducted for each microcontroller to model possible attack scenarios and determine how effectively each type of encryption could withstand these threats.

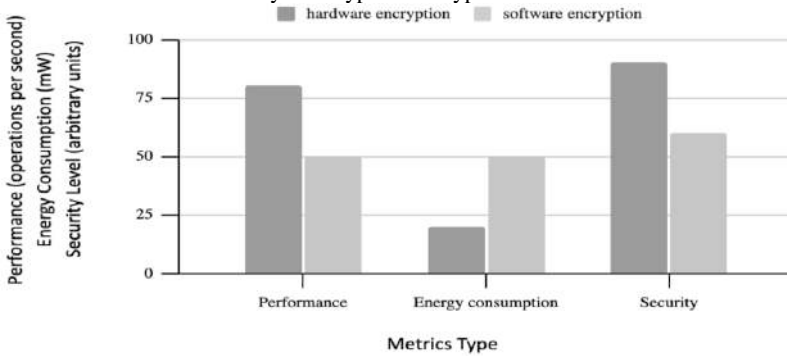


Figure 2. Performance, energy consumption and security levels in hardware and software encryption

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

Data on the physical protection of keys and the results of tests for resistance to attacks were collected and analyzed to determine the overall security level of each type of encryption. Graphs were then constructed to visualize the comparison of security levels between hardware and software encryption.

The results showed that hardware encryption on the STM32F407VG provides a significantly higher level of security compared to software encryption on the ESP32-WROOM-32 (Figure 2). This confirms the importance of using hardware encryption to protect critical data in the face of increasing threats in the field of information security.

6. Discussion

Further research in the field of hardware and software encryption on microcontrollers could focus on several key aspects. Firstly, analyzing the efficiency of hardware encryption on new and emerging microcontrollers in the market would be worthwhile.

This would allow assessing the potential of new hardware platforms in terms of security and performance.

Secondly, it's important to develop and optimize software cryptographic libraries to achieve better performance and energy efficiency across different hardware platforms.

Optimization may include algorithm enhancements, reducing memory consumption, and lowering energy consumption, which is particularly crucial for resource-constrained devices.

Integrating hardware and software encryption with other security protocols, such as TLS, is another promising direction. This would provide comprehensive protection for IoT systems, enhancing their resilience to various types of attacks and ensuring secure data transmission.

Also, one of the directions of future research is the integration of post-quantum protocols in encryption on microcontrollers for IoT devices [32]. Given the future threat of quantum computers capable of breaking traditional cryptographic algorithms, the development and implementation of quantum attack-resistant encryption methods is a critical task. The primary focus should be on adapting post-quantum algorithms, such as CRYSTALS-DILITHIUM, Kyber, NTRUEncrypt, and others, to the limited resources of microcontrollers. This includes optimizing memory usage, power consumption, and ensuring compatibility with existing communication protocols and hardware interfaces. Expanding the scope of testing is also an important aspect of further research. Conducting more extensive tests using different scenarios and data types would provide a more comprehensive picture of the efficiency and security of encryption under various conditions. This would help identify potential weaknesses and refine existing encryption methods.

Overall, further research has the potential to significantly enhance the security and efficiency of IoT systems. It would assist developers in selecting the best solutions for data protection, considering the specific requirements of their projects.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

The results of this research could serve as a basis for creating more reliable and energy-efficient IoT devices that meet modern security challenges.

7. Conclusion

Based on the research findings, it is recommended to use microcontrollers with built-in hardware encryption engines, such as STM32, for projects requiring high performance, low power consumption, and high security levels. Hardware encryption is the most efficient solution for critical IoT applications where data reliability and processing speed are crucial.

Software cryptographic libraries like mbed TLS, AESLib, TinyAES, and others remain essential tools for projects where hardware encryption engines are unavailable or where flexibility in choosing encryption algorithms is needed. The choice of a specific library should be based on the performance, power consumption, and security requirements of the particular project.

Thus, encryption on microcontrollers serves not only as a means of data protection but also as a critical component for supporting functional security and stability in IoT systems. Implementing effective encryption methods helps mitigate risks associated with data breaches, unauthorized access, and other cyber threats, ensuring the reliability and longevity of connected devices in the modern Internet of Things world.

8. References

- [1] I. Rozlomii, A. Yarmilko, S. Naumenko, Data security of IoT devices with limited resources: challenges and potential solutions, in: Proceedings of the 4th Edge Computing Workshop (doors-2024), 5 April 2024, Zhytomyr, Ukraine, ceur-ws.org, vol. 3666, 2024, pp. 85-96.
- [2] W. H. Hassan, Current research on Internet of Things (IoT) security: A survey. *Computer networks* 148 (2019): 283-294.
- [3] B. Pearson, C. Zou, Y. Zhang, Z. Ling, X. Fu, Sic 2: Securing microcontroller based IoY devices with low-cost crypto coprocessors, in: 2020 IEEE 26th International Conference on Parallel and Distributed Systems (ICPADS), 02-04 December 2020, Hong Kong, pp. 372-381. doi: 10.1109/ICPADS51040.2020.00057
- [4] S. Rajagopalan, S. Janakiraman, A. Rengarajan, Medical image encryption: Microcontroller and fpga perspective, in: *Medical Data Security for Bioengineers*, IGI Global, 2019, pp. 278-304. doi: 10.4018/978-1-7998-7705-9.ch013
- [5] P. Arpaia, F. Bonavolonta, A. Cioffi, Problems of the advanced encryption standard in protecting Internet of Things sensor networks. *Measurement* 161 (2020): 107853.
- [6] D. Dinu, A. S. Krishnan, P. Schaumont, SIA: Secure intermittent architecture for off-the-shelf resource-constrained microcontrollers, in: 2019 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), 05-10 May 2019, McLean, VA, USA, pp. 208-217. doi: 10.1109/HST.2019.8740834

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

- [7] N. Ahmad, S. R. Hasan, A new ASIC implementation of an advanced encryption standard (AES) crypto-hardware accelerator. *Microelectronics Journal* 117 (2021): 105255.
- [8] R. Ueno, S. Morioka, N. Miura, K. Matsuda, M. Nagata, S. Bhasin, Y. Mathieu, T. Graba, J.-L. Danger, N. Homma, High throughput/gate AES hardware architectures based on datapath compression. *IEEE Transactions on Computers* 69(4) (2019): 534-548.
- [9] W. El Hadj Youssef, A. Abdelli, F. Dridi, M. Machhout, Hardware implementation of secure lightweight cryptographic designs for IoT applications. *Security and Communication Networks*, 2020(1), (2020): 8860598.
- [10] B. Aslan, Yavuzer F. Aslan, M. T. Sakalli, Energy consumption analysis of lightweight cryptographic algorithms that can be used in the security of Internet of Things applications. *Security and Communication Networks* 2020(1) (2020): 8837671.
- [11] P. Kietzmann, L. Boeckmann, L. Lanzieri, T. C. Schmidt, A Performance Study of Crypto-Hardware in the Low-end IoT, in: *Proceedings of the 2021 International Conference on Embedded Wireless Systems and Networks (EWSN '21)*, 17 February 2021, Delft, The Netherlands, pp. 79-90.
- [12] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, A. Zanella, IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices. *IEEE Internet of Things Journal* 6(5) (2019): 8182-8201.
- [13] M. Yabu, K. Sakiyama, T. Sugawara, Low-memory implementation of authenticated encryption algorithm saeae on arm cortex-m0 microcontroller, in: *2020 IEEE 9th Global Conference on Consumer Electronics (GCCE)*, 13-16 October 2020, Kobe, Japan, 181-185. doi: 10.1109/GCCE50665.2020.9291948
- [14] S. Mitsenko, S. Naumenko, I. Rozlomii, A. Yarmilko, Information Protection and Recovery Hamming Codes Based' Hash Technique, in: *Proceedings of the 11-th International Conference «Information Control Systems & Technologies» (ICST-2023)*, 21-23 September 2023, Odesa, Ukraine, CEUR Workshop Proceedings, vol. 3513, pp. 64-77, 2023.
- [15] A. Yarmilko, I. Rozlomii, H. Kosenyuk, Hash Method for Information Stream's Safety in Dynamic Cooperative Production System. In: *Shkarlet, S., et al. Mathematical Modeling and Simulation of Systems (MODS 2021). Selected Papers of 16th International Scientific-practical Conference, 28 June – 01 July 2021, Chernihiv, Ukraine. Lecture Notes in Networks and Systems*, vol 344 (2022): pp. 173–183. Springer, Cham. doi: 10.1007/978-3-030-89902-8_14
- [16] I. Rozlomii, A. Yarmilko, S. Naumenko, P. Mykhailovskiy, IoT Smart Implants: Information Security and the Implementation of Lightweight Cryptography, in: *6th International Conference on Informatics & Data-Driven Medicine (IDDM'2023)*, 17-19 November 2023, Bratislava, Slovakia, ceur-ws.org, vol. 3609, 2023, pp. 145–156.
- [17] A. Vahi, S. Jafarali Jassbi, SEPAR: A new lightweight hybrid encryption algorithm with a novel design approach for IoT. *Wireless Personal Communications* 114 (2020): 2283-2314.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

- [18] H. Kwon, H. Kim, S. J. Choi, K. Jang, J. Park, H. Kim, H. Seo, Compact implementation of CHAM block cipher on low-end microcontrollers, in: *Information Security Applications: 21st International Conference (WISA 2020)*, 26-28 August 2020, Jeju, Korea, pp. 127-141. doi: 10.1007/978-3-030-65299-9_10
- [19] Z. Temirbekova, A. Pyrkova, Z. Abdiakhmetova, A. Berdaly, Library of fully homomorphic encryption on a microcontroller, in: *2022 International Conference on Smart Information Systems and Technologies (SIST)*, 28-30 April 2022, Nur-Sultan, Kazakhstan, pp. 1-5. doi: 10.1109/SIST54437.2022.9945722
- [20] J. Říha, J. Klemsa, M. Novotný, Multiprecision ANSI C Library for Implementation of Cryptographic Algorithms on Microcontrollers, in: *2019 8th Mediterranean Conference on Embedded Computing (MECO)*, 10-14 June 2019, Budva, Montenegro, pp. 1-4. doi: 10.1109/MECO.2019.8760285
- [21] D. Natarajan, W. Dai, Seal-embedded: A homomorphic encryption library for the internet of things. *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2021(3) (2021): 756-779. doi: 10.46586/tches.v2021.i3.756-779
- [22] P. Panahi, C. Bayılmış, U. Çavuşoğlu, S. Kaçar, Performance evaluation of lightweight encryption algorithms for IoT-based applications. *Arabian Journal for Science and Engineering* 46(4) (2021): 4015-4037.
- [23] A. Pyrkova, Z. Temirbekova, Compare encryption performance across devices to ensure the security of the IOT. *Indonesian Journal of Electrical Engineering and Computer Science* 20(2) (2020): 894-902.
- [24] S. Maitra, D. Richards, A. Abdelgawad, K. Yelamarthi, Performance evaluation of IoT encryption algorithms: memory, timing, and energy, in: *2019 IEEE sensors applications symposium (SAS)*, 11-13 March 2019, Sophia Antipolis, France, pp. 1-6. doi: 10.1109/SAS.2019.8706017
- [25] G. Lymperopoulos, P. Ioannou, Building temperature regulation in a multi-zone HVAC system using distributed adaptive control. *Energy and Buildings* 215 (2020): 109825.
- [26] I. Rozlomii, A. Yarmilko, S. Naumenko, Analysis of Information Security Issues in Balancing Multiple Independent Containers on a Single Server, in: *Proceedings of the 3rd International Workshop on Information Technologies: Theoretical and Applied Problems (ITTAP 2023)*, 22–24 November 2023, Ternopil, Ukraine, Opole, Poland, ceur-ws.org, vol. 3628, 2023, pp. 450-461.
- [27] C. Gao, L. Luo, Y. Zhang, B. Pearson, X. Fu, Microcontroller based IoT system firmware security: Case studies, in: *2019 IEEE International Conference on Industrial Internet (ICII)*, 11-12 November 2019, Orlando, FL, USA, pp. 200-209. doi: 10.1109/ICII.2019.00045
- [28] Y. Kim, H. Kwon, S. An, H. Seo, S. C. Seo, Efficient implementation of ARX-based block ciphers on 8-Bit AVR microcontrollers. *Mathematics* 8(10) (2020): 1837.
- [29] K. Rzepka, P. Szary, K. Cabaj, W. Mazurczyk, Performance evaluation of Raspberry Pi 4 and STM32 Nucleo boards for security-related operations in IoT environments. *Computer Networks* 242 (2024): 110252.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

- [30] J. H. Guo, L. T. Yuan, K. H. Hsia, Development of the IoT module SCADA using MQTT Protocol and AES. *Journal of Advances in Artificial Life Robotics* 2(3) (2021): 109-114.
- [31] M. Al-Mashhadani, M. Shujaa, IoT security using AES encryption technology based ESP32 platform. *Int. Arab J. Inf. Technol.* 19(2) (2022): 214-223.
- [32] P. Galkin, L. Golovkina, I. Klyuchnyk, Analysis of single-board computers for IoT and IIoT solutions in embedded control systems, in: 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), 9-12 October 2018, Kharkiv, Ukraine, pp. 297-302. doi: 10.1109/INFOCOMMST.2018.8632069.
- [33] K. Tomar, PIC18F452 Microcontroller Home Security System: A Review Paper. *International Journal of Innovative Research in Computer Science & Technology* 10(2) (2022): 34-37.
- [34] K. Yoshimoto, Y. Uetake, Y. Kodera, T. Kusaka, Y. Nogami, Evaluating a Side-Channel Resistance against Order 4 Rational Points in Arduino Cryptography Library, in: 2019 Seventh International Symposium on Computing and Networking (CANDAR), 25-28 November 2019, Nagasaki, Japan, pp. 245-250. doi: 10.1109/CANDAR.2019.00040
- [35] L. Li, T. Riom, T. F. Bissyandé, H. Wang, J. Klein, Revisiting the impact of common libraries for android-related investigations. *Journal of Systems and Software* 154 (2019): 157-175.
- [36] H. Li, M. Ninan, B. Wang, J. M. Emmert, TinyPower: Side-Channel Attacks with Tiny Neural Networks, in: 2024 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), 6-9 May 2024, Tysons Corner, VA, USA, pp. 320-331. doi: 10.1109/HOST55342.2024.10545382
- [37] R. A. Nofal, N. Tran, C. Garcia, Y. Liu, B. Dezfouli, A comprehensive empirical analysis of tls handshake and record layer on iot platforms, in: Proceedings of the 22nd International ACM Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM '19), 25-29 November 2019, Miami Beach, FL, USA, pp. 61-70.
- [38] İ. K. Çekiş, A. Toros, N. Apaydın, İ. Özcelik, Performance comparison of ECC libraries for IoT devices. *Eskişehir Technical University Journal of Science and Technology A-Applied Sciences and Engineering* 25.2 (2024): 278-288.
- [39] L. Popa, B. Groza, P. S. Murvay, Performance evaluation of elliptic curve libraries on automotive-grade microcontrollers, in: Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES'19), 26-29 August 2019, University of Kent, Canterbury, UK, pp. 1-7. doi: 10.1145/3339252.3341480
- [40] K. Bürstinghaus-Steinbach, C. Krauß, R. Niederhagen, M. Schneider, Post-quantum tls on embedded systems: Integrating and evaluating kyber and sphincs+ with mbed tls, in: Proceedings of the 15th ACM Asia Conference on Computer and Communications Security (ASIA CCS '20), 5-9 October 2020, Taipei, Taiwan, pp. 841-852. doi: 10.1145/3320269.3384725

**СУЧАСНІ МЕТОДИ ШИФРОВАННЯ В ІОТ: АПАРАТНІ
РІШЕННЯ ТА КРИПТОГРАФІЧНІ БІБЛІОТЕКИ ДЛЯ ЗАХИСТУ
ДАНИХ**

Ph.D. I. Розломій ORCID: 0000-0001-5065-9004

Черкаський державний технологічний університет, Україна

E-mail: inna-roz@ukr.net

Ph.D. A. Ярмілко ORCID: 0000-0003-2062-2694

Черкаський національний університет імені Богдана Хмельницького, Україна

E-mail: a-ja@ukr.net

С. Науменко ORCID: 0000-0002-6337-1605

Черкаський національний університет імені Богдана Хмельницького, Україна

E-mail: naumenko.serhii1122@vu.cdu.edu.ua

П. Михайловський ORCID: 0009-0008-4324-1724

Черкаський національний університет імені Богдана Хмельницького, Україна

E-mail: mykhailovskyi.pavlo1123@vu.cdu.edu.ua

Анотація. У цій статті представлено детальний аналіз апаратних шифраторів і криптографічних бібліотек для забезпечення безпеки в системах IoT. Інтернет речей (IoT) наразі є однією з найбільш динамічних сфер, де безпека даних стає критично важливою. У дослідженні розглядається, як різні мікроконтролери використовують апаратні та програмні методи шифрування для захисту даних, і надається порівняльний аналіз ефективності цих методів. Для забезпечення безпеки даних, що передаються через системи IoT, важливо використовувати надійні методи шифрування. Апаратні шифратори, вбудовані в мікроконтролери, забезпечують високу продуктивність і енергоефективність. Програмні криптографічні бібліотеки, такі як *tbed*, *TLS*, *AESLib*, *TinyAES* та інші, пропонують гнучкість і можуть використовуватися на різних платформах. У статті розглядаються методи шифрування, як апаратні, так і програмні, на прикладі популярних мікроконтролерів, таких як *STM32F407VG* і *ESP32-WROOM-32*. Вимірювали продуктивність, споживання енергії та рівень безпеки. Продуктивність оцінювалася шляхом визначення кількості операцій шифрування в секунду, що дозволяє оцінити швидкість шифрування в реальному часі. Споживання енергії було виміряно за допомогою прецизійного мультиметра для визначення кількості енергії, спожитої під час шифрування. Рівень безпеки оцінювався за допомогою аналізу фізичної безпеки ключів і стійкості до різних типів атак, включаючи атаки грубої сили та сторонні атаки. Результати дослідження показали, що апаратне шифрування на мікроконтролері *STM32F407VG* забезпечує значно вищу продуктивність, менше енергоспоживання та вищу безпеку порівняно з програмним шифруванням на *ESP32-WROOM-32*. Це підтверджує високу ефективність апаратного шифрування для використання в системах IoT, які потребують надійного захисту даних.

Ключові слова. Апаратний шифратор; криптографічні бібліотеки; *STM32*; *ESP32*; безпека даних; споживання енергії; продуктивність

**AGENT-DRIVEN APPROACH TO ENHANCING E-LEARNING
EFFICIENCY**

Dr.Sci. N. Axak ORCID: 0000-0001-8372-8432

Kharkiv National University of Radio Electronics, Ukraine

E-mail: nataliia.axak@nure.ua

Ph.D. M. Kushnaryov ORCID: 0000-0002-3772-3195

Kharkiv National University of Radio Electronics, Ukraine

E-mail: maksym.kushnarov@nure.ua

A. Tatarnykov ORCID: 0000-0002-1632-8188

Kharkiv National University of Radio Electronics, Ukraine

E-mail: andrii.tatarnykov@nure.ua

Abstract. *The paper discusses the problems of modern distance learning, such as individualization of the learning process. The need to improve the methods of supporting remote learning to enhance the quality of education is substantiated. The study aims to improve the quality of education and the organization of the educational process in distance learning. A set of interrelated tasks is proposed, the solution of which is to organize effective interaction between the teacher and the learning management system (LMS) using an agent-based approach. The main result that defines the novelty of the work is the formalization and integration of the following processes: (i) generating real-time suggestions to the teacher to control the performance of tasks during exams or electronic testing; (ii) monitoring students' learning during the semester with the possibility of changing the learning trajectory; (iii) monitoring parents' presence in online classes; (iv) generating recommendations for management and other stakeholders to improve online learning. Also presented are verification of the formal specification of an agent-based support system decision-making for distance learning using the SPIN tool and and the Promela modeling language. Verification is carried out using the formulas of linear temporal logic (LTL), which allows you to check the correctness of the interaction between agents and the fulfillment of key system properties, such as timely data processing, response to violations of students' compliance with testing rules and teachers' recommendations. The modelling of the prototype of the proposed system confirms the effectiveness of its use as a means of studying the organization of the educational process. It shows how agents can help collect and analyze data on how effectively electronic resources are used for learning by students and teachers.*

Keywords: *Learning management system, monitoring, learning process, agents, cloud computing, distributed system temporal logic specifications, alternating-time temporal logic, verification*

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

1. An overview of the accomplishments of multi-agent systems in education

Decision-making is a crucial step in the educational process, as it affects the quality of learning and student success. Some issues can arise when making decisions in the educational process: Insufficient processing or the absence of necessary data can lead to the decision-making process being insufficiently informed and reducing its effectiveness; limited resources, such as budget, staff, and time, can force decisions that are not the best for the quality of education and student success; the lack of education staff's qualifications can result in misunderstanding and data analysis, which can result in incorrect decisions; the variety of students in a classroom can complicate decision-making, as their needs and interests may differ; students who lack motivation can decrease the effectiveness of learning and result in lower-quality solutions; the quality of education and student success can be negatively impacted by social issues, such as poverty, violence, and discrimination, which can complicate decision-making. These problems can reduce the efficiency of decision-making in the educational process. The primary strengths of utilizing agents for decision making lie in their ability to: process automation - agents can help automate complex decision-making processes, which can increase productivity and reduce time spent on decisions; data collection and analysis - agents can help collect and analyze large amounts of data, which allows you to identify trends and patterns that can be used to make better decisions; intelligent decisions - agents can be trained to make decisions based on previous experiences and training using machine learning and other technologies, allowing them to make better decisions based on the analysis of many factors; individualized approach - agents can help to develop customized solutions for participants in the queuing process, which allows for a more personalized approach and meet the needs of different groups.

Consequently, applying agents in the educational process is both relevant and capable of enhancing decision-making quality.

2. Related works

Recently, research related to agent-based decision-making in education has taken a big step forward. The book [1] focuses on Intelligent Tutoring Systems, which are one of the most common uses of agents in education for decision-making. The discussion chapters in this book look at topics through the lens of the Generalized Intelligent Framework for Tutoring (GIFT). Tutoring techniques, strategies, and tactics play a central role in the development of GIFT. The techniques within GIFT are expected to be implemented as software agents, where the agent monitors the learner's progress and the learning context to determine whether best practices (agent policies) have been followed or violated. Over time, the agent will learn to apply the agent policies in a way that optimizes learning and performance.

Many researchers interested in education and learning around the world have realized the potential of data analytics and artificial intelligence and have intensified

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

research around them. This interest has led to the emergence of the fast-growing and multidisciplinary field of learning analytics and increased research into how artificial intelligence can support learning and teaching methods [2]. Artificial intelligence in education (AIED) opens up new opportunities, potential, and challenges in education. Throughout its history, AIED has undergone several paradigm shifts, which are characterized in [3] by three paradigms: AI-driven, learner as recipient, AI-supported, learner as collaborator and AI-empowered, and learner as leader. In the three paradigms, artificial intelligence methods are used to solve education and learning problems in different ways. One of the potential roles of artificial intelligence in education is to provide opportunities to augment human intelligence, with AI supporting us in decision-making processes rather than replacing us through automation. The authors of the study [4] present a case study in the context of debate tutoring, in which they use prediction and classification models to increase the transparency of intuitive decision-making processes by expert tutors for extended reflection and feedback. The trend of AIED is evolving to empower learners and personalize their learning, enable learners to reflect on their learning and inform artificial intelligence systems to adapt accordingly, and lead to the iterative development of learner-centered, data-driven personalized learning [5]. Study [6] proposes agent-based virtual and intelligent recommendations that require information about users' profiles and preferences to recommend the right content. They applied natural language processing (NLP) techniques and semantic analysis approaches to recommend course selection for e-learners and teachers. The content-based recommendation method provides content suggestions related to students' requests and preferences. The use of social media from an educational perspective makes it possible to provide a user-friendly interface for recommending the highest level of interaction in terms of collaboration between users and contacts. E-learning is the threshold of social network-based learning (SN-Learning). SN-Learning consists of a new term introduced in [7] and includes e-learning systems with social networking characteristics or learning through social networking platforms. The authors provide guidelines for designing and implementing SN-Learning platforms using artificial intelligence and modeling techniques. Article [8] explores the possibility of disaggregating query information in online lectures of an e-learning system or course recommendations. Information organization includes reading, parsing, and classifying question messages. Data extraction is a type of surface content processing. It finds a set of predefined applicable content in the feature language archives and performs general language processing using artificial intelligence strategies. Learners often have difficulty finding and retrieving relevant materials to support their learning goals because they lack the subject matter knowledge to create effective queries that convey what they want to learn. In addition, the unfamiliar vocabulary often used by subject matter experts makes it difficult to match a learner's query with relevant learning material. The authors of [9] solve these problems by introducing an innovative method that automatically creates basic knowledge for a learning domain. The effectiveness of the proposed method is evaluated using a collection of machine learning and data analysis documents. The article [10] identifies the features of human and artificial intelligence decision-

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

making along five key contingency factors: specificity of the decision space, ability to interpret the decision-making process and results, size of the alternative set, speed of decision-making, and repeatability. Based on a comparison of human and artificial intelligence decision-making along these dimensions, the article creates a new framework that describes how both decision-making methods can be combined to optimally improve the quality of organizational decision-making. The authors of [11] propose future research directions in a triple perspective: key methodologies for Large Scale Decision Making (LSDM), AI, and data fusion for LSDM. In [12], the authors describe a meta-reasoning policy that can be implemented by a team of agents to make effective control decisions at the meta-level based on the availability of communication in the environment. The authors synthesize the meta-reasoning policy as a solution to the reactive synthesis problem involving the level of communication in the environment and the choice of the agent's algorithm. The authors of [13] argue that in a multi-agent environment, it is appropriate to ask what behavior the system will exhibit under the assumption that agents act rationally, following their preferences. They promote a paradigm of rational verification for multi-agent systems, as an analog of classical verification. The authors tried to automatically determine whether the given properties of a system, expressed in the form of temporal logic formulas, will be preserved in this system under the assumption that the system components (agent) behave rationally by choosing (for example) strategies that form a game-theoretic equilibrium. The article [14] aims to provide a comprehensive view of the relationship between agents and multi-agent systems (MAS) on the one hand, and logic-based technologies on the other, by making them the subject of a systematic literature review. The resulting technologies are discussed and evaluated from two different perspectives: MAS and logic-based. The paper lists the most common logic-based technologies (47 in total) for MAS, but only a relatively small number of them conform to major technology standards. Temporal logics have been widely used in model checking as a formalism for reasoning about the execution of computer systems. They are powerful enough to define most of the properties that can be verified by reactive systems, while also providing very efficient verification algorithms [15]. Temporal logic and model checking have had a major impact on computer science and have been applied in many industrial cases. Several attempts have been made to extend temporal logic to multi-agent systems where multiple components interact, for example, Computation-Tree Logic (CTL) can only express the existence (or not) of an execution of a global system with certain properties, where the goal is to quantify the possible behavior of individual components interacting in the system. In 1997, CTL was extended to Alternating-time Temporal Logic (ATL) with the introduction of strategy quantifiers. In ATL, strategy quantifiers express the existence (or not) of a behavior of one of the agents (or a coalition), so that any final execution in the global system satisfies this property. Study [16] is related to multi-agent logic and its application in computer science. The authors work with multi-agent logic based on relational models. They determine that time availability relations can have gaps or places of forgotten time. The authors of [17] study the problem of learning to satisfy temporal logic specifications with a group of agents in an unknown environment that can exhibit

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

probabilistic behavior. From a learning perspective, these specifications provide a rich formal language with which to capture tasks or goals, while from a logic and automated verification perspective, the implementation of learning capabilities allows for practical applications in large, stochastic, unknown environments. The temporal logic of actions (TLA) — is a logic for specifying and reasoning about parallel systems. The systems and their properties are represented in the same logic, so the statement that a system conforms to its specification and the statement that one system implements another are expressed by logical consequence. TLA is very simple; its syntax and full formal semantics are summarized in about a page. Report [18] introduces TLA and describes how it is used to define and verify parallel algorithms. Education systems include a variety of components such as learning management, progress tracking systems, e-textbooks, etc. The challenge is to interact and integrate intelligent agents with these systems to ensure that they work together effectively. For a system to be successful, agents need to be able to quickly adapt to new requirements and change their behavior accordingly. Thus, the fundamental role of logic-based technologies in MAS today is to meet the need for intelligence that characterizes agent abstractions, i.e., the cognitive abilities required by components of a distributed intelligent system. However, logic-based technologies can rarely be considered mature enough to meet the requirements of industrial and real-world domains. Research on the use of intelligent agents in decision support systems in the educational process reveals new opportunities and approaches that help improve learning and provide an individual approach to students. But despite the significant progress in the use of an agent-based approach to support decision-making in the educational process, there are some problems that remain to be fully resolved. Although intelligent agents show the potential to improve the educational process, their widespread adoption and accessibility to all educational institutions can be a challenge. This is due to high development and implementation costs, the need for specialized skills and infrastructure. Education systems include a variety of components such as learning management, progress tracking systems, e-textbooks, etc. The challenge is to interact and integrate intelligent agents with these systems to ensure that they work together effectively. Some intelligent agents may be limited in their flexibility and adaptability to the changing needs of students and teachers. For a system to be successful, agents need to be able to quickly adapt to new requirements and change their behavior accordingly. The use of intelligent agents in the education system raises ethical and privacy issues. The collection and processing of students' personal data may raise privacy concerns and the use of this data without authorization or in countries other than its intended destination. It is also important to ensure active interaction and involvement of students in the process of using intelligent agents. Uncontrolled use of agents can lead to student passivity and loss of motivation to learn. Given these problems, further research and development of intelligent agents in the educational process is aimed at solving these issues, ensuring accessibility, flexibility, ethical use and involvement of all participants in the educational process. The objective of this work is to elevate the standard of decision-making in distance learning by examining video data on student behavior.

To achieve this aim, the following tasks are completed:

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

- design a model of an agent-based decision support system for distance learning, including its elements and their interaction;
- determine user requirements using collected data and emerging trends in education;
- formalize the recommendation process for supporting teacher decision-making;
- verify that the system works correctly in all possible scenarios, including detecting violations, blocking access to tests in case of using prohibited tools, sending warnings, and processing appeals correctly.

3. The design of an agent-driven decision support system for online learning

This work introduces a system that combines multiple components: a video surveillance subsystem designed to detect actions or circumstances that may suggest potential violations during e-testing [19]; a multi-agent system where agents engage with the video surveillance system in real time [20], analyze gathered data, and offer recommendations; temporal logic for defining the system's real-time responses to different events and states; a decision-making system that autonomously reacts to identified violations; and automated mechanisms to address violations, such as sending alerts to administrators or instructors. We propose a model for an agent-oriented decision support system (AoDSS) for distance learning, offering a conceptual view of the system's architecture and its core principles. This model leverages the agent-based paradigm to enhance and optimize remote learning, with agents serving as key contributors to the organization and refinement of the learning environment. The proposed model of a decision support system for distance learning is based on set theory and temporal logic:

$$AoDSS = \langle S, A, T, L, R \rangle, \quad (1)$$

where $S = \{s_1, s_2, \dots, s_M\}$ – a set of students, where each student $s_i \in S$ ($i = \overline{1, M}$), $A = \{a_1, a_2, \dots, a_N\}$ – is a set of agents, where each agent $a_j \in A$ performs certain functions in the system, such as providing recommendations, monitoring progress, analyzing results, etc. ($j = \overline{1, N}$); T – a set of learning materials or tasks, where each element $t_k \in T$ presents a separate learning task or material ($k = \overline{1, K}$); L – a set of knowledge or competence levels, $l_u \in L$ determines the level of success of each student ($u = \overline{1, U}$); R – is a set of recommendations or actions proposed by the system, where $r_\varphi \in R$ meets specific agent recommendations for students ($\varphi = \overline{1, \Psi}$)

Key elements of the model include. Defining the roles and functions of agents within the system, such as conducting requirements analysis, managing the training process, monitoring progress, facilitating interactions, and more. Mechanisms for agent interaction and information exchange to support decision-making. Adaptation mechanisms that enable agents to tailor the learning experience and offer recommendations based on the unique characteristics of each student. Identification of the technologies and platforms utilized for the implementation and coordination of

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

agents within the system. Mechanisms for evaluating and tracking student progress through the use of agents and their functionalities. The agent-based decision support system model for distance learning is designed to optimize the educational process, enhance communication, and assist students in achieving superior outcomes. The goal of the system is to ensure that students' results improve through optimization of the learning process and personalized recommendations.

$$G(F_L(s_i) \uparrow), \quad (2)$$

that is, at each moment of time, the level of students' knowledge increases or remains the same, which means the effectiveness of agents in the system. Here G —temporal operator “Globally” (or “Always”). It means that a certain condition must be fulfilled at every moment of time in the future, i.e. what is happening now must continue at all subsequent moments of time; $F_L(s_i)$ — is a function that maps a student s_i to his or her current level of knowledge or competencies. In other words, $F_L(s_i)$ means the level of knowledge of the student s_i at a certain point in time; \uparrow means “increase” or “improvement”, in this context, this symbol means that the student's knowledge level is increasing. Thus, expression (2) means that at all times (at any given time), the student's knowledge level s_i is either increasing or at least not decreasing. In other words, the system must ensure that the student's knowledge is constantly improving or remains at the same level, without deterioration. Expression (2) formalizes the requirement for the system: to ensure continuous improvement or stability of students' knowledge at all stages of learning. Each action or function has its own mapping between sets, and the dynamics of the system is described by temporal logic to determine the interaction between agents and students and optimize the learning process. Functions and mappings between sets in this model describe the relationships between elements of different sets (students, agents, learning materials, etc.) and reflect how each element of one set interacts or is related to elements of another set. This allows you to formalize the processes taking place in an agent-

based decision support system for distance learning. Function. $F_A: S \rightarrow A$ відображає кожного студента $s_i \in S$ на певного агента $a \in A$, який відповідає за його навчальний процес. Іншими словами, кожен студент отримує підтримку від конкретного агента, який виконує функції, пов'язані з аналізом вимог студента, організацією його навчання, моніторингом його прогресу і наданням рекомендацій. Якщо студенту s_i призначається агент a_j , який буде моніторити його успішність і надавати необхідну підтримку, тому $F_A(s_i) = a_j$.

Function. $F_T: S \rightarrow T$ displays each student $s_i \in S$ for certain training materials or assignments $t_k \in T$, that he or she has to perform or learn. These materials can be selected according to the student's level of knowledge or needs. That is, the student s_i a task is assigned t_k , which corresponds to his level of training: $F_T(s_i) = t_k$.

Function. $F_L: S \rightarrow L$ connects every student $s_i \in S$ with his level of knowledge $l_k \in L$, which reflects his or her success or progress in learning. The level of knowledge changes depending on the learning outcomes and the effectiveness of the tasks, which reflects his or her success or progress in learning. The level of

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

knowledge changes depending on the learning outcomes and the effectiveness of the tasks s_i has a level of knowledge l_u , to $F_L(s_i) = l_u$. As a student improves their performance, this feature can be updated, for example, $F_L(s_i) = l_{u+1}$. Function. $F_R: S \rightarrow R$ maps students to specific recommendations provided by agents to improve their learning. The recommendations can be individualized and take into account the student's progress, needs, and characteristics. The agent provides the student with s_i recommendation r_φ , which involves reviewing certain training material or performing additional exercises $F_R(s_i) = r_\varphi$.

These functions describe how the system manages learning processes, assignment selection, progress monitoring, and recommendation. They formalize the relationship between students and the system, allowing the system to provide personalized learning paths and improve the learning experience based on student data. Through these functions, the model determines how each student will receive personalized support to improve their performance in distance learning.

3.1 Multi-agent system

In formula (3), a multi-agent system is represented as a set of three components:

$$MAS = \{A, Act, E\}, \quad (3)$$

which consists

- a set of program agents $A = \{A_s, A_L, A_D, A_M, A_Q\}$, that operate in the environment Env, where A_s – student agent monitors the activity and academic progress of students, collects data on completed assignments, tests, and other information for further analysis; A_L – the teaching agent monitors courses, assignments, and student feedback, generates recommendations for improving materials and teaching methods to enhance teaching and decision-making in the educational environment; A_D – the data analytics agent is responsible for processing and analyzing data collected from students and teachers, identifying patterns, trends, and important connections to support decision-making; A_M – the system agent manages the interaction between other agents, distributes tasks, ensures the continuity of the system and coordination of processes; A_Q – the survey agent sends questionnaires to users, collects responses and stores them in the database;

- a set of actions of agents $Act(A_i) = \{a^1, a^2, \dots, a^n\}$; $i = S, L, D, M, Q$; for the student $A_s: Act(A_s) = \{complete_task, pass_test, review_material\}$; for the learning agent $A_L: Act(A_L) = \{generate_recommendation, analyze_reviews\}$, for the data analysis agent $A_D: Act(A_D) = \{process_data, detect_patterns\}$; for the system agent $A_M: Act(A_M) = \{distribute_tasks, ensure_synchronization\}$; for the survey agent $A_Q: Act(A_Q) = \{send_survey, collect_responses\}$; actions for each agent are defined as: $Act(A_i) \subseteq Act, \forall A_i \in A$,

- a set of possible states of the environment, which changes depending on the actions of agents and events occurring in the system $E = \{E_{Mn}, E_{Md}, E_{Un}\}$ – a set of

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

states of the environment of Student behavior monitoring subsystem (E_{Mn}), the environment of LMS Moodle (E_{Md}) and the environment of University Web portal (E_{Un}), ($E_j = \{e_1, e_2, \dots, e_m\}, j = (Mn, Md, Un)$). For example, the set of states E_{Md} may include the following elements: e_1 – all tasks are completed, e_2 – the student needs help, e_3 – all reviews are collected, e_4 – the analytical report is ready.

The transition between states of the environment depends on the actions of agents. Let's introduce the function of transition between states:

$$\delta: E \times Act \rightarrow E.$$

This function determines how the agent's action affects the state of the environment. For example:

$$\delta(e_i, a_j) = e_{i+1}.$$

This means that after performing an action a_j (for example, completion of a task), the state of the environment changes from e_i (all tasks completed) on e_{i+1} (student needs help).

Recording changes in environment states over time $G(\delta(e_i, a_j) = e_{i+1})$ means that always after performing an action a_j , the state will change from e_i on e_{i+1} .

For example, an agent A_s performs an action a_1 (completes the task), which changes the state of the environment from e_1 on e_2 : $\delta(e_1, a_1) = e_2$. Learning agent A_L performs an action a_2 (generates a recommendation) after analyzing student feedback, which changes the state of the environment to e_3 (all reviews are collected): $\delta(e_2, a_2) = e_3$.

This model describes a multiagent system through sets of agents, actions, and environment states. The transition function allows you to track how the actions of agents affect the environment, and temporal logic allows you to control the change of states over time. The function of the learning agent $F_L: C \times R \rightarrow Act(A_L)$ generates recommendations based on student feedback, where C — courses, R — reviews. The behavior specification of a polling agent is described by the expression $F_Q: U \rightarrow Q$, where U – system users, and Q – Questionnaires. The agent sends questionnaires to users and collects responses:

$$G(F_Q(u) = q), u \in U, q \in Q.$$

For the system as a whole, optimization of the learning process corresponds to

$$G(\forall s \in S, a \in Act(A_s): \delta(e_i, a_j) = e_{i+1}),$$

which means that the student's actions always lead to changes in the environment that contribute to better results.

The survey agent always helps to improve communication by collecting responses:

$$G(\forall a \in Act(A_Q): \delta(e_i, a_j) = e_{i+1}).$$

Assistance in achieving results looks like this:

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

$$F(\forall a \in Act(A_L): \delta\delta(e_i, a_j) = e_{i+1}),$$

i.e., the recommendations of the learning agent ultimately lead to better results for students. These formulas formally describe a multi-agent decision support system, defining its structure, agent behavior, actions, and interactions with the environment through sets and logic.

3.2 Application of temporal logic

Temporal logic is important for analyzing and managing temporal aspects in systems where various events and processes occur over time. Therefore, we will create a formal specification of agents using temporal logic for decision making in distance learning. This approach allows us to create accurate and systematic models of agents and their behavior in a virtual learning environment. The formalization of agents and their behavior allows you to ensure the quality of learning and optimize the process, which is especially important in distance learning. Formulas in temporal logic express relationships between events, states, or properties of objects at different points in time. To create formulas, we use:

- Logical operators. Temporal logic uses logical operators such as AND, OR, NOT, IMPLIES, EQUIV to build complex expressions from basic temporal or logical statements.

- Temporal operators. Temporal logic has its own temporal operators, such as "Next" (X(r) – in the next step: agents automatically adapt the curriculum for the student at the next stage based on the analysis results), "Until" (U(p, q) – “until”: students complete current learning tasks until an improvement in their knowledge level is achieved), "Future" (F(q) or \diamond – in the future: for each student there is a point in time when the system will offer optimized recommendations to improve academic performance.), "Globally" (G(p) or [] – globally (always): if p is true in all future states of the system, then each student receives educational materials according to his/her level of knowledge), which are used to express relationships between events at different points in time, operator "Release" (R) indicates that the event it wraps will be true until the second event occurs.

- Parameterization. Formulas can contain parameters that depend on a specific context or system conditions. This allows you to generalize formulas and ensure their use in different scenarios.

- Quantifiers. Temporal logic can use quantifiers such as "For All" (\forall) and "Exists" (\exists) to express general or existing relationships between events.

- Event and state identifiers. Formulas can contain identifiers of events, states, or object properties that are used to describe temporal aspects and their relationships with system states.

- Actions and events. Formulas can include a description of actions, events, or observations that occur in the system and their impact on the states and properties of the system over time.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

• Relationships to other logical and mathematical systems. Formulas in temporal logic can use constructs and concepts from other logical and mathematical systems to further express temporal properties.

Temporal logic allows you to describe the evolution of the system state in time.

Let t — moment in time. Then formalizing the situation when the learning process for a student s_i at any given time must comply with:

- specific learning material or task t_k , that he is working on,
- and a fixed level of knowledge l_u , that this student has at the moment

$$G(F_T(s_i) = t \wedge F_L(s_i) = l_u), \quad (4)$$

$$F(F_R(s_i) = r_\varphi), \quad (5)$$

$$X(F_T(s_i) = t_k' \wedge F_R(s_i) = r_\varphi'), \quad (6)$$

$$(F_T(s_i) = t_k) \cup F_L(s_i) = l_u'), \quad (7)$$

where t_k' – new training materials, a r_φ' – new recommendations, $l_u' > l_u$.

Expression (4) means that always (at each stage or at each moment in time):

- student s_i a specific task or learning material is assigned t_k ,
- and at the same time the level of knowledge of this student s_i is equal to l_u .

This formalizes the situation when the educational process for a student s_i at any given time must comply with:

- specific learning material or task t_k , that he is working on,
- and a fixed level of knowledge l_u , that this student has at the moment.

This logical formula can be used to check the correctness of the learning process in the system: the student should always know his or her current level of knowledge and the material he or she is studying. Expression (5) means that in the future (at some point) the student s_i achieve the result r_φ . In other words, in the future, the condition must be met that the student's result s_i will be equal to r_φ . If it is a student

s_i will be evaluated $r_\varphi=85$, the expression $F(F_R(s_i) = 85)$, means that in the future the student s_i will achieve a score of 85 points. This condition does not require immediate or constant fulfillment, but it must occur at some point in the future. That is, the temporal operator F sets the condition for achieving a certain result in the future, and the expression $F_R(s_i) = r_\varphi$ determines what kind of result the student s_i should achieve. The entry (6) means that at the next moment in time, the student s_i a new task will be assigned t_k' , at the same time the student's result s_i will be equal to r_φ' . Function. $F_T(s_i) = t_k$ reflects the student s_i to a learning task or material t_k' in the system. That is, a student s_i at the next time a new task will be assigned t_k' .

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

Function. $F_R(s_i) = r_{\varphi}'$ determines the student's result s_i у системі. У наступний момент часу результат студента s_i will be equal to r_{φ}' , де r_{φ}' – a certain level of performance or score. For example, if a student s_i is currently performing the following tasks t_k , and its result is currently equal to r_{φ} . Recording $X(F_T(s_i) = t_k' \wedge F_R(s_i) = 85)$ means that at the next point in time, the student s_i a new task will be assigned t_k' , and at the same time its result will be 85 points. Expression (7) means that either the student s_i a task has been assigned t_k , or the student's level of knowledge s_i is equal to l_u' , or both conditions can be met simultaneously. For example, if a student s_i a task has been assigned t_3 (e.g., the third assignment in the course), and its level of knowledge may be equal to l_5 (level five). Expression. $((F_T(s_i) = t_3) \cup F_L(s_i) = l_5')$, means that either the student is assigned a task t_3 , or his level of knowledge is l_5 (or both statements are true at the same time). One approach is to use a formal language such as LTL to define temporal logic rules. LTL expressions include time operators that allow you to express conditions and state changes over time. A rule for detecting misbehavior over time, i.e., if there is a moment in time when misbehavior is detected, then the agent should respond:

LTL expression: \diamond (Unlawful_Behavior).

A rule to check for misbehavior at a certain frequency, i.e., if misbehavior is detected during each "Period" of steps, then the agent should react:

LTL expression: \diamond (Unlawful_Behavior) U (every_n_steps(Period)).

The rule for the appeal period, i.e.: "There is a point in time when the breach notification was sent, and this event is true until the appeal response is received."

LTL expression: \diamond (Sent_Notification_of_Violation) R \diamond (Received_Appeal_Response).

A rule to prohibit the use of aids, i.e. if a student has used aids, the agent must block the test:

LTL expression: \diamond (Used_Auxiliary_Tools) \rightarrow \diamond (Block_Test).

The rule for applying warnings, i.e. if a violation is detected, the agent must send a warning:

LTL expression: \diamond (Violation_Detected) \rightarrow \diamond (Send_Warning).

For the formal specification of agent-based decision making in distance learning, we use the formal description language TLA+ (Temporal Logic of Actions). TLA+ allows modeling and formalizing systems with temporal aspects, and helps to express and verify the properties of specific systems, including distributed systems and algorithms. This specification language allows you to formally define systems, taking into account their logic and dynamics. This helps to avoid misunderstandings and allows you to accurately define the expected behavior of the system.

The formal specification of an agent-oriented decision support system for distance learning is given by the following formulas:

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

Specification 1:

```

◇ (Unlawful_Behavior)
◇ (Unlawful_Behavior) U (every_n_steps(Period))
◇ (Sent_Notification_of_Violation) R ◇ (Received_Appeal_Response)
◇ (Used_Auxiliary_Tools) → ◇ (Block_Test)
◇ (Violation_Detected) → ◇ (Send_Warning)
G (time = 0 → (testQuestions = <<q1, q2, q3>> ∧ studentAnswers = <<>> ∧
teacherRecommendations = <<>> ∧ violations = <<>> ∧ appeals = <<>>))
G (time < MaxTime → (∃ student ∈ DOMAIN(studentAnswers): X
(studentAnswers[student][time] = CHOOSE answer ∈ testQuestions)))
G (time = MaxTime → X GenerateTeacherRecommendations)
G (GenerateTeacherRecommendations → (CheckForViolations ∧
CheckForAppeals ∧ CheckForWarning))
G (CheckForViolations → (violations' = ...))
G (CheckForAppeals → (appeals' = ...))
G (CheckForWarning → (IF violations' > WarningThreshold THEN
teacherRecommendations' = AppendWarning(teacherRecommendations) ELSE
teacherRecommendations' = teacherRecommendations ENDIF))
G (AppendWarning(recommendations) → (teacherRecommendations' =
Append(recommendations, "Warning")))
G (AppealDecision → (∃ appeal ∈ appeals: (IsValidAppeal(appeal) ∧
ProcessAppeal(appeal))))
G (WarningDecision → (IF violations > WarningThreshold THEN
teacherRecommendations' = AppendWarning(teacherRecommendations) ELSE
teacherRecommendations' = teacherRecommendations ENDIF))

```

3.3. Verification of multi-agent systems in education

To verify the correctness of concurrent software models, a generic tool called SPIN is used, which is aimed at efficiently verifying multithreaded software. Spin has been used to track down logical errors in the design of distributed systems such as operating systems, data communication protocols, switching systems, parallel algorithms, railroad signaling protocols, spacecraft control software, nuclear power plants, and more. The tool checks the logical sequence of the specification and interlock reports, competition conditions, different types of incompleteness, and unreasonable assumptions about the relative speed of processes. The properties to be checked are expressed as linear time logic (LTL) formulas. That is, you can formally specify the expected behavior of the system and check its fulfillment. To verify the proposed model using SPIN, we define the main components of the system, including agents, their actions, possible states, and state transition functions in Promela:

Each agent is presented as a separate procedure proctype

- Agent actions are represented as conditional blocks if/else or do/od, where the agent changes its state depending on the conditions.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

- Agent states are defined through variables of type mtype.
- Transitions between states are realized with the help of conditional structures.

Then the model of a multiagent system will be presented in the following form:

```
mtype = {idle, active, analyzing, communicating, done}; // The set of agent states
```

```
mtype = {complete_task, pass_test, view_material, generate_recommendation,  
analyze_feedback, send_survey, collect_responses, process_data, detect_patterns}; //
```

A set of agent actions

```
chan communication = [1] of {mtype}; // A channel for exchanging messages  
between agents
```

```
// Procedure for a student agent
```

```
proctype AgentStudent() {
```

```
    mtype state = idle; //Initial state of the student agent
```

```
    do
```

```
        :: (state == idle) -> state = complete_task;
```

```
        :: (state == complete_task) -> state = pass_test;
```

```
        :: (state == pass_test) -> state = view_material;
```

```
        :: (state == view_material) -> communication!done
```

```
        :: (state == done) -> break;
```

```
    od;
```

```
}
```

```
// Procedure for a training agent
```

```
proctype AgentLearning() {
```

```
    mtype state = idle; // The initial state of the training agent
```

```
    do
```

```
        :: (state == idle) -> state = analyze_feedback;
```

```
        :: (state == analyze_feedback) -> state = generate_recommendation;
```

```
        :: (state == generate_recommendation) -> communication?done -> state =
```

```
done;
```

```
    od;
```

```
}
```

```
// Procedure for a data analysis agent
```

```
proctype AgentDataAnalysis() {
```

```
    mtype state = idle; // The initial state of the data analysis agent
```

```
    do
```

```
        :: (state == idle) -> state = process_data;
```

```
        :: (state == process_data) -> state = detect_patterns;
```

```
        :: (state == detect_patterns) -> communication!done;
```

```
        :: (state == done) -> break;
```

```
    od;
```

```
}
```

```
// Procedure for a survey agent
```

```
proctype AgentSurvey() {
```

```
    mtype state = idle; // The initial state of a survey agent
```

```
    do
```

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

```
    :: (state == idle) -> state = send_survey;
    :: (state == send_survey) -> state = collect_responses;
    :: (state == collect_responses) -> communication!done;
    :: (state == done) -> break;
  od;
}
// Procedure for system agent
proctype AgentSystem() {
  mtype state = idle; // The initial state of the system agent
  do
    :: (state == idle) -> state = active; // System activation
    :: (state == active) -> state = done; // Termination of interactions with other
agents
  od;
}
// Initialization of all agents
init {
  atomic {
    run AgentStudent();
    run AgentLearning();
    run AgentSurvey();
    run AgentDataAnalysis();
    run AgentSystem();
  }
}
```

States idle, active, analyzing, communicating, done represent different stages in the work of agents: waiting, active work, analysis, communication, and completion. Each agent performs its actions depending on its current state. The transitions between agent states are defined in conditional statements do/od, where each agent changes its state in accordance with the specified conditions. After reviewing the materials, the agent AgentStudent sends messages via the communication channel. Agent AgentLearning receives notifications from the channel after the agent completes tasks AgentStudent and exits the survey. When the collection of responses is complete, AgentSurvey sends a message through the channel. To simplify the system, we assume that AgentSystem remains unchanged, only activates the system and exits. Channel. communication is used to exchange states between agents. Agent AgentStudent and agent AgentSurvey send messages to the channel, and the agent AgentLearning receives them and reacts accordingly. We use this model to test the interaction of agents in SPIN to make sure that they perform their actions correctly and communicate with each other through the communication channel.

In the simulation mode, we can see how agents change their states and transmit messages through channels. For example, an agent AgentStudent completes its task and sends a message through the channel, and the agent AgentLearning receives this message and continues its work. After executing the simulation command: spin -p -g -l model.pml, we get the following result:

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

```

1: proc 0 (init) line 26 "model.pml" (state 1) [atomic {run AgentStudent();run
AgentLearning();}]
2: proc 1 (AgentStudent) line 6 "model.pml" (state 1) [state == idle]
2: proc 1 (AgentStudent) line 6 "model.pml" (state 2) [state = active]
3: proc 1 (AgentStudent) line 7 "model.pml" (state 2) [communication!done]
3: proc 1 (AgentStudent) line 8 "model.pml" (state 3) [state == done]
4: proc 2 (AgentLearning) line 12 "model.pml" (state 1) [state == idle]
4: proc 2 (AgentLearning) line 12 "model.pml" (state 2) [state = analyzing]
5: proc 2 (AgentLearning) line 13 "model.pml" (state 2) [communication?done]
5: proc 2 (AgentLearning) line 14 "model.pml" (state 3) [state =
communicating]
6: proc 2 (AgentLearning) line 15 "model.pml" (state 4) [state == done]

```

Thus, the process of proc 1 (AgentStudent) means that the AgentStudent agent starts in the idle state (line 2), moves to the active state (line 2); the AgentStudent agent sends a done message through the communication channel (line 3); the AgentStudent agent completes its work by moving to the done state (line 3). The process proc 2 (AgentLearning) means that the AgentLearning agent starts in the idle state (line 4), enters the analyzing state (line 4); the AgentLearning agent waits for a message through the channel. As soon as it receives a done message, it enters the communicating state (line 5). After that, the AgentLearning agent completes its work by switching to the done state (line 6). The analysis shows that the transmission of a message through the communication!done channel from the AgentStudent agent is successful, and the AgentLearning agent receives this message through communication?done. Both agents correctly change their states and complete their work, which is evident at the end of the simulation for both processes in the done state. This simulation result demonstrates the correctness of the interaction of agents through the communication channel and the execution of their actions.

LTL formulas make it possible to formally describe the behavioral properties of multi-agent systems and check their correctness using SPIN. For this purpose, the following operators are used [], <>, X, U and others, which are translated into Promela through the corresponding expressions ltl. (Table 1).

Table 1
Designation of specific LTL operators in keywords in Promela

Operators LTL	Promela keywords
[](p)	ltl always_p { [](p) }
<>(q)	ltl eventually_q { <>(q) }
X(r)	ltl next_r { X(r) }
p U q	ltl until_p_q { (p) U (q) }
p -> q	ltl implication_p_q { (p -> q) }
[](p -> <>q)	ltl always_p_eventually_q { [](p -> <>q) }

To verify the formal specification of an agent-based decision support system for distance learning using SPIN and the Promela language, we translate logical formulas based on linear temporal logic (LTL) (Specification 1) into the Promela code:

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

Step 1. Translate LTL formulas into Promela to check system properties:

```

ltl p1 { <> (Unlawful_Behavior) }
ltl p2 { <> (Unlawful_Behavior U every_n_steps(Period)) }
ltl p3 { <> (Sent_Notification_of_Violation) R <> (Received_Appeal_Response)
}

ltl p4 { <> (Used_Auxiliary_Tools) -> <> (Block_Test) }
ltl p5 { <> (Violation_Detected) -> <> (Send_Warning) }
...

```

Step 2. Creating a system model in Promela based on the specification of agents, their actions, states, and possible events (e.g., violations, test blocking, etc.).

```

mtype = {idle, active, analyzing, violation_detected, send_warning, block_test};
proctype AgentStudent() {
    mtype state = idle;
    do
        :: (state == idle) -> state = active;
        :: (state == active) -> // Actions like completing tasks, answering questions
    od;
}
proctype AgentLearning() {
    mtype state = idle;
    do
        :: (state == idle) -> state = analyzing;
        :: (state == analyzing) -> // Generate recommendations
    od;
}
// Define LTL formula for detecting violations and warnings
ltl p1 { <> (violation_detected) }
ltl p2 { violation_detected -> <> (send_warning) }
// Initialize system
init {
    atomic {
        run AgentStudent();
        run AgentLearning();
    }
}

```

Step 3. Generate a model for verification

Step 4. Compile the generated code

Step 5. Run the verification of each formula.

Step 6. Analyze the results.

For example, we check the property that guarantees that “sooner or later a violation will occur in the system,” i.e. Unlawful_Behavior: `ltl p1 { <> (Unlawful_Behavior) }`

This means that on any system execution path, the Unlawful_Behavior event must occur at least once in the future.

When checking this property, SPIN can return several different results:

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

- Successful verification, if the system always has at least one execution path on which the Unlawful_Behavior event occurs at least once, SPIN will confirm that the system meets the specified formula (Fig. 1):

Valid: The formula holds in all executions of the system.

Figure 1. Successful verification

- Verification error, if SPIN finds an execution path where the Unlawful_Behavior event never occurs (for example, the system can run indefinitely without a violation occurring), SPIN will return an error message and we will get an execution trace showing exactly how this situation occurred (Fig. 2).

Error: The formula does not hold in all executions.

Figure 2. Verification error

If the system loops, if the system enters an infinite loop and Unlawful_Behavior is never called, SPIN can determine this as an LTL formula violation. That is, in an infinite loop, the system never reaches a state where Unlawful_Behavior can occur.

If the verification fails, SPIN provides an execution trace that shows the sequence of states the system went through and the events that did or did not occur. The execution trace is presented as a sequence of events and states of the system, which allows us to recreate how the system moved between states and where the verified property (LTL formula) was violated.

The execution trace contains information about the values of variables, communication channels, process states, and events that occurred at each step:

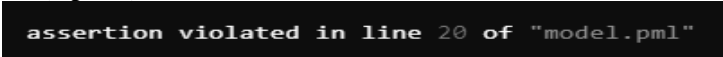
Trace for assertion violation

```
proc 0 (AgentStudent) line 10 "model.pml" (state 3)
proc 1 (AgentLearning) line 15 "model.pml" (state 2)
proc 2 (AgentDataAnalysis) line 20 "model.pml" (state 1)
proc 3 (AgentSystem) line 25 "model.pml" (state 4)
proc 4 (AgentSurvey) line 30 "model.pml" (state 2)
step 0: proc 0 (AgentStudent)
  state change: state -> active
step 1: proc 1 (AgentLearning)
  state change: state -> analyzing
step 2: proc 0 (AgentStudent)
  state change: state -> done
step 3: proc 2 (AgentDataAnalysis)
  state change: state -> done
step 4: proc 3 (AgentSystem)
  state change: state -> done
step 5: proc 1 (AgentLearning)
  state change: state -> communicating
step 6: proc 4 (AgentSurvey)
  state change: state -> analyzing_survey
step 7: assertion violated in line 20 of "model.pml"
```

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

Each “step” represents one step of system execution. Steps include information about which process (agent) was active and what state changes occurred. For example, in step 0, the AgentStudent process went to the active state, and in step 2, the same agent changed its state to done.

Processes represent system agents or other independent parts of the program. Each process has its own number and name (for example, AgentStudent), as well as a line of code and the state of the process at the time of the trace. If the trace leads to a specification violation, SPIN indicates the line of code where the violation occurred (Figure 3):



```
assertion violated in line 20 of "model.pml"
```

Figure 3. Property violation on line 20 of the code

Thus, specification verification using SPIN and Promela ensures high reliability and accuracy of agent-based system development, helps minimize risks, and improves the overall quality of the system, especially in the context of distance learning, where the requirements for process correctness are particularly high.

3.4. Recommendation subsystem

To solve the urgent problems of each of the participants in the educational process, a subsystem for assessing student and teacher satisfaction has been developed. This approach allows for effective management of internal learning processes in an educational institution. The implementation of the subsystem for assessing student satisfaction using the online platform consists of the following stages.

Stage 1: Set the goal of increasing student and faculty satisfaction to a certain level. To measure satisfaction, we define key performance indicators (KPIs).

We develop questionnaires with questions that cover all aspects of using the platform. This questionnaire includes both closed and open-ended questions, which allows us to obtain both quantitative and qualitative data on student satisfaction with the online platform.

Stage 2. The online platform Google Forms was chosen for the surveys.

Questionnaire processing consists of collecting responses, processing data, analyzing results, and preparing a report.

Questionnaire processing algorithm:

Step 1. Placement of the questionnaire: Publish the questionnaire on an online platform or send it out by email. Set a deadline for submitting responses.

Step 2. Data collection: Saving all answers in a single database or spreadsheet.

Step 3. Data preparation: Exporting the collected responses to a format convenient for processing (CSV or Excel). Checking the data for completeness and correctness.

Step 4. Categorization of answers: Dividing data into categories according to the questionnaire questions.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

Step 5. Calculation of quantitative indicators: For closed-ended questions (scoring on a scale from 1 to 5), calculate mean, median, mode, and other statistics. Build graphs and charts to visualize the results.

Step 6. Calculation of quantitative indicators: For closed-ended questions (scoring on a scale from 1 to 5), calculate mean, median, mode, and other statistics. Build graphs and charts to visualize the results.

Step 7. Analysis of open responses: Analyzing open-ended responses to identify key themes and trends. Build word clouds or other visual representations to help interpret the results.

Step 9. Interpretation of quantitative data: Identify key trends and problem areas based on the calculated statistical indicators. Comparison of results between different groups (e.g., among students by age, course, etc.).

Step 9. Interpretation of qualitative data: Identification of the main topics and problems mentioned by participants in open-ended responses. Assessment of the general mood and tone of the answers.

Step 10. Preparation of the report: Prepare a report that includes key findings from the data analysis. Include graphs, charts and other visuals to illustrate the results.

Step 11. Recommendations: Developing recommendations based on the results to improve the online platform. Identification of priority areas for implementation of changes.

Step 12. Communication of results: Presentation of the report to the stakeholders (school administration, teachers, technical support). Publishing a summary of the main results for participants.

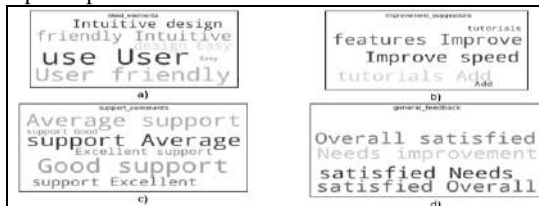


Figure 4. a) The "liked_elements" cloud shows the most popular or frequently mentioned elements or features that user liked about the product. b) The "improvement_suggestions" cloud shows user recommendations for improvements in the product. c) The "support_comments" cloud displays user comments about the quality of support. d) The "general_feedback" cloud shows the general feedback users have given to the product.

Create the file `survey_responses.csv`, which will contain the survey data, containing columns that correspond to the survey questions. This file contains data from the survey, where each row represents the response of one survey participant to different questions. Each column corresponds to a specific question or aspect that was rated by the participants on a scale from 1 to 5, where 1 is very bad and 5 is very good. These graphs help to understand how users perceive a product or service and identify possible areas for improvement. In this case, qualitative data processing

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

graphs are word clouds that visualize the most common words or phrases found in user comments. Each of these graphs corresponds to a specific question in the questionnaire (Fig. 4). This data will be used to analyze user satisfaction and identify areas for product or service improvement (Fig. 5).

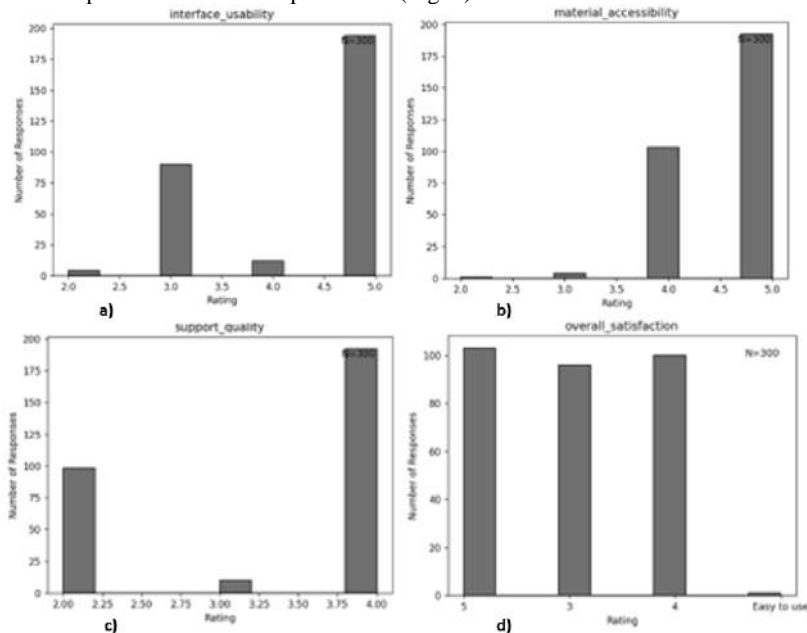


Figure 5. a) The *interface_usability* graph shows the distribution of user ratings on the interface usability scale. b) The *material_accessibility* graph shows the distribution of material accessibility scores. c) The *support_quality* graph shows the distribution of support quality scores. d) The *overall_satisfaction* graph shows the distribution of overall user satisfaction with the product or service

Based on the data analysis, the following recommendations were made for teachers:

- Improve support for technical and methodological issues – if the average value for this criterion is less than 4, technical and methodological support for teachers should be improved.
- Enhance opportunities for interactive interaction with students - if the average value for this criterion is less than 4, you need to increase opportunities for interactive interaction with students.
- Provide more options for professional development – if the average value for this criterion is less than 4, more opportunities for professional development of teachers should be provided.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

Based on the analysis of the results of the survey of teachers on their satisfaction with the use of the online platform, several main areas for improvement can be identified:

1. Increase the efficiency of using electronic resources for teaching.

According to the survey, teachers evaluate the effectiveness of the use of electronic resources for teaching with an average of 4 out of 5 points. This shows overall satisfaction, but also indicates that there is room for improvement.

Recommendations: Simplify navigation and access to materials. Add the ability to create interactive learning materials (e.g., interactive presentations, video tutorials with interactive elements). Introduce new test formats and automatic tools for assessing students' knowledge.

2. Support for teachers in the use of e-learning systems.

Technical and methodological support received an average score of 4 out of 5, which indicates a sufficient level of satisfaction, but also points to the need for improvement.

Recommendations: Provide round-the-clock technical support through various channels (chat, phone, email). Regularly conduct trainings on how to use the platform, including new features and best practices. Provide an opportunity to order individual consultations to solve specific problems.

3. Expanding opportunities for interactive interaction with students.

Opportunities for interactive interaction with students are rated 4 out of 5, which shows the need for additional features to improve interaction.

Recommendations: Introduce additional tools for video conferencing, interactive forums and chats. Expand feedback opportunities, for example, by adding the ability to conduct surveys and questionnaires in real time. Introduce gamification elements to increase student motivation.

4. Assessment of opportunities for professional development of teachers.

Opportunities for professional development through the use of e-learning systems received an average score of 4 out of 5, which indicates the need to expand such opportunities.

Recommendations: Introduce professional development programs that include courses, webinars, and the possibility of obtaining certificates. Create a platform for the exchange of experience and best practices among teachers. Introduce a system of incentives for participation in professional development programs. The results of the survey show the overall satisfaction of teachers with various aspects of e-learning, as the average scores are at the level of 4 or higher.

4. Conclusion

The article proposes an agent-based method for improving the efficiency of e-learning, which consists of the following stages:

Stage 1: Analysis and preparation. The main goals of the system are identified: improving learning efficiency, automating processes, increasing student and teacher

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

satisfaction. Existing systems and limitations were analyzed, and suitable technologies for agent-based systems were explored.

Stage 2. System design. The main components of the system were identified: a video surveillance subsystem, a multi-agent system, and a decision-making system. The architecture of interaction between the components was designed. Agents' roles and functions (data collection, analysis, recommendations) were established, and their interaction algorithms were formalized.

Stage 3. Verification. Formal confirmation of the correctness of the specification of the agent-based decision support system for distance learning was conducted using SPIN and the Promela language, which provides confidence that the system will work as expected, especially for critical properties such as preventing violations, providing timely feedback, and guaranteeing the accuracy of recommendations. Using SPIN allowed us to test different scenarios of agents' operation and their interaction at the design stage, which helps to avoid mistakes during the development phase or during system operation. The correctness of agent interactions was checked.

Stage 4. Development and implementation. Program modules for agents were developed, a video surveillance subsystem implemented, and both functional and integration testing were performed.

This method automates monitoring, analysis, and decision-making, improving education quality and satisfaction. Verification ensures system reliability and security. Simulation results show agents interact correctly and fulfill their tasks.

5. References

- [1] Graesser, C. Arthur, Hu Xiangen, and Robert Sottolare, "Intelligent tutoring systems," *International handbook of the learning sciences*. Routledge, 2018. pp.246-255.
- [2] Nouri Jalal, "Editorial of the First Issue of the International Journal of Learning Analytics and Artificial Intelligence for Education," *International journal of learning analytics and artificial intelligence for education* 1.1, 2019. pp. 4-7.
- [3] F. Ouyang, P. Jiao, "Artificial intelligence in education: The three paradigms," *Computers and Education: Artificial Intelligence*, 2, 2021,100020.
- [4] M. Cukurova, C. Kent, R. Luckin, "Artificial intelligence and multimodal data in the service of human decision-making: A case study in debate tutoring," *British Journal of Educational Technology*, 50 (6), 2019, pp. 3032-3046.
- [5] C. Campbell, "The three paradigms of Artificial intelligence in secondary school education," *Computers and Education: Artificial Intelligence*, 2, 2022, 100020.
- [6] Shahbazi, Zeinab, and Yung-Cheol Byun, "Agent-based recommendation in E-learning environment using knowledge discovery and machine learning approaches," *Mathematics* 10.7, 2022, 1192.
- [7] Krouska, C. Troussas, M. Virvou, "SN-Learning: An exploratory study beyond e-learning and evaluation of its applications using EV-SNL framework," *J. Comput. Assist. Learn.* 2019, 35, pp. 168–177.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

- [8] M.S. Rafiq, X. Jianshe, M. Arif, P. Barra, “Intelligent query optimization and course recommendation during online lectures in E-learning system,” *J. Ambient. Intell. Humaniz. Comput.* 2021, 12, pp. 10375–10394.
- [9] Mbipom, S. Craw, S. Massie, “Improving e-learning recommendation by using background knowledge,” *Expert Syst.* 2021, 38, e12265.
- [10] Y.R. Shrestha, S. M. Ben-Menahem, G. Von Krogh, “Organizational decision-making structures in the age of artificial intelligence,” *California Management Review*, 61(4), 2019, pp. 66-83.
- [11] R. X. Ding, I. Palomares, X. Wang, G. R. Yang, B. Liu, Y. Dong, & F. Herrera, “Large-Scale decision-making: Characterization, taxonomy, challenges and future directions from an Artificial Intelligence and applications perspective,” *Information fusion*, 59, 2020, pp. 84-102.
- [12] E. Carrillo, S. Yeotikar, S. Nayak, M. K. M. Jaffar, S. Azarm, J. W. Herrmann, H. Xu, “Communication-aware multi-agent metareasoning for decentralized task allocation”, *IEEE Access*, 2021, 9, pp. 98712-98730.
- [13] Abate, J. Gutierrez, L. Hammond, P. Harrenstein, M. Kwiatkowska, M. Najib, M. Wooldridge, “Rational verification: game-theoretic verification of multi-agent systems”, *Applied Intelligence*, 2021. 51(9), pp. 6569-6584.
- [14] R. Calegari, G. Ciatto, V. Mascardi, et al., “Logic-based technologies for multi-agent systems: a systematic literature review”, *Auton Agent Multi-Agent Syst* 35, 1, 2021. <https://doi.org/10.1007/s10458-020-09478-3>
- [15] Nicolas Markey. Temporal Logics for Multi-Agent Systems (Invited Talk). In 42nd International Symposium on Mathematical Foundations of Computer Science (MFCS 2017). Leibniz International Proceedings in Informatics (LIPIcs), Volume 83, pp. 84:1-84:3, Schloss Dagstuhl - Leibniz-Zentrum für Informatik. 2017 <https://doi.org/10.4230/LIPIcs.MFCS.2017.84>
- [16] Rybakov, V. V. Temporal Multi-Agents’ Logics Modelling Dynamic Temporal Accessibility Relations. *Procedia Computer Science*, 207, 2022, pp. 475-482.
- [17] Hammond, L., Abate, A., Gutierrez, J., & Wooldridge, M. Multi-agent reinforcement learning with temporal logic specifications. *arXiv preprint arXiv:2102.00582*, 2021.
- [18] Lamport, L. The temporal logic of actions. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, 16(3), 1994, pp. 872-923.
- [19] Axak N., Tatarnykov A., The Behavior Model of the Computer User, *IEEE 17th International Conference on Computer Sciences and Information Technologies (CSIT)*, 2022, pp. 458-461.
- [20] Axak N., Kushnaryov M., Tatarnykov A., The Agent-Based Learning Platform. *ICST-2023: XI International Scientific and Practical Conference “Information Control Systems and Technologies”*, September 21-23, 2023, Odessa, Ukraine, Vol-3513, pp. 263-275.
- [21] Axak N. G., Gryzun L. E., Shcherbakov O. V. [and others]; in general ed. V. S. Ponomarenko, “Modern information technologies and systems”: monograph /— *Electron. text data (22.9 MB)*. — Kharkiv: HNEU named after S. Kuznetsia, 2022. — pp. 7–34. URL: <http://repository.hneu.edu.ua/handle/123456789/29233>. (in Ukrainian).

АГЕНТНИЙ ПІДХІД ДО ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ
ЕЛЕКТРОННОГО НАВЧАННЯ

Dr.Sci. Н. Аксак ORCID: 0000-0001-8372-8432

*Харківський національний університет радіоелектроніки, Україна
E-mail: nataliia.axak@nure.ua*

Ph.D. М. Кушнарєв ORCID: 0000-0002-3772-3195

*Харківський національний університет радіоелектроніки, Україна
E-mail: maksym.kushnarov@nure.ua*

А. Татарников ORCID: 0000-0002-1632-8188

*Харківський національний університет радіоелектроніки, Україна
E-mail: andrii.tatarnykov@nure.ua*

Анотація. У роботі розглядаються такі проблеми сучасного дистанційного навчання, як індивідуалізація навчального процесу. Обґрунтовано необхідність вдосконалення методів підтримки дистанційного навчання для підвищення якості освіти. Дослідження спрямоване на підвищення якості освіти та організації навчального процесу за дистанційної форми навчання. Запропоновано комплекс взаємопов'язаних завдань, розв'язання яких полягає в організації ефективної взаємодії викладача та системи управління навчанням (LMS) за допомогою агентного підходу. Основним результатом, який визначає новизну роботи, є формалізація та інтеграція таких процесів: (i) генерування в режимі реального часу пропозицій викладачеві щодо контролю за виконанням завдань під час іспитів чи електронного тестування; (ii) моніторинг навчання студентів протягом семестру з можливістю зміни траєкторії навчання; (iii) моніторинг присутності батьків на онлайн-класах; (iv) створення рекомендацій для керівництва та інших зацікавлених сторін щодо покращення онлайн-навчання. Також представлено перевірку формальної специфікації системи прийняття рішень на основі агентів для дистанційного навчання з використанням інструменту SPIN та мови моделювання Promela. Верифікація здійснюється за формулами лінійної часової логіки (LTL), що дозволяє перевірити коректність взаємодії між агентами та виконання ключових властивостей системи, таких як своєчасна обробка даних, реагування на порушення виконання студентами тестування, правила та рекомендації вчителів. Моделювання прототипу запропонованої системи підтверджує ефективність її використання як засобу дослідження організації навчального процесу. Він показує, як агенти можуть допомогти збирати й аналізувати дані про те, наскільки ефективно використовуються електронні ресурси для навчання студентів і викладачів.

Ключові слова: система управління навчанням, моніторинг, навчальний процес, агенти, хмарні обчислення, специфікації часової логіки розподіленої системи, часова логіка змінного часу, верифікація

Section 2. Intelligent systems and data analysis

UDC 004.71

**METHOD OF ASSESSING AND FORECASTING THE TECHNICAL
STATE OF COMPLEX SYSTEMS OF CRITICAL APPLICATION
BASED ON PRECEDENTS**

Ph.D. O. Vychuzhanin ORCID: 0000-0001-8779-2503

Odesa Polytechnic National University, Ukraine

E-mail: vychuzhanin.o.v@op.edu.ua

Dr.Sci. V. Vychuzhanin ORCID: 0000-0002-6302-1832

Odesa Polytechnic National University, Ukraine

E-mail: v.v.vychuzhanin@op.edu.ua

***Abstract.** A method of assessing and forecasting the technical condition of complex critical application systems based on precedents has been developed. When presenting a precedent in the form of a set of parameters with specific values and decisions, the following are taken into account: parameters describing the precedent; risk assessment, probability of failure and assessment of damage from failure of complex systems; recommendations of the decision-maker; assessments of working capacity (partial or full); refined estimates of parameters of the technical condition of complex systems; the predicted values of the parameters of the technical state of complex systems are specified. An information intelligent system for assessing and forecasting the technical condition of complex systems of critical application has been developed using the method of reasoning based on precedents (CBR) and a decision-making strategy has been developed for finding equipment failures based on established assessments of their technical condition. To check the performance, the simulation of the full cycle of functioning of the information intelligent evaluation system, forecasting the probability (risk) of failures of complex systems was carried out using the example of a ship's power plant. The obtained values of probability (risk) estimates of subsystems, components, elements and their mutual relations, which do not contradict expert assessments, testify to the effectiveness of diagnostics, evaluation and forecasting of the technical state of complex systems, taking into account full and partial failures of performance. Taking into account partial (full) equipment failures of complex systems of critical application will allow making decisions aimed at pre-failure maintenance of systems, ensuring operational efficiency, and, therefore, increasing the efficiency of their operation. The sequence of decision-making using the proposed information intelligent system with a CBR cycle, which takes into account the operations of data processing and structuring according to precedents, within the framework of the functioning of the developed software, ensures the operation of the information intelligent system with incomplete information. The results of calculating the efficiency of the operation of complex systems of critical application, taking into account the partial failures of the equipment and carrying out its pre-failure*

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

maintenance, took into account that the efficiency is determined by the probability of maintaining the system's operability.

Keywords: *model, method, simulation, algorithm, software, intelligent, method of reasoning based on precedents, diagnosis, evaluation, prediction, decision maker, complex technical system, ship power plant.*

1. Introduction.

One of the main causes of man-made accidents associated with complex technical systems (CTS) used in transport, aviation, energy, etc., remains failures during the operation of system equipment. Thus, from the analysis of the results of the operation of ships, it follows that, despite the measures to ensure the safety of navigation, the number of accidents at sea remains high. The main one of the many causes of accidents is CTS failure. In this regard, such CTS belong to complex systems of critical application (KA).

Complex technical short-circuit systems are hierarchical structures with a non-trivial internal structure, multi-functional numerous subsystems, components, elements and complex connections between them, which are in various states of failure. A characteristic feature of the operation of the short-circuit system is uncertainty during operation, incompleteness of information in the data characterizing the technical condition (TC) of the systems. In connection with the increase in requirements for the safety and reliability of expensive shipboard CTS short-circuits, their effectiveness depends significantly on the need to increase the time and resources of operation. Increasing the effective operation of the CTS can be achieved by applying the results of the development of models and methods of diagnosis, assessment and forecasting of the TC of complex systems and their use in intelligent information systems (IIS), which allow evaluating and forecasting the TC based on the results of diagnostics.

Well-known methods of evaluating and forecasting TC of complex systems, which are implemented in IIS: reasoning based on precedents; analogies; systemic; heuristics for optimization tasks (genetic algorithm, artificial immune networks, annealing method, methods of swarm intelligence, including ant algorithms); structural mapping taking into account precedents for OWL ontologies. A number of the listed methods have disadvantages: high growth of algorithmic and computational complexity during application; the need to implement non-trivial stages of pre-processing of various data; lack of effective opportunities for visual interpretation of results. A general disadvantage is the large dimension of the number of possible problems for further use during decision-making.

Increasing the efficiency of the operation of short-circuit systems by applying the results of model development and methods of diagnosis, assessment and forecasting of complex system systems, taking into account partial and complete failures of their equipment, is an urgent scientific task.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

2. Comparative analysis of models and methods of intellectualization of assessment and forecasting of the technical condition of complex critical application systems.

The development of conceptual models and methods of evaluation of TCs of complex short-circuit systems requires taking into account the possibility of continuing the operation of CTS in conditions of partial failure of operation with a plurality of scenarios of their development [1]. This approach helps to increase the efficiency of operation of the CTS by increasing the period of productive work before scheduled maintenance and restoration measures.

The measure of man-made accidents is the risk of equipment failure with consequences determined by the level and period of operation of the CTS [2]. Risk analysis is associated with the process of risk assessment of failures - it is the identification of hazards with an assessment based on the criteria of acceptable risk of failure with qualitative and quantitative results and with the transfer of hazards to the level of measurable categories [3].

When assessing the risk of CTS failures, the following should be taken into account: hierarchy, topology and variety of equipment, which differs in terms of physical principles, parameters and modes of operation; functional state; operating conditions under uncertainties; results of diagnosis of TC; difficulties in obtaining statistical and expert data on failures [3, 4, 5, 6, 7]. Only the OREDA database and the service method for safety assessment of CTS [8] are available sources of statistics for risk assessments of failures, for example, of ship's CTS.

Known methods of assessing the risk of CTS failures differ in the methods of obtaining the probability and losses from failures [9].

Assessments of the risk of CTS failures within the framework of the technocratic concept are performed using methods that are divided into deterministic, probabilistic, expert assessments under conditions of uncertainty, combined, performed based on the results of diagnosing complex system TCs.

Advantages of the probabilistic method: accident scenarios and consequences of failures are analyzed; interdependencies between CTS equipment regarding failures are taken into account in an explicit form; the possibility of quantifying the impact of uncertainty on risk assessments; ranking of security flaws and issues. However, it follows from the literature that models based on probabilistic approaches to estimating the risk of shipboard CTS failures are used in a limited way, allowing to obtain approximate estimates of the risk of failures without a sufficient amount of objective information. The most common methods of assessing failure risk indicators are expert methods. However, the disadvantages of such methods are associated with the high complexity of selecting experts with the necessary qualifications and the subjectivity of their assessments.

The significant advantages of the Bayesian trust network (BTN) method make it a promising application for risk assessments of CTS failures. Cognitive simulation modeling technology is also used in models for assessing the risk of equipment

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

failure from the point of view of its significance and criticality for the operation of the CTS [10, 11].

The method of fuzzy probabilistic modeling is used to construct the relationship between the actual resource and the probability of CTS failure [12, 13]. However, the availability of fuzzy logic apparatus standards does not solve the problem of numerical evaluations of the risk of CTS failures. This is due to the fact that the standards formulate criteria without models, which are necessary for the comparative analysis of options for assessing the risk of CTS failures. From the conducted analysis of models and methods, it follows that, despite a number of advantages, they cannot be used in their original form as conceptual models, methods for assessing the risk of CTS failures due to a narrow industry focus. Most of the models and methods are based on the assumption of operation of the CTS equipment in standard modes, without taking into account their partial failures. However, the application of the results of the development of information technologies is possible to solve many of the listed problems for assessing the risk of CTS failures [14, 15, 16]. The level of safety, for example, of ship's CTS, is largely determined by the quality of TC forecasting based on the results of risk assessments of their equipment failures [17, 18]. Forecasting, as well as diagnosis of TC, should take into account the specifics of CTS, which are operated under uncertain, extreme impacts, with insensitivity to incomplete data on the equipment and their interconnections, partial or complete failures [7, 12, 17]. TC forecasting can be carried out using machine learning methods based on specified indicators of the TC functioning [19], but this approach can be applied when only binary TC is taken into account. PHM (Prognostic Health Management) [20] is a promising forecasting method for calculating the remaining service life of CTS.

The analysis of models and methods of forecasting showed that changes in the TC of ship CTS are difficult to predict. This is due to the following reasons: lack of qualitative and quantitative expert data on system reliability; dynamics of operating conditions; human factor [21].

Known models and methods of TC forecasting based on deterministic and formalized statistical models are not universal. There are no opportunities to fully account for the specifics of the functioning of system equipment, especially in conditions of uncertainty of the effects on the CTS of various external or internal factors. An important drawback is that similar models and methods are not recommended for shipboard CTS because they do not meet the requirements of the International Convention for the Safety of Life at Sea SOLAS-74, the provisions of the International Safety Management Code. A significant shortcoming of models and methods of forecasting CTS is that they have not been tested by long-term practical use.

Structural models based on mechanisms and methods of artificial intelligence have a significant advantage for adequate forecasting of CTS failure risk assessments [22]. Similar models make it possible to predict the risk of CTS failures using mechanisms for identifying implicit dependencies between input and output data samples, supporting various learning algorithms. This has a significant advantage for CTS when evaluating and forecasting scenarios of loss of working capacity

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

containing hundreds of criteria and indicators. The possible solution of problems is also connected with the development and development of complexes of problem-oriented programs [15, 23, 24]. At the same time, the role of methods based on modern software for evaluating and forecasting complex systems' TC is growing. Ensuring the guaranteed safety of the operation of the CTS due to the timely and prompt prevention of the transition of normal situations to critical, emergency or emergency situations is the basis of the failure risk management strategy [1, 25]. Such a strategy is based on a systematic analysis of the multifactorial risk of failure, its reliable assessment in different modes of operation of CTS and forecasting of their TC during the period of operation [4].

The analysis of publications, regulatory materials on assessments and forecasting of the risk of failure of various types of CTS showed that the existing diversity of models and methods requires the removal of complex and significant uncertainties, the improvement of the accuracy of assessments and forecasts. Many models and methods take into account the operation of CTS equipment in standard modes, without taking into account partial failures of performance, and are based on engineering, expert and other approaches with complex and expensive calculations, which limits wide application and has a narrow focus of models and methods.

Thus, in order to ensure the efficiency of operation of CTS, the tasks of development and development of new models, methods and their algorithms, implemented in the form of complexes of problem-oriented programs for evaluation and forecasting of TC systems, remain relevant.

3. Comparative analysis of information intelligent systems for diagnosis, assessment and forecasting of the technical condition of complex critical application systems

Traditionally, information intelligent systems are understood as interactive computer systems that help a decision-maker to use information, a complex of mathematical and heuristic models and methods to solve poorly structured or difficult to formalize problems [26]. The efficiency of IIS functioning affects the efficiency of CTS operation throughout the entire period of their life cycle. IIS is united by the general method of forming alternatives of management decisions in CTS, determining the consequences of their implementation and justifying the choice of an acceptable management decision [27]. The IIS includes: data sources and model, model database and software subsystem, which consists of database management systems (DBMS), model database (SBM) and user interface. The main tasks that are solved in the IIS are data entry, storage and analysis.

Main functionality of IIS:

- gathering the necessary information from various data sources;
- transformation of collected information into a single data format;
- generating requests to the data warehouse, processing them, searching for information, forming and providing information in a format convenient for analysis and decision-making.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

The IIS should have a web client-side interface or be completely web-oriented [28]. IIC data storage can be built on different types of DBMS, but given the web orientation and the increasing share of cloud technologies on the market, it is better to rely on web-oriented DBMS MySQL and PostgreSQL, as well as on specialized cloud DBMS - MS Azure. Data sources come from the information system of the operational level from a special database and contain engineering and data from external sources. The data model is built on the basis of: data sources and repositories; operational staff and data showcase; metadata. The database of models provides analysis in IIS. Almost all DBMSs have OLAP extensions in one form or another, therefore operationally, the analytical part of IIS is considered ready already by choosing the type of DBMS for the data warehouse. When building a data repository, the task of building a mechanism for working with metadata to describe the data structure in the database is relevant. The design and construction of the metadata tree is carried out by IIS developers. The classification at the conceptual level distinguishes managed IISs: by messages (Communication-Driven DSS); by data (Data-Driven DSS); documents (Document-Driven DSS); knowledge (Knowledge-Driven DSS); models (Model-Driven DSS). The classification of architecture can be as follows: functional; independent data stores; two-level and three-level data warehouses. Depending on the type of data these systems work with, IIS can be conditionally divided into operational and strategic. OLAP and Data Mining are two components of the decision support process. Data operations are carried out by OLAP - a machine that implements the concept of operational analytical processing. According to the method of data storage, MOLAP, ROLAP and HOLAP are distinguished. Depending on the location of OLAP machines, OLAP clients and OLAP servers are distinguished. The OLAP client builds a multidimensional cube based on the raw data (to obtain the necessary sections - reports) and calculates on the client PC, while the OLAP server receives the request, calculates and stores the aggregate data on the server, issuing the results. Cubes and other analytical reporting must be configured. IIS classification is also carried out by levels (initial, medium, higher) and by level of distribution (concentrated, distributed) [29].

IIS uses various methods for analysis and development of proposals: information search; intelligent data analysis; knowledge search in the database; reasoning based on precedents; simulation modeling; evolutionary computing and genetic algorithms; neural networks; situational analysis; cognitive modeling, etc. The use of artificial intelligence in IIC will allow to expand the functionality of the system, increase the operational efficiency and reliability of the CTS.

One of the most important functions of the IIS software is the evaluation of the possible results of the decisions made and the prediction of the TC of the CTS [30]. The choice of the applied specific IIS forecasting method remains with the system developer. Most often, factographic methods are used in software as the least dependent on subjective factors. In conditions of weakly formalized initial data, expert methods are used, but with limitations associated with the availability of a sufficient number of experts.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

As it follows from [4, 7], during the functioning of the CTS, adverse impact and factors (AI and AF) can disable individual subsystems, components, and also affect the performance of the systems. Incidents and disasters are usually difficult to predict or unpredictable (for example, personnel errors, natural disasters, etc.). Their influence can have consequences of varying degrees of severity - up to the complete destruction of the CTS [31]. The development of IIC for managing the risk of equipment failures in order to ensure the survivability of shipboard CTS in case of AI and AF is a promising direction in ensuring the safety of CTS [25]. Such IISs can be implemented both in the form of individual stand-alone solutions and in the form of modules that complement the necessary functionality of ready-made general purpose management and decision-making systems. They make it possible to quickly make decisions at the stage of eliminating the consequences of AI and AF, to ensure the reliability of the CTS, thanks to the ability to identify, analyze and assess the existing risks of failure of the CTS equipment [25, 31].

Therefore, most IISs are developed to solve a specific task or a general class of tasks, and also targeting different types of users. The development of IIS to manage the risk of failures in order to ensure the survivability of the CTS in the conditions of incompleteness and uncertainty of the information received in the presence of unpredictable AI and AF is one of the promising directions for the effective and reliable operation of subsystems, components, elements and the CTS as a whole.

The main concept of IIS is to solve classic problems arising in the field of unstructured and poorly formalized CTS [32]. These problems include the impossibility of obtaining complete and objective information for making rational decisions, as well as the need to use subjective and heuristic information. Additional challenges are the presence of uncertainties in the initial data and even ambiguity in the process of finding the optimal solution. In addition, the solution in such cases must interact with the user in the form of dialogue or other forms of communication between a human and a machine system.

Given these factors, there is a need to abandon traditional algorithmic methods and management and decision-making models. Instead, it is necessary to move to the use of technologies of intelligent systems.

IISs must implement the scheme: assessment - forecast - decision - action. IIS provides a decision maker with an analysis of the problem to be solved. The main functions of IIS are assessment, forecasting of events, self-learning and adaptation, work from the knowledge base (including formation, structuring, storage, as well as content of the database), formation of decisions and their implementation.

The following methods implemented in IIS are known [33, 34]:

- analogy and system;
- heuristics for optimization tasks (genetic algorithm, artificial immune networks, annealing method, methods of swarm intelligence, including ant algorithms);
- reasoning based on precedents (nearest neighbor, extraction of precedents based on decision trees, precedents based on knowledge, taking into account the application of precedent);
- structural mapping based on precedents based on OWL ontologies.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

IISs are often created based on a combination of artificial intelligence systems using the knowledge and technologies of expert systems, machine learning, and agents [33, 35]. To automate the risk assessment process and predict possible failures, machine learning is widely used (analysis of large volumes of data, detection of patterns and trends, modeling and simulation of systems). However, the use of a large amount of data is associated with limitations in failure risk assessments, possible errors that lead to incorrect forecasts.

The well-known method of structural mapping has the following advantages: the possibility of formalizing the nature of multi-linked hierarchical interactions between CTS equipment operating in stochastic conditions; flexibility of implementation of the production approach to the formation of the knowledge base in IIS; convenience of software implementation taking into account the object-oriented approach. Most of the models that make it possible to obtain new knowledge on the basis of existing ones can be reduced to production models. The disadvantage of such models is a shallow representation of the problem area, which affects the flexibility of forming user dialog requests with the expert system [33].

BTN can be used for IIS in multi-equipment CTS to model the relationships between various factors and their uncertainties, providing a structured framework for assessing the risk of failure under uncertainty and helping the decision maker to prioritize the accepted. In the IIS, methods of reasoning based on precedents can be used to evaluate and forecast the TC of the CTS in order to generalize and apply the accumulated experience [36]. When operating CTS associated with uncertainty, the use of a precedent approach simplifies the decision-making process. Advantages of the method: the ability to learn based on experience; versatility; ability to work with incomplete or unstructured data; flexibility in adapting to new situations.

Stages of Case-based Reasoning (CBR) - method cycle (Fig. 1):

1. Capturing precedents from the library of precedents (LP).
2. Indexing (for quick search of similar cases).
3. Finding the most suitable precedents for a new task.
4. Review and adaptation (modification for the current task).
5. Assessment of suitability, retention and implementation.

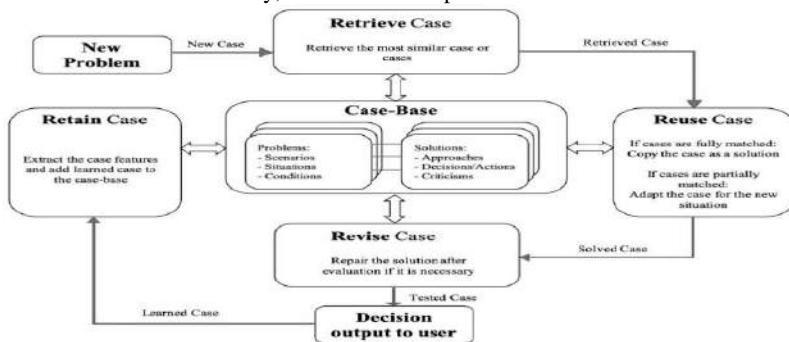


Figure 1. Case-based Reasoning cycle [36]

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

Classic IIC architecture (Fig. 2):

- provides justification of alternatives based on models and methods using expert assessments;
- includes decision-making methods under conditions of uncertainty with modeling of problematic decision-making situations;
- contains knowledge base - a set of rules for choosing appropriate models and decision-making methods for justifying alternatives depending on the specific implementation of the elements of the task;
- contains a database for storing information;
- carries out multidimensional analysis of tasks and generation of analytical reports using the OLAP server.

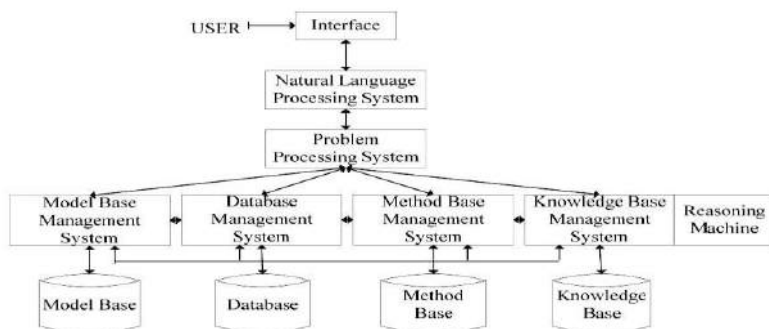


Figure 2. Architecture of IIS

Currently, the implementation of artificial intelligence technologies continues to improve the efficiency of operation of the CTS. Thus, in accordance with the requirements of the Maritime Shipping Register, all ships must be equipped with systems based on artificial intelligence technology [17]. For this, algorithmic and software tools are needed, which provide assessment and forecasting of TC systems, adequate to the set goal [14, 37]. An example of the use of IIS is the PHM method, which covers the entire process from data collection to the use of decision-making results. Information about the status of the CTS received in real time is used to evaluate the IIS TC. The following can be used for vehicle modeling: fault tree analysis; event tree analysis; Bayesian trust networks. BTN is preferred as a tool for assessing the risk of CTS failures.

Crystal Info (Seagate Info) - IIS, based on a flexible technology of data access and data processing, is used among the software complexes that solve decision-making tasks. Open OLAP technology allows integration of multidimensional OLAP data from disparate sources (Crystal Info, Crystal Holos, Hyperion Essbase, OLE DB for OLAP providers (Microsoft SQL Server OLAP Services and Applix TM 1, IBM DB 2 OLAP Services and Informix MetaCube). All OLAP sources can be presented within a single interface. For many years, researchers have been working on the

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

creation of IIS for various purposes, but there are problems, from the point of view of efficiency, of knowledge formalization in CTS, which need to be solved:

- increasing the objectivity and reliability of the decisions made in the presence of uncertainties in the evaluation tasks, forecasting the risk of failures;
- accounting for the factors of incompleteness, ambiguity and inconsistency of source information (data and knowledge) and rules;
 - provision and processing of various types of knowledge, data and models, development of relevant databases, databases and models;
 - collection, storage and accumulation of declarative, expert information about the problem industry in the database and knowledge base, library of precedents;
 - increasing the accuracy of evaluations of CTS vehicles on the basis of new models, methods, algorithms, software invariant to the subject area for evaluations, forecasting the risk of failures in order to identify signs of the pre-failure state of the equipment at an early stage of development;
 - the application of adequate and technically feasible formal models for solving the tasks, taking into account the structural, functional, informational and subject features of the CTS.

4. Development of a method of reasoning based on precedents of the technical state of complex critical application systems

The development of a method of reasoning based on precedents of the technical state of complex systems of critical application includes the following stages:

1. Presentation of a precedent set of parameters with specific values and solutions.
2. Entering the data of vehicle diagnostics of a complex short-circuit system into the IIS of evaluation and forecasting of a vehicle of a complex system.
3. Obtaining evaluation data and forecasting of the vehicle of a complex short-circuit system.
4. Transmission of assessment data and TC forecasting of a complex system to decision maker system.

IIS can be implemented both in the form of individual stand-alone solutions and in the form of modules that supplement the necessary functionality of ready-made management and decision-making systems of general purpose. They will make it possible to quickly make decisions at the stage of eliminating the consequences of adverse effects and impressive factors, to ensure the efficiency of the operation of ship's CTS thanks to the possibility of evaluating and forecasting their TC [34].

The construction of the IIS is based on the formulation of the decision-making task in general:

$$N = f(F, G, A, FR, SG, P, C, PC, NS) \quad (1)$$

where F - is the number of failures of FE (functional elements) and FC (functional components) of the CTS;

G — sets of set goals;

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

A - is a set of possible alternatives;

FR - equal sets of FE and FC CTS failures;

SG, P, C - a set of characteristics, advantages, criteria for ensuring the reliability of FE and FC CTS;

RS - set of principles of coordination of evaluation of alternatives taking into account individual criteria;

NS - necessary solution to the problem

The development and research of IIS using CBR, with the aim of increasing the effectiveness of the implementation of learning mechanisms and adaptation to the specifics of the problem environment for the relevant specific applications, as well as increasing the effectiveness of decision-making in ODA based on the results of evaluation, forecasting of TC of complex systems is relevant.

Such development and research was carried out taking into account: partial and complete failures of FE and FC performance; a precedent model of knowledge based on a vehicle dynamics model from a serviceable state to complete failure. The TC dynamics model takes into account cause-and-effect relationships and the hierarchical structure of the TC, which consists of: elements (E); components (C); subsystems (S).

The description of the problematic situation during the operation of the CTS consists in the consequences of partial or complete loss of FE and FC of a complex system.

When using the method of reasoning based on precedents for the representation of precedents, a fairly simple parametric representation, i.e. presentation of a precedent in the form of a set of parameters with specific values and decisions (estimates, TC forecasts and recommendations to the person making the decision):

$$CASE = \left(R, P, D, W_{S(C,E)_{n(m)}}^f, W_{I_{S(C)_{a(z)}}}^f, RE, FS, RF, FF, DR \right), \quad (2)$$

where R, P, D are parameters (risk, probability, loss) describing the precedent;

$R \left\{ R_{S(C,E)_{n(m)}}, R_{I_{S(C)_{a(z)}}} \right\}$ - sets of FE and FC CTS failure risk assessments and

a decision maker recommendations;

$P \left\{ P_{S(C,E)_{n(m)}}, P_{I_{S(C)_{a(z)}}} \right\}$ - sets of FE and FC CTS failure probability

estimates and a decision maker recommendations;

$D \left\{ D_{S(C,E)_{n(m)}}, D_{I_{S(C)_{a(z)}}} \right\}$ - sets of estimates of losses from failures of FE and

FC CTS and recommendations of a decision maker;

$W_{S(C,E)_{n(m)}}^f$ - assessments of working capacity (partial or full) of FE and

recommendations of a decision maker;

$W_{I_{S(C)_{a(z)}}}^f$ - evaluations of the operational capacity (partial or full) of the FC

and recommendations of the decision maker:

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

RE – sets of refined specific estimates of parameters of TC FE and FC CTS, decision-making ($r_{e_1}, \dots, r_{e_N} \in RE$);

FS - saving a set of refined estimates of parameters of TC FE and FC CTS, adopted decisions;

RF - sets of refined certain predicted values of parameters of TC FE and FC of CTS decision-making ($r_{f_1}, \dots, r_{f_N} \in RF$);

FF - preservation of a set of refined forecasted values of TC parameters FE and FC of TC, adopted decisions;

DR - diagnosis and recommendations of a decision maker [38]

$$R_{s(c,e)_{n(m)}} = \{r_{s(c,e)_{n(m)}} \mid s(c,e) = \overline{1}, S(C,E), n_{s(c,e)} = \overline{1}, N_{S(C,E)}, m_{s(c)} = \overline{1}, M_{S(C)}\}, \quad (3)$$

$$R_{I_{s(c)a(z)}} = \{r_{I_{s(c)a(z)}} \mid i_{s(c)} = \overline{1}, I_{S(C)}, a = \overline{1}, A, z = \overline{1}, Z\},$$

where $r_{s(c,e)_{n(m)}}$ - is the risk of failures of FE CTS;

$r_{I_{s(c)a(z)}}$ - the risk of FC CTS failures;

$n_{s(c,e)}$ - FE number in CTS;

$m_{s(c)}$ - the number of the hierarchical level of FC CTS;

$N_{S(C,E)}$ - number of FE CTS;

$M_{S(C)}$ - the number of hierarchical levels of FC CTS;

S, C, E – FE CTS;

I_S, I_C – FC CTS;

n, m – number, hierarchical level in the CTS;

a – number of intercomponent communication;

z - is the number of intersystem communication.

A - the number of intercomponent connections;

Z - is the number of intersystem connections

$$P_{S(C,E)_{n(m)}} \cdot \lambda(t)_{S(C,E)_{n(m)}} = \frac{\alpha_{S(C,E)_{n(m)}} \cdot \exp(-\alpha_{S(C,E)_{n(m)}} \cdot T_{S(C,E)_{n(m)}})}{\exp(-\alpha_{S(C,E)_{n(m)}} \cdot T_{S(C,E)_{n(m)}})} = \alpha_{S(C,E)_{n(m)}}, \quad (4)$$

$$P_{I_{S(C)a(z)}} \cdot \lambda_{I_{S(C)a(z)}}(t) = \frac{\alpha_{I_{S(C)a(z)}} \cdot \exp(-\alpha_{I_{S(C)a(z)}} \cdot T_{I_{S(C)a(z)}})}{\exp(-\alpha_{I_{S(C)a(z)}} \cdot T_{I_{S(C)a(z)}})} = \alpha_{I_{S(C)a(z)}}$$

where λ - is the intensity of failures;

α – distribution parameter, $\alpha \approx 1/(T_0)$, (T_0) – estimate of average service life before failure

Quantitative assessment of damage from failure $n(m, e)$ - subsystem, component, element to determine the risk of failure:

**ADVANCES
IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES**

$$D_{S(C,E)n(m)} = \{d_{s(c,e)n(m)} \mid s(c,e) = \overline{1}, S(C,E), n = \overline{1}, N, m = \overline{1}, M\}, \quad (5)$$

where $d_{s(c)n(m)}$ - losses from failure of FE CTS

Quantitative assessment of losses from failure $a(z)$ - FC determination of the risk of failure:

$$D_{I_{S(C)a(z)}} = \{d_{I_{s(c)a(z)}} \mid i_{s(c)} = \overline{1}, I_{S(C)}, a = \overline{1}, A, z = \overline{1}, Z\}, \quad (6)$$

where $d_{I_{s(c)a(z)}}$ - is the loss from failure FC

Performance of FE at different degrees of its loss:

$$W_{v_{S(C,E)n(m)}}^f = \{W_f^{<n_s(c), m_s(c)>} \mid f = \overline{0,1}; n_{s(c,e)} = \overline{1}, N_{S(C,E)}; m_{s(c)} = \overline{1}, M_{S(C)}\} \quad (7)$$

Functional capacity of FC at different degrees of its loss:

$$W_{\omega_{IS(C)a(z)}}^f = \{W_f^{<a,z>} \mid f = \overline{0,1}; a = \overline{1}, A; z = \overline{1}, Z;\} \quad (8)$$

In the process of functioning of FE CTS in emergency scenarios, taking into account Harrington's generalized desirability function, they can be in one of the following TC [38]: 0 - 0.2 - the level of risk and consequences are minimal, which do not affect the operation of CTS (RMi); 0.2 - 0.37 - the level of risk is acceptable and the consequences are insignificant, allowing the operation of the CTS without repair (RA); 0.37 - 0.63 - the level of risk is maximum, the consequences are significant, but allowing the operation of the CTS during repair work (RMa); 0.63 - 1.0 - the level of risk is critical, the consequences are catastrophic, preventing the operation of the CTS (RC). Taking into account [39] for the hierarchical structure of CTS, TC transitions are possible in the form of a TC matrix (Fig. 3). In Fig. 3, ke, kc, ks are the weight (significance) coefficients of an element, component, subsystem in the structures of the CTS.

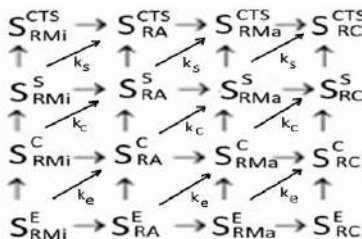


Figure 3. TC CTS matrix

The construction of the method is based on: presentation of a precedent set of parameters with specific values and solutions; obtaining assessment data and forecasting of complex system vehicles; formation of recommendations to ensure the efficiency of operation of CTS equipment.

**ADVANCES
IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES**

5. Designing an information intelligent system of diagnostics, assessment and forecasting of the technical condition of complex critical application systems

Methods of finding solutions in IIS based on precedents are an approach based on the use of analogies with previously solved problems to find and adapt solutions to new situations. Similar methods include the stages that make up the CBR cycle:

1. Capturing precedents from the library of precedents (LP).
2. Indexing (organization of precedents to find similar cases).
3. Finding the most suitable precedents for a new task.
4. Adaptation (modification of the found precedent to match the current task).
5. Evaluation and implementation (checking the adapted solution for its suitability and, if necessary, implementation).

Advantages of the method of reasoning based on precedents: adaptability; work with incomplete information; versatility; learning Case studies can be presented in ways including text description, diagrams, tables, prototypes and use case scenarios, modeling through UML. Each of these methods can be effective depending on the context and goals of the project.

The method of presenting precedents is implemented as follows. In the proposed CBR cycle (Fig. 4) to support the exchange of knowledge, a set of input parameters of the diagnosed TC and an array of ontologies that represent a structured description of the domain area of the ship CTS are received at the initial block of task formation.

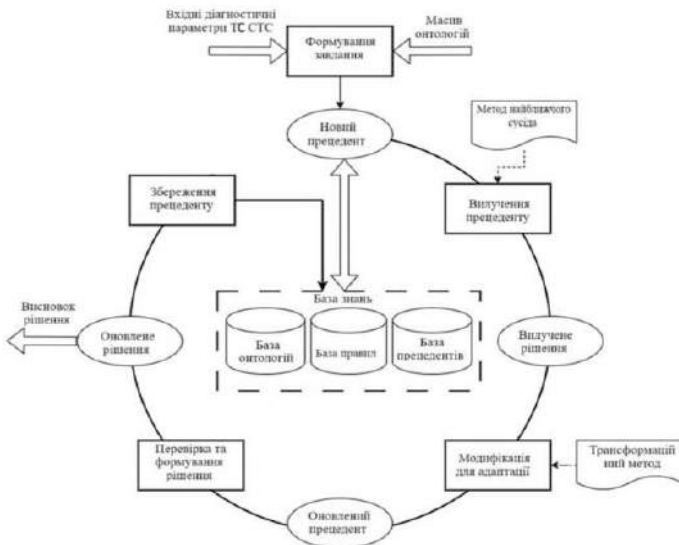


Figure 4. The structure of the CBR cycle

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

As a result, the structure of the object of a new precedent is generated and content is extracted, which is performed using the nearest neighbor method based on the results of the assessment of the degree of similarity (closeness) of the analyzed scenario with the TC and taking into account the data in the knowledge base. Based on the implementation of this procedure, a solution object is formed, which can be changed for its targeted adaptation, taking into account all aspects of the scenarios of partial and complete failures of the FE and FC CTS using the transformation method [40]. The updated precedent is checked for logical inconsistency taking into account the use of predicative products using the Hermit ontological method of constructing a logical conclusion [40]. The decision obtained as a result of the performed actions is exported as a separate object containing recommendations for the decision-maker and metadata. After that, the precedent is stored in the basis of precedents, which is a component of the knowledge base (Fig. 4). The decision-making sequence (Fig. 5) using the proposed CBR cycle, taking into account data processing and structuring operations regarding precedents within the framework of the application software system, is carried out as follows.



Figure 5. Decision-making sequence diagram

When the software system is started, the main form of the user interface is initialized, in which the possibility of importing input data for task formation is provided. Then the control parameters and configuration options for the operation of all modules involved in the information processing cycle are set, including the data processing (DPMoD), precedent extraction (PEMoD) and adaptation (AMoD) modules. Next, a request is made to transfer the generated data arrays to DPMoD, in which data processing procedures are performed step by step (including checking for consistency and splitting into fragments), forming a collection for storing precedents taking into account metadata (such as a short text description of the target, its identifier, date of formation and some statistical indicators). After that, a request is

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

made to obtain a specific PMod precedent, in which actions from the metric evaluation based on the nearest neighbors method are performed. The resulting result is sent to DMod as a collection based on an associative array.

After checking and verifying the results, DMod sends the formed collection to AMod for the purpose of carrying out the adaptation procedure. For this, the method of transformation is used, taking into account the comparison of the precedent with a set of rules, the logical products of compliance are taken into account. As a result, the updated collection of precedents is sent to DMod to form a list of final decisions and their validation. To output results in the form of text records and graphical representation, the resulting solution in serialized form (in json format) is sent to the main form of the interface. This is necessary for further initialization of the process of sending case data, saving them in the knowledge base, and issuing an informational message to the user about the transaction results. For the formation of precedents, a simple parametric representation is sufficient, i.e. presentation of a precedent in the form of a set of parameters with specific values and a decision (diagnosis and recommendations of the person making the decision).

Different methods of extracting precedents and their modifications are known. The most common methods are: determination of the nearest neighbor (NN - Nearest Neighbor) [41]; extraction of precedents based on decision trees; obtaining precedents based on knowledge [34]; extraction of precedents taking into account their application. The listed methods use a variety of metrics.

From the main metrics, the method of determining the nearest neighbor was used, which allows you to easily calculate the degree of similarity of the current problem situation and precedents with LP. The method of determining the nearest neighbor uses a simple coordinate-by-coordinate comparison of the current situation with a precedent, where each parameter of the description of precedents is perceived as one of the coordinates. The DCT distance between the point corresponding to the current situation and the point corresponding to the precedent is determined. The effectiveness of the nearest neighbor method depends on the choice of metric. If the precedent C and the current problem situation T are given in an n-dimensional property space, then the degree of similarity or closeness S(C,T) of the precedent C and the current situation T can be determined using one of the metrics defining the distance between two points x_i^C and x_i^T , in particular, the Euclidean distance:

$$D_{CT} = \sqrt{\sum_{i=1}^n (x_i^C - x_i^T)^2} \quad (9)$$

To determine the similarity degree value (SIM), the maximum distance Dmax in the selected metric is calculated using the limits of the parameter ranges to describe the precedents. After that, the value of the degree of similarity is determined, using the limit of the ranges of parameters to describe the initial and final precedents, $i = 1, \dots, n$. The value of the degree of similarity can be calculated as follows:

$$SIM = 1 - D_{CT} / D_{max} \quad (10)$$

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

6. Implementation of an information intelligent system of diagnostics, assessment and forecasting of the technical condition of complex critical application systems

The implementation of IIS with CBR (Fig. 6) connects the developed models and the method of diagnosing a vehicle with a database, a knowledge base, an expert system containing calculation, experimental, as well as data obtained by experts during the operation of the vehicle. The development of the software structure began with a schematic presentation of the main interacting modules of the IIS. The structural diagram of modules and relationships (Fig. 6) reflects a visual representation of the interaction of FE and FC in IIS.

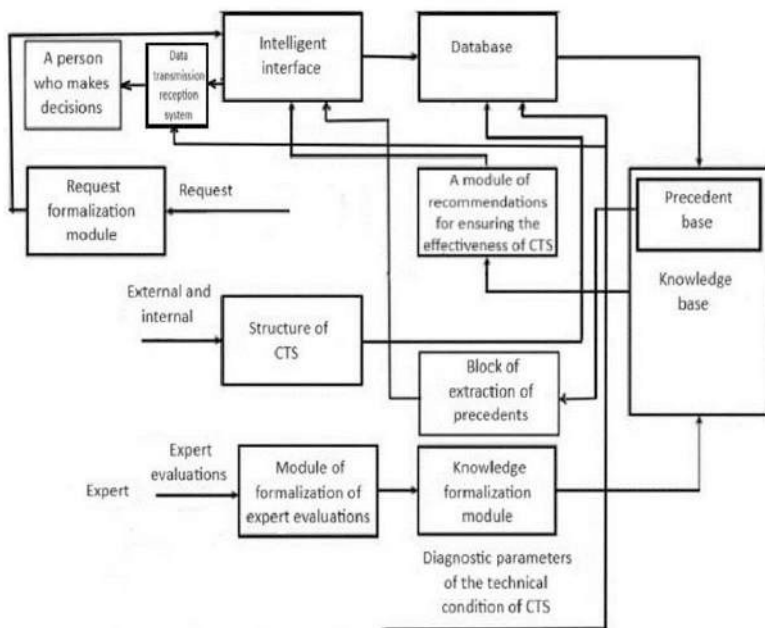


Figure 6. Structural diagram of the implementation of the method of reasoning based on precedents for evaluating and forecasting the TC of a complex short-circuit system

During the development of the IIS, a ship's power plant was chosen as an object of evaluation and forecasting of the vehicle. When assessing the reliability of the ship's power plant, it was taken into account that the CTS is characterized by a large number of parameters that are diagnosed, which differ in informativeness and the degree of availability when there is insufficient information for the evaluation of the TC, as well as specific and diverse operating conditions with uncertainty. The cores of IIS are: DB; a knowledge base with methods for calculating reliability indicators

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

(risks and failure probabilities) and a set of decisive rules for choosing appropriate decision-making methods; the model of intellectualization of evaluation of TC FE and FC CTS.IIS includes: interface module knowledge base with a library of precedents and a knowledge base; request formalization module; a module of recommendations for ensuring the effectiveness of the CTS; libraries of ship CTS structural diagrams; module of formalization of expert evaluations; knowledge formalization module. The implementation of the developed strategy in IIS is ensured by purposeful actions in accordance with decision support for finding FE and FC failures based on the established estimates of their TC. The model base is known as production, in relation to the implementation of its software functionality, it is object-oriented. The developed knowledge base is represented by rules obtained on the basis of intellectual data analysis (a multi-level hierarchical structure of the tree of the knowledge base), expert evaluations, the results of the application of models of diagnostics of complex system vehicles, which functions according to the developed sequence of decision-making (Fig. 5) and taking into account the vehicle matrix of the vehicle control system (Fig. 3).

Upon request, the entire list of data and expert evaluations are sent to the knowledge base from the database. As a result, evaluations of TC subsystems, components, elements and their mutual relations are formed at the output of the knowledge base. The vehicle evaluations are sent to the module of recommendations for ensuring the effective operation of the vehicle and then the person who makes decisions for the vehicle management of the complex system. The database contains: DB of CTS structures; database of failure risk criteria; Database of vehicles of complex systems; Database of degradation processes; Database of measures to reduce the risk of CTS failures. The library of precedents consists of LP of incidents and BP of emergency situations. Diagnosis of a problematic situation - complete or partial failure of equipment and their mutual connections of the CTS is carried out by modeling their diagnosis based on data on the risk (probability) of failures, as well as on losses from failures. Taking into account the diagnostic data, the established assessment of the vehicle of a complex system is entered into the LP knowledge base, and recommendations are formed for the decision-making of a decision maker. Based on the results of the evaluations, the TC of a complex system is forecasted. The output may include a list of actions taken, additional comments, and references to other precedents. The hierarchical structure of the key program logic of fragments of data processing modules according to precedents and considerations is shown in Fig. 7. To form the level of abstractions and ensure polymorphism when implementing the behavior of objects implementing different stages of data processing, three interfaces have been implemented. IData – formation of the path to the location of the input data set, initialization of data structures and collections, transformation of data into a single normalized view with a check for missing rows, setting of the structure. IOntology - storage of structures of attributes, classes and relationships, formation of the composition of the structure of the ontology with its verification and validation. IPrecedent - operation with the properties of scenarios of situations, problems and solutions, as well as the formation of the process of creating a precedent, its preservation and serialization, checking for logical consistency.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

Each has a different implementation of the logger() method of providing processes for logging the intermediate results of performing computational operations over time. The DataLoader class implements the IData interface, performing contact with loading data into the system and operations of forming precedent collections, checking data integrity, performing the necessary precedent transformations, filtering and aggregation, as well as setting the structure and issuing messages based on the results of the performed actions in the status bar. The OntologyMaker class implements the IOntology interface, operating with a partial collection of ontologies of a dynamic array for aggregating individual elements of the ontology and is designed to form the logical base of the system structure when building each individual precedent, providing visualization of the ontology in a graph-oriented form.

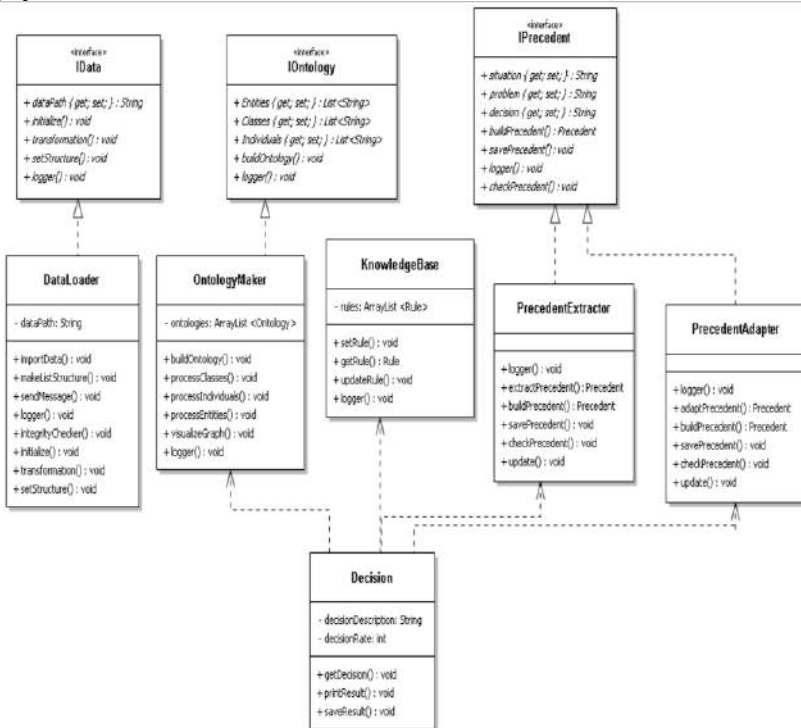


Figure 7. Hierarchical structure of the key program logic of fragments of data processing modules regarding precedents and considerations

The PrecedentExtractor and PrecedentAdapter classes implement the IPrecedent interface, overriding the precedent data management methods for use in the extractPrecedent() and adaptPrecedent() methods, respectively, resulting in a Precedent object. The

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

KnowledgeBase class is separately implemented for the implementation of CRUD operations on rule management. Based on the use of instances of data classes, a Decision object is formed, the state of which is described using the private properties decisionDescription and decisionRate, and the behavior is expressed using public methods of forming the decision object, its output and saving the results. The Visual Studio development environment, the .NET 4.7 framework, the technology for creating WinForms graphic interfaces, as well as functional libraries supporting Hermit ontologies and working with JSON were used for the software implementation of IIS with the CBR cycle [42]. The interface of the main form of the software system with the control tab of the process of creating precedents within the framework of the proposed CBR cycle for evaluation and forecasting of the TC, using the example of the ship's CTS, is shown in Fig. 8.



Figure 8. The interface of the main form of the software system with the tab for managing the process of creating precedents

The main menu is provided for navigation between the processes of connecting data sources and the knowledge base (item File), management and processing of data (item Data processing), the selection of computing operations and their implementation (item Operations), configuration of system modules and settings for its operation (item Settings), issuance of reference information on the operation of the system (item Help).

The functionality supports data manipulation from precedents, ontologies, rules and decisions. A separate graphic widget is provided for the hierarchical representation of the structure of ship CTS and their FE and FC in the form of a tree of nodes. Data entry by precedents is carried out through the appropriate text field, options are provided for providing a detailed description of the parameters, building a summary cross-table of all values of the ship's CTS and their equipment, as well as forms for extracting, adapting and validating (checking) compiled precedents.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

The formation of a table displaying the obtained results according to precedents with an assessment of their degree of similarity, a description and a short set of typical recommendations has been implemented. For ease of management, a separate component for quick table navigation with CRUD operations and search is provided. The means of visualization of the most priority options for adaptation of precedents for a specific scenario of CTS operation, which is considered after performing all analytical procedures, have been introduced. The possibility of local saving of visualization results in pdf and csv formats, respectively, has been implemented. The results of assessments of the risk of failures of the subsystems of the studied ship's power plant, formed taking into account the compiled precedents, are shown in fig. 9.

Precedents: Ontologies Rules Decisions Risk assessment		
System name	Risk assessment value	Details
BS	27	
BAS	65	
FES	14	
DWSS	21	
WS	54	
MS	12	
SPP	67	→ Boiler Plant - 16%
RS	33	Control System - 22%
HSS	21	Fire Fighting System - 11%
CAS	26	Main Engine - 51%
PCS	40	
CSSE	29	
HS	11	
SS	5	

Figure 9. The interface of the risk assessment form for the analyzed subsystems of the ship's power plant

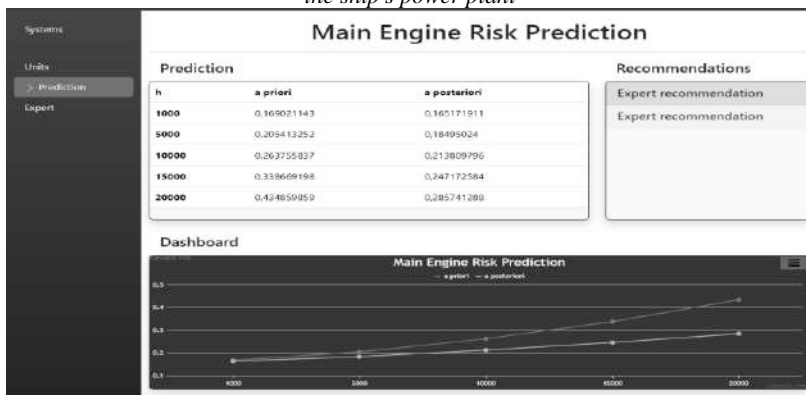


Figure 10. Main Engine subsystem failure risk prediction block

The results of forecasting the risk of failures FE and FC of the ship's power plant, for example, for the Main Engine subsystem can be seen in the block of the interface for viewing the risk of failures when navigating to the Predictions web page (Fig. 10). A block for displaying a priori and a posteriori values of the risk of Main Engine failures and a widget for displaying the dependence of the values of predicted

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

a priori and a posteriori risk of Main Engine failures are provided. The user interface of the viewing module of the output of the obtained results according to the generated system solution is shown in Fig. 11. Support for navigating decision scenarios has been implemented, as well as data presentation components for decisions, causes of violations, consequences of scenarios for further system operation, and a list of recommended actions to improve the performance of the CTS. There are options for opening a log file for viewing the intermediate stages of computing operations and calculations, as well as saving the results of the database.

To control the process of building a fault tree model, components for setting the parameters of node construction methods, tree graph visualization algorithms, graphical representations, and report generation have been developed. The functionality of building a decision tree, viewing its structure, and adding to the model in the editor mode are provided.

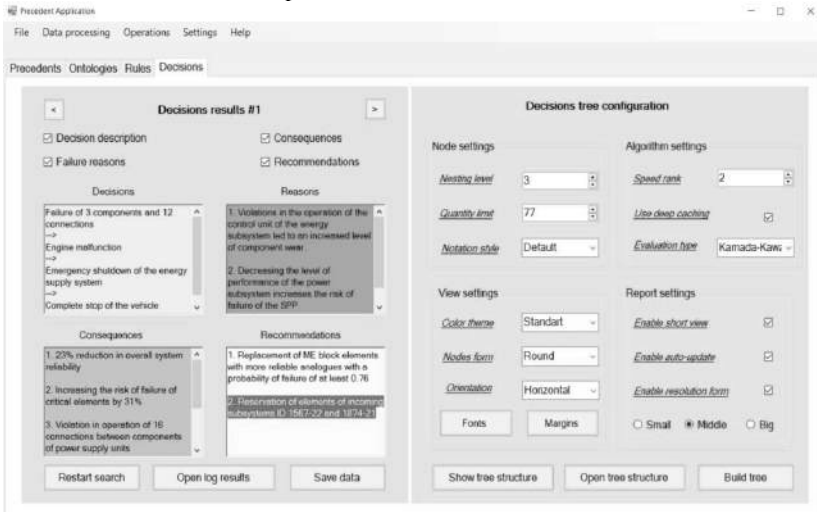


Figure 11. User interface

The disadvantage of the method of precedents with a CBR cycle is an increase in the time of searching for the nearest precedents. Therefore, a comparative analysis of the time of searching for the closest precedent was carried out depending on the size of the precedent database, taking into account data caching when initializing the data structure as an associative array collection. The graph showing the time of determining the TC of a complex system from the number of precedents is shown in Fig. 12. The time spent on the closest precedent for 10,000 precedents in the knowledge base was about 370 ms. The first closest precedent out of 5000 precedents was obtained in about 50ms. With the increase in the number of precedents in the library of precedents, the time to determine the TC of a complex system increases, but it does not significantly affect the total time spent on evaluating the TC of the subsystems of the studied ship's power plant. Despite such a

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

shortcoming, research has shown the possibilities of applying the method of reasoning based on CBR precedents and its appropriate use for decision-making in real operating conditions. The developed IIS has high performance.

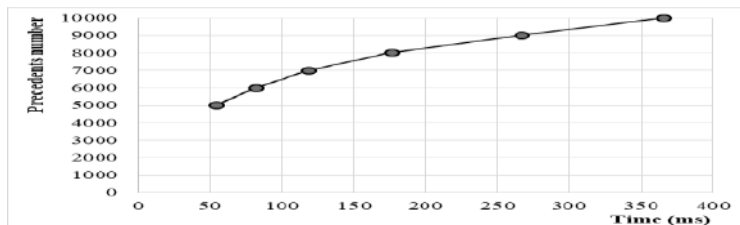


Figure 12. Time to determine the TS of a complex system depending on the size of the precedent base

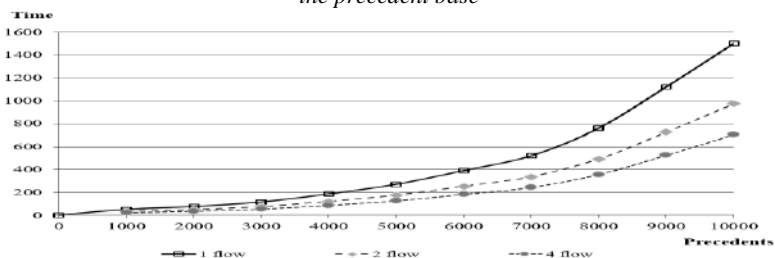


Figure 13. Execution time of computational processes based on the number of formed precedents

In order to estimate the time spent on the formation of the knowledge base as part of the implementation of the proposed method with the help of the developed IIS, a comparison of the execution time of computing processes was carried out when starting the system in the following modes: single-threaded; two-flow; four-flow (Fig. 13). It should be noted the general exponential nature of the dependence of the time of execution of computational processes of estimations and forecasting of TC of a ship's power plant on the number of precedents in the knowledge base.

Thanks to the distributed computing mode, it becomes possible to reduce time costs by up to 28% when using two data streams isolated from each other, and up to 42% in the case of dividing the computing load into four separate data streams. The presented interface of the main form of the software system with the tab for managing the process of creating precedents implements the functionality of determining the serviceability of the IIS with the CBR cycle and the implementation of the functions embedded in it.

Taking into account partial and complete failures of the ship's CTS short-circuit equipment in the IIS will allow the decision-maker to make decisions aimed at pre-failure maintenance of complex systems, and thereby extend the service life of the systems, which means increasing the efficiency of their operation.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

7. Conclusion

Thus, the development and research of IIS with CBR was carried out, intended for effective evaluation and forecasting of TC of complex short-circuit systems by ensuring the speed of operation of IIS.

The effective functioning of IIS with CBR is based on the use of the method of reasoning based on precedents. IIS with CBR consists of: interface module; database with library of precedents and database; request formalization module; a module of recommendations for ensuring the effectiveness of the CTS; CTS structural scheme libraries; modules of formalization of expert assessments and formalization of knowledge. Experimental studies of IIS for evaluation and forecasting of TC of complex systems showed that the time spent for the closest precedent to be found in the database of 10,000 precedents was about 370 ms.

The sequence of decision-making, using the proposed IIS system with a CBR cycle, which takes into account the operations of data processing and structuring according to precedents within the framework of the functioning of the developed application software system, has high speed, provides work with incomplete information, versatility and learning with decision-making support. Thanks to the distributed computing mode, it becomes possible to reduce time costs by up to 28% when using two data streams isolated from each other, and up to 42% in the case of dividing the computing load into four separate data streams. In the operation of the proposed IIS, partial and complete failure of subsystems, components, elements and their mutual connections in the CTS of the circuit are taken into account. Increasing the efficiency of operation of the CTS is ensured by the speed of evaluation and forecasting of the TC, as well as by the actions of the decision-maker aimed at making decisions regarding the pre-failure maintenance of the equipment of complex systems in the early stages of the development of failures. The design of the IIS was carried out to ensure the efficiency of the CTS operation using the method of reasoning based on precedents. The design of IIS with CBR connects the developed models and methods of diagnosis, assessment and forecasting of TC of complex short-circuit systems with an expert system containing calculation, experimental, as well as data obtained by experts during the operation of CTS. The cores of IIS are: database; a knowledge base with a library of precedents, with methods for calculating probability indicators, failure risks and a set of decisive rules for decision-making; request formalization module; a module of recommendations for ensuring the effectiveness of the CTS; CTS structural scheme libraries; module of formalization of expert evaluations; knowledge formalization module. The implementation of the developed strategy in the IIS is ensured by purposeful actions in accordance with decision-making to find equipment failures based on the established evaluations of their TCs. In order to check the performance, a simulation of the full cycle of the IIS evaluation, risk prediction (probability) of CTS failures was carried out using the example of a ship's power plant using the developed knowledge base. The received assessments of the risks (probabilities) of failures of subsystems, components, and elements of their mutual relations, which do not

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

contradict expert assessments, testify to the effectiveness of diagnostics, assessment and forecasting of complex systems, taking into account their partial and complete failures.

7. References

- [1] ISO/IEC/IEEE 15288:2015 "Systems and software engineering - System life cycle processes".
- [2] Aven, T. Foundations of Risk Analysis. England: John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex PO19 8SQ, 2003. 205 p. DOI: <https://doi.org/10.1002/0470871245>.
- [3] ISO/IEC 31010:2019. Risk management-Risk assessment techniques, 2019. 127 p.
- [4] Vychuzhanin V., Rudnichenko N. Assessment of risks structurally and functionally complex technical systems. Eastern-European Journal of Enterprise Technologies. 2014. 1. 2. P.18-22. DOI: <https://doi.org/10.15587/1729-4061.2014.19846>.
- [5] Asuquo M., Wang J., Zhang L., Phylip-Jones, G. An integrated risk assessment for maintenance prediction of oil wetted gearbox and bearing in marine and offshore industries using a fuzzy rule base method. Proc. Inst. Mech. Eng. Part M J. Eng. Marit. Environ, 2020. 234 p. DOI: <https://doi.org/147509021989952>.
- [6] Zhang M., Montewka J., Manderbacka T., Kujala P., Hirdaris S. A Big Data Analytics Method for the Evaluation of Ship. Ship Collision Risk reflecting Hydrometeorological Conditions. Reliability Engineering & System Safety. 2021. 213. 21 p. Doi: <https://doi.org/10.1016/j.res.2021.107674>.
- [7] Vychuzhanin V.V., Rudnichenko N.D. Tekhnicheskkiye riski slozhnykh kompleksov funktsional'no vzaimosvyazannykh strukturnykh komponentov sudovykh energeticheskikh ustanovok. Vísnik Odes'kogo natsional'nogo mors'kogo uníversitetu, zbirnik naukovikh prats. 2014. 2(40). P. 68-77.
- [8] IEC 60812. Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA), 2018. 93 p.
- [9] IEC 60812. Failure modes and effects analysis (FMEA and FMECA), 2018. 165 p.
- [10] George-Williams H., Santhosh T. V., Patelli E. Simulation Methods for the Analysis of Complex Systems. Oxford, United Kingdom. 2022. 19 p.
- [11] Vychuzhanin V.V. Informatsionnaya kognitivnaya model' tekhnologicheskoy vzaimozavisimosti slozhnykh tekhnicheskikh system. Informatika ta matematichní metodi v modelyuvanní. 2013. 3.3. P. 240-247.
- [12] Raptodimos Y., Lazakis I. Using artificial neural network-self-organising map for data clustering of marine engine condition monitoring applications. Ships Offshore Struc. 2018. 13. P. 649–656. DOI: <https://doi.org/10.1080/17445302.2018.1443694>.
- [13] Phylip-Jones G. An integrated risk assessment for maintenance prediction of oil wetted gearbox and bearing in marine and offshore industries using a fuzzy rule base method. Proc. Inst. Mech. Eng. Part M J. Eng. Marit. Environ. 2020, 234 p.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

- [14] Vychuzhanin V.V., Rudnichenko N.D. Metody informatsionnykh tekhnologiy v diagnostike sostoyaniya slozhnykh tekhnicheskikh sistem: monografiya. Odessa: Ekologiya, 2019. 178 p.
- [15] Rudnichenko N., Vychuzhanin V., Polyvianchuk A., Mateichyk V. Complex Technical System Condition Diagnostics and Prediction Computerization. CMIS-2020 Computer Modeling and Intelligent Systems / CEUR Workshop Proceedings, 2608. 2020. P. 42–56.
- [16] Vychuzhanin V.V., Rudnichenko N.D., Vychuzhanin A.V., Kozlov A.Ye. Programmnoye obespecheniye avtomatizatsii otsenki riska otkazov slozhnykh tekhnicheskikh sistem. Informatics and Mathematical Methods in Simulation. 2019. 9. 4. P. 315-323. DOI: <https://doi.org/10.15276/imms.v9.no4>.
- [17] Zhang P., Gao Z., Cao L., Dong F., Zou Y. Marine Systems and Equipment Prognostics and Health Management: A Systematic Review from Health Condition Monitoring to Maintenance Strategy. Machines, 2022. 53 p. DOI: <https://doi.org/10.3390/machines10020072>,
- [18] Vychuzhanin V. V. Information support remote risk assessment of complex technological systems. Computer science is the method in matematichni modelyuvanni. 2016. 2. P. 133–141.
- [19] Cordeiro-Costas M., Villanueva D., Eguina-Oller P., Martnez-Comesaca M., Ramos S. Load Forecasting with Machine Learning and Deep Learning Methods. Basel, Switzerland. 2023. 25 p. DOI: <https://doi.org/10.3390/app13137933>
- [20] Dumargue T., Pugeon J., Masse J. An Approach to Designing PHM Systems with Systems Engineering. Eur Conf PHM Soc, 2016. 12 p.
- [21] ISO 13381-1:2015 Condition monitoring and diagnostics of machines – Prognostics – Part 1: General guidelines. Enter. 2015-03-01, 2015. 21 p.
- [22] Vychuzhanin V.V., Rudnichenko N.D. Development of the neural network model for prediction failure risk's of the complex technical systems components. Informatics and Mathematical Methods in Simulation. 2016. 6. 4. P. 333-338.
- [23] Vychuzhanin V.V., Shibaeva N.O. Information support remote risk assessment of complex technological systems. Computer science is the method in matematichni modelyuvanni. 2016. 2. P. 133–141.
- [24] Rudnichenko N.D., Vychuzhanin V.V. Metod upravleniya riskami sudovykh slozhnykh tekhnicheskikh sistem. Problemi tekhniki, 2014. 2. P. 138-142.
- [25] Vychuzhanin V., Rudnichenko N., Boyko V. et al. Devising a method for the estimation and prediction of technical condition of ship complex systems. Eastern-European Journal of Enterprise Technologies. 2016. 84. 6/9. P. 4-11.
- [26] Burstein F., Holsapple C. Handbook on Decision Support Systems. New York: Springer-Verlag, 2008. 854 p. DOI: <https://doi.org/10.1007/978-3-540-48713-5>.
- [27] Turikov M.I. Dynamics of Systems, Mechanisms and Machines (Dinamics). IEEE Xplore Digital Library. - Electronic text data, 2018. P. 1-7. URL: <https://ieeexplore.ieee.org/document/8601472>. (дата звернення: 15.10.2023).
- [28] Sai Van Kwong. A predictive maintenance modeling tool implemented as R-package and web-application. SoICT 2019: Proceedings of the Tenth International Symposium on Information and Communication Technology (Hanoi, Ha Long Bay,

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

- Viet Nam, December 4-6, 2019). New York (NY, USA): ACM, 2019. P. 433-440. DOI: <https://doi.org/10.1145/3368926.3369693>.
- [29] Aqel Musbah J., Nakshabandi Omar A., Adeniyi Ayodeji. Decision Support Systems Classification in Industry. *Periodicals of Engineering and Natural Sciences*. 2019. 7.2. P.774-785.
- [30] Ran, Y. A Survey of Predictive Maintenance: Systems, Purposes and Approaches. *IEEE communications surveys & tutorials*. 2019. P.1-36.
- [31] Siepermann M. Risk Cost Accounting and Bottom Price Calculation—A Risk Management Information System. *International Conference on the Economics of Grids, Clouds, Systems, and Services*. – Springer, Cham. 2017. P. 43-55.
- [32] Borra N., Dey S., Bhattacharyya M.S. Bouhleb, Intelligent Decision Support Systems: Applications in Signal Processing, De Gruyter Frontiers. *Computational Intelligence*. 2019. 4. 195 p. DOI: <https://doi.org/10.1515/9783110621105>.
- [33] Lopez C., Ishizaka A. A scenario-based modeling method for controlling ECM performance. *Expert systems with applications*. 2018. 97. P. 253-265. DOI: <https://doi.org/10.1016/j.eswa.2017.12.024>.
- [34] Luger D. *Artificial intelligence: strategies and methods for solving complex problems*. Williams, 2003, 779 p.
- [35] Ocampo E, MacEiras M, Herrera S, Maurente C, Rodríguez D. *Expert Systems with Applications*, 2011. 38 p.
- [36] Shaoli C, Jianjun Yi, Hui J, Xiaomin Z. Ontology and CBR based automated decision-making method for the disassembly of mechanical products. *Advanced Engineering Informatics*, 2016. 30. 3. P. 564-584.
- [37] Boullosa-Falces D., Barrena J.L.L., Lopez-Arraiza A., Menendez J. Monitoring of fuel oil process of marine diesel engine. *Appl. Therm. Eng.* 2017. 127. P. 517–526. DOI: <https://doi.org/10.1016/j.applthermaleng.2017.08.036>.
- [38]. Harrington E.C. The desirability Function. *Industrial Quality Control*, 21(10), 1965 P. 494–498.
- [39] Berman A. F. Method of synthesis and analysis of fault trees based on the concepts of mechanism and kinetics of events. *Problems of risk analysis*. 2018. 15. 3. P. 62 - 77.
- [40] Mosavi A. The Multiobjective Optimization Package of IOSO; Applications and Future Trends. Conference: Conference of PhD Students in Computer Science, Szeged, Hungary. 2010. P. 55-56. DOI: <https://doi.org/10.13140/RG.2.1.3788.5286>.
- [41] Shunkun Yang, Chong Bian, Xing Li, Lin Tan.. Optimized fault diagnosis based on FMEA-style CBR and BN for embedded software system. *The International Journal of Advanced Manufacturing Technology*. 2018. 94. P. 3441 – 3453. DOI: <https://doi.org/10.1007/s00170-017-0110-y>.
- [42] Sumana De, Baisakhi Chakraborty. A Novel CBR-Decision Tree Based Intelligent Car Fault Diagnosis System (CFDS). *International Journal of Recent Technology and Engineering*. 2019. 8. P. 2180-2193. DOI: <https://doi.org/10.35940/ijrte.B2390.078219>.

МЕТОД ОЦІНКИ ТА ПРОГНОЗУВАННЯ ТЕХНІЧНОГО СТАНУ
СКЛАДНИХ СИСТЕМ КРИТИЧНОГО ЗАСТОСУВАННЯ НА
ОСНОВІ ПРЕЦЕДЕНТІВ

Ph.D. О. Вичужанін ORCID: 0000-0001-8779-2503

Національний університет «Одеська політехніка», Україна

E-mail: vuchuzhanin.o.v@op.edu.ua

Dr.Sci. В.Вичужанін ORCID: 0000-0002-6302-1832

Національний університет «Одеська політехніка», Україна

E-mail: v.v.vuchuzhanin@op.edu.ua

***Анотація.** Розроблено метод оцінки та прогнозування технічного стану складних систем критичного застосування на основі на основі прецедентів. При поданні прецеденту у вигляді набору параметрів з конкретними значеннями та рішеннями враховано: параметри, що описують прецедент; оцінки ризику, ймовірності відмов та оцінки збитків від відмов складних систем; рекомендації особи, яка приймає рішення; оцінки працездатності (часткової або повної); уточнені оцінки параметрів технічного стану складних систем; уточнені прогнозовані значення параметрів технічного стану складних систем. Розроблено інформаційну інтелектуальну систему оцінки та прогнозування технічного стану складних систем критичного застосування з використанням методу міркувань на основі прецедентів (CBR) та розроблено стратегію прийняття рішень щодо пошуку відмов обладнання на основі встановлених оцінок їх технічного стану. Для перевірки працездатності було здійснено моделювання повного циклу функціонування інформаційної інтелектуальної системи оцінювання, прогнозування ймовірності (ризиків) відмов складних систем на прикладі суднової енергетичної установки. Отримані значення оцінок ймовірностей (ризиків) підсистем, компонентів, елементів та їх взаємних зв'язків, що не суперечать експертним оцінкам, свідчать про ефективність діагностики, оцінки та прогнозування технічного стану складних систем, враховуючи повні та часткові відмови працездатності. Врахування часткових (повних) відмов обладнання складних систем критичного застосування дозволить приймати рішення, спрямовані на передвідмовне обслуговування систем, забезпечити працездатність, підвищувати ефективність їх експлуатації. Послідовність прийняття рішень з використанням запропонованої інформаційної інтелектуальної системи з CBR циклом, що враховує операції обробки та структуризації даних за прецедентами, в рамках функціонування розробленого програмного забезпечення, забезпечує роботу інформаційної інтелектуальної системи з неповною інформацією.*

***Ключові слова:** метод, моделювання, алгоритм, програмне забезпечення, інтелектуальна, метод міркувань на основі прецедентів, діагностика, оцінка, прогнозування, особа, яка приймає рішення, складна технічна система, суднова енергетична установка.*

УДК 004.89

**ПРОГНОЗУВАННЯ ФІНАНСОВОГО РИНКУ НА ОСНОВІ
МОДЕЛІ АНАЛІЗУ АКЦІЙ, ЯКА ВРАХОВУЄ ЇХ ЗВ'ЯЗКИ**

Dr.Sci. М. Корабльов ORCID: 0000-0002-8931-4350

Харківський національний університет радіоелектроніки, Україна

E-mail: mykola.korablyov@nure.ua

Д. Антонов ORCID: 0009-0000-2079-3413

Харківський національний університет радіоелектроніки, Україна

E-mail: danylo.antonov@nure.ua

О. Ткачук ORCID: 0009-0006-2943-9887

Харківський національний університет радіоелектроніки, Україна

E-mail: alexander.k.tkachuk@gmail.com

Анотація. *Здатність передбачати ціни на акції має важливе значення для обґрунтування інвестиційних рішень на фінансовому ринку. Для аналізу акцій з метою прогнозування фінансового ринку використовуються різні підходи: статистичні методи, розпізнавання образів, графіки, машинне навчання тощо. Так як акції існують на великому та взаємопов'язаному ринку, то традиційні методи, що ґрунтуються на інформації про часові ряди для окремої акції, не враховують взаємозв'язків між іншими акціями. Ефект зв'язку на фінансовому ринку, де на ціни акцій впливають ціни взаємопов'язаних акцій, вимагає використання інших підходів. Врахування взаємозв'язків між акціями може підвищити ефективність прогнозування цін на акції. Пропонується гібридна модель аналізу акцій, в якій використовується комбінація різних інтелектуальних технологій: рекурентних нейронних мереж для визначення характеристик часових рядів акцій; штучних імунних мереж для визначення взаємозв'язків між акціями; графових нейронних мереж, що дозволяють прогнозувати фінансовий ринок для прийняття більш обґрунтованих рішень з метою отримання високих прибутків за низьких ризиків. Проведено експериментальні дослідження з акціями 16 відомих технологічних компаній, які показали, що показник середньоквадратичної помилки для всіх акцій не перевищив 2%. Це вказує на достатньо високу ефективність запропонованої гібридної моделі аналізу акцій для прогнозування фінансового ринку.*

Ключові слова *акція, фінансовий ринок, прогнозування, прибуток, взаємодія, нейронна мережа, штучна імунна мережа*

1. Вступ

Фінансові ринки завжди впливали на багато сфер людської діяльності, такі як бізнес, освіта, технології та ін., що в цілому впливає на економіку. Протягом багатьох років фахівці займалися розробкою та дослідженням моделей поведінки цін на акції. Слід зазначити, що аналіз поведінки ціни акції є дуже складним процесом, оскільки рух ринку цін має динамічний, нелінійний,

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

нестационарний, непараметричний, зашумлений і хаотичний характер [1-4]. Крім того, на ринок цін на акції впливає безліч тісно взаємопов'язаних факторів, таких як економічні, політичні, психологічні, специфічні для конкретної компанії та ін.

Зі збільшенням обсягу даних використання традиційних методів аналізу фінансових ринків, заснованих на інформації про часові ряди для окремої акції, дає велику похибку прогнозу. Тому були запропоновані алгоритми інтелектуального аналізу даних для підтримки прийняття рішень інвесторами на різноманітних фінансових ринках. Аналіз фінансового ринку сьогодні побудований з використанням комбінації різних технологій [5-8], таких як машинне навчання, статистика, експертні системи та ін., які взаємодіють одна з одною для полегшення ухвалення більш обґрунтованих рішень.

У той самий час існує взаємозв'язок між змінами цін кількох пов'язаних акцій, які можуть виявлятися в одночасному зміні цін. Тому розробка моделей аналізу акцій, що використовують різні технології інтелектуального оброблення інформації та враховують взаємозв'язки між акціями, є актуальним завданням, що дозволяє підвищити точність прогнозування цін на акції.

2. Методи аналізу фінансових ринків

Для інвестування в акції з метою отримання високого прибутку за низьких ризиків інвестори використовують два основних підходи до прийняття рішень на фінансових ринках [9] – технічний та фундаментальний аналізи.

Технічний аналіз (ТА) – це комплекс методів оцінки та прогнозування ситуації на фінансових ринках. Методи ТА є ключовим інструментом для аналізу ринку, допомагаючи зрозуміти, коли та які акції варто купувати чи продавати. ТА на основі статистичних закономірностей у динаміці цін допомагає приймати виважені торговельні та інвестиційні рішення. Виявлені закономірності використовуються як індикатори для прогнозування. ТА спирається на вивчення цінових рухів, виявлення повторюваних моделей та визначення моделей, які дозволяють передбачати зміни цін у найближчому майбутньому.

Біржові аналітики використовують різні індикатори ТА, які допомагають аналізувати ринок. Власне, це є математичні функції, що засновані на динаміці ціни, обсязі торгів та інших статистичних даних, і навіть на кореляціях між ними. Вони допомагають формувати торгові сигнали, тобто, підказки трейдерам продавати чи купувати, які акції та у якій кількості, які торгові пари використовувати та ін.

Проте використання лише ТА не завжди давало бажаний результат. Тому купівля чи продаж акцій має ґрунтуватися на використанні додаткових факторів, таких як фундаментальний аналіз (ФА) [1]. Для ФА існують різні підходи до оцінки, такі як метод апроксимації середнього зростання та метод апроксимації постійного зростання.

Останні досягнення в галузі аналізу акцій та прогнозування фінансових ринків відносяться до чотирьох категорій [10-12]: статистика, розпізнавання

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

образів, машинне навчання (МО) та аналіз настроїв. Ці категорії переважно підпадають під ширшу категорію ТА, проте є деякі методи машинного навчання, які також поєднують ширші категорії ТА з підходами ФА для прогнозування фінансових ринків [13-15]. Розпізнавання образів є складовою машинного навчання, але стосовно біржового аналізу ці два методи застосовуються зовсім по-різному. Розпізнавання образів фокусується на виявленні закономірностей та тенденцій у даних. Паттерни на фондових ринках – це послідовності, що повторюються і зустрічаються на графіках, які трейдери використовували як сигнали на купівлю і продаж.

Технічний аналіз спирається на закономірності, виявлені безпосередньо у біржових даних. Він включає візуальний аналіз графіків, побудованих з плином часу, щоб показати зміни ціни, обсягу або інших похідних показників, таких як імпульс ціни тощо. Машинне навчання широко вивчалось щодо його використання у прогнозуванні фінансових ринків [6-8]. Для прогнозування ціни на акції використовувалися такі прості методи як дерева рішень, дискримінантний аналіз та наївний байєсівський аналіз.

Потім були використані ефективніші методи, такі як випадковий ліс, логістична регресія та нейронні мережі. Використання глибоких нейронних мереж стало основним інструментом аналізу фінансового ринку завдяки своїм нелінійним, керованим даними та легко узагальнюваним характеристикам.

Водночас підвищення якості аналізу та точності прогнозування фінансового ринку можна отримати шляхом використання гібридного підходу, який реалізує комбінацію кількох різних методів. Гібридний підхід використовує комбінацію кількох різних підходів підвищення продуктивності, наприклад, гібрид статистичних підходів і підходів до розпізнавання образів, чи гібрид статистичних підходів і підходів машинного навчання. Слід зазначити, що традиційні методи, що базуються на інформації про часові ряди окремих акцій, не враховують взаємозв'язки між іншими акціями. На фінансовому ринку існує кореляційний зв'язок між акціями, який необхідно враховувати під час аналізу та прогнозуванні [10].

В даний час інформація про взаємозв'язок акцій в основному виходить із використанням даних галузевої класифікації, але ці дані часто є приблизними. Тому мета даного дослідження полягає в тому, щоб побудувати модель аналізу акцій для прогнозування фінансового ринку, яка б інтегрувала інформацію про зміну цін акцій у часі та взаємозв'язки між ними з використанням різних технологій інтелектуальної обробки інформації.

3. Модель аналізу акцій з урахуванням їх взаємозв'язків

3.1. Структура моделі аналізу акцій

Побудуємо модель аналізу акцій, яка об'єднує інформацію про час та взаємозв'язки. Для отримання характеристик часового ряду кожної акції доцільно використовувати рекурентну нейронну мережу (RNN). Для отримання відповідних взаємозв'язків між акціями у вигляді графа відносин

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

необхідно виконати кластеризацію акцій із використанням однієї з моделей, наприклад, штучну імунну мережу (aiNET). Для інтеграції інформації про часові ряди, отриманої з використанням RNN, з інформацією про взаємозв'язки між акціями, отриманої з використанням моделі кластеризації у вигляді графа, використовуємо графову нейронну мережу (GNN). Це дозволить більш обґрунтовано прогнозувати ціни на акції. Структура гібридної моделі аналізу акцій для прогнозування фінансового ринку наведена на рис. 1.

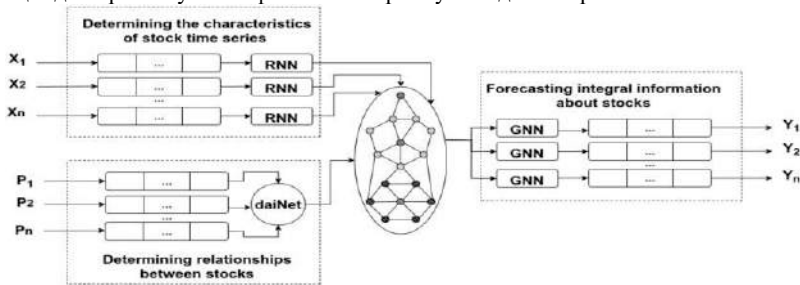


Рисунок 1. Структура гібридної моделі аналізу акцій

На входи RNN подаються часові ряди торгових характеристик акцій $X_i = (X_1^i, X_2^i, \dots, X_t^i, \dots, X_T^i)$, $i = \overline{1, N}$, де $X_t^i = (x_1, x_2, \dots, x_n)$, n – розмірність акції, N – число акцій, t – торговий день, T – довжина часового ряду. RNN дозволяє отримати характеристики часових рядів зміни цін на акції $P_i = (p_1^i, p_2^i, \dots, p_t^i, \dots, p_T^i)$, що подаються на вхід моделі кластеризації, за допомогою якої можна отримати інформацію про взаємозв'язки між акціями у вигляді графа. Отриманий граф відносин та характеристики часових рядів акцій, які використовуються як параметри вузлів графа, подаються на вхід GNN для прогнозування цін на акції. На виході GNN отримуємо оцінки дохідності акцій $Y_i = (Y_1, Y_2, \dots, Y_N)$, $i = \overline{1, N}$ на наступний період.

Таким чином, запропонована гібридна модель аналізу акцій для прогнозування фінансового ринку, яка враховує взаємозв'язки між акціями і включає в себе три модуля, кожен з яких реалізує відповідну модель інтелектуальної обробки інформації: рекурентну нейронну мережу (RNN), штучну імунну мережу (aiNET) та графову нейронну мережу (GNN).

3.2. Визначення характеристик часових рядів акцій

Для аналізу акцій та прогнозування фінансових ринків широко використовується статистичний підхід [12]. Часові ряди в аналізі фінансових ринків є хронологічним набором спостережень, таких як щоденні підсумки продажу та ціни акцій. Проте статистичні методи, які дозволяють аналізувати та прогнозувати акції, передбачають лінійність, стаціонарність та нормальність, що суттєво обмежує їх можливості. Тому сучасні методи

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

інтелектуального аналізу даних, представлені машинним навчанням, є ефективнішим засобом для аналізу акцій та прогнозування фінансових ринків.

Для отримання часової інформації про акції доцільно використовувати рекурентні нейронні мережі (RNN) (рис. 2) [16]. RNN – це модель глибокого навчання, яка навчена обробляти та перетворювати послідовний набір вхідних даних у послідовний набір вихідних даних. Тобто, RNN представляє собою архітектуру, яка здатна працювати з послідовними даними. Вона використовує механізм повторного входу, що дозволяє враховувати попередні стани та використовувати їх при обробці вхідних даних [16]. RNN називається рекурентною, тому що вона виконує одну і ту ж задачу для кожного елемента послідовності, причому вихід залежить від попередніх обчислень. Крім того, RNN – це мережа, яка має «пам'ять», що враховує попередню інформацію. Теоретично RNN може використовувати інформацію у довільно довгих послідовностях, але на практиці вона обмежена лише кількома кроками.

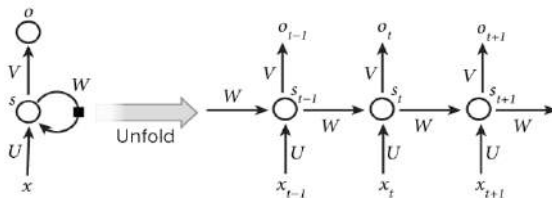


Рисунок 2. Рекурентна нейронна мережа та її розгортання

На відміну від традиційної глибокої нейронної мережі, яка використовує різні параметри в кожному шарі, RNN має однакові параметри (U , V , W) на всіх етапах. Це означає те, що виконується одне й те завдання на кожному кроці, використовуючи лише різні входи.

Це значно зменшує кількість параметрів, які потрібно підібрати. Основною особливістю RNN є прихований стан, який містить деяку інформацію про послідовність. Хоча RNN повинна працювати з усією послідовністю, на жаль, є проблема "загасаючого градієнта" (vanishing gradient problem). Це означає, що старші входи не впливають на вихід.

Різновидом RNN є довга короткострокова пам'ять (Long Short-Term Memory – LSTM) [17, 18]. Модель LSTM вирішує проблему "загасаючого градієнта", додаючи додаткові параметри (separate memory). LSTM принципово не відрізняється від RNN, але вона використовує функцію для обчислення прихованого стану (рис. 3).

LSTM є розширенням RNN, спроектованим для подолання проблем втрати та зсуву градієнтів. Для вирішення проблем зникнення та вибуху градієнта під час навчання довгих послідовностей у LSTM використовується кілька шарів нейронної мережі в одному рекурентному блоці. Вона використовує спеціальні блоки пам'яті, які дозволяють зберігати та оновлювати інформацію на тривалій термін. Пам'ять в LSTM є осередками, які можна розглядати як чорні

скриньки, що приймають попередній стан h_{t-1} як вхідні дані і поточний вхідний параметр x_t .

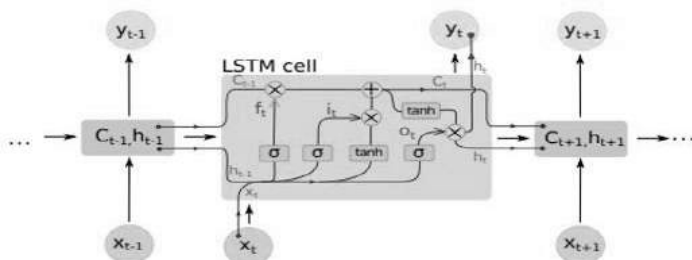


Рисунок 3. Довга короткострокова пам'ять (LSTM) та її комірка

Усередині ці осередки вирішують, яку пам'ять зберегти і яку стерти. Потім вони поєднують попередній стан, поточну пам'ять та вхідний параметр. Виявляється, ці типи одиниць дуже ефективні у захопленні (зберіганні) довгострокових залежностей.

Модель LSTM описується наступними рівняннями [18]:

$$\begin{aligned} f_t &= \sigma(W_f[h_{t-1}, x_t] + b_f), \quad i_t = \sigma(W_i[h_{t-1}, x_t] + b_i), \\ \tilde{C}_t &= \tanh(W_C[h_{t-1}, x_t] + b_C), \quad C_t = f_t \times C_{t-1} + i_t \times \tilde{C}_t \\ y_t &= \sigma(W_y[h_{t-1}, x_t] + b_y), \quad h_t = y_t * \tanh(C_t). \end{aligned} \quad (1)$$

де x_t – вхідний вектор; h_t – вихідний вектор; C_t – вектор станів; W_f, W_i, W_C, W_y – матриці параметрів; b_f, b_i, b_C, b_y – вектори параметрів; f_t, i_t – вектори вентилів, σ – сигмоподібна функція активації; \tanh – функція активації “гіперболічний тангенс”.

Таким чином, використання довготривалої короткочасної пам'яті (LSTM) дозволяє ефективно отримувати інформацію про часові ряди акцій та прогнозувати ціни на них.

3.3. Визначення взаємозв'язків між акціями

Задача визначення зв'язків між акціями вважається задачею кластеризації, що забезпечує отримання кореляцій між акціями. Для цих цілей може бути використаний один із методів кластеризації. Широке поширення інформаційних технологій призвело до створення великої кількості методів кластеризації, які широко використовуються в машинному навчанні, інтелектуальному аналізі даних, аналізі бізнес-процесів, розпізнаванні образів, завданнях із звуковими даними тощо. Ієрархічні методи, дерева рішень, метод С-середніх і метод опорних векторних машин сьогодні широко використовуються для вирішення практичних задач кластеризації [19]. Однак ці методи мають свої особливості, які ускладнюють їх застосування для

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

вирішення практичних завдань. Тому широкого поширення набули методи, що використовують біологічні принципи організації обчислювальної техніки, серед яких можна виділити штучні імунні системи [20].

Для вирішення завдання кластеризації акцій на основі імунного підходу доцільно використовувати модель штучної імунної мережі (aiNet). Це пояснюється тим, що модель aiNet передбачає аналіз не лише взаємодії типу антитіло-антиген, але й взаємодії типу антитіло-антитіло. Пропонується використовувати модель деревоподібної штучної імунної мережі (daiNet), запропонованої в [21], яка дозволяє формувати K -зв'язний граф. Вершинами графа є антитіла, що описують показники цін на акції $P_i = (p_1^i, p_2^i, \dots, p_T^i)$, $i = \overline{1, N}$, а ребрами – значення афінностей, що визначають ступінь зв'язності між ними.

Формування деревоподібної структури імунної мережі є багатоетапним оптимізаційним процесом, орієнтованим на скорочення кількості зв'язків між антитілами, використовуючи для цього значення афінностей та авідностей між антитілами. Результатом кластеризації буде мережа антитіл із визначеними кластерами.

На першому кроці мережа антитіл формується у вигляді графа (рис. 4) [22], де кожна вершина з'єднана з усіма іншими вершинами цього графа.

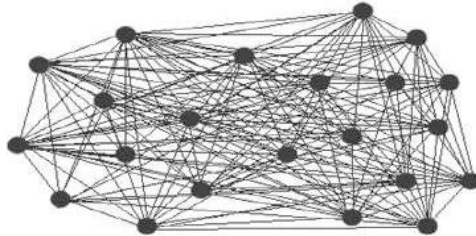


Рисунок 4. Перший етап формування деревовидної імунної мережі

Процес формування мережі антитіл – це процес оптимізації повнозв'язного графа, вершинами якого є антитіла, а ребрами – спорідненості між ними. Оптимізація означає зменшення кількості зв'язків між антитілами. Поріг природної спорідненості (NAT), який є спорідненістю між усіма антитілами в популяції, використовується як критерій, що регулює кількість афінних зв'язків між антитілами [23]:

$$NAT(AB) = \frac{\sum_{i=1}^n \sum_{j=1}^{n-1} aff(ab_i, ab_j)}{n(n-1)}, \quad (2)$$

де n – кількість антитіл у популяції; $aff(ab_i, ab_j)$ – значення афінності між i -м та j -м антитілами:

$$aff_{ij} = (1 + d_{ij})^{-1}, \quad (3)$$

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

де d_{ij} – евклідова або манхеттенська відстань між ознаками i -го та j -го імунних об'єктів.

Відповідно до цього зв'язки між антитілами видаляються, якщо їх афінності не перевищують значення NAT . При зменшенні кількості зв'язків між антитілами мережі daiNet передбачається використання деякого вхідного параметру K , який обмежує кількість зв'язків між антитілами мережі. Тобто, кожне антитіло може створювати не більше ніж K зв'язків з іншими антитілами мережі. Інші зв'язки, які створює це антитіло, видаляються. Ця ідея запозичена з алгоритму класифікації K найближчих сусідів (kNN) [19].

На другому етапі після формування K -пов'язаної мережі антитіл відбувається обчислення рівня стимуляції s_i кожного антитіла на основі його афінності з іншими імунними об'єктами, що формують мережу:

$$s_i = \frac{1}{K} \sum_{j=1}^K aff(ab_i, ab_j). \quad (4)$$

На основі значення рівня стимуляції $s_i, i = \overline{1, n}$ кожного антитіла відбувається визначення кандидатів в центри кластерів.

На третьому етапі формування мережі daiNet формується множина антитіл, які характеризуються високими рівнями стимуляції та кількістю зв'язків, що перевищують зазначений раніше параметр K . Під час вибору центрів кластерів з усіх антитіл-кандидатів у центри обирається антитіло, яке характеризується максимальною кількістю зв'язків з іншими антитілами мережі та максимальним рівнем стимуляції. Таке антитіло буде обрано у якості центра першого кластеру. Центри інших кластерів визначаються відносно обраного центру першого кластеру.

На четвертому етапі після розподілу центрів кластерів відбувається процес визначення приналежності до них антитіл імунної мережі. Спочатку кластеризуються імунні об'єкти, які характеризуються міцним афінним зв'язком з антитілами, які є центрами кластерів, тобто об'єкти, які мають прямі зв'язки з кластерами в daiNet з K зв'язками. Для проведення кластеризації інших антитіл, які не характеризуються міцним по афінності зв'язком з жодним із центрів сформованих кластерів, відбувається визначення авідностей до кожного з кластерів та його антитіл, що формують центр сильного згущення. Визначення авідності базується на спорідненості та афінності між імунними об'єктами. У цьому випадку авідність антитіла з іншими антитілами, що належать до одного кластера, визначається як сума афінностей між ними:

$$av_i = \sum_{j=1}^m aff(ab_i, ab_j), \quad (5)$$

де av_i – значення авідності i -го антитіла з іншими антитілами кластеру; m – кількість антитіл у кластері; $aff(ab_i, ab_j)$ – значення афінності між антитілами одного кластера згідно з (3).

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

Визначена таким чином авідність відображає рівень міцності імунного зв'язку між об'єктами кластеру та цим антитілом. Поняття авідності між антитілами та антигенами, або між антитілами імунної мережі часто використовується в моделях штучних імунних мереж, які використовуються для вирішення задач класифікації, кластеризації та аналізу даних.

На п'ятому етапі відбувається кластеризація інших об'єктів за величиною авідності i -го антитіла до інших антитіл кластера шляхом запуску імунних процесів в деревовидній імунній мережі антитіл з використанням операторів клонування, мутації, супресії клонів та мережі антитіл, що не належать до жодного кластеру. При цьому для кожного клону після його мутації відбувається визначення авідностей з цільовими об'єктами, якими є антитіла, що кластеризовані, і які формують кластери з центром сильного згущення.

Під час відбору для кожного клонованого антитіла зі всієї множини його клонів обирається один об'єкт, що характеризується максимальною авідністю з антитілами, що формують центр кластеру сильного згущення. Цей клон замінює собою антитіло, від якого він був створений під час роботи оператора супресії популяції антитіл з невизначеною приналежністю до кластеру. Слід зазначити, що імунний процес клонування, мутації, супресії клонів та супресії антитіл деревовидної імунної мережі завершиться у випадку, коли у мережі не залишиться жодного антитіла, що має авідність до одного з центрів кластеру, яка буде меншою за авідність у кластерах з центрами сильного згущення. Результатом кластеризації деревовидної штучної імунної мережі буде мережа антитіл з визначеними кластерами.

Приклад кластеризації штучної імунної деревовидної мережі антитіл, розподілених між двома визначеними кластерами, наведено на рис. 5. Внаслідок роботи моделі daiNet відбувається кластеризація початкової популяції антитіл. При цьому об'єкти належать до одного з виділених кластерів у процесі імунної взаємодії деревовидної К-зв'язної мережі антитіл. Проведення етапу визначення авідностей дозволяє провести кластеризацію антитіл до кластерів сильного згущення.

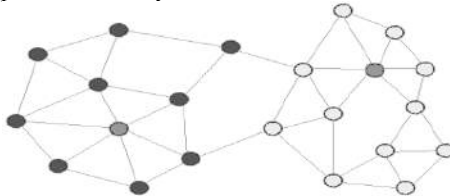


Рисунок 5. Приклад кластеризації антитіл, розподілених між двома кластерами

Процес кластеризації набору вхідних об'єктів на основі імунної моделі daiNET можна представити як послідовність виконання наступних етапів:

- 1) встановлення параметрів кластеризації та отримання початкового набору об'єктів;
- 2) визначення шкал ознак досліджуваних об'єктів;

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

- 3) формування K -зв'язної деревовидної імунної мережі;
- 4) виділення центрів кластерів;
- 5) визначення авідностей кластерів;
- 6) імунна саморегуляція мережі;
- 7) висновок про кластеризацію об'єктів.

Відповідно до цього, на рівні імунних операторів модель daiNet представляється виконанням відповідних етапів, поданих виразом (6):

У виразі (6) $Dendric-aiNet(AB, K, C)$ є умовним позначенням методу кластеризації вхідних об'єктів AB при використанні деревоподібної K -зв'язної імунної мережі антитіл та критерію C , що використовується для вказівки кількості кластерів, що формуються методом набору об'єктів.

Етап підготовки до кластеризації позначається скороченням PRP і містить кілька операторів: оператор $Scaling(AB)$ – використовується для проведення шкалювання об'єктів; оператор $Presentation(AB)$ – використовується для визначення афінностей між антитілами формованої імунної мережі; оператор $NATCalculation(AB)$ – використовується для визначення порогової афінності NAT в популяції антитіл.

Етап роботи, спрямований на формування K -зв'язної імунної мережі, має умовне позначення DKN і містить такі оператори: оператор $DKnetCreation(AB, K)$ – застосовується для формування K -зв'язної деревовидної мережі антитіл; оператор $CalcStimulation(AB)$ – застосовується для визначення рівня стимуляції антитіл; оператор $CentersSelection(AB, c, NAT)$ – використовується для виділення центрів кластерів; оператор $DendricClustering(AB')$ – використовується для формування кластерів сильного згущення.

$$Dendric - aiNet(AB, K, c) = \overset{PRP}{\left[\begin{array}{l} Scaling(AB) \rightarrow \\ Presentation(AB) \rightarrow \\ NATCalculation(AB) \end{array} \right]} \Rightarrow$$

$$\Rightarrow \overset{DKN}{\left[\begin{array}{l} DKnetCreation(AB, K) \rightarrow \\ CalcStimulation(AB) \rightarrow \\ CentersSelection(AB, c, NAT) \rightarrow \\ DendricClustering(AB') \end{array} \right]} \Rightarrow \quad (6)$$

$$\Rightarrow \overset{NET}{\left[\begin{array}{l} Cloning(AB'', CL) \rightarrow \\ Mutation(CL) \rightarrow \\ Presentation(CL, AB', AB'') \rightarrow \\ CLSupression(CL, AB', AB'') \rightarrow \\ NetSupression(CL, AB'') \rightarrow \\ AvCalculation(AB'') \rightarrow \\ ClusterSelection(AB'') \end{array} \right]},$$

Етап мережевої взаємодії має позначення NET і містить наступні оператори: оператор клонування $Cloning(AB'', CL)$ – що використовується

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

для поширення популяції антитіл, не пов'язаних з жодним із сформованих кластерів; оператор мутації $Mutation(CL)$ – використовується для зміни ознак клонів; оператор подання цільових об'єктів $Presentation(CL, AB', AB'')$ – використовується для визначення афінностей між клонами та об'єктами, що формують кластери сильного згущення; оператор супресії клонів $CLSupression(CL, AB', AB'')$ – використовується для редагування популяції клонів; оператор супресії мережі антитіл $NetSupression(CL, AB'')$ – використовується задля скорочення кількості об'єктів; оператор визначення авідностей між антитілами та кластерами сильного згущення $AvCalculation(AB'')$ – використовується для розподілу не кластеризованих об'єктів між кластерами, що формуються; оператор $ClusterSelection(AB'')$, який використовується задля визначення належності антитіл кластерам.

Таким чином, використання теорії графів для створення дендритної моделі імунної мережі daiNet дозволяє вирішити проблему підвищення продуктивності та зменшення складності формування мережі антитіл і областей розпізнавання, тим самим спростити визначення зв'язків між акціями.

3.4. Витяг інформації про взаємозв'язки між акціями

Для оцінки впливу зв'язків між акціями та характеристиками їх часових рядів на прогнозування курсу акцій використаємо графову нейронну мережу (GNN) [24, 25]. На вході GNN подається граф, вузли якого відображають ознаки часових рядів акцій, а дуги показують зв'язок між ними.

GNN є багаторівневою мережею, кожен рівень якої описується виразом [24]:

$$h_v^k = \sigma \left(W_k \sum_{u \in N(v)} \frac{h_u^{k-1}}{|N(v)|} + B_k h_v^{k-1} \right), \quad (6)$$

де σ – функція активації, W_k – вагові коефіцієнти, B_k – зсув, k – кількість шарів мережі.

Таким чином, на вході GNN надходять два типи даних: матриця суміжності, яка представляє зв'язок між акціями, і матриця особливостей часових характеристик акцій. Вихідний шар описується виразом:

$$y_v = h_v^k \quad (7)$$

і представляє прибутковість акцій на наступний період, що дозволяє прогнозувати інтегральну інформацію про акції для прийняття більш обґрунтованих рішень та підвищення стійкості фінансових ринків з метою отримання високих прибутків за низьких ризиків.

Результатом роботи GNN є доходність акцій.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

4. Експериментальні дослідження

Експериментальні дослідження проводилися з акціями 16 відомих технологічних компаній: Apple (AAPL), Amazon (AMZN), Cisco (CSCO), Electronic Arts (EA), eBay (EBAY), Meta (META), Google (GOOG), IBM (IBM), Intel (INTC), Microsoft (MSFT), Netflix (NFLX), NVIDIA (NVDA), Oracle (ORCL), Qualcomm (QCOM), Tesla (TSLA) і Adobe (ADBE).

Запропонована модель була реалізована за використанням Python.

За допомогою Yahoo Finance API через бібліотеку *pandas_datareader* були зібрані дані про щодобові ціни акцій за період з 1 січня 2021 р. по 1 січня 2023 р. На рис. 6 наведені графіки зміни цін на акції, де кожна точка на графіку – це середня ціна акції за місяць.

Дані про окремі акції були об'єднані в єдиний DataFrame, з якого була вилучена відповідна інформація, така як дата, ціна закриття та символ акції.

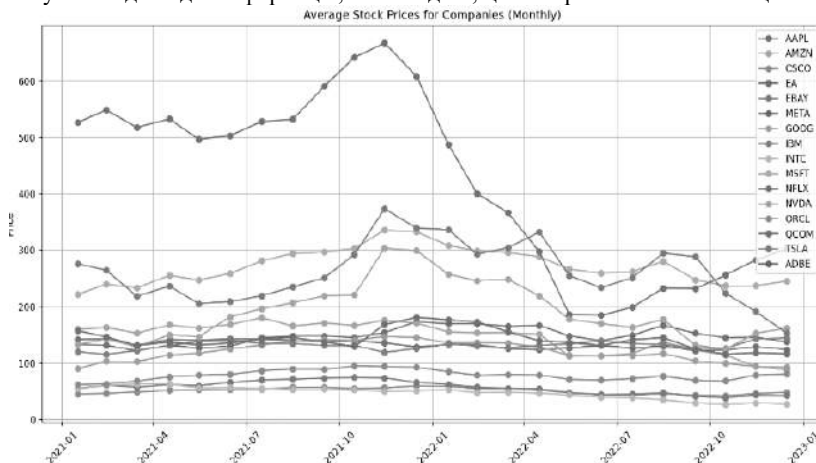


Рисунок 6. Графіки зміни цін на акції технологічних компаній

Експериментальні дані про щодобові ціни на акції за період з 1 січня 2021 р. по 1 січня 2023 р. були поділені на три інтервали:

- 1) навчальна вибірка (1 січня 2021 р. – 1 липня 2022 р.);
- 2) перевірна вибірка (1 липня 2022 р. – 1 жовтня 2022 р.);
- 3) тестовий набір (з 1 жовтня 2022 р. по 1 січня 2023 р.).

Під час навчання нейронних мереж кількість ітерацій моделі було встановлено рівним 500. В якості характеристик акцій було взято шість типів внутрішньо денних торгових даних: ціна відкриття, ціна закриття, висока ціна, низька ціна, обсяг і швидкість обороту, оскільки вони типові, поширені та легко доступні. Для оцінки якості моделі використовувалася середня квадратична помилка (MSE). Проведене моделювання показало, що цей показник для всіх акцій не перевищував 2%, що свідчить про досить високу ефективність запропонованої гібридної моделі аналізу акцій та прогнозування

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

фінансового ринку. Для отримання характеристик часових рядів про акції використовувалася рекурентна нейронна мережа LSTM, кількість шарів якої було взято рівним 2, а довжина часового ряду була встановлена рівною 30, тобто один місяць. Завдання визначення взаємозв'язків між акціями розглянуто як завдання кластеризації, для вирішення якої застосовано імунний підхід, а саме модель деревоподібної імунної мережі daiNet. Це дозволило отримати інформацію про акції технологічних компаній у вигляді графа (рис. 7), вершини якого відображають характеристики часових рядів про акції, а дуги – кореляції між акціями. Щоб дослідити кореляцію між цінами на момент закриття акцій технологічних компаній, використано DataFrame. Це дозволило впорядкувати дані за датою у вигляді рядків та кожний символ акцій у вигляді стовпців (матриця кореляції). Візуалізація теплової карти (рис. 8) створена за допомогою бібліотеки *seaborn* і *matplotlib*, що забезпечує інтуїтивно зрозуміле представлення кореляційної матриці.

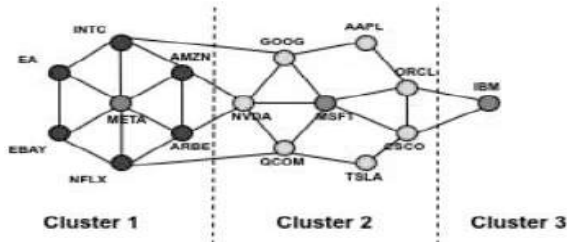


Рисунок 7. Граф кластеризації технологічних компаній

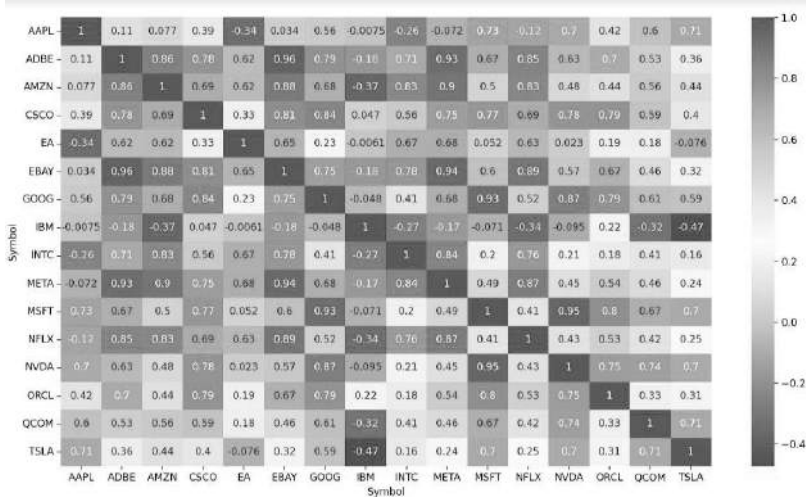


Рисунок 8. Візуалізація теплової карти кореляцій акцій технологічних компаній

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

На тепловій карті більш темні відтінки зеленого вказують на позитивні взаємозв'язки, тоді як відтінки червоного вказують на негативні взаємозв'язки. Чим ближче значення до +1, тим сильніша позитивна кореляція, і навпаки, чим ближче до -1, тим сильніша негативна кореляція. Значення близько 0 вказують на слабкий взаємозв'язок або на його відсутність. За допомогою цього аналізу можна зрозуміти, як ціна акцій технологічних компаній пов'язана протягом заданого періоду часу. Виявляючи сильні позитивні чи негативні кореляції, можна отримати уявлення про потенційні моделі чи залежності між різними акціями. Це дослідження може надати цінну інформацію інвесторам, трейдерам і фінансовим аналітикам, оскільки воно може виявити, які акції мають тенденцію рухатися разом, а які демонструють контрастні рухи. Крім того, досліджуючи кореляційні тенденції, інвестори можуть потенційно оптимізувати свої стратегії диверсифікації портфеля, мінімізувати ризик і підвищити прибутки шляхом розподілу активів між позитивно зв'язаними акціями. Дослідження також може призвести до виявлення технологічних компаній, які мають більший вплив на загальний рух ринку протягом зазначеного періоду. Ці акції можуть впливати на ринкові настрої та є актуальними для аналізу та прогнозування ринкових тенденцій.

Дослідження дозволяють виявити технологічні компанії, які мають більший вплив на загальний рух ринку протягом зазначеного періоду. Крім того, розуміння взаємозв'язку між акціями в технологічному секторі може вказати на загальний стан і стабільність галузі. Наприклад, високий ступінь позитивної кореляції між технологічними акціями може свідчити про те, що галузь переживає зростання або занепад, у той час як низькі кореляції можуть вказувати на відмінності в продуктивності окремих компаній. Це може привести до використання більш складних методів моделювання та прогнозування, які включають взаємозв'язки між акціями. У результаті, наглядно видно що є досить висока позитивна кореляція в парах Microsoft & Nvidia, Microsoft & Google та ін. Як наслідок, результати цього дослідження можуть сприяти поповненню існуючого масиву знань у сферах фінансів, економіки та інвестицій. Отриманий після кластеризації граф взаємозв'язків між акціями технологічних компаній (рис 7) вказав на створення трьох кластерів. До першого кластеру ввійшли наступні компанії: Adobe, Amazon, EA, eBay, Intel, Meta, Netflix, центром кластера є компанія Meta. Компанії в цьому кластері мають високу позитивну кореляцію одна з одною, що вказує на те, що ціни на їхні акції мають тенденцію рухатися разом. Ці компанії можуть належати до технологічних або пов'язаних із технікою секторів, оскільки вони мають подібну ринкову динаміку та на них можуть впливати загальні галузеві тенденції. До другого кластеру ввійшли наступні компанії: Apple, Cisco, Google, Microsoft, Nvidia, Oracle, Qualcomm, Tesla, центром кластера є компанія Microsoft. Цей кластер складається з компаній, які мають позитивні кореляції одна з одною, але не такі сильні, як компанії в кластері 1. Ці компанії можуть належати до різних секторів, але мають спільні ринкові тенденції або мають взаємопов'язану динаміку бізнесу. До третього кластеру ввійшла компанія IBM, яка є єдиною компанією в цьому кластері, що вказує на те, що її

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

взаємозв'язок з курсами акцій інших компаній у наборі даних відносно низький. Вона має тільки слабкий взаємозв'язок з компаніями Oracle та Cisco з кластеру 1. Це може бути унікальним у своїй поведінці на ринку порівняно з іншими компаніями. Отриманий граф взаємозв'язків між акціями технологічних компаній, який містить три кластери, з характеристиками часових рядів акцій, що використовуються як вираз вузлів на графі, подається на дві графові нейронні мережі GNN, кожна з яких є тришаровою і створена для кластерів 1 і 2. Для кластеру 3 немає необхідності створювати мережу GNN, так як він складається тільки з однієї компанії IBM.

Таким чином, кожна GNN дозволяє отримати прогнозовані ціни акцій наступного дня, після чого можна обирати акції з найбільшою прогнозованою прибутковістю на наступний період.

5. Висновки

Аналіз поведінки цін на акції є складним процесом. На ринок цін на акції впливає багато тісно взаємопов'язаних факторів. Крім того, дані про ціни на акції мають низьке відношення сигнал/шум, що робить прогнозування цін на акції складним завданням. Фінансовий ринок сьогодні збудований з використанням комбінації різних технологій, які взаємодіють один з одним для полегшення прийняття більш обґрунтованих рішень. У той самий час існує взаємозв'язок між коливаннями цін кількох пов'язаних акцій, які можуть виявлятися у одночасному зростанні чи падінні цін. Тому актуальним є розробка моделей аналізу акцій та прогнозування фінансових ринків, що враховують взаємозв'язки між акціями, що дозволяє підвищити точність прогнозування цін на акції.

Дослідження методів аналізу акцій та прогнозування фінансових ринків дозволило вибрати гібридний підхід, який використовує різні технології інтелектуальної обробки інформації та інтегрує інформацію про зміни цін на акції у часі і взаємозв'язки між ними. Запропоновано модель аналізу акцій та прогнозування фінансових ринків, у якій:

1. Для отримання часової інформації про акції використано рекурентну нейронну мережу LSTM, яка може ефективно витягувати інформацію про часові ряди акцій та прогнозувати ціни на акції.

2. Для вирішення завдання кластеризації акцій використано модель деревовидної штучної імунної мережі daiNet, яка дозволяє формувати K -пов'язаний граф, що враховує зв'язки, відносини та характеристики часових рядів акцій.

3. Для інтеграції інформації про часові ряди, отриманої з використанням моделі LSTM, з інформацією про взаємозв'язки між акціями, отриманої за допомогою моделі daiNet у вигляді графа, використана графова нейронна мережа GNN, на входи якої надходять дані двох видів: матриця зв'язків між акціями, та матриця ознак часових характеристик акцій. Виходами GNN є прибутковість акцій.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

Проведено експериментальні дослідження з акціями 16 відомих технологічних компаній, дані про щодобові ціни акцій яких були взяті за період з 1 січня 2021 р. по 1 січня 2023 р.

Проведене моделювання показало, що показник середньоквадратичної помилки для всіх акцій не перевищив 2%, що вказує на достатньо високу ефективність запропонованої гібридної моделі аналізу акцій для прогнозування фінансового ринку. Дослідження дозволили виявити технологічні компанії, які мають більший вплив на загальний рух ринку у вказаний період.

6. Література

- [1] R. Bhowmik, S. Wang, “Stock Market Volatility and Return Analysis: A Systematic Literature Review”, *Journals Entropy*, Vol., 22 Iss. 5, 2020, 522. doi 10.3390/e22050522.
- [2] P. Li, J. Xu, “A Study of Different Existing Methods for the Stock Selection in the Field of Quantitative Investment”, *Wireless Communications and Mobile Computing*, 2022. <https://doi.org/10.1155/2022/2695099>.
- [3] D. Shah, H. Isah, and F. Zulkernine, “Stock Market Analysis: A Review and Taxonomy of Prediction Techniques”, *Int. J. Financial Stud.*, 7(2), 2019, 26. <https://doi.org/10.3390/ijfs7020026>.
- [4] H. Liu, S. Huang, P. Wang, Z. Li, “A review of data mining methods in financial markets”, *Data Science in Finance and Economics*, Vol. 1, Iss. 4, 2021, pp. 362-392. doi 10.3934/DSFE.2021020.
- [5] K. Olorunnimbe, H. Viktor, “Deep learning in the stock market – a systematic survey of practice, backtesting, and applications”, *Artificial Intelligence Review*, Vol. 56, 2023, pp. 2057–2109. <https://doi.org/10.1007/s10462-022-10226-0>.
- [6] M. M. Kumbure, C. Lohrmann, P. Luukka, J. Porras, “Machine learning techniques and data for stock market forecasting: A literature review”, *Expert Systems With Applications*, 197, 2022, 116659.
- [7] Y. Guo, “Stock Price Prediction Using Machine Learning”, *Södertörn University / School of Social Science Master, Dissertation 30hp, Economics Spring, 2022*, 41 p.
- [8] A. Singh, P. Gupta, N. Thakur, “An Empirical Research and Comprehensive Analysis of Stock Market Prediction using Machine Learning and Deep Learning Techniques”, *IOP Conf. Series: Materials Science and Engineering*, 1022, 2021, 012098, <https://doi:10.1088/1757-899X/1022/1/012098>.
- [9] Y.J. Chen, Y.M. Chen, S.T. Tsao, et al., “A novel technical analysis-based method for stock market forecasting”, *Soft Comput* 22, 2018, pp. 1295–1312. <https://doi.org/10.1007/s00500-016-2417-2>.
- [10] C. Zhao, P. Hu, X. Liu, X. Lan, H. Zhang, “Stock Market Analysis Using Time Series Relational Models for Stock Price Prediction”, *Journals Mathematics*, 11(5), 2023, 1130. <https://doi.org/10.3390/math11051130>.
- [11] Y. Chen, J. Liu, Y. Gao, W. He, H. Li, G. Zhang, and H. Wei. “A new stock market analysis method based on evidential reasoning and hierarchical belief rule

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

- base to support investment decision making”. *Frontiers in Psychology*. 2023; 14: 1123578. <https://doi.org/10.3389/fpsyg.2023.1123578>.
- [12] C. Xiao, W. Xia, & J. Jiang, “Stock price forecast based on a combined model of ARI-MA-LS-SVM. *Neural Computing and Applications*”. Vol. 32, 2020, pp. 5379–5388. <https://doi.org/10.1007/s00521-019-04698-5>.
- [13] H. Widiputra, A. Mailangkay, E. Gautama, “Multivariate CNN-LSTM Model for Multiple Parallel Financial Time-Series Prediction”. *Complexity*, 2021, 9903518. <https://doi.org/10.1155/2021/9903518>.
- [14] S. Barra; S. Mario Carta; A. Corriga; A. S. Podda, and D. R. Recupero. “Deep learning and time series-to-image encoding for financial forecasting”. *IEEE/CAA Journal of Automatica Sinica*, Vol. 7, Iss, 2020, pp. 683 – 692. <https://doi.org/10.1109/JAS.2020.1003132>.
- [15] J. Wang, J. Kim. Predicting Stock Price Trend Using MACD Optimized by Historical Volatility. *Mathematical Problems in Engineering*, 2018(4), pp. 1-12. <https://doi.org/10.1155/2018/9280590>.
- [16] L. Zheng, H. He. Share price prediction of aerospace-relevant companies with recurrent neural networks based on PCA. “*Expert Systems with Applications*”. Vol. 183, 2021, 115384. <https://doi.org/10.1016/j.eswa.2021.115384>.
- [17] S. Arifin, A. K. Wijaya, R. Nariswari, A. Yudistira, Suwarno, Faisal, D. Wihardini. “Long Short-Term Memory (LSTM): Trends and Future Research Potential”. *International Journal of Emerging Technology and Advanced Engineering*, 2023. https://doi.org/10.46338/ijetae0523_04.
- [18] G.V. Houdt, C. Mosquera, G. Nápoles. “A Review on the Long Short-Term Memory Model”. *Artificial Intelligence Review*, 53, 2020. <https://doi.org/10.1007/s10462-020-09838-1>.
- [19] R.O. Duda, P.E. Hart, D.G. Stork, “*Pattern classification*”. Wiley & Sons, 2010.
- [20] H. Park, J.E. Choi, D. Kim, S.J. Hong, Artificial immune system for fault detection and classification of semiconductor equipment. *Electronics*, Vol. 10, No. 8, 944, 2021, pp. 1-14. <https://doi.org/10.3390/electronics10080944>.
- [21] M. Korablyov, O. Fomichov, M. Ushakov, M. Khudolei, “Dendritic Artificial Immune Network Model for Computing”, *Proceedings of the 7th International Conference on Computational Linguistics and Intelligent Systems (CoLInS 2023)*. Volume III: Intelligent Systems Workshop, Kharkiv, Ukraine, April 20-21, 2023, pp.206-217.
- [22] R. Diestel, *Extremal Graph Theory*. In: *Graph Theory*. Graduate Texts in Mathematics, Vol 173, Springer, Berlin, Heidelberg, 2017. <https://doi.org/10.1007/978-3-662-53622-3>.
- [23] K.B. Bahekar, Classification techniques based on Artificial immune system algorithms for Heart disease using Principal Component Analysis. *International Journal of Scientific Research in Science, Engineering, and Technology, IJSRSET*, Vol. 7, Iss. 5, 2020, pp. 150-160. <https://doi.org/10.32628/IJSRSET207542>.
- [24] L. Wu, P. Cui, J. Pei, L. Zhao, “Graph Neural Networks. *Foundations, Frontiers, and Applications*”. Springer, Singapore, 2022, 689 p.

[25] A. Keramatfar, M. Rafiee, H. Amirkhani, “Graph Neural Networks: a bibliometrics overview”, ELSEVIER, Machine Learning with Applications. Vol. 10, 2022, 100401. <https://doi.org/10.48550/arXiv.2201.01188>.

**FORECASTING THE FINANCIAL MARKET BASED ON A STOCK
ANALYSIS MODEL THAT TAKES INTO ACCOUNT THEIR
RELATIONSHIPS**

Dr. Sci. M. Korablyov¹, ORCID: 0000-0002-8931-4350

D. Antonov², ORCID: 0009-0000-2079-3413

O. Tkachuk³, ORCID: 0009-0006-2943-9887

Kharkiv National University of Radio Electronics, Ukraine,

E-mail: ¹mykola.korablyov@nure.ua, ²danylo.antonov@nure.ua,

³alexander.k.tkachuk@gmail.com

***Abstract.** The ability to predict stock prices is essential for justifying investment decisions in the financial market. Various approaches are used to analyze stocks for the purpose of forecasting the financial market: statistical methods, pattern recognition, graphs, machine learning, etc. Because stocks exist in a large and interconnected market, traditional methods based on time series information for an individual stock do not take into account the relationships between other stocks. The linkage effect in the financial market, where stock prices are influenced by the prices of related stocks, requires other approaches. Taking into account the relationships between stocks can improve the effectiveness of stock price forecasting. A hybrid model of stock analysis is proposed, which uses a combination of various intelligent technologies: recurrent neural networks to determine the characteristics of time series of stocks; artificial immune networks to determine the relationships between actions; graph neural networks that allow forecasting the financial market to make more informed decisions in order to obtain high profits at low risks. Experimental studies were conducted with the shares of 16 well-known technology companies, which showed that the average squared error for all shares did not exceed 2%. This indicates the sufficiently high efficiency of the proposed hybrid model of stock analysis for forecasting the financial market.*

***Keywords** stock, financial market, forecasting, profit, interaction, neural network, artificial immune network*

**AUTOMATED DATA MINING OF THE SINGLE ASTRONOMICAL
OBJECTS FROM THE BLURRED CCD-FRAMES**

Ph.D. S. Khlamov ORCID: 0000-0001-9434-1081

Kharkiv National University of Radio Electronics, Ukraine

E-mail: sergii.khlamov@gmail.com

Dr. Sci. V. Savanevych ORCID: 0000-0001-8840-8278

Kharkiv National University of Radio Electronics, Ukraine

E-mail: vadyim.savanevych1@nure.u

Ph.D. V. Vlasenko ORCID: 0000-0001-8639-4415

National Space Facilities Control and Test Center, Ukraine,

E-mail: vlasenko.vp@gmail.com

E. Hadzhyiev ORCID: 0009-0003-6752-7827

Kharkiv National University of Radio Electronics, Ukraine

E-mail: emil.hadzhyiev@nure.ua

***Abstract.** The chapter is devoted to the sophisticated data mining pipeline, which was designed for restoring the high-quality images from the blurred frames made by the Charge-Coupled Device (CCD) cameras. The developed data mining pipeline leverages the modern informational technologies for the horizontal and vertical scalability. The core methodology integrates the following mathematical methods and algorithms: an inverse median filtration method for the noise reduction and the Lucy-Richardson algorithm for deblurring. The inverse median filtration effectively reduces impulsive noise while preserving edges, and the Lucy-Richardson algorithm iteratively refines the image by correcting for blurring effects encoded in the point spread function (PSF). The proposed system's architecture of the processing pipeline for automated data mining of the single astronomical objects from blurred CCD frames utilizes the following modern technologies: Python programming language, Redis, FastAPI, React, Docker, and Caddy to ensure high performance, scalability, and ease of deployment. This integrated approach significantly enhances the accuracy of astronomical observations, facilitating more precise studies of celestial objects. The proposed pipeline addresses the unique challenges of astronomical image processing, offering a robust solution for automated data mining of single astronomical objects. Our work demonstrates the potential to advance astronomical research by improving image clarity and reliability, contributing to various fields within astronomy. The combination of effective noise reduction and deblurring techniques, along with a scalable and high-performance system architecture, provides a comprehensive solution to the challenges faced in processing astronomical images.*

***Keywords:** Data mining, automated pipeline, scalability, CCD frame, astronomical image, blurred image, image processing, image analysis, object*

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

detection, point spread function, Lucy-Richardson algorithm, noise reduction, inverse median filter, deconvolution, Python, Docker, FastAPI

1. Introduction

Astronomical imaging has significantly advanced our understanding of the universe [1]. However, capturing high-resolution images of celestial objects presents various challenges, one of the most prominent being image blur. This blur can obscure critical details necessary for astronomical research [2], thus necessitating sophisticated deblurring techniques. In the quest to observe and understand celestial phenomena, astronomers rely on highly sensitive imaging devices. Charge-Coupled Device (CCD) cameras [3] have become the cornerstone of modern astronomical research due to their superior sensitivity to light and ability to produce high-quality images with fine detail and low noise. These attributes make CCD cameras indispensable for capturing faint celestial objects and critical details necessary for astronomical observations [4]. Despite the advantages of CCD cameras, various factors contribute to the blurring of astronomical images. These include atmospheric conditions, optical imperfections, mechanical issues, and intrinsic properties of light. Understanding these causes is essential for developing effective deblurring techniques [5]. Astronomical image blur primarily results from atmospheric turbulence, where heterogeneities in atmospheric density and temperature cause differential refraction of celestial light, leading to distortions and the twinkling effect observed in stars. This phenomenon, known as "seeing," significantly impacts the clarity of astronomical observations [6]. Optical aberrations in telescopes, arising from imperfections in the design or misalignment of optical components, introduce further degradation. Aberrations such as spherical, chromatic, and astigmatic distortions compromise image fidelity, even in high-quality telescopes.

Examples of blurry astronomical objects are shown in Fig. 1.

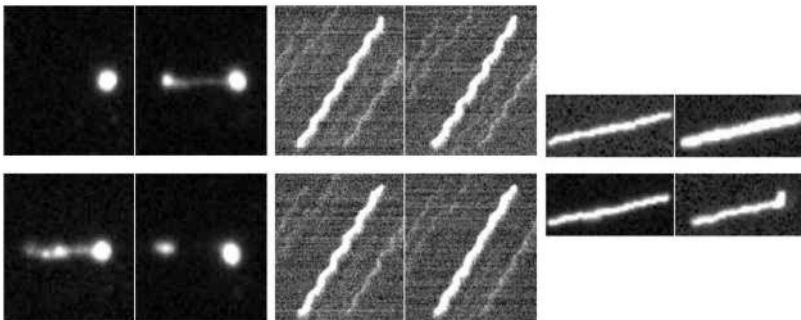


Figure 1. Examples of blurry astronomical objects

Without effective mathematical methods [7] to counteract blur, identifying features of distant galaxies, studying nebulae structures, and detecting exoplanets

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

become exceedingly difficult, often leading to incorrect interpretations and conclusions. Thus, developing various approaches to mitigate blur is critical for advancing astronomical research [8]. In this context, our work focuses on the implementation of the information system based on the processing pipelines for automated data mining [9] of single astronomical objects from blurred CCD frames. Our system is built upon cloud technologies, allowing us to scale the system efficiently, which is crucial when handling the large volumes of data common in astronomical research. The core of our methodology leverages the Lucy-Richardson algorithm [10], powerful deconvolution technique, to restore the original, unblurred images. The significance of our work lies in its potential to enhance the accuracy of astronomical observations and interpretations. By effectively mitigating the effects of blur, our system facilitates more precise studies of celestial objects, contributing to advancements in various fields of astronomy [11], from galaxy formation and evolution to the search for exoplanets. This chapter aims to the analysis of main focuses and features of the sophisticated data mining pipeline, which was designed for restoring the high-quality images from the blurred frames made by the CCD cameras using an inverse median filtration method and the Lucy-Richardson algorithm. Such methods and algorithms are implemented in scope of the mathematical module for intraframe processing in the Lemur software. Section 2 presents the literature review with mentioning advantages and disadvantages of the reviewed papers. Section 3 elaborates an architecture of the processing pipeline for data mining of the single astronomical objects from the blurred CCD-frames. Detailed description of steps of the processing pipeline are also presented in this section as well as the description of the inverse median filtration method and the Lucy-Richardson algorithm. This section also aims to the main features and advantages of the Lemur software for the astronomical data processing purposes. The developed data mining pipeline leverages the modern informational technologies for the horizontal and vertical scalability. Section 4 presents the results received during processing astronomical data with the different SSOs using the developed processing pipeline for data mining of the single astronomical objects from the blurred CCD-frames. The chapter ends with a conclusion in section 5, which illustrates the conclusions and outlines of the future work and research as well as possibilities for future investigations and enhancements.

2. Literature review

Data mining in astronomical image processing [12] is a critical area of research, focusing on extracting valuable information from the vast amounts of data generated by modern telescopes and imaging devices. Despite significant advancements in technology, numerous challenges impede the effectiveness of current data mining techniques. These challenges range from image quality issues to algorithmic limitations, making it difficult to achieve accurate and reliable results.

Common approaches to handle astronomical image blurring include machine learning algorithms, deconvolution techniques, and various image processing

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

methods. Machine learning algorithms, particularly deep learning, have shown promise in image restoration tasks. Convolutional neural networks (CNNs) [13] are widely used for their ability to learn complex patterns and features from large datasets. However, these models require extensive training data, which is often limited in astronomy, and are computationally intensive, posing challenges for real-time processing. Deconvolution techniques [14] are another prevalent approach. These methods iteratively restore images by reversing the effects of blurring. While effective, they rely heavily on accurate point spread function (PSF) estimates, which can be difficult to obtain. Misestimation of the PSF can lead to artifacts and suboptimal image restoration. Other methods include wavelet-based techniques [15] and matched filtration methods [16]. Wavelet-based approaches can effectively denoise and deblur images by decomposing them into different frequency components. However, these methods may struggle with the multi-scale nature of astronomical data, requiring additional techniques to enhance performance of the short time series [17]. Matched filtration methods [18], which utilize pre-defined filter shapes to enhance signal detection, can be useful but depend on precise knowledge of the blurring characteristics, limiting their flexibility in varying conditions. In the papers focusing on computer and machine vision [19], researchers developed foundational algorithms but lacked specific adaptations for astronomical image processing. The general algorithms discussed often fall short when dealing with the high noise levels and specific distortions found in astronomical images. This highlights the need for specialized techniques to handle unique challenges, such as cosmic ray hits and varying illumination. Further studies suggest using the different image processing algorithms [20] including Sobel filter [21] for astronomical image recognition, which is effective in edge detection but struggles with the high levels of noise and blur typical in astronomical images. The Sobel filter [22], designed for general edge detection, fails to adequately enhance the fine details necessary for accurate astronomical analysis, potentially leading to misidentifications of celestial objects. Moreover, image recognition [23] indicates that processing speed decreases significantly as the size of the image frames increases, thereby limiting their applicability for high-speed processing tasks required in astronomical observations.

In a paper [24] suggested approach has the requirement for a stable and controlled environment for accurate measurements. This dependency may limit the practical application of the approach in more variable or field conditions, where maintaining such controlled conditions is challenging. Additionally, the approach relies on selecting and observing multiple markers in different positions, which introduces the risk of incorrect marker selection or observation errors. If the markers are not placed or observed correctly, it can lead to significant inaccuracies in the reference point determination, further complicating the process and reducing the reliability of the results.

3. Data mining of the Solar System objects

The proposed astronomical objects data mining pipeline is designed to address the challenges posed by blurred CCD frames in astronomical imaging and

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

astronomical big data analysis [25]. The following sections provide a detailed description of each component of the designed pipeline and its role in restoring high-quality astronomical images including photometry [26].

Implemented pipeline have been integrated inside the fully functional information system with the web-based interface which allows to automate the astronomical objects data mining process. The given pipeline integrates the median filter [27] and the Lucy-Richardson algorithm [28] in order to enhance the quality of astronomical images affected by blurring. This integration leverages the strengths of both techniques to effectively reduce noise and recover fine details, ultimately improving the accuracy of data mining processes for single astronomical objects considering the different typical forms [29].

The whole pipeline is shown in Fig. 2:

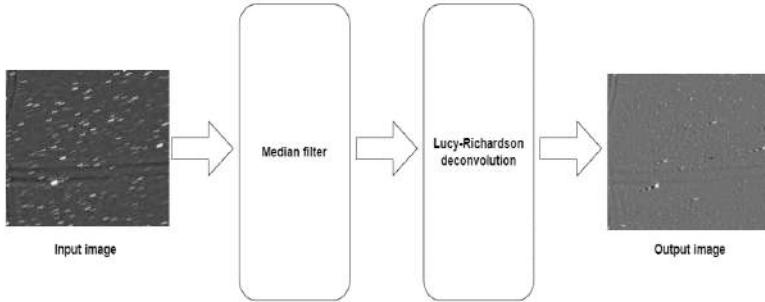


Figure 2. Astronomical objects data mining pipeline

The initial phase of our data mining [30] pipeline entails the application of a median filter [31], a sophisticated non-linear digital filtering technique renowned for its efficacy in noise reduction. The median filter operates by traversing the image pixel by pixel, substituting each pixel value with the median value derived from the surrounding neighborhood of pixels. This method is particularly adept at mitigating impulsive noise, such as salt-and-pepper noise, while preserving the integrity of edges and fine details, making it an indispensable tool for pre-processing astronomical images prior to deblurring.

The median filtering can be described using the following formula:

$$A_{out}(m, n) = A_{in}(m, n) - A_{med}(m, n), \quad (1)$$

where $A_{out}(m, n)$ – represents the output pixel value at coordinates (m, n) after applying the median filter;

$A_{in}(m, n)$ – denotes the input pixel value at coordinates (m, n) in the original image;

$A_{med}(m, n)$ – is the median value of the pixel values within the neighborhood centered around (m, n) .

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

The resulting image with equalized background brightness may have pixels with a negative value, so an additional correction should be performed and the minimum value between all pixels should be subtracted from each pixel:

$$A_{out}(m, n) = A_{in}(m, n) - A_{min} \quad (2)$$

where $A_{out}(m, n)$ – represents the output pixel value at coordinates (m, n) after applying the correction;

$A_{in}(m, n)$ – denotes the input pixel value at coordinates (m, n) in the original image;

A_{min} – the minimal value of the pixel in the image.

The median filter is uniquely advantageous in its ability to preserve edge sharpness, which is crucial in astronomical imaging where the accurate delineation of celestial bodies is paramount. Traditional linear filters, like the mean filter, tend to blur edges along with noise reduction, leading to a loss of critical information.

In the context of our pipeline, the use of the median filter is a critical pre-processing step. Astronomical images often suffer from various types of noise introduced during the capture process by CCD cameras, atmospheric conditions, or electronic interference. By applying the median filter, we can significantly enhance the quality of the raw images, thereby facilitating more accurate subsequent deblurring using the Lucy-Richardson algorithm. Furthermore, the median filter's robustness against noise and its edge-preserving properties makes it highly suitable for astronomical applications, where precision and clarity are essential.

After noise reduction via the median filter, the deblurring process is executed using the Lucy-Richardson algorithm [32]. This algorithm is specifically tailored to recover a latent image that has been subjected to blurring by a known PSF.

The PSF characterizes the response of the imaging system to a point source or a point object, encapsulating the spread of the point source's light due to factors such as atmospheric turbulence, motion, or lens aberrations.

The observed image can be decomposed as a sum of individual points and represented through a transition matrix:

$$d_i = \sum_j p_{i,j} u_j \quad (3)$$

where d_i – is the intensity of the pixel in the output image;

$p_{i,j}$ – is the element of the transition matrix representing the shift between the initial pixel j and the output pixel i;

u_j – is the intensity of the pixel j in the input image.

The transition matrix can be expressed as the shift between the initial and output pixels using the following equation:

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

$$p_{i,j} = P(i - j), \quad (4)$$

where $P(i - j)$ – is the point spread function;

$p_{i,j}$ – is the element i, j in the transition matrix p .

The iterative nature of the Lucy-Richardson algorithm allows for progressive refinement of the image, with each iteration enhancing the clarity and detail by correcting for the blurring effects encoded in the PSF. It operates by maximizing the likelihood that the observed blurred image could be obtained from the deblurred image when convolved with the PSF. The Lucy-Richardson method on each iteration can be described using following equation:

$$A_{deb}^{t+1} = A_{deb}^t \left(h'_{PSF} \otimes \frac{A_{out}}{h_{PSF} \otimes A_{deb}^t} \right), \quad (5)$$

where A_{deb}^{t+1} – is an updated image on the current iteration;

A_{deb}^t – is an input image on the current iteration;

h_{PSF} – is the point spread function;

h'_{PSF} – is the flipped point spread function;

A_{out} – is the initially blurred image;

\otimes – is the convolution operation.

One of the key strengths of the Lucy-Richardson algorithm is its efficacy in restoring images degraded by various forms of blur, including motion blur, out-of-focus blur, and atmospheric distortion. Its robustness is further underscored by its ability to produce high-quality deblurred images even when the PSF is not perfectly known, leveraging iterative refinements to converge towards an accurate representation of the latent image.

Overall, the combination of the median filter for noise reduction and the Lucy-Richardson algorithm for deblurring forms a powerful pipeline for enhancing the quality of astronomical images. This pipeline is particularly advantageous in the context of processing blurred CCD frames, where high precision and clarity are paramount for accurate data mining and analysis of single astronomical objects.

The system architecture for the astronomical objects data mining pipeline is constructed using a combination of modern technologies and frameworks to ensure high performance, scalability, and ease of deployment. The architecture is built upon Python, Redis, FastAPI, React, PostgreSQL, Docker, Docker-Compose, and Caddy, each playing a critical role in the functionality and efficiency of the pipeline. The suggested architecture is provided in the Fig. 3. Python [33] serves as the orchestrator for the data mining pipeline, overseeing the coordination and execution of tasks. However, the computationally intensive parts of the pipeline, including the implementation of the median filter and the Lucy-Richardson algorithm, are developed as precompiled binary files to maximize performance and efficiency.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

Redis is utilized as a task queue [34], effectively managing the distribution and scheduling of tasks within the system. This ensures that the processing of data is both streamlined and efficient, reducing latency and optimizing resource usage.

FastAPI functions as the backend framework, providing a high-performance, scalable API for handling client requests and managing the data mining pipeline. The asynchronous capabilities of FastAPI significantly enhance performance by enabling the concurrent handling of multiple requests. Additionally, FastAPI auto-generates interactive API documentation using Swagger UI, facilitating ease of use and integration. React is employed to develop the web-based interface of the information system. This interface allows users to interact with the pipeline, upload images, and visualize the processed results. React's component-based architecture ensures a modular and maintainable codebase, while libraries such as Redux efficiently manage application state, enhancing the user experience.

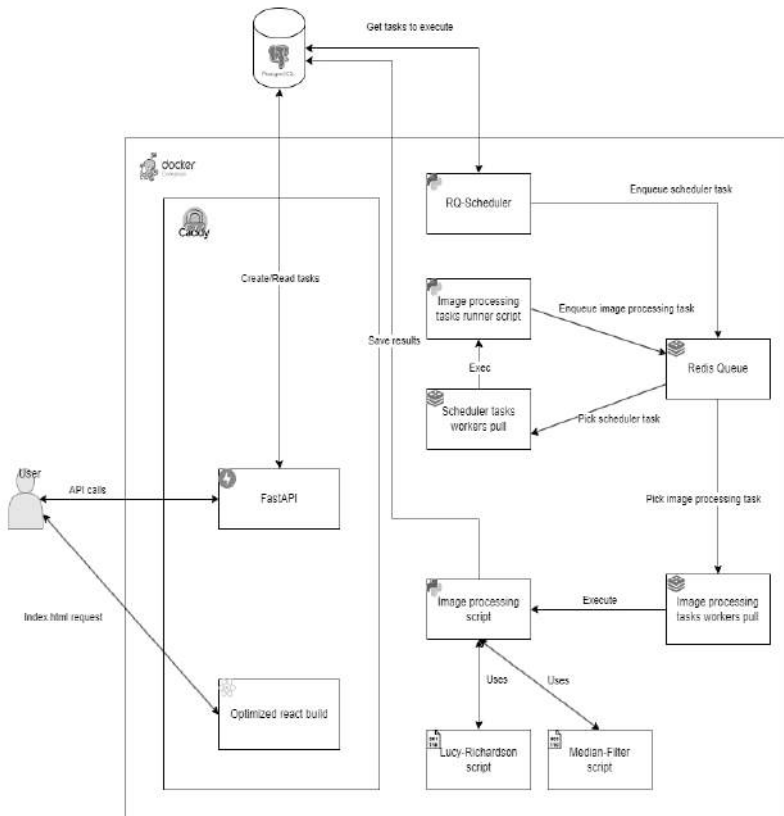


Figure 3. Implemented system architecture

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

PostgreSQL is used as the primary database for storing and managing the metadata associated with the images and processed results. PostgreSQL's robustness [35], support for complex queries, and ACID compliance make it an ideal choice for handling the relational data required by the system. Caddy is utilized as the web server and reverse proxy, offering several advantages, including automatic HTTPS for secure communication with automated TLS certificate management, and simplified setup and configuration compared to traditional web servers.

For deployment, Docker-Compose [36] is employed to set up a local development environment, ensuring that all services run seamlessly together. In production, the application is deployed on a cloud platform using Docker containers, with Caddy managing secure HTTP traffic and load balancing.

In summary, the described system architecture leverages a sophisticated list of technologies to construct an efficient and scalable data mining pipeline for astronomical images. By integrating Python for task orchestration, precompiled binaries for computationally intensive processing, Redis as a task queue, FastAPI for backend services, React for the frontend interface, and Docker with Caddy for deployment, the pipeline achieves high performance and user-friendliness.

This architecture not only enhances the quality of astronomical images but also ensures that the entire process, from data ingestion to result retrieval, is seamless and efficient. The data flow within the system initiates with users uploading blurred CCD images through the React-based web interface as a task (see Fig. 4).

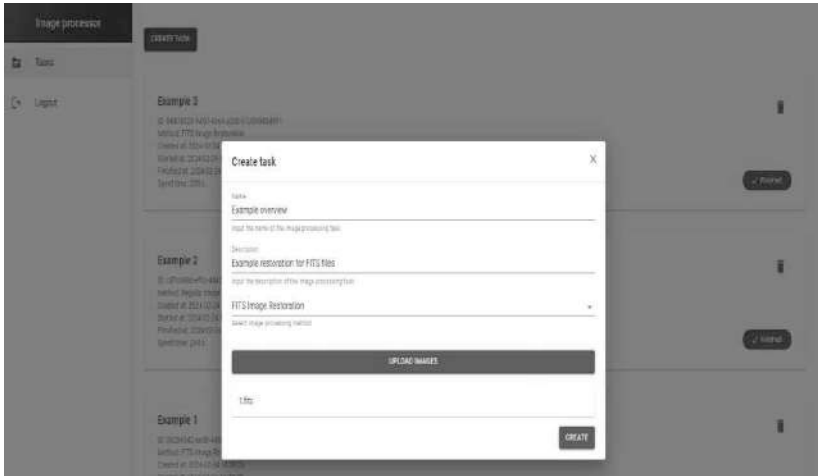


Figure 4. Blurred CCD images uploading

These uploaded images are transmitted to the FastAPI backend, where they are stored in the local filesystem on the server side and enqueued for the future processing using the pipeline.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

Once the processing task is selected to be executed, it's reflected on the user interface (UI) by updating the processing task status to «In progress» as it's shown in the Fig. 5.



Figure 5. Image processing task status update

Once the pipeline is executed the processing results are reflected in the UI as it's shown in the Fig. 6 **Error! Reference source not found.**

We can see the processing task information, which is extended with the details about the data processing time (time of the task created in the UTC format, time of the task started in the UTC format, time of the task finished in the UTC format and total processing time in seconds).

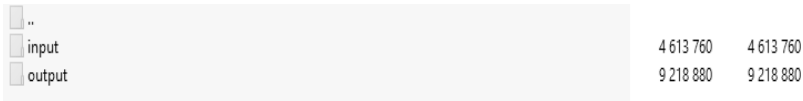


Figure 6. Complete task representation in the UI

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

Finally, the end user can download the processing results by pressing the download button shown in the Fig. 6.

The structure of the downloaded archive is shown in the Fig. 7.



..		
input	4 613 760	4 613 760
output	9 218 880	9 218 880

Figure 7. Structure of the downloaded archive

The downloaded archive contains input folder with the initial raw blurred images and the output folder with the processed images after deblurring process.

4. Results

The created processing pipeline for the automated data mining of the single astronomical objects from the blurred CCD-frames works in combination with the especially developed mathematical module for the intraframe processing of the Lemur software in scope of the Collection Light Technology (CoLiTec) project (<https://colitec.space>) [37].

The main specific functional features of the Lemur software are:

- processing images with the very wide FOV (<10 degrees²);
- automated frame calibration [11];
- cosmetic frame correction;
- track-and-stack feature;
- brightness equalization [26];
- background alignment;
- astronomical image filtering [38];
- determining the contours of objects [39];
- image recognition [21];
- typical shape formation [29];
- detection of the moving objects (with near-zero, normal, fast apparent motion) [40];
- fully automated robust method of the astrometric reduction;
- fully automated robust method of the photometric reduction [41];
- support of the multi-threaded processing;
- On-Line Data Analysis System (OLDAS) for managing the processing pipeline at the different stages of processing;
- transferring of astronomical data with intermediate storage;

More extended details about the Lemur software and the CoLiTec project are presented in these papers [42, 43] and research [44].

The high-level processing pipeline of the Lemur software with the developed appropriate modules with implemented of the different mathematical methods and algorithms is presented in the Fig. 8.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

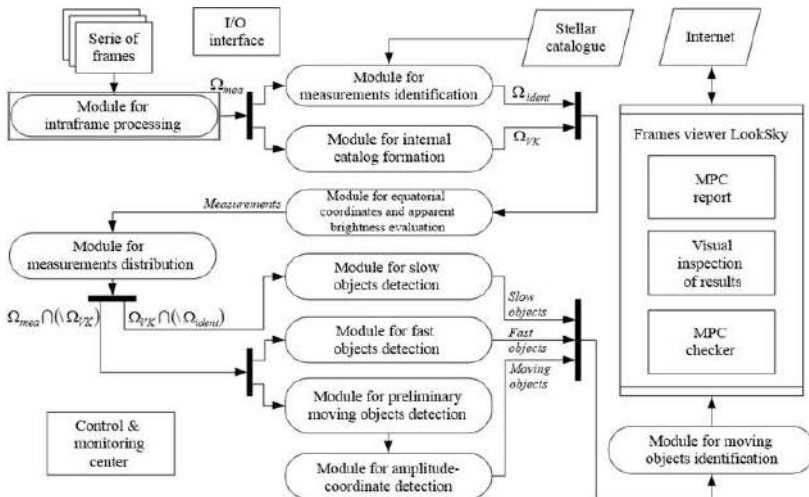


Figure 8. The high-level processing pipeline of the Lemur software

The Lemur software in scope of the CoLiTec project was installed at the different telescopes at the various observatories in Ukraine and around the world:

- OMT-800 and AZT-3 telescopes installed at the Odesa-Mayaky observatory [45];
- SANTEL-400AN telescope installed at the ISON-NM observatory;
- ISON-Uzhgorod [46];
- VNT and Celestron C11 telescopes installed at the Vihorlat Observatory [26];
- PROMPT-8 telescope installed at Cerro Tololo observatory [47];
- NARIT (National Astronomical Research Institute of Thailand) [48];
- AZT8 and Takahashi BRC-250M telescopes.

All listed above telescopes installed at the observatories have the official identifiers received from the Minor Planet Center (MPC) (<https://minorplanetcenter.net>) – MPC code from the International Astronomical Union (IAU) (<https://iau.org>).

Especially developed mathematical module in the Lemur software for the intraframe processing, which is responsible for data mining of the single astronomical objects from the blurred CCD-frames contains the following mathematical methods and algorithms: high-frequency filtration method for the noise reduction [38]; inverse median filtration method for the background alignment [41]; Lucy-Richardson algorithm for deblurring [10]. The Fig. 9 illustrates the effectiveness of the proposed data mining pipeline in the context of astronomical image processing. On the left side of the image, we see an example of a blurred astronomical image, where stars appear as elongated streaks due to motion blur or

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

atmospheric disturbances during the capture. This blurring effect can obscure important details and hinder the analysis of celestial objects. On the right side of the image, the same scene has been processed using the implemented pipeline.

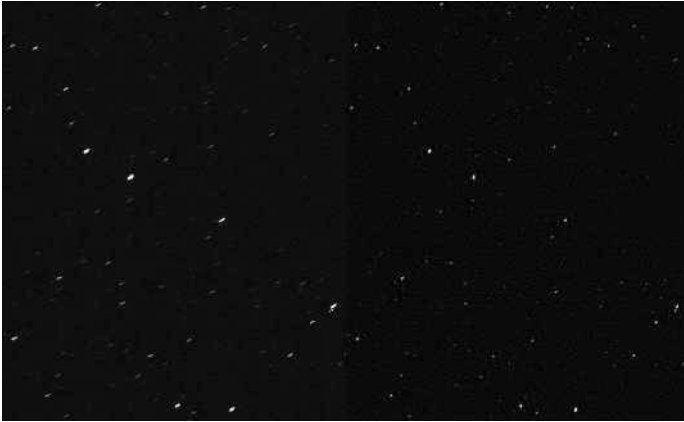


Figure 9. Example of the input and output frames

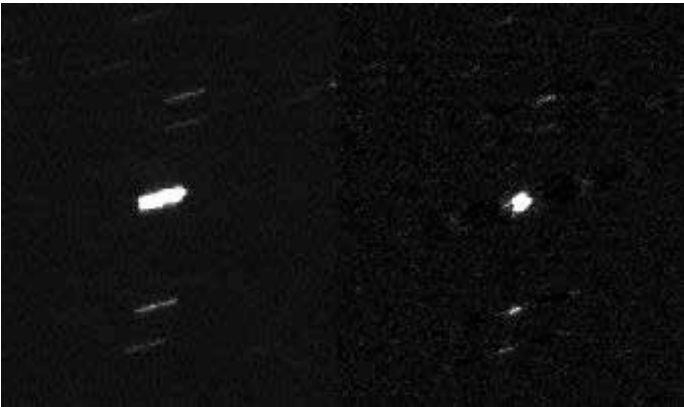


Figure 10. Closer view of the input and output frames

The result is a significantly clearer image where the stars are now sharp points of light, revealing more detailed and accurate representations of the astronomical scene including reference stars [42].

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

On the closer view of the provided raw blurred and processed frames this difference is even more observable (see Fig. 10Error! Reference source not found.).

5. Conclusions

This paper presents a sophisticated data mining pipeline designed for the automated restoration and analysis of the single astronomical objects from the blurred CCD frames. The research was conducted in scope of the CoLiTec (Collection Light Technology) project.

The pipeline incorporates advanced methodologies, specifically the median filter and the Lucy-Richardson algorithm, to effectively mitigate noise and deblur images, thereby enhancing the quality of astronomical observations, which is very important for the photometry tasks.

The median filter is crucial for noise reduction, particularly in mitigating impulsive noise while preserving essential image details and edges. This pre-processing step is fundamental in preparing images for subsequent deblurring.

The Lucy-Richardson algorithm then iteratively refines the deblurred images by compensating for the blurring effects characterized by the PSF.

This combination ensures that the images are not only clearer but also retain critical astronomical details necessary for accurate data analysis. Our pipeline is embedded within a robust information system designed for high performance and scalability, leveraging contemporary technologies such as Python, Redis, FastAPI, React, Docker, and Caddy. This architectural design ensures the system's ability to handle large volumes of data efficiently, addressing the common requirements in astronomical research.

The effectiveness of the implemented pipeline is demonstrated through significant improvements in image clarity, as illustrated in our results section.

The developed pipeline can be also used for the different automated monitoring and visualization systems [49] to track the astronomical objects in real-time.

In conclusion, the developed pipeline offers a powerful solution to the challenges posed by blurred astronomical images. By integrating efficient noise reduction and deblurring techniques within a scalable system architecture and data stream clustering [50], this work significantly advances the capabilities of automated data mining [51] in astronomy.

Also, the results of our implementation with a higher quality will be useful in application of the machine learning methods [52].

The results underscore the potential of this approach to improve the accuracy and reliability of astronomical observations, thereby supporting more detailed and precise astronomical research of the Solar System objects and even of the high-speed aircraft and low-altitude mobile robots.

6. Acknowledgements

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

The research was supported by the Ukrainian project of fundamental scientific research “Development of computational methods for detecting objects with near-zero and locally constant motion by optical-electronic devices” #0124U000259 during 2024-2026 years.

7. References

- [1] J. Bennett, S. Shostak, N. Schneider, and M. MacGregor, *Life in the Universe*. Princeton University Press, 2022.
- [2] V. Troianskyi, V. Kashuba, O. Bazyey, et al., First reported observation of asteroids 2017 AB8, 2017 QX33, and 2017 RV12, *Contributions of the Astronomical Observatory Skalnaté Pleso*, vol. 53, pp. 5-15, 2023. doi: 10.31577/caosp.2023.53.2.5.
- [3] F. Chierchie, et al., Detailed modeling of the video signal and optimal readout of charge- coupled devices, *International Journal of Circuit Theory and Applications*, vol. 48, issue 7, pp. 1001-1016, 2020. doi: 10.1002/cta.2784.
- [4] D. Oszkiewicz, et al., Spins and shapes of basaltic asteroids and the missing mantle problem, *Icarus*, vol. 397, 115520, 2023. doi: 10.1016/j.icarus.2023.115520.
- [5] Y. Luxin, J. Mingzhi, F. Houzhang, et al., Atmospheric-Turbulence-Degraded Astronomical Image Restoration by Minimizing Second-Order Central Moment. *IEEE Geoscience and Remote Sensing Letters*, in: *IEEE GEOSCI REMOTE SENS LETT*. 2012, pp. 672-676. doi: 10.1109/LGRS.2011.2178016.
- [6] V. Troianskyi, V. Godunova, A. Serebryanskiy, G. Aimanova, L. Franco, A. Marchini, P. Bacci, et al., Optical observations of the potentially hazardous asteroid (4660) Nereus at opposition 2021, *Icarus*, vol. 420, 116146, 2024. doi: 10.1016/j.icarus.2024.116146.
- [7] V. Savanevych, et al., Mathematical methods for an accurate navigation of the robotic telescopes, *Mathematics*, vol. 11, issue 10, 2246, 2023. doi: 10.3390/math11102246.
- [8] D. Oszkiewicz, et al., Spin rates of V-type asteroids, *Astronomy and Astrophysics*, vol. 643, A117, 2020. doi: 10.1051/0004-6361/202038062.
- [9] S. Cavuoti, M. Brescia, and G. Longo, Data mining and knowledge discovery resources for astronomy in the Web 2.0 age, *SPIE Astronomical Telescopes and Instrumentation, Software and Cyberinfrastructure for Astronomy II*, vol. 8451, 2012. doi: 10.1117/12.925321.
- [10] S. Khetkeeree, Optimization of Lucy-Richardson Algorithm Using Modified Tikhonov Regularization for Image Deblurring, *J. Phys.: Conf. Ser.*, vol. 1438, 012014, 2020, doi: 10.1088/1742-6596/1438/1/012014.
- [11] V. Akhmetov, et al., Astrometric reduction of the wide-field images, *Advances in Intelligent Systems and Computing*, vol. 1080, pp. 896–909, 2020. doi: 10.1007/978-3-030-33695-0_58.
- [12] R. Mor, et al., Expanding Big Data mining for Astronomy, XIV Scientific Meeting of the Spanish Astronomical Society, p. 235, 2020. doi: 2020sea..confE.235M.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

- [13] Y. Bodyanskiy, S. Popov, F. Brodetskiy, and O. Chala, Adaptive Least-Squares Support Vector Machine and its Combined Learning-Selflearning in Image Recognition Task, International Scientific and Technical Conference on Computer Sciences and Information Technologies, pp. 48–51, 2022. doi: 10.1109/CSIT56902.2022.10000518.
- [14] Peng, L. Xiyu, L. Zhengyang, et al., Point spread function modelling for wide-field small-aperture telescopes with a denoising autoencoder, MNRAS, vol. 493, pp. 651-660, 2020. doi: 10.1093/mnras/staa319.
- [15] M. Dadkhah, et al., Methodology of wavelet analysis in research of dynamics of phishing attacks. International Journal of Advanced Intelligence Paradigms, vol. 12, issue 3-4, pp. 220-238, 2019. doi: 10.1504/IJAIP.2019.098561.
- [16] S. Khlamov, et al., Development of computational method for matched filtration with analytic profile of the blurred digital image, Eastern-European Journal of Enterprise Technologies, vol. 5, issue 4-119, pp. 24–32, 2022. doi: 10.15587/1729-4061.2022.265309.
- [17] L. Kirichenko, A.S.A. Alghawli, T. Radivilova, Generalized approach to analysis of multifractal properties from short time series, International Journal of Advanced Computer Science and Applications, vol. 11, issue 5, pp. 183–198, 2020. doi: 10.14569/IJACSA.2020.0110527.
- [18] R. Klette, Concise computer vision. An Introduction into Theory and Algorithms. Springer, 2014.
- [19] S. Khlamov, V. Savanevych, V. Vlasenko, et al., Development of the matched filtration of a blurred digital image using its typical form, Eastern-European Journal of Enterprise Technologies, vol. 1 (9-121), pp. 62–71, 2023. doi: 10.15587/1729-4061.2023. 273674.
- [20] R. Gonzalez, and R. Woods, Digital image processing, Fourth edition, NY: Pearson, 2018.
- [21] S. Khlamov, I. Tabakova, T. Trunova, Recognition of the astronomical images using the Sobel filter, Proceedings of the 29th IEEE IWSSIP 2022, Sofia, Bulgaria, June 1st – 3rd, 4 p., 2022. doi: 10.1109/IWSSIP55020.2022.9854425.
- [22] K. S. Chethan, G. S. Sinchana, K. R. Nataraj, and A. L. Choodarathnakara, Analysis of image quality using sobel filter, Third International Conference on Inventive Systems and Control (ICISC), pp. 526-531, 2019. doi: 10.1109/ICISC44355.2019.9036369.
- [23] S. Khlamov, V. Savanevych, I. Tabakova, T. Trunova, The astronomical object recognition and its near-zero motion detection in series of images by in situ modeling, Proceedings of the 29th IEEE IWSSIP 2022. doi: 10.1109/IWSSIP55020.2022.9854475.
- [24] M. Lösler, C. Eschelbach, and S. Riepl, A modified approach for automated reference point determination of SLR and VLBI telescopes: First investigations at Satellite Observing System Wettzell, Technisches Messen, vol. 85, pp. 616–626, 2018. doi: 10.1515/teme-2018-0053.
- [25] M. Faaique, Overview of Big Data Analytics in Modern Astronomy, Int. Journal of Mathematics, Statistics, and Computer Science, vol. 2, pp. 96–113, 2023. doi: 10.59543/ijmscs.v2i.8561.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

- [26] I. Kudzej, et al., CoLiTecVS – A new tool for the automated reduction of photometric observations, *Astronomische Nachrichten*, vol. 340, pp. 68–70, 2019. doi: 10.1002/asna.201913562.
- [27] L. Yin, R. Yang, M. Gabbouj and Y. Neuvo, Weighted median filters: a tutorial, *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, vol. 43, no. 3, pp. 157-192, 1996, doi: 10.1109/82.486465.
- [28] R. F. H. Torres, and R. Garcia, Image Restoration for Blurred License Plates Extracted from Traffic Video Surveillance using Lucy Richardson Algorithm, *IEEE 14th HNICEM*, pp. 1-6, 2022. doi: 10.1109/HNICEM57413.2022.10109437.
- [29] V. Savanevych, et al., Formation of a typical form of an object image in a series of digital frames, *Eastern-European Journal of Enterprise Technologies*, vol. 6, issue 2-120, pp. 51–59, 2022. doi: 10.15587/1729-4061.2022.266988.
- [30] Ž. Ivezić, et al., *Statistics, Data Mining, and Machine Learning in Astronomy: A Practical Python Guide for the Analysis of Survey Data*, Princeton University Press, 2019.
- [31] H. Hwang, and R. Haddad, Adaptive median filters: new algorithms and results, *IEEE Transactions on Image Processing*, vol. 4 (4), pp. 499-502, 1995. doi: 10.1109/83.370679.
- [32] Z. He, et al., A Deconvolutional Reconstruction Method Based on Lucy–Richardson Algorithm for Joint Scanning Laser Thermography, *IEEE Transactions on Instrumentation and Measurement*, vol. 70, pp. 1-8, 2021, doi: 10.1109/TIM.2020.3034967.
- [33] Python 3.12.2 documentation. Available at: <https://docs.python.org/3>.
- [34] Python RQ documentation. Available at: <https://python-rq.org/docs>.
- [35] H. Schönig, *Mastering PostgreSQL 15: Advanced techniques to build and manage scalable, reliable, and fault-tolerant database applications*, Packt Publishing Ltd, 2023.
- [36] M. H. Ibrahim, M. Sayagh, and A. E. Hassan, A study of how Docker Compose is used to compose multi-component systems, *Empirical Software Engineering*, vol. 26, 128, 2021. doi: 10.1007/s10664-021-10025-1.
- [37] S. Khlamov, et al., Big astronomical datasets and discovery of new celestial bodies in the Solar System in automated mode by the CoLiTec software, *Knowledge Discovery in Big Data from Astronomy and Earth Observation, Astrogeoinformatics*, pp. 331–345, 2020. doi: 10.1016/B978-0-12-819154-5.00030-8.
- [38] V. Vlasenko, et al., Devising a procedure for the brightness alignment of astronomical frames background by a high frequency filtration to improve accuracy of the brightness estimation of objects, *Eastern-European Journal of Enterprise Technologies*, vol. 2, issue 2-128, pp. 31–38, 2024. doi: 10.15587/1729-4061.2024.301327.
- [39] H. Khudov, I. Ruban, O. Makoveichuk, H. Pevtsov, V. Khudov, I. Khizhnyak, S. Fryz, V. Podlipaiev, Y. Polonskyi, R. Khudov, Development of methods for determining the contours of objects for a complex structured color image based on the ant colony optimization algorithm, *EUREKA, Physics and Engineering*, vol. 2020, issue 1, pp. 34–47, 2020. doi: 10.21303/2461-4262.2020.001108.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

- [40] V. Savanevych, et al., A method of immediate detection of objects with a near-zero apparent motion in series of CCD-frames. *Astronomy & Astrophysics*, 609, A54: 11, 2018. doi: 10.1051/0004-6361/201630323.
- [41] Š. Parimucha, et al., CoLiTecVS – A new tool for an automated reduction of photometric observations, *Contributions of the Astronomical Observatory Skalnaté Pleso*, vol. 49, issue 2, pp. 151-153, 2019. doi:2019CoSka..49..151P.
- [42] V. Savanevych, et al., Selection of the reference stars for astrometric reduction of CCD-frames, *Advances in Intelligent Systems and Computing*, vol. 1080, pp. 881–895, 2020. doi: 10.1007/978-3-030-33695-0_57.
- [43] S. Khlamov, et al., Machine Vision for Astronomical Images using The Modern Image Processing Algorithms Implemented in the CoLiTec Software, *Measurements and Instrumentation for Machine Vision*, pp. 269–310, 2024. doi: 10.1201/9781003343783-12.
- [44] V. Savanevych, et al., Comparative analysis of the positional accuracy of CCD measurements of small bodies in the solar system software CoLiTec and Astrometrica, *Kinematics and Physics of Celestial Bodies*, vol. 31, issue 6, pp. 302–313, 2015. doi: 10.3103/S0884591315060045.
- [45] V. Troianskyi, P. Kankiewicz, and D. Oszkiewicz, Dynamical evolution of basaltic asteroids outside the Vesta family in the inner main belt, *Astronomy and Astrophysics*, vol. 672, A97, 2023. doi: 10.1051/0004-6361/202245678.
- [46] V. Kudak, V. Epishev, V. Perig, and I. Neybauer, Determining the orientation and spin period of TOPEX/Poseidon satellite by a photometric method, *Astrophysical Bulletin*, vol. 72, issue 3, pp. 340-348, 2017. doi: 10.1134/S1990341317030233.
- [47] T. Li, D. DePoy, J. Marshall, et al., Monitoring the atmospheric throughput at Cerro Tololo Inter-American Observatory with aTmCam, *Ground-based and Airborne Instrumentation for Astronomy V*, vol. 9147, pp. 2194–2205, 2014.
- [48] S. Rattanasoon, E. Semenko, D. Mkrtychian, and S. Poshyachinda, Spectroscopic Devices for Asteroseismology With Small Telescopes in NARIT, *arXiv -> astro-ph*, vol. 2307.03985, 5 p., 2023. doi: 10.48550/arXiv.2307.03985.
- [49] V. Lyashenko, A. T. Abu-Jassar, V. Yevsieiev, and S. Maksymova, Automated Monitoring and Visualization System in Production, *Int. Res. J. Multidiscip. Technovation*, vol. 5(6), pp. 09-18, 2023. doi: 10.54392/irjmt2362.
- [50] Zhernova, P. Data stream clustering in conditions of an unknown amount of classes [Text] / P. Zhernova, A. Deyneko, Zh. Deineko, I. Pliss, V. Ahafonov // *Advances in Intelligent Systems and Computing*. – 2019. – Vol. 754. – P. 410–418. doi: 10.1007/978-3-319-91008-6_41.
- [51] I. Perova, Y. Brazhnykova, N. Miroshnychenko, and Y. Bodyanskiy, Information Technology for Medical Data Stream Mining, *15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering*, pp. 93–97, 2020. doi: 10.1109/TCSET49122.2020.235399.
- [52] L. Kirichenko, O. Pichugina, T. Radivilova, and K. Pavlenko, Application of Wavelet Transform for Machine Learning Classification of Time Series, *Lecture Notes on Data Engineering and Communications Technologies*, vol. 149, pp. 547 – 563, 2023. doi: 10.1007/978-3-031-16203-9_31.

**АВТОМАТИЗОВАНИЙ МАЙНІНГ ДАНИХ ОДИНОЧНИХ
АСТРОНОМІЧНИХ ОБ'ЄКТІВ З РОЗМИТИХ ПЗЗ-КАДРІВ**

Ph.D. С. Хламов ORCID: 0000-0001-9434-1081

Харківський національний університет радіоелектроніки, Україна

E-mail: sergii.khlamov@gmail.com

Dr.Sci. В. Саваневич ORCID: 0000-0001-8840-8278

Харківський національний університет радіоелектроніки, Україна

E-mail: vadym.savanevych1@nure.u

Ph.D. В. Власенко ORCID: 0000-0001-8639-4415

Національний центр управління і випробувань космічної техніки, Україна,

E-mail: vlasenko.vp@gmail.com

Е. Гаджисв ORCID: 0009-0003-6752-7827

Харківський національний університет радіоелектроніки, Україна

E-mail: emil.hadzhiev@nure.ua

Анотація. Глава присвячена складному конвеєру інтелектуального аналізу даних, який був розроблений для відновлення високоякісних зображень із розмитих кадрів, створених камерами із зарядним зв'язком (CCD). Розроблений конвеєр інтелектуального аналізу даних використовує сучасні інформаційні технології для горизонтальної та вертикальної масштабованості. Основна методологія об'єднує наступні математичні методи та алгоритми: метод зворотної медіанної фільтрації для зменшення шуму та алгоритм Люсі-Річардсона для зменшення розмиття. Зворотна медіанна фільтрація ефективно зменшує імпульсивний шум, зберігаючи краї, а алгоритм Люсі-Річардсона ітеративно покращує зображення, коригуючи ефекти розмиття, закодовані у функції розповсюдження точки (PSF). Запропонована системна архітектура конвеєра обробки для автоматизованого аналізу даних окремих астрономічних об'єктів із розмитих кадрів CCD використовує такі сучасні технології: мова програмування Python, Redis, FastAPI, React, Docker і Caddy для забезпечення високої продуктивності, масштабованості та простоти розгортання. Такий комплексний підхід значно підвищує точність астрономічних спостережень, полегшуючи точніші дослідження небесних об'єктів. Запропонований конвеєр вирішує унікальні проблеми обробки астрономічних зображень, пропонуючи надійне рішення для автоматизованого аналізу даних окремих астрономічних об'єктів. Поєднання ефективних методів шумозаглушення та видалення розмиття, а також масштабована та високопродуктивна архітектура системи забезпечують комплексне вирішення проблем, що виникають під час обробки астрономічних зображень.

Ключові слова: інтелектуальний аналіз даних, автоматизований конвеєр, масштабованість, ПЗЗ-кадр, астрономічне зображення, розмите зображення, обробка зображень, аналіз зображень, виявлення об'єктів, функція розподілу точок, алгоритм Люсі-Річардсона, шумозаглушення, зворотний медіанний фільтр, деконволюція, Python, Docker, FastAPI

UDC 004.75

**DISTRIBUTED MICROSERVICES-ORIENTED INFORMATION
SYSTEM FOR ASTRONOMICAL DATA PROCESSING USING
OPENAPI SPECIFICATION**

Ph.D. S. Khlamov ORCID: 0000-0001-9434-1081

Kharkiv National University of Radio Electronics, Ukraine

E-mail: sergii.khlamov@gmail.com

S. Orlov ORCID: 0009-0008-0680-206X

National Aerospace University – Kharkiv Aviation Institute, Ukraine,

E-mail: s.v.orlov@student.khai.edu

T. Trunova ORCID: 0000-0003-2689-2679

Kharkiv National University of Radio Electronics, Ukraine

E-mail: tetiana.trunova@nure.ua

Y. Bondar ORCID: 0009-0001-5309-0084

Kharkiv National University of Radio Electronics, Ukraine

E-mail: bndr@gmail.com

Y. Netrebin ORCID: 0009-0001-8778-3241

INTIVE Limited, O'Connell Bridge House, Ireland,

E-mail: yuriy.n.netrebin@gmail.com

Abstract. *The chapter is devoted to the usage of OpenAPI specification in distributed microservices-oriented information system for astronomical data processing. A common goal of all scientific and technological algorithms and methods is to automate as much as available processes without any human actions. In general cases it can be done by the different astronomical distributed microservices-oriented information system. In these pipelines the various data mining and knowledge discovery in databases (KDD) tasks are used for speeding up and optimizing the astronomical data processing. Suggested using of the OpenAPI specification in a distributed microservices-oriented information system for astronomical data processing significantly improves the system's interoperability, scalability, and maintainability. The developed skeleton of the real example of astronomical data-processing system is implemented using .Net Core framework and C# programming language. Implementing Swagger in a microservices architecture presents numerous benefits, significantly enhancing both the development and maintenance phases of service-oriented applications. The developed skeleton and the proposed approach will be useful for the different microservices-oriented information system for astronomical data processing. It can be used for all kind of processing astronomical images using the different mathematical methods and algorithms implemented as a tool, module, or service. Another one good example of application the proposed skeleton is a realization of the Virtual Observatory (VO) concept or integration with CI/CD tools.*

Keywords: *Information system, client-server architecture, microservices-oriented architecture, scalability, processing pipeline, data mining, knowledge discovery in databases, astronomical observations, image processing, Solar System objects, Swagger, OpenAPI, REST API, JSON, .NET, C#, RabbitMQ*

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

1. Introduction

The asteroid-comet hazard becomes a huge potential problem in the XXI century [1], which can cause the global destructions, collisions with geostationary artificial satellites [2], space debris, etc. To avoid such situation the humanity is continuously developing and improving mathematical methods [3] and algorithms for the astronomical scientific direction like an astronomical image processing and computer vision [4], which includes the background alignment [5], brightness equalization [6], astrometric reduction [7], photometric reduction [8], detection of moving objects in series of frames, or even discovery of the Solar System objects (SSOs) [9], like comets, asteroids [10], small planets, galaxies, stars, etc.

All astronomical scientific observations are created by the charge-coupled device (CCD) [11] that are used as a main equipment in telescopes or any other optical system at the observatories. Such astronomical scientific observations are collected during the specified observational period of the investigated small celestial SSOs [12], as well as the artificial satellites. After performing the series of observations of the investigated SSOs it is required to analyze the results of observation, which can include the period and shape of rotations determining of such investigated SSOs. It means that there are a lot of astronomical big data and to process it we need to apply the different approaches of the information technologies.

The astronomical scientific information is also can be collected from the different historical clusters, archives, Virtual Observatories [13], data clouds, astronomical astrometric and photometric catalogues [14], different servers and other storages. A common goal of all scientific and technological algorithms and methods is to automate as much as available processes without any human actions. In general cases it can be done by the different astronomical scientific information systems. In these information systems the various data mining [15] and knowledge discovery in databases (KDD) [16] tasks are used for speeding up and optimizing the astronomical data processing. In case if the astronomical scientific information system is a very complex and consists of the different mathematical modules and libraries it becomes distributed microservices-oriented information system for astronomical data processing. Microservices, also known as the microservice architecture, is an architectural style that structures an application as a collection of loosely coupled services, each of which implement business capabilities. The microservice architecture enables the continuous delivery and deployment of large, complex information systems. It also enables an organization to evolve its technology stack, scale and be more resilient with time. Microservice architecture advocates for developing a single information system into a collection of loosely associated services. These units also enable the continuous delivery and deployment of large, monolithic information systems with minimal need for centralization.

As microservices architecture [17] continues to grow in popularity, the complexity of managing multiple, interrelated services increases. Documentation becomes essential not just for external users but also for internal developers who need to understand the APIs provided by each service. That's where Swagger comes

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

into play. Swagger, now known as the OpenAPI Specification, is a powerful tool for describing, producing, consuming, and visualizing RESTful web services.

Swagger simplifies API development and maintenance by providing a language-agnostic interface to REST APIs [18]. With Swagger, you can generate client libraries, server stubs, and API documentation that facilitates clear communication amongst your development team and beyond. It ensures that all microservices speak the same 'language' when it comes to API endpoints, parameters, and data models.

This chapter aims to the analysis of main focuses and features of the OpenAPI specification for the microservices-oriented information system development. Real examples of astronomical data-processing system are implemented using .Net Core framework and C# programming language, which is perfectly designed for the developing of distributed microservices-oriented information system.

Section 2 presents the several technologies related to our work for solving of API documentation task.

Section 3 elaborates the system architecture based on microservices architecture style, presents the integration of Swagger OpenAPI specification in real microservice implementation. Integrated data models for astronomical data-processing system are also presented in this section as well as the result of execution is illustrated in it. This section also aims to the discussions about advantages of the proposed usage of OpenAPI specification in distributed microservices-oriented information system for astronomical data processing.

Section 4 presents discussions panel with advantages and disadvantages, pros & cons of the proposed components of the distributed microservices-oriented information system for astronomical data processing and their analogues.

The chapter ends with a conclusion in section 4, which illustrates the conclusions and outlines of the future work and research as well as possibilities for future investigations and enhancements.

2. Literature review

Each SSO in a digital frame has a typical form of its image [19]. The common methods for the image processing [20] and machine vision [21] are developed for detection/recognition such images of SSOs and an estimation of their positional and motion parameters [22]. Such methods are based on the analysis of only those pixels that potentially belong to the investigated object. The disadvantages of such methods are very low accuracies when the typical form of object has a different shape [23].

The methods for assessing the aperture brightness [24] of object's images will work only with a single image of each SSO. Any methods for the matched filtration [25, 26] and high-frequency filtration [27], which are devoted to the improving the quality of corrupted images are very resource consuming. The disadvantages of the methods are the big complexity and low accuracy during the astronomical data processing, when an object's image has a several peaks of magnitude.

Methods for the Wavelet analysis [28] or even time series analysis [29] are not so effective, because we do not have a big volume of the input data to be analyzed. Also, the disadvantage of such algorithms is the corrupting of the general statistics

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

and possibility to process only clear measurements without any deviations in the typical form of image. Any methods for the deep learning and pattern recognition [30, 31] also require a big amount of astronomical data for training. The problem of such methods that astronomical image has a lot of artifacts, so there are a lot of false objects are detected in series of frames. In this case to work with resource consuming mathematical algorithms, methods, and modules, which implement them, the distributed microservices-oriented information system architecture for astronomical data processing is required. And OpenAPI specifications is a good approach for such purposes. There are several alternatives to Swagger for implementing OpenAPI specifications, each offering unique features and benefits that might be more suitable depending on your specific requirements. Here are some notable alternatives mentioned below. Postman is a versatile tool for API development and testing [32]. Postman enables automated testing, team collaboration, and integration with various CI/CD tools. It also includes features like mock servers and interactive API documentation, making it a comprehensive solution for managing the API lifecycle. Author describes microservice architecture as a scalable method for designing and implementing online applications. Due to their network-based nature, microservice applications require testing within a network environment. Automating these tests involves generating artificial network traffic, typically in the form of HTTP requests to APIs such as REST APIs. These topics are explored from the perspectives of test design and implementation, alongside key features of microservice architecture and automated testing in general. The core of this thesis details the process of designing and implementing a test automation framework for Intel Insight as well as an automatic image storage and photogrammetry processing platform built as a microservice system. The Stoplight platform excels in the areas of API design, documentation, and governance [33]. It features a user-friendly interface for creating API specifications with OpenAPI or RAML, and includes capabilities such as interactive documentation, code generation, and API governance tools. Notably, Stoplight stands out for its strengths in visual API design and its integration with development tools like GitHub and Jira. In the mentioned article author covers the problem occurring during creation and maintaining of OpenAPI standards for REST API testing. A special tool called Respector was introduced as a first technique to employ static and symbolic program analysis to generate specifications for REST APIs from their source code [34].

Provided experiments showed that Respector successfully detected numerous missing endpoint methods, parameters, constraints, and responses, as well as identified several discrepancies between developer-provided specifications and actual API implementations. Moreover, Respector outperformed other techniques that deduce specifications from API annotations or by invoking the APIs. With the rise of object-oriented languages and the portability of Java APIs, the development and utilization of reusable software components are becoming increasingly feasible [35]. The effectiveness of component reuse relies heavily on the reliability of these components, which is achieved through comprehensive testing. However, the literature lacks practical approaches for generating inputs and verifying outputs for the numerous test cases required. Author introduces the "Roast" tool and associated

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

techniques for testing Java APIs. The practicality and effectiveness of these methods are demonstrated using two complex components, with quantitative results provided to validate the different approaches.

Each of these papers describes different strengths, whether it's in collaboration, integration, interactive documentation, or API management. Depending on the astronomical project specific needs for astronomical data processing, one of these alternatives might serve as a better fit than Swagger for implementing OpenAPI specifications.

3. Distributed microservices-oriented information system for astronomical data processing

Designing a HTTP API service related to astronomical data processing involves creating endpoints that allow clients to interact with and retrieve data about celestial objects, astronomical phenomena, and other relevant information. On the diagram below high-level architecture of designed system is presented. It consists of multiple architectural components including client applications, back-end API aggregators and domain microservices. Microservices provides multiple communication channels including asynchronous and synchronous ways.

Synchronous communication channel is implemented via exposing HTTP APIs for reading data model. Any data model is performed in asynchronous way via message bus (RabbitMQ in a current case). Since data fetching is performed via HTTP request, we can see the importance of OpenAPI and Swagger instrument. Once data is updated via message broker in asynchronous way, Swagger allows to access HTTP REST API in synchronous way by making a direct HTTP call to the microservice accessing the data storage and checking its saved information. The provided diagram in Fig. 1 illustrates a high-level architecture for an astronomy-related system using microservices.

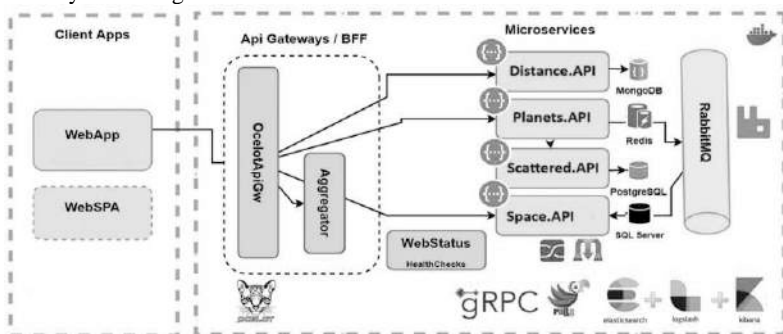


Figure 1. High-level architecture for an astronomy-related system using microservices

Here's a detailed description of each component and their interactions:

ADVANCES

IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

1. Client Apps:
 - a. **WebApp**: A traditional web application interface that interacts with the API Gateway.
 - b. **WebSPA**: A Single Page Application (SPA) that provides a more dynamic user experience, also interacting with the API Gateway.
2. API Gateways / BFF (Backend for Frontend):
 - a. **OcelotApiGw**: Ocelot is an API Gateway that handles requests from client applications and routes them to the appropriate microservices. It provides functionalities like authentication, authorization, request aggregation, and more.
 - b. **Aggregator**: This component aggregates data from multiple microservices into a single response, optimizing the number of calls needed by client applications.
3. Microservices:
 - a. **Distance.API**: Handles operations related to astronomical distances. It uses MongoDB for data storage, providing flexible and scalable storage of distance data.
 - b. **Planets.API**: Manages data related to planets. It leverages Redis, an in-memory data store, to enhance the speed of data access and caching.
 - c. **Scattered.API**: Likely deals with scattered objects in space such as asteroids or comets. It uses PostgreSQL, a powerful, open-source relational database.
 - d. **Space.API**: Manages general space-related data. It relies on SQL Server, a robust relational database system from Microsoft.
4. RabbitMQ as a message broker used for asynchronous communication between microservices. It enables event-driven architecture, where services can publish and subscribe to events without tight coupling.
5. Additional Components:
 - a. **WebStatus (HealthChecks)**: A service that monitors the health status of various microservices, ensuring they are running optimally. It can provide insights into service uptime and performance.
 - b. **gRPC**: A high-performance, open-source RPC framework that can be used for communication between microservices, offering advantages such as language-agnosticism, low latency, and efficient data serialization.
 - c. **Polly**: A .NET resilience and transient-fault-handling library that allows developers to express policies such as Retry, Circuit Breaker, Timeout, Bulkhead Isolation, and Fallback.
 - d. **ELK Stack (Elasticsearch, Logstash, Kibana)**: A set of tools for logging, searching, and visualizing data:
 - i. **Elasticsearch**: A search and analytics engine.
 - ii. **Logstash**: A data processing pipeline that ingests data from multiple sources, transforms it, and then sends it to a stash like Elasticsearch.
 - iii. **Kibana**: A visualization tool used to explore data stored in Elasticsearch, providing graphical representations and dashboards.
6. Data Flow:
 - a. **Client Interaction**: Users interact with the WebApp or WebSPA, which sends requests to the OcelotApiGw.
 - b. **API Gateway Routing**: The API Gateway routes these requests to the appropriate microservice (Distance.API, Planets.API, Scattered.API, Space.API).

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

c. **Data Aggregation:** For complex queries needing data from multiple sources, the Aggregator compiles the necessary information.

d. **Database Operations:** Each microservice interacts with its respective database (MongoDB, Redis, PostgreSQL, SQL Server) to perform CRUD operations.

e. **Asynchronous Communication:** Microservices communicate asynchronously through RabbitMQ, allowing for scalable and decoupled architecture.

f. **Health Monitoring:** The WebStatus service continuously monitors the health of all services.

g. **Logging and Visualization:** Logs and metrics are collected, processed, and visualized using the ELK Stack, facilitating monitoring and debugging.

This architecture demonstrates a robust and scalable approach to managing an astronomy-related system using microservices, an API Gateway, asynchronous communication, and comprehensive health monitoring and logging capabilities. It leverages modern technologies to ensure high performance, resilience, and maintainability. As we can mention from the diagram above, Microservices represented by API HTTP services provide OpenAPI documentation by exposing Swagger endpoints. The provided OpenAPI specification describes an API for an astronomy-related service with several endpoints for managing and retrieving data about distances, planets, scattered disks, space, and reference stars [36]. Below is a detailed breakdown of each part of the specification. Specification provided using OpenAPI Version: 3.0.1. Specification is implemented via open-source tool called Swagger UI and examples are provided below using that API tool.

The first section of the specification (`/api/Distance`) is related to astronomical distance measurement. Existing HTTP endpoints accept HTTP GET and POST request to the service, allowing to enter a record regarding any distance as well as fetch already existing information.

The OpenAPI specification can be found below:

- **GET:** Retrieves a list of distances.
 - **Tags:** Distance
 - **Responses:**
 - 200: Success returns an array of Distance objects in text/plain, application/json, or text/json formats.
- **POST:** Creates a new distance entry.
 - **Tags:** Distance
 - **Request Body:** Accepts a Distance object in application/json, text/json, or application/*+json formats.
 - **Responses:**
 - 200: Success returns the created Distance object.

The Swagger specification (`/api/Planets`) is related to the planets in the universe providing endpoints for accessing all the information including names, ordering and planetary system. Existing contracts allow retrieve existing list of planets and record a new planet entry which has been discovered recently.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

The OpenAPI specification can be found below:

- **GET:** Retrieves a list of planets.
 - **Tags:** Planets
 - **Responses:**
 - 200: Success returns an array of strings representing planet names in text/plain, application/json, or text/json formats.
- **POST:** Creates a new planet entry.
 - **Tags:** Planets
 - **Request Body:** Accepts a string in application/json, text/json, or application/*+json formats.
 - **Responses:**
 - 200: Success

The scattered disk is a distant region of the Solar System that extends beyond the orbit of Neptune. It is populated by a group of small icy bodies known as scattered disk objects (SDOs). These objects have highly elliptical orbits that take them far from the Sun at their aphelion (the point in their orbit farthest from the Sun) and closer to the Sun at their perihelion (the point in their orbit closest to the Sun). Key characteristics of the scattered disk include orbital characteristics, origins, composition, known Objects.

Listed characteristics are covered by the OpenAPI specification (*/api/ScatteredDisk*) listed below:

- **GET:** Retrieves a list of space-related objects.
 - **Tags:** Space
 - **Responses:**
 - 200: Success returns an array of strings in text/plain, application/json, or text/json formats.
- **POST:** Creates a new space entry.
 - **Tags:** Space
 - **Request Body:** Accepts a string in application/json, text/json, or application/*+json formats.
 - **Responses:**
 - 200: Success

The Fig. 2 illustrates the effectiveness of Swagger usage in a context of astronomical data processing. On the image below, we can see an example of transforming OpenAPI JSON specification to user-friendly GUI via Swagger tool.

Data models define the structure of your data entities in C#. For an astronomy API, these models represent celestial objects and their attributes. The purpose of the following architecture component is to define domain model and main attributes are required during the astronomical data processing. The following important attributes should be defined inside the astronomical domain model of SSOs [37]: mass, radius, identifier (name), etc.

Instances of these models are used throughout your application to represent and manipulate data related to stars. The visual representation of the database models

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

highlights the different structures and technologies used for each microservice. The following diagram in Fig. 3 showcases these models.

The visual representation of the database models highlights the different structures and technologies used for each microservice. The following diagram showcases these models.

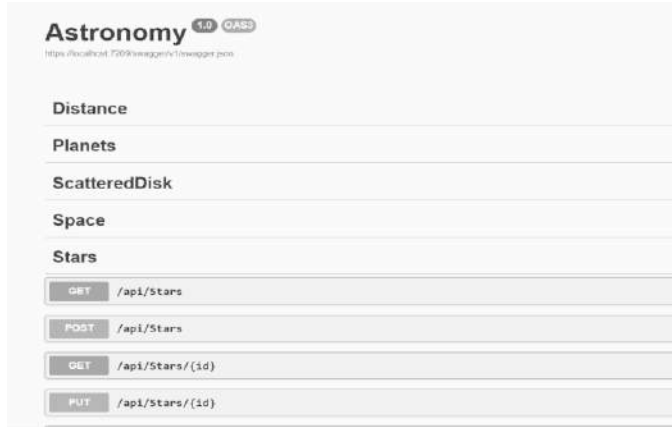


Figure 2. Example of transforming OpenAPI JSON specification to user-friendly GUI via Swagger tool

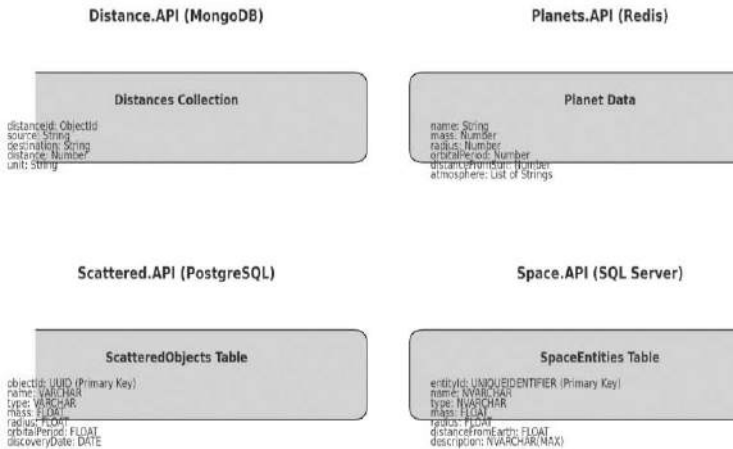


Figure 3. Data models for an astronomy-related system using microservices

Distance.API (MongoDB): A document collection with various fields for distance data. This collection will store information about the distances between

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

different astronomical objects. Each document will represent a specific distance measurement, including the source and destination of the measurement, the distance value, and the unit of measurement.

Distance JSON model is represented by NoSQL (Document-Oriented) Database. Database collection is called Distances, and it includes following set of fields.

```
{
  "distanceId": "60c72b2f4f1a4e3d5c8b4567",
  "source": "Earth",
  "destination": "Mars",
  "distance": 0.52,
  "unit": "AU"
}
```

Planets.API (Redis): In-memory data structures for storing planet data. In Redis, each planet will be stored as a hash where the key is a unique identifier for the planet (e.g., planet:1) and the value is a hash containing various attributes of the planet such as name, mass, radius, orbital period, distance from the sun, and atmosphere composition. Redis is used here for its fast read and write operations, which are beneficial for frequently accessed data.

Planets JSON model is represented by NoSQL (Key-Value storage) Database. Since it is a key-value storage, data should be stored via single string by hashing or serializing into JSON string.

```
{
  "name": "Earth",
  "mass": 5.972e24,
  "radius": 6371,
  "orbitalPeriod": 365.25,
  "distanceFromSun": 1.00,
  "atmosphere": ["Nitrogen", "Oxygen", "Argon", "Carbon Dioxide"]
}
```

Scattered.API (PostgreSQL): A relational table with fields for scattered object data. This table will store data about scattered astronomical objects like asteroids and comets. Each row represents an object with attributes including its ID, name, type, mass, radius, orbital period, and discovery date. PostgreSQL is chosen for its ACID compliance and powerful querying capabilities.

Scattered objects are stored in relational SQL database with its unique identifier as primary key for each scattered object and the list of related attributes.

```
CREATE TABLE ScatteredObjects (
  objectId UUID PRIMARY KEY,
  name VARCHAR(255),
  type VARCHAR(50),
  mass FLOAT,
  radius FLOAT,
  orbitalPeriod FLOAT,
  discoveryDate DATE
);
```

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

Space.API (SQL Server): A relational table for space entity data with comprehensive fields for detailed information. This table will store general information about various space entities such as stars, galaxies, and nebulas. Each row represents an entity with attributes including its ID, name, type, mass, radius, distance from Earth, and a description. SQL Server is used here for its enterprise features and robust performance.

Space SQL model is represented as relational database table as well with corresponding primary attribute and the list of attributes assigned.

```
CREATE TABLE SpaceEntities (  
    entityId UNIQUEIDENTIFIER PRIMARY KEY,  
    name NVARCHAR(255),  
    type NVARCHAR(50),  
    mass FLOAT,  
    radius FLOAT,  
    distanceFromEarth FLOAT,  
    description NVARCHAR(MAX)  
);
```

This architecture leverages the strengths of each database technology, ensuring optimal performance, scalability, and flexibility for handling diverse data requirements in an astronomy-related HTTP service.

A skeleton of the proposed OpenAPI specification in distributed microservices-oriented information system for astronomical data processing was tested in scope of the Lemur software of the Collection Light Technology (CoLiTec) project (<https://colitec.space>) [38].

The specific modules and services related to the mathematical methods and algorithms in the Lemur software are:

- automated frame calibration;
- cosmetic frame correction;
- track-and-stack feature;
- brightness equalization;
- background alignment [6];
- astronomical image filtering [5, 27];
- determining the contours of objects;
- image recognition [30, 31];
- typical shape formation [19];
- detection of the moving objects (with near-zero, normal, fast apparent motion) [39];
- fully automated robust method of the astrometric reduction [7];
- fully automated robust method of the photometric reduction [40];
- support of the multi-threaded processing;
- transferring of astronomical data with intermediate storage;

More extended details about the Lemur software of the CoLiTec project are presented in these papers [41, 42, 43] and research [44, 45].

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

The example of JSON data implemented in scope of the distributed microservices-oriented information system for astronomical data processing for the Lemur software represents a response for an API that provides distance-related information between celestial bodies mentioned below.

```
{
  "origin": {
    "name": "Earth",
    "type": "Planet",
    "coordinates": {
      "x": 0.0, "y": 0.0, "z": 0.0
    }
  },
  "destination": {
    "name": "Mars",
    "type": "Planet",
    "coordinates": {
      "x": 1.5, "y": 0.5, "z": 0.2
    }
  },
  "distance": {
    "unit": "AU",
    "value": 1.52
  },
  "travelTime": {
    "unit": "days",
    "value": 300
  },
  "path": [
    {
      "x": 0.0, "y": 0.0, "z": 0.0
    },
    {
      "x": 0.5, "y": 0.2, "z": 0.1
    },
    {
      "x": 1.0,
      "y": 0.4,
      "z": 0.15
    },
    {
      "x": 1.5,
      "y": 0.5,
      "z": 0.2
    }
  ],
}
```

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

```
"metadata": {  
  "requestTime": "2024-06-18T12:34:56Z",  
  "responseTime": "2024-06-18T12:34:57Z",  
  "service": "DistanceAPI"  
}
```

Presented JSON structure contains following valued information:

- **origin:** Information about the starting point of the distance calculation, including the name, type (e.g., planet, star), and coordinates in a 3D space.
- **destination:** Information about the endpoint of the distance calculation, similar to the origin.
- **distance:** The calculated distance between the origin and destination, along with the unit of measurement (e.g., Astronomical Units - AU).
- **travelTime:** An estimated travel time to cover the distance, along with the unit of measurement (e.g., days).
- **path:** An array of coordinates representing the path taken from the origin to the destination.
- **metadata:** Additional information about the API request, including the request and response times and the name of the service that provided the data.

This JSON structure is designed to be comprehensive and can be extended further based on the specific requirements and additional attributes that might be relevant for the Distance API in a microservices architecture.

4. Discussions

Implementing Swagger in a microservices architecture presents numerous benefits, significantly enhancing both the development and maintenance phases of service-oriented applications. Swagger, as an open-source framework, facilitates the design, build, documentation, and consumption of RESTful web services. Its ability to generate interactive API documentation from code annotations ensures that all stakeholders have access to up-to-date and accurate API details, fostering better communication and collaboration within development teams.

One of the primary advantages of using Swagger is the standardized documentation it provides. This standardization ensures that each microservice adheres to a consistent format, simplifying the understanding and usage of APIs across different services. This consistency is crucial in a microservices architecture where multiple services need to interact seamlessly, and developers might need to work with various APIs concurrently.

Swagger's interactive documentation also enables developers to test APIs directly from the documentation interface. This feature streamlines the development and debugging process, allowing for quicker iterations and more efficient troubleshooting. By providing a clear and interactive way to visualize and test API endpoints, Swagger reduces the learning curve for new developers and enhances productivity.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

Moreover, Swagger supports automated code generation for API clients in various programming languages, which accelerates the development of client-side applications and services. This automation minimizes manual coding errors and ensures that client implementations are aligned with the API specifications, further promoting consistency and reliability across the system.

In a microservices ecosystem, where services are often developed, deployed, and scaled independently, maintaining up-to-date documentation can be challenging. Swagger addresses this by integrating directly with the codebase, ensuring that any changes to the API are automatically reflected in the documentation. This integration is particularly beneficial for continuous integration and continuous deployment (CI/CD) pipelines, ensuring that API changes are documented and tested throughout the development lifecycle.

The use of Swagger also enhances API discoverability and usability. With a well-documented API, internal and external developers can easily explore available endpoints, understand input and output requirements, and integrate services more effectively. This discoverability is crucial for fostering innovation and enabling developers to leverage existing services to build new functionalities.

Furthermore, Swagger's support for API versioning ensures that changes and updates to APIs can be managed without disrupting existing consumers. This capability is essential in a microservices architecture, where different services and clients might depend on different versions of the same API. By clearly documenting versioned endpoints, Swagger helps maintain backward compatibility and smooth transitions during updates.

Overall, using Swagger in a microservices architecture streamlines development workflows, improves API quality, and enhances collaboration among teams. Its comprehensive documentation, interactive features, and automation capabilities make it an indispensable tool for managing complex service ecosystems. By ensuring that APIs are well-documented, easily testable, and consistently implemented, Swagger contributes to the robustness, scalability, and maintainability of microservices-based applications. In conclusion, integrating Swagger into a microservices architecture is a strategic decision that can significantly improve both the development experience and the operational efficiency of service-oriented systems.

The provided JSON representation of the astronomical data processing system demonstrates an effective and structured approach to delivering essential astronomical data within a microservices architecture. By encapsulating origin and destination details, including their coordinates and types, the API offers precise and comprehensive information about celestial bodies. The inclusion of distance measurements in Astronomical Units (AU) ensures that the data is scientifically relevant and usable for various astronomical calculations and analyses. Additionally, the estimated travel time between the celestial bodies, expressed in days, provides valuable insights for planning hypothetical space missions or understanding relative distances in the cosmos.

The path array, which details the coordinates from the origin to the destination, adds another layer of utility, potentially aiding in the visualization of the journey

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

through space. This feature is particularly useful for educational tools, simulations, and visual representations in applications that require a detailed trajectory of space travel. Metadata encompassing request and response times, along with service identification, enhances the API's transparency and traceability. Such metadata is crucial for monitoring and debugging purposes within a distributed system, ensuring that the service remains reliable and maintainable.

In the context of a microservices architecture, this JSON structure exemplifies how services can be designed to be modular and independently scalable, promoting better resource utilization and simplified management. The use of well-defined endpoints and clear data contracts makes the Distance API a robust component that can seamlessly integrate with other microservices, such as those dealing with planetary information or scattered disk objects.

This modular approach not only improves system resilience but also allows for independent updates and scaling of individual services, enhancing overall system performance and maintainability.

Moreover, the JSON structure's extensibility ensures that the API can evolve alongside the growing needs of its users, accommodating new data points and features without disrupting existing functionality. This foresight in design supports long-term sustainability and adaptability of the service. The detailed information provided by the Distance API can serve various stakeholders, from researchers and educators to space enthusiasts and developers, making it a versatile tool in the domain of astronomy.

The structured data model aids in the creation of user-friendly interfaces and intuitive visualizations, fostering greater engagement and understanding among users. By adhering to best practices in API design, such as clear naming conventions and consistent data formats, the Distance API sets a standard for other services within the microservices architecture. This consistency ensures a cohesive user experience and simplifies the development process for new features and services.

5. Conclusions

We presented the usage of OpenAPI specification in distributed microservices-oriented information system for astronomical data processing. A common goal of all scientific and technological algorithms and methods is to automate as much as available processes without any human actions.

In general cases it can be done by the different astronomical distributed microservices-oriented information system. In these pipelines the various data mining and knowledge discovery in databases tasks are used for speeding up and optimizing the astronomical data processing. Suggested using of the OpenAPI specification in a distributed microservices-oriented information system for astronomical data processing significantly improves the system's interoperability, scalability, and maintainability.

The developed skeleton of the real example of astronomical data-processing system is implemented using .Net Core framework and C# programming language. Implementing Swagger in a microservices architecture presents numerous benefits,

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

significantly enhancing both the development and maintenance phases of service-oriented applications.

The developed skeleton and the proposed approach will be useful for the different microservices-oriented information system for astronomical data processing. It can be used for all kind of processing astronomical images using the different mathematical methods and algorithms implemented as a tool, module, or service. Another one good example of application the proposed skeleton is a realization of the Virtual Observatory (VO) concept.

The modern international astronomical astrometric and photometric catalogues are available now in cloud, so any interactions with such data from them require services integration for processing. The microservices-oriented architecture will be also very helpful in the complex information systems for astronomical data processing with integration of the Continuous Integration/Continuous Delivery (CI/CD) principles.

The further research will be conducted on integrating proposed OpenAPI specification in distributed microservices-oriented information system for astronomical data processing in scope of the Lemur software of the Collection Light Technology (CoLiTec) project [46].

6. Acknowledgements

The research was supported by the Ukrainian project of fundamental scientific research “Development of computational methods for detecting objects with near-zero and locally constant motion by optical-electronic devices” #0124U000259 in 2024-2026 years.

7. References

- [1] L. Wheeler, et al., Risk assessment for asteroid impact threat scenarios, *Acta Astronautica*, vol. 216, pp. 468–487, 2024, doi: 10.1016/j.actaastro.2023.12.049.
- [2] V. Akhmetov, et al., Cloud computing analysis of Indian ASAT test on March 27, 2019, *IEEE International Scientific-Practical Conference: Problems of Infocommunications Science and Technology*, pp. 315–318, 2019. doi: 10.1109/PICST47496.2019.9061243.
- [3] V. Savanevych, et al., Mathematical methods for an accurate navigation of the robotic telescopes, *Mathematics*, vol. 11, issue 10, 2246, 2023. doi: 10.3390/math11102246.
- [4] R. Klette, *Concise computer vision. An Introduction into Theory and Algorithms*, London: Springer, 233, 2014.
- [5] V. Vlasenko, et al., Devising a procedure for the brightness alignment of astronomical frames background by a high frequency filtration to improve accuracy of the brightness estimation of objects, *Eastern-European Journal of Enterprise Technologies*, vol. 2, issue 2-128, pp. 31–38, 2024. doi: 10.15587/1729-4061.2024.301327.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

- [6] Š. Parimucha, et al., CoLiTecVS – A new tool for an automated reduction of photometric observations, *Contributions of the Astronomical Observatory Skalnaté Pleso*, vol. 49, issue 2, pp. 151-153, 2019.
- [7] V. Akhmetov, et al., Astrometric reduction of the wide-field images, *Advances in Intelligent Systems and Computing*, vol. 1080, pp. 896–909, 2020. doi: 10.1007/978-3-030-33695-0_58.
- [8] V. Kudak, V. Epishev, V. Perig, and I. Neybauer, Determining the orientation and spin period of TOPEX/Poseidon satellite by a photometric method, *Astrophysical Bulletin*, vol. 72, issue 3, pp. 340-348, 2017. doi: 10.1134/S1990341317030233.
- [9] S. Khlamov, and V. Savanevych, Big astronomical datasets and discovery of new celestial bodies in the Solar System in automated mode by the CoLiTec software, *Knowledge Discovery in Big Data from Astronomy and Earth Observation*, *Astroinformatics*, pp. 331–345, 2020. doi: 10.1016/B978-0-12-819154-5.00030-8.
- [10] V. Troianskyi, V. Godunova, A. Serebryanskiy, et al., Optical observations of the potentially hazardous asteroid (4660) Nereus at opposition 2021, *Icarus*, vol. 420, 116146, 2024. doi: 10.1016/j.icarus.2024.116146.
- [11] G. Adam, P. Kontaxis, L. Doulos, E.-N. Madias, C. Bouroussis, and F. Topalis, Embedded Microcontroller with a CCD Camera as a Digital Lighting Control System, *Electronics*, vol. 8, issue 1, 2019. doi: 10.3390/electronics8010033.
- [12] D. Oszkiewicz, et al., Spins and shapes of basaltic asteroids and the missing mantle problem. *Icarus*, 397, 115520, 2023. doi: 10.1016/j.icarus.2023.115520.
- [13] I. B. Vavilova, Y. S. Yatskiv, L. K. Pakuliak, et al., UkrVO astroinformatics software and web-services, *Proceedings of the International Astronomical Union*, vol. 12, issue S325, pp. 361-366, 2016. doi: 10.1017/S1743921317001661.
- [14] V. Akhmetov, et al., Fast coordinate cross-match tool for large astronomical catalogue. *Advances in Intelligent Systems and Computing*, vol. 871, pp. 3–16, 2019. doi: 10.1007/978-3-030-01069-0_1.
- [15] K. D. Borne, *Scientific data mining in astronomy*, *Next Generation of Data Mining*, Chapman and Hall/CRC, pp. 115-138, 2008.
- [16] Y. Zhang, and Y. Zhao, *Astronomy in the big data era*, *Data Science Journal*, vol. 14, 2015.
- [17] N. Raychev, *Test Automation in Microservice Architecture*, *IEEE Spectrum*, vol. 8, issue 7, 15 p., 2020.
- [18] R. Huang, M. Motwani, I. Martinez, and A. Orso, Generating REST API Specifications through Static Analysis, *IEEE ACM 46th International Conference On Software Engineering (ICSE)*, 107, pp. 1–13, 2024. doi: 10.1145/3597503.3639137.
- [19] V. Savanevych, et al., Formation of a typical form of an object image in a series of digital frames, *Eastern-European Journal of Enterprise Technologies*, vol. 6, issue 2-120, pp. 51–59, 2022. doi: 10.15587/1729-4061.2022.266988.
- [20] W. Burger, and M. Burge, *Principles of digital image processing: fundamental techniques*, NY: Springer, 2009.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

- [21] S. Khlamov, I. Tabakova, T. Trunova, and Z. Deineko, Machine Vision for Astronomical Images Using the Canny Edge Detector, CEUR Workshop Proceedings, vol. 3384, pp. 1–10, 2022.
- [22] V. Troianskyi, P. Kankiewicz, and D. Oszkiewicz, Dynamical evolution of basaltic asteroids outside the Vesta family in the inner main belt, *Astronomy and Astrophysics*, vol. 672, A97, 2023. doi: 10.1051/0004-6361/202245678.
- [23] D. Oszkiewicz, et al., Spin rates of V-type asteroids, *Astronomy & Astrophysics*, vol. 643, A117, 2020. doi: 10.1051/0004-6361/202038062.
- [24] V. Savanevych, et al., CoLiTecVS software for the automated reduction of photometric observations in CCD-frames, *Astronomy and Computing*, vol. 40 (100605), 15 p., 2022. doi: 10.1016/j.ascom.2022.100605.
- [25] S. Khlamov, V. Savanevych, V. Vlasenko, O. Briukhovetskyi, T. Trunova, I. Levykin, V. Shvedun, I. Tabakova, Development of the matched filtration of a blurred digital image using its typical form. *Eastern-European Journal of Enterprise Technologies*, vol. 1, issue 9 (121), pp. 62-71, 2023. doi: 10.15587/1729-4061.2023.273674.
- [26] S. Khlamov, et al., Development of computational method for matched filtration with analytic profile of the blurred digital image, *Eastern-European Journal of Enterprise Technologies*, vol. 5, issue 4-119, pp. 24–32, 2022. doi: 10.15587/1729-4061.2022.265309.
- [27] C. A. Politsch, et al., Trend filtering–I. A modern statistical tool for time-domain astronomy and astronomical spectroscopy, *MNRAS*, vol. 492, issue 3, pp. 4005-4018, 2020. doi: 10.1093/mnras/staa106.
- [28] M. Dadkhah, et al., Methodology of wavelet analysis in research of dynamics of phishing attacks, *International Journal of Advanced Intelligence Paradigms*, vol. 12(3-4), pp. 220-238, 2019. doi: 10.1504/IJAIP.2019.098561.
- [29] L. Kirichenko, A.S.A. Alghawli, T. Radivilova, Generalized approach to analysis of multifractal properties from short time series, *International Journal of Advanced Computer Science and Applications*, vol. 11, issue 5, pp. 183–198, 2020. doi: 10.14569/IJACSA.2020.0110527.
- [30] S. Khlamov, et al., The astronomical object recognition and its near-zero motion detection in series of images by in situ modeling, *Proceedings of the 29th IEEE International Conference on Systems, Signals, and Image Processing, IWSSIP 2022, Sofia, Bulgaria, June 1st – 3rd, 4 p., 2022.* doi: 10.1109/IWSSIP55020.2022.9854475.
- [31] S. Khlamov, I. Tabakova, T. Trunova, Recognition of the astronomical images using the Sobel filter. In *Proceedings of the International Conference on Systems, Signals, and Image Processing*, 4 p., 2022. doi: 10.1109/IWSSIP55020.2022.9854425.
- [32] D.N.N. da Costa, Guidelines for Testing Microservice-based Applications, Dissertation for obtaining the master’s degree, 80 p., 2022.
- [33] Stoplight. Available at: <https://stoplight.io/solutions>.
- [34] A. Golmohammadi, M. Zhang, and A. Arcuri, Testing Restful Apis: A Survey, *ACM Transactions on Software Engineering and Methodology*, vol. 33 (1), pp. 1-41, 2023.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

- [35] D. Hoffman, and P. Strooper, Tools and Techniques for Java API Testing, Australian Software Engineering Conference, pp. 235-245, 2002. doi: 10.1109/ASWEC.2000.844580.
- [36] S. Khlamov, et al., Automated data mining of the reference stars from astronomical CCD frames, CEUR Workshop Proceedings, vol. 3668, pp. 83–97, 2024.
- [37] V. Troianskyi, V. Kashuba, O. Bazyey, et al., First reported observation of asteroids 2017 AB8, 2017 QX33, and 2017 RV12, Contributions of the Astronomical Observatory Skalnaté Pleso, vol. 53, pp. 5-15, 2023. doi: 10.31577/caosp.2023.53.2.5.
- [38] S. Khlamov, et al., Machine vision for astronomical images using the modern image processing algorithms implemented in the CoLiTec software, Measurements and Instrumentation for Machine Vision, Chapter 12: CRC Press, Taylor & Francis Group, pp. 269-310, 2024. doi: 10.1201/9781003343783-12.
- [39] S. Khlamov, et al., Development of computational method for detection of the object's near-zero apparent motion on the series of CCD–frames, EEJET, vol. 2, issue 9(80), pp. 41-48, 2016. doi: 10.15587/1729-4061.2016.65999.
- [40] I. Kudzej, et al., CoLiTecVS – A new tool for the automated reduction of photometric observations, Astronomische Nachrichten, vol. 340, issue 1-3, pp. 68-70, 2019. doi: 10.1002/asna.201913562.
- [41] V. Savanevych, et al., A new method based on the subpixel Gaussian model for accurate estimation of asteroid coordinates, MNRAS, vol. 451, issue 3, pp. 3287–3298, 2015. doi: 10.1093/mnras/stv1124.
- [42] L. Mykhailova, et al., Method of maximum likelihood estimation of compact group objects location on CCD-frame, Eastern-European Journal of Enterprise Technologies, vol. 5, issue 4, pp. 16-22, 2014. doi:10.15587/1729-4061.2014.28028.
- [43] V. Savanevych, et al., A method of immediate detection of objects with a near-zero apparent motion in series of CCD-frames. Astronomy & Astrophysics, 609, A54: 11, 2018. doi: 10.1051/0004-6361/201630323.
- [44] V. Shvedun, et al., Statistical modelling for determination of perspective number of advertising legislation violations, Actual Problems of Economics, vol. 184, issue 10, pp. 389-396, 2016.
- [45] V. Savanevych, et al., Comparative analysis of the positional accuracy of CCD measurements of small bodies in the solar system software CoLiTec and Astrometrica, Kinematics and Physics of Celestial Bodies, vol. 31, issue 6, pp. 302–313, 2015.
- [46] S. Khlamov, et al., Data Mining of the Astronomical Images by the CoLiTec Software, CEUR Workshop Proceedings, vol. 3171, pp. 1043–1055, 2022.

**РОЗПОДІЛЕНА МІКРОСЕРВІСНО-ОРІЄНТОВАНА
ІНФОРМАЦІЙНА СИСТЕМА ДЛЯ ОБРОБКИ
АСТРОНОМІЧНИХ ДАНИХ ЗА СПЕЦИФІКАЦІЮ OPENAPI**

Ph.D. С. Хламов ORCID: 0000-0001-9434-1081

Харківський національний університет радіоелектроніки, Україна

E-mail: sergii.khlamov@gmail.com

С. Орлов ORCID: 0009-0008-0680-206X

Національний аерокосмічний університет – Харківський авіаційний інститут, Україна,

E-mail: s.v.orlov@student.khai.edu

Т. Трунова ORCID: 0000-0003-2689-2679

Харківський національний університет радіоелектроніки, Україна

E-mail: tetiana.trunova@nure.ua,

Ю. Бондар ORCID: 0009-0001-5309-0084

Харківський національний університет радіоелектроніки, Україна

E-mail: bndr@gmail.com

Ю. Нетребін ORCID: 0009-0001-8778-3241

INTIVE Limited, O'Connell Bridge House, Ірландія,

E-mail: yuriy.n.netrebin@gmail.com

***Анотація.** Розділ присвячено використанню специфікації OpenAPI в розподіленій мікросервіс-орієнтованій інформаційній системі обробки астрономічних даних. Загальна мета всіх наукових і технологічних алгоритмів і методів – максимально автоматизувати доступні процеси без будь-яких дій людини. У загальних випадках це можна зробити різними астрономічними розподіленими мікросервісами, орієнтованими на інформаційні системи. У цих конвеєрах різні завдання інтелектуального аналізу даних і виявлення знань у базах даних (KDD) використовуються для прискорення й оптимізації обробки астрономічних даних. Запропоноване використання специфікації OpenAPI в розподіленій інформаційній системі, орієнтованій на мікросервіси, для обробки астрономічних даних значно покращує сумісність, масштабованість і зручність обслуговування системи. Розроблений скелет реального прикладу системи обробки астрономічних даних реалізовано за допомогою фреймворку .Net Core та мови програмування C#. Впровадження Swagger в архітектурі мікросервісів дає численні переваги, значно покращуючи етапи розробки та обслуговування сервіс-орієнтованих програм. Розроблений скелет і запропонований підхід будуть корисні для різних мікросервісно-орієнтованих інформаційних систем для обробки астрономічних даних. Його можна використовувати для всіх видів обробки астрономічних зображень за допомогою різних математичних методів і алгоритмів, реалізованих як інструмент, модуль або сервіс. Ще одним гарним прикладом застосування запропонованого скелета є реалізація концепції віртуальної обсерваторії (VO) або інтеграція з інструментами CI/CD.*

***Ключові слова:** інформаційна система, клієнт-серверна архітектура, мікросервісно-орієнтована архітектура, масштабованість, конвеєр обробки, інтелектуальний аналіз даних, відкриття знань у базах даних, астрономічні спостереження, обробка зображень, об'єкти Сонячної системи, Swagger, OpenAPI, REST API, JSON, .NET, C#, RabbitMQ*

UDC 004.048

**DATA MINING OF THE PRIMARY ORBITS OF THE SOLAR
SYSTEM OBJECTS USING THE COLITEC SOFTWARE AND THE
VÄISÄLÄ METHOD**

Ph.D. V. Troianskyi ORCID: 0000-0002-5899-2300

Odesa I. I. Mechnikov National University, Ukraine

E-mail: v.troianskyi@onu.edu.ua,

Dr.Sci. O. Bazyey ORCID: 0000-0001-6886-4575

Odesa I. I. Mechnikov National University, Ukraine

E-mail: o.bazyey@onu.edu.ua

Ph.D. H. Okhotko ORCID: 0009-0002-1403-4298

Odesa I. I. Mechnikov National University, Ukraine

E-mail: hannaokhotko@gmail.com

Ph.D. S. Khlamov 0000-0001-9434-1081

Kharkiv National University of Radio Electronics, Ukraine

E-mail: sergii.khlamov@gmail.com

Abstract. The chapter is devoted to the processing pipeline for data mining of the primary orbits and discovery of the new Solar System objects using the CoLiTec software and classical Väisälä method. The first step of a such processing pipeline is performing the sequential astronomical observations and the classical astrometric data reduction. It is implemented as a combination of the general mathematical algorithms and methods for processing of the astronomical frames encapsulated in the CoLiTec software. It contains the inverse median filter, astronomical calibration with usage of the calibration master-frames (bias, dark, flat, dark-flat), detection of the astronomical objects and its trajectories in series of frames and other very useful and important features. After that the especial parameters of the object's orbit (right ascension and declination) are calculated at the certain time. When we receive at least two observations of the same object under study at different moments, the classic Väisälä algorithm can be applied. For this, the primary orbit from the two nearest observations is calculated. Then the geocentric rectangular coordinates and the appropriate geocentric velocity components are computed. This give us an opportunity for determining the Keplerian elements of orbit of the investigated object at any time we are interested in. The developed algorithm is implemented as a processing pipeline that includes a combination of the CoLiTec software and created tool with encapsulation of the Väisälä method. The created processing pipeline for data mining of *the primary orbits and discovery of the new Solar System objects using the CoLiTec software and classical Väisälä method is practically verified. Using it a few new asteroids are first reported and a few lost small bodies of the Solar System are found in the Kyiv comet station and the Odesa - Mayaky observatory.*

Keywords: *Data mining, processing pipeline, astronomical observations, CoLiTec software, Väisälä method, image processing, image calibration, astrometric reduction, photometric reduction, object detection, positional coordinates, orbit determination, Solar System objects*

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

1. Introduction

The asteroid-comet hazard is a big potential problem in the XXI century. It leads to the developing astronomical scientific direction like an image processing, which includes the following algorithms for astrometric reduction [1], photometric reduction [2], detection or even discovery of the Solar System objects [3], etc.

A common goal of all scientific and technological algorithms is to automate as much as available processes without any human actions. In general cases it can be done by the different astronomical scientific processing pipelines. In these pipelines the various data mining [4] and knowledge discovery in databases (KDD) [5] tasks are used for speeding up and optimizing the astronomical data processing.

The astronomical scientific information is collected from the different historical archives, clusters, Virtual Observatories [6], clouds, astronomical astrometric and photometric catalogues [7], different servers and other storages. Almost all astronomical scientific observations are created by the charge-coupled device (CCD) [8] and performed during the specified observational period of the investigated small celestial objects of the Solar System (SSOs) [9] (like, comets or asteroids [10]), as well as the artificial satellites [11]. After performing the series of observations of the investigated SSOs it is required to analyze the results of observation, which can include the period and shape of rotations determining of such investigated SSOs.

That is why it is required to create a mathematical method to determine a primary orbit and discovery of the new Solar System objects using the CoLiTec software and the classical Väisälä method. Such a method gives a possibility for estimating the geocentric rectangular positional coordinates of a SSO under study with and calculating the different Keplerian elements of the SSO's orbit. At the same time this algorithm can improve the conditional expectation of the correct discovery [12] of the real SSOs. The Väisälä algorithm is a very useful algorithm when used in the different situations [13]. Its importance becomes noticeable with the particularly short observation arcs, which are insufficient to confirm an exact orbit and predict a position of the investigated small astronomical Solar System object during the next week. This chapter aims to the analysis of main focuses and features of the processing pipeline for data mining of the primary orbits and discovery of the new Solar System objects using the CoLiTec software and classical Väisälä method.

Section 2 presents the literature review with mentioning advantages and disadvantages of the reviewed papers. Section 3 elaborates an architecture of the processing pipeline for data mining of the primary orbits and discovery of the new Solar System objects. Detailed description of steps of the processing pipeline are also presented in this section as well as the description of the Väisälä algorithm. This section also aims to the main features and advantages of the CoLiTec software for the astronomical data processing purposes.

Section 4 presents the results received during processing astronomical data with the different SSOs from the Kyiv comet station and the Odesa - Mayaky observatory. Such results include identifiers of the new asteroids that were firstly discovered and the lost SSOs that were found again and re-discovered. The chapter ends with a

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

conclusion in section 5, which illustrates the conclusions and outlines of the future work and research as well as possibilities for future investigations and enhancements.

2. Literature review

Each Solar System object presented in a CCD-frame has a typical form of its image [14]. The common methods for the image processing [15] are developed for detection/recognition such images of SSOs and an estimation of their positional and motion parameters [16]. Such methods are based on the analysis of only those pixels that potentially belong to the investigated object. The disadvantages of such methods are very low accuracies when the typical form of object has a different shape [17].

The methods for pixelization and segmentation by the aperture brightness [18] will work only with a single image of each SSO. A method for the matched filtration [19] uses a model of the object's image, which is analytically determined. The disadvantages of the methods above are the big complexity and low accuracy during the processing, when an image has a several peaks of magnitude. Methods for the Wavelet analysis [20] or even time series analysis [21] are not so effective, because we do not have a big volume of the input data to be analyzed. Also, the disadvantage of such algorithms is the corrupting of the general statistics and possibility to process only clear measurements without any deviations in the typical form of image.

The methods for assessing the aperture brightness [22] of object's images will work only with a single image of each SSO. Any methods for the matched filtration [23] and high-frequency filtration [24], which are devoted to the improving the quality of corrupted images are very resource consuming. The disadvantages of the methods are the big complexity and low accuracy during the astronomical data processing, when an object's image has a several peaks of magnitude.

Computer vision methods [25] have the main disadvantage that they are not able to provide the required level of processing speed using standard libraries. Classical methods for object image recognition [26, 27] require analysis of all pixels of potential objects to determine their typical shape. This also significantly affects processing time. In the case of heterogeneity of the standard typical shape or form, objects become confused, and this, in turn, increases the processing time of both the strobe with the image of the object and the entire frame. Methods for estimating of the image parameters [28, 29] are based on the analysis of only those pixels that potentially belong to the Solar System object under study. Their disadvantage is the inability to determine specific pixels and reject those whose intensity exceeds a specified limit value initially accurately. Because of this, the processing time of each frame increases. The authors of [30] use automatic selection of a reference point as preprocessing to select calibration frames. This algorithm requires quite a lot of execution time because it involves first analyzing the image to find reference points. Next, these points are identified with astronomical catalogs to obtain coordinates on the celestial sphere. After this, the telescope is pointed at the coordinates of the desired area of the sky and takes calibration frames. This entire algorithm requires

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

the coherence of all systems, including the automated telescope mount. At the same time, if there are artifacts in the images, these control points may be false, this leads to an increase in processing time (to search for new control points), or even the impossibility of executing the algorithm. The median pooling algorithm [31] proposes to accumulate a large number of frames for pre-calibration to get rid of real objects, leaving only a uniform background signal. The disadvantage of this approach is the fact that the formation and use of data arrays for each such image requires huge volume of RAM. Any methods for the machine learning [32] and pattern recognition [33] also require a big amount of astronomical data for training. The problem of such methods that astronomical image has a lot of artifacts, so there are a lot of false objects are detected in series of frames.

3. Data mining of the primary orbits of the Solar System objects

Astronomical image calibration is a critical process in astrophotography and observational astronomy [34]. These calibration frames are used to correct different imperfections and artifacts introduced during the image acquisition process, ensuring the accuracy and quality of the final images:

- **Bias Frames.** Bias frames capture the electronic signal present in the camera sensor when no light is allowed to enter the telescope. They record the baseline electronic offset or zero signal level of the sensor. Bias frames help correct for the sensor's inherent electronic noise, such as readout noise and amplifier offsets;
- **Dark Frames.** Dark frames are images taken with the telescope or camera covered, capturing the thermal signal produced by the sensor itself. This signal is a result of heat generating random electronic noise in the detector. Dark frames help in correcting thermal noise, hot pixels, and other sensor-specific imperfections;
- **Flat Frames.** Flat frames are images of a uniformly illuminated surface or a blank, evenly illuminated part of the sky. They are used to correct for variations in sensitivity across the camera sensor, as well as for dust specks or imperfections in the optical system. Flat frames help to normalize the pixel-to-pixel sensitivity differences in the sensor and remove any vignetting or dust shadows.

The calibration process involves the following steps:

1. **Acquisition:** Bias, dark, and flat frames are captured under specific conditions matching the settings used for the actual astrophotography session. It's important to ensure that the exposure times and temperatures match those of the light frames (images of celestial objects).
2. **Subtraction:** The bias frame is subtracted from all the frames (light, dark, and flat) to remove the electronic offset and noise present in the images.
3. **Dark Subtraction:** Dark frames are subtracted from the light frames to eliminate the thermal signal caused by the camera sensor's temperature during image acquisition.
4. **Flat Fielding:** Flat frames are used to normalize the response of the sensor. Light frames are divided by the normalized flat frames to correct variations in pixel

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

sensitivity and eliminate artifacts caused by dust, vignetting, or optical imperfections.

5. **Post-Processing:** Once the calibration process is completed, further image processing techniques, such as stacking, alignment, and color calibration, are often applied to enhance the final image quality.

Calibrating images with bias, dark, and flat frames is crucial in producing high-quality astrophotographs and ensuring accurate scientific analysis by removing unwanted noise and artifacts introduced during the imaging process.

In the developed algorithm we performed the different actions for the astronomical data calibration, like calibration dark frames subtracting, calibration bias frames subtracting and calibration flat frames fielding/dividing [35].

Every astronomical observation of the investigated astronomical object provides the topocentric directions to it:

$$\begin{cases} X_i = -G_{1i} \cos \varphi_i \cos \theta_i, \\ Y_i = -G_{1i} \cos \varphi_i \sin \theta_i, \\ Z_i = -G_{2i} \sin \varphi_i, \end{cases} \quad (1)$$

where a coefficient G and a local sidereal time (θ) are calculated by the following equations:

$$G_{1i} = \frac{a_e}{\sqrt{1 - (2f - f^2) \sin^2 \varphi_i}} + H_i, \quad (2)$$

$$G_{2i} = \frac{(1 - f)^2 a_e}{\sqrt{1 - (2f - f^2) \sin^2 \varphi_i}} + H_i,$$

$$\theta_i = \theta_{g0} + \frac{d\theta}{dt} (t_i - t_0) + \lambda_{Ei}, \quad (3)$$

where φ_i , λ_{Ei} are the geodetic latitude and longitude of the observer;

H_i is the altitude of the observer;

Earth ellipsoid model recommended by the IERS [36];

semi-major axis (aE) of 6378171.364331512 m;

inverse of polar flattening ($1/f$) of 297.7736994668283;

θ_{g0} is Greenwich Mean Sidereal Time (GMST).

After astrometric reduction to the Earth center, we received the right ascension (α_i) (RA) and declination (δ_i) (DE) for the current time (t_i).

This gives us a possibility to create a system of connection equations:

$$\begin{cases} \rho_i \cos \alpha_i \cos \delta_i = x_i + X_i, \\ \rho_i \sin \alpha_i \cos \delta_i = y_i + Y_i, \\ \rho_i \sin \delta_i = z_i + Z_i, \end{cases} \quad (4)$$

where X_i , Y_i , Z_i are rectangular geocentric equatorial coordinates of the Sun;

x_i , y_i , z_i are rectangular heliocentric equatorial coordinates of an investigated astronomical object.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

The geocentric coordinates of the Sun can be taken from the Solar System model. And the geocentric distances (ρ_i) and heliocentric coordinates (x_i, y_i, z_i) of an investigated astronomical are unknown in system 4. General representation of the Väisälä algorithm requires the 2 nearest astronomical observations of the same investigated object at times t_1 and t_2 . So, we can calculate the primary orbit from such two observations using a set of the following parameters ($t_1, \alpha_1, \delta_1, t_2, \alpha_2, \delta_2$).

To calculate the geocentric rectangular coordinates of an investigated object we can use the following system of equations:

$$\begin{cases} x_2 = \Delta_2 \cos \alpha_2 + X_2, \\ y_2 = \Delta_2 \sin \alpha_2 + Y_2, \\ z_2 = \Delta_2 \tan \delta_2 + Z_2, \end{cases} \quad (5)$$

where $\Delta_2 = \rho_2 \cos \delta_2$.

To calculate the geocentric velocity components of an object we can use the following system:

$$\begin{cases} \dot{x}_2 = \frac{\Delta_1 \cos \alpha_1 - F_1 x_2 + X_1}{G_1}, \\ \dot{y}_2 = \frac{\Delta_1 \sin \alpha_1 - F_1 y_2 + Y_1}{G_1}, \\ \dot{z}_2 = \frac{\Delta_1 \tan \delta_1 - F_1 z_2 + Z_1}{G_1}, \end{cases} \quad (6)$$

$$\begin{aligned} \Delta_1 &= \frac{F_1 r_2 + X_1 x_1 + Y_1 y_1 + Z_1 z_1}{x_2 \cos \alpha_1 + y_2 \sin \alpha_1 + z_2 \tan \delta_1}, \\ F_1 &= 1 - A\tau^2, G_1 = \tau - B\tau^3, \\ A &= \frac{r^3}{2}, B = \frac{A}{3}, \end{aligned} \quad (7)$$

where $\tau = k(t_1 - t_2)$ is a time interval between two nearest observations;
 k is a gravitation constant.

The determined parameters $(x_2, y_2, z_2, \dot{x}_2, \dot{y}_2, \dot{z}_2)$ will be used for calculation the Keplerian elements of the orbit of an investigated object at a time t_2 .

An architecture of a processing pipeline for data mining of the primary orbits and discovery of the new Solar System objects using the CoLiTec software and classical Väisälä method is presented in Fig. 1. Such method contains the next steps:

1. Perform the observations of the investigated SSOs.
2. Perform the classic data reduction process using the calibration bias, flat, and dark CCD frames.
3. Perform the astrometric reduction of the investigated SSOs using the CoLiTec software.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

4. Calculation of a primary orbit of the investigated SSOs by the Väisälä algorithm implemented as a tool.

5. Repeat the astronomical observations of the investigated SSOs to confirm a discovery of the new SSOs.

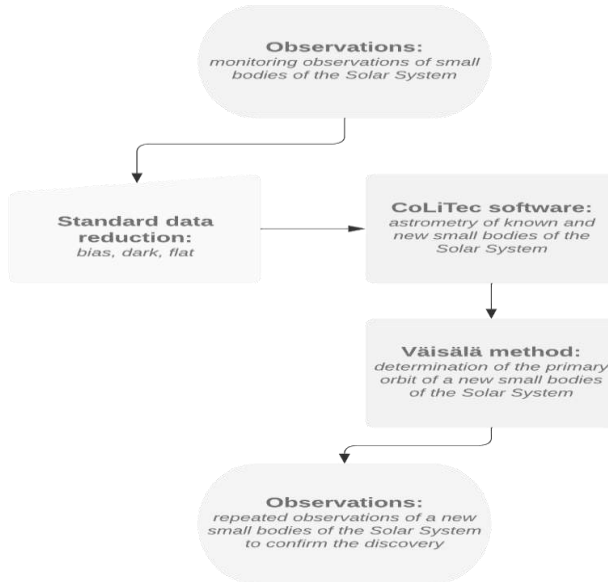


Figure 1. Architecture of a processing pipeline for data mining of the primary orbits and discovery of the new Solar System objects using the CoLiTec software and classical Väisälä method

4. Results

The created algorithm to determine a primary orbit and discoveries of the SSOs using the Väisälä algorithm works in combination with the CoLiTec software (<https://colitec.space>) [37]. The specific functional features related to the mathematical method for determining the primary orbits and discovery of asteroids in the CoLiTec software are:

- processing images with the very wide FOV (<10 degrees²);
- automated frame calibration [9];
- cosmetic frame correction;
- track-and-stack feature;
- brightness equalization [2];
- background alignment;

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

- astronomical image filtering [26];
- determining the contours of objects [38];
- image recognition [33];
- typical shape formation [14];
- detection of the moving objects (with near-zero, normal, fast apparent motion) [39];
- fully automated robust method of the astrometric reduction;
- fully automated robust method of the photometric reduction [23];
- support of the multi-threaded processing;
- On-Line Data Analysis System (OLDAS) for managing the processing pipeline;
- transferring of astronomical data with intermediate storage.

More extended details about the CoLiTec software are presented in these papers [40, 41, 42] and research [43]. The high-level processing pipeline with the developed modules and implemented methods of the CoLiTec software is presented in the Fig. 2.

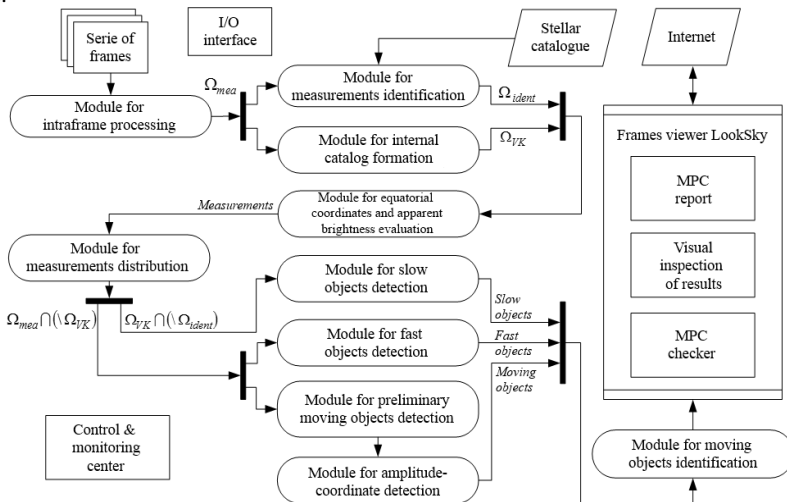


Figure 2. The high-level processing pipeline of the CoLiTec software

The CoLiTec software is installed at the different telescopes at the various observatories in Ukraine and around the world:

- OMT-800 and AZT-3 telescopes installed at the Odesa-Mayaky observatory [44];
- SANTEL-400AN telescope installed at the ISON-NM observatory;
- ISON-Uzhgorod [45];
- VNT and Celestron C11 telescopes installed at the Vihorlat Observatory [34];
- PROMPT-8 telescope installed at Cerro Tololo observatory [46];

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

- NARIT (National Astronomical Research Institute of Thailand) [47];
- AZT8 and Takahashi BRC-250M telescopes.

All listed above telescopes installed at the observatories have the official identifiers received from the Minor Planet Center (MPC) (<https://minorplanetcenter.net>) – MPC code from the International Astronomical Union (IAU) (<https://iau.org>).

Astronomical observations were made on the OMT-800 telescope installed at the Mayaky observational station of the Astronomical Observatory of the Odesa I. I. Mechnykov National University.

The official MPC code of the Odesa-Mayaky station is 583 (see Fig. 3) (<https://www.minorplanetcenter.net/iau/lists/ObsCodesF.html>):

Code	Long.	cos	sin	Name
580	15.4936	0.68242	+0.72862	Graz
581	22.80	0.830	-0.556	Sedgefield
582	1.2408	0.61682	+0.78447	Orwell Park
583	30.2717	0.69087	+0.72056	Odesa-Mayaky
584	30.2946	0.50213	+0.86189	Leningrad
585	30.52462	0.640067	+0.765748	Kyiv comet station
586	0.1423	0.73358	+0.67799	Pic du Midi
587	9.22918	0.697459	+0.714479	Sormano
588	11.25	0.715	+0.697	Eremo di Tizzano
589	12.64369	0.738223	+0.672386	Santa Lucia Stroncone
590	7.46	0.678	+0.734	Metzerlen

Figure 3. The official MPC codes of the Odesa-Mayaky observatory

The 0.8-m main hyperbolic mirror is installed at the OMT-800 telescope and has a useful focus ratio as $f = 1/2.7$. The FLI ML09000 CCD-camera is used as an image CCD-detector along with a 4-lens field corrector for a primary focus, which allows receiving the field of view (FOV) as $58.6' \times 58.6'$ and the scale of image as 1.15 arcseconds per pixel. The real photography of the OMT-800 telescope is presented in Fig. 4. During the astronomical observations at the OMT-800 telescope and research after processing the results, the next lost SSOs were found again:

- 2012 FN61 = 2010 VP219 (MPS 441842);
- 2017 AB8 = 2014 OD380 (MPS 525811).



Figure 4. The real photography of the OMT-800 telescope

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

Astronomical observations were made on the AZT-8 telescope installed at the Kyiv comet station of the “Lisnyky” observational station of the Taras Shevchenko National University of Kyiv. The official MPC code of the Kyiv comet station is 585 (see Fig. 5) (<https://www.minorplanetcenter.net/iau/lists/ObsCodesF.html>):

Code	Long.	cos	sin	Name
580	15.4936	0.68242	+0.72862	Graz
581	22.80	0.830	-0.556	Sedgefield
582	1.2408	0.61682	+0.78447	Orwell Park
583	30.2717	0.69087	+0.72056	Odesa-Mayaky
584	30.2946	0.50213	+0.86189	Leningrad
585	30.52462	0.640067	+0.765748	Kyiv comet station
586	0.1423	0.73358	+0.67799	Pic du Midi
587	9.22918	0.697459	+0.714479	Sormano
588	11.25	0.715	+0.697	Eremo di Tizzano
589	12.64369	0.738223	+0.672386	Santa Lucia Stroncone
590	7.46	0.678	+0.734	Metzerlen

Figure 5: The official MPC codes of the Kyiv comet station

The installed AZT-8 telescope is a telescope-reflector. The FLI PL4710 CCD-camera (63.5 mm) was used as an image CCD-detector, which allows receiving the FOV as 16.2'×16.7' and the scale of image as 0.948 arcseconds per pixel.

The real photography of the AZT-8 telescope is presented in Fig. 6.

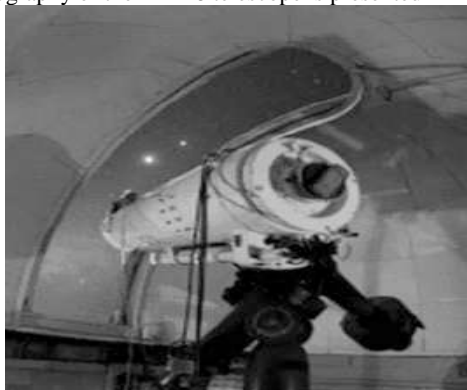


Figure 6. The real photography of the AZT-8 telescope



Figure 7. The detected astronomical object #3548

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

During the astronomical observations on the Kyiv comet station and research after processing the results, the new asteroid 2017 SV39 (MPS 828365) was firstly discovered and the next lost SSOs were found again:

- (536266) = 2007 HU101 = 2015 CX48 = 2017 ST39 (MPS 891037);
- (540584) = 2000 WN134 = 2007 XY37 = 2010 RD162 = 2015 DH168 = 2017 TS7 (MPS 23003).

Table 2

The main parameters of the detected astronomical object #3548

Parameter	Value
Epoch (Julian date)	2460400.5
Perihelion (Julian date)	2459673.41574
Argument of perihelion (°)	27.92959
Ascending node (°)	43.54101
Inclination (°)	8.05416
Eccentricity	0.0912182
Perihelion distance (AU)	4.7350370
Tisserand w.r.t. Jupiter	3.0
Semimajor axis (AU)	5.2103122
Mean anomaly (°)	60.25501
Mean daily motion (°/day)	0.08287210
Aphelion distance (AU)	5.686
Period (years)	11.89
P-vector [x]	0.32097397
P-vector [y]	0.84074355
P-vector [z]	0.43603439
Q-vector [x]	-0.94215715
Q-vector [y]	0.23653103
Q-vector [z]	0.23747207
Absolute magnitude	9.83
Phase slope	0.15

There are different examples of the discovered objects by the Odesa-Mayaky observatory (MPC code is 583) are presented below.

The detected astronomical object #3548 is presented in Fig. 7.

The main parameters of the detected astronomical object #3548 (orbit type: Jupiter Trojan) are presented in Table 1. All such parameters were received from the official MPC web-site – https://www.minorplanetcenter.net/db_search/show_object?utf8=%E2%9C%93&object_id=3548.

The observation details of the detected astronomical object #3548 by the Odesa-Mayaky observatory (MPC code is 583) are presented in Fig. 8 below.

The new detected asteroid 2017 QX33 (MPS 813479) is presented in Fig. 9.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

Date (UT)	J2000 RA	J2000 Dec	Magn	Location	Ref
2021 11 15.271637	03 43 08.51	+22 14 11.9	16.17 G	G96 – Mt. Lemmon Survey	MPS 1513473
2021 11 15.277205	03 43 08.31	+22 14 11.6	16.18 G	G96 – Mt. Lemmon Survey	MPS 1513473
2021 11 21.85044	03 39 08.35	+22 08 16.5	15.7 R	583 – Odesa-Mayaky	MPS 1518978
2021 11 21.85692	03 39 08.10	+22 08 16.1	15.7 R	583 – Odesa-Mayaky	MPS 1518978
2021 11 21.86340	03 39 07.86	+22 08 15.8	15.7 R	583 – Odesa-Mayaky	MPS 1518978
2021 11 21.86988	03 39 07.63	+22 08 15.4	15.7 R	583 – Odesa-Mayaky	MPS 1518978
2021 11 21.87637	03 39 07.38	+22 08 15.0	15.7 R	583 – Odesa-Mayaky	MPS 1518978
2021 11 21.88285	03 39 07.15	+22 08 14.7	15.7 R	583 – Odesa-Mayaky	MPS 1518978
2021 11 21.89581	03 39 06.65	+22 08 14.0	15.7 R	583 – Odesa-Mayaky	MPS 1518978
2021 11 23.446970	03 38 10.11	+22 06 43.3	15.96 o	T08 – ATLAS-MLO, Mauna Loa	MPS 1518978
2021 11 23.451328	03 38 09.94	+22 06 43.1	15.93 o	T08 – ATLAS-MLO, Mauna Loa	MPS 1518978
2021 11 23.453731	03 38 09.855	+22 06 42.88	15.85 i	F52 – Pan-STARRS 2, Haleakala	MPS 1518978

Figure 8. The observation details of the detected astronomical object #3548 by the Odesa-Mayaky observatory

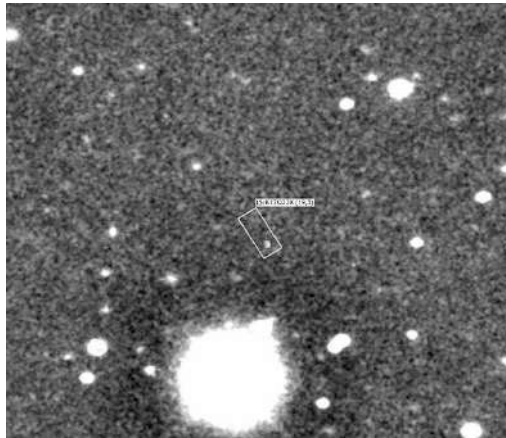


Figure 9. The new detected asteroid 2017 QX33 (MPS 813479)

The main parameters of the new detected asteroid 2017 QX33 (orbit type: Jupiter Trojan) are presented in Table 2.

All such parameters were received from the official MPC web-site – https://www.minorplanetcenter.net/db_search/show_object?utf8=%E2%9C%93&object_id=2017+QX33.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

Table 2

The main parameters of the new detected asteroid 2017 QX33

Parameter	Value
Epoch (Julian date)	2460400.5
Perihelion (Julian date)	2459294.27298
Argument of perihelion (°)	173.50876
Ascending node (°)	193.83235
Inclination (°)	7.66939
Eccentricity	0.2957998
Perihelion distance (AU)	1.6009058
Tisserand w.r.t. Jupiter	3.5
Semimajor axis (AU)	2.2733673
Mean anomaly (°)	318.08555
Mean daily motion (°/day)	0.28754090
Aphelion distance (AU)	2.946
Period (years)	3.43
P-vector [x]	0.99156124
P-vector [y]	0.11213188
P-vector [z]	0.06505954
Q-vector [x]	-0.12565127
Q-vector [y]	0.95478909
Q-vector [z]	0.26942450
Absolute magnitude	18.58
Phase slope	0.15

The observation details of the new detected asteroid 2017 QX33 by the Odesa-Mayak observatory (MPC code is 583) are presented in Fig. 10 below.

2017 QX33

Initial reported observation by Odesa-Mayak on 2017-08-25.

Date (UT)	J2000 RA	J2000 Dec	Magn	Location	Ref
2017 07 29.60683	23 08 02.059	+07 14 27.70	20.3 H	F51 - Pan-STARRS 1, Haleakala	MPS 1049947
2017 08 25.90477	23 11 03.83	+06 26 26.1	19.2	583 - Odesa-Mayak	MPS 813479
2017 08 25.91872	23 11 03.64	+06 26 20.5	18.9	583 - Odesa-Mayak	MPS 813479
2017 08 25.93113	23 11 03.41	+06 26 15.2	19.7	583 - Odesa-Mayak	MPS 813479
2017 08 26.67447	23 10 52.31	+06 20 34.6	19.4 R	D29 - Purple Mountain Observatory, XuYi Station	MPS 813479
2017 08 26.68862	23 10 52.03	+06 20 28.4	19.1 R	D29 - Purple Mountain Observatory, XuYi Station	MPS 813479
2017 08 26.70276	23 10 51.75	+06 20 21.3	19.6 R	D29 - Purple Mountain Observatory, XuYi Station	MPS 813479
2017 08 29.45836	23 10 04.96	+05 57 09.3	19.2 o	T05 - ATLAS-HKO, Haleakala	MPS 813479
2017 08 29.46636	23 10 04.75	+05 57 05.0	19.1 o	T05 - ATLAS-HKO, Haleakala	MPS 813479
2017 08 29.47484	23 10 04.55	+05 57 00.9	19.1 o	T05 - ATLAS-HKO, Haleakala	MPS 813479
2017 08 29.48254	23 10 04.42	+05 56 55.5	18.9 o	T05 - ATLAS-HKO, Haleakala	MPS 813479
2017 08 30.01831	23 09 54.28	+05 51 57.4	18.9	583 - Odesa-Mayak	MPS 813479
2017 08 30.03589	23 09 53.83	+05 51 46.6	19.3	583 - Odesa-Mayak	MPS 813479
2017 08 30.05153	23 09 53.49	+05 51 38.6	19.3	583 - Odesa-Mayak	MPS 813479
2017 08 31.44004	23 09 26.97	+05 38 31.3	19.0 o	T08 - ATLAS-MLO, Mauna Loa	MPS 1049047

Figure 10. The observation details of the new detected asteroid 2017 QX33 by the Odesa-Mayak observatory

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

The detected astronomical object #21900 is presented in Fig. 11.



Figure 11. The detected astronomical object #21900

The main parameters of the detected astronomical object #21900 (orbit type: Jupiter Trojan) are presented in Table 3.

All such parameters were received from the official MPC web-site – https://www.minorplanetcenter.net/db_search/show_object?utf8=%E2%9C%93&object_id=21900.

Table 3

The main parameters of the detected astronomical object #21900

Parameter	Value
Epoch (Julian date)	2460400.5
Perihelion (Julian date)	2460053.88476
Argument of perihelion (°)	182.13714
Ascending node (°)	258.55425
Inclination (°)	8.46880
Eccentricity	0.0376942
Perihelion distance (AU)	4.9306527
Tisserand w.r.t. Jupiter	3.0
Semimajor axis (AU)	5.1237899
Mean anomaly (°)	29.45537
Mean daily motion (°/day)	0.08498000
Aphelion distance (AU)	5.317
Period (years)	11.6
P-vector [x]	0.16215070
P-vector [y]	0.90751066
P-vector [z]	0.38746814
Q-vector [x]	-0.97615189
Q-vector [y]	0.20496114
Q-vector [z]	-0.07154318
Absolute magnitude	10.06
Phase slope	0.15

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

The observation details of the detected astronomical object #21900 by the Odesa-Mayaky observatory (MPC code is 583) are presented in Fig. 12 below.

Date (UT)	J2000 RA	J2000 Dec	Magn	Location	Ref
2021 10 16.380259	01 51 43.96	+19 49 30.3	16.62 G	G96 – Mt. Lemmon Survey	MPS 1490408
2021 10 16.385973	01 51 43.77	+19 49 29.3	16.64 G	G96 – Mt. Lemmon Survey	MPS 1490408
2021 10 16.386116	01 51 43.87	+19 49 29.7	16.47 o	T05 – ATLAS-HKO, Haleakala	MPS 1490408
2021 10 16.391670	01 51 43.59	+19 49 28.2	16.66 G	G96 – Mt. Lemmon Survey	MPS 1490408
2021 10 16.392126	01 51 43.68	+19 49 28.6	16.49 o	T05 – ATLAS-HKO, Haleakala	MPS 1490408
2021 10 16.397352	01 51 43.41	+19 49 27.2	16.66 G	G96 – Mt. Lemmon Survey	MPS 1490408
2021 10 17.82575	01 50 59.08	+19 44 51.7	16.7 R	583 – Odesa-Mayaky	MPS 2132569
2021 10 17.82943	01 50 58.96	+19 44 51.3	16.8 R	583 – Odesa-Mayaky	MPS 2132569
2021 10 17.83681	01 50 58.75	+19 44 49.5	16.7 R	583 – Odesa-Mayaky	MPS 2132569
2021 10 17.84049	01 50 58.61	+19 44 48.4	16.7 R	583 – Odesa-Mayaky	MPS 2132569
2021 10 17.84425	01 50 58.51	+19 44 48.1	16.7 R	583 – Odesa-Mayaky	MPS 2132569
2021 10 17.84792	01 50 58.38	+19 44 47.2	16.6 R	583 – Odesa-Mayaky	MPS 2132569
2021 10 17.85160	01 50 58.22	+19 44 46.5	16.6 R	583 – Odesa-Mayaky	MPS 2132569
2021 10 17.85542	01 50 58.08	+19 44 46.1	16.7 R	583 – Odesa-Mayaky	MPS 2132569
2021 10 17.85910	01 50 58.02	+19 44 45.3	16.9 R	583 – Odesa-Mayaky	MPS 2132569
2021 10 18.446572	01 50 39.61	+19 42 51.4	16.64 o	T08 – ATLAS-MLO, Mauna Loa	MPS 1490408
2021 10 18.452573	01 50 39.43	+19 42 50.3	16.73 o	T08 – ATLAS-MLO, Mauna Loa	MPS 1490408
2021 10 18.461006	01 50 39.16	+19 42 48.5	16.57 o	T08 – ATLAS-MLO, Mauna Loa	MPS 1490408
2021 10 18.464113	01 50 39.05	+19 42 47.9	16.69 o	T08 – ATLAS-MLO, Mauna Loa	MPS 1490408
2021 10 24.459891	01 47 30.770	+19 22 15.84	16.33 i	F52 – Pan-STARRS 2, Haleakala	MPS 1492531
2021 10 24.472773	01 47 30.351	+19 22 13.03	16.29 i	F52 – Pan-STARRS 2, Haleakala	MPS 1492531
2021 10 24.485810	01 47 29.932	+19 22 10.21	16.32 i	F52 – Pan-STARRS 2, Haleakala	MPS 1492531
2021 10 24.498698	01 47 29.516	+19 22 07.45	16.33 i	F52 – Pan-STARRS 2, Haleakala	MPS 1492531

Figure 12. The observation details of the detected astronomical object #21900 by the Odesa-Mayaky observatory

5. Conclusions

We present a processing pipeline for data mining of the primary orbits and discovery of the new Solar System objects using the CoLiTec software and classical Väisälä method. The literature review showed the benefits and disadvantages of the existing methods and algorithms. So, we made a decision to improve such algorithms for the better accuracy and quality of detection of the new or lost SSOs.

The first step of such computational algorithm is to perform the observations and the standard data reduction. It was performed in scope of the common mathematical methods for the astronomical image processing and numeric analysis implemented in the CoLiTec software. It includes inverse median filtration, calibration using the master frames, object detection, etc. Then the orbit parameters, like the right ascension and declination, were determined for a certain moment. After receiving the two observations of an investigated object at different times, the classic Väisälä method is applied. The created algorithm is implemented as a processing pipeline

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

that contains a cooperation between the CoLiTec software pipeline and a special implemented plugin based on the general Väisälä algorithm. Such a plugin is realized as a console application based on the programming language Delphi. The created mathematical method was verified in practice based on the classical mathematical models and fuzzy clustering data arrays with omitted observations as well as statistical modeling [48]. With help of the developed processing pipeline, the several new SSOs (Main-belt asteroid 2017 AB8 (2014 OD380), Mars-crossing asteroid 2017 QX33, Main-belt asteroid 2017 RV12) were firstly discovered and some of the lost SSOs were found again during the astronomical observations at the Kyiv comet station and the Odesa-Mayaky observatory [49].

The further research will be conducted on processing newly created series of CCD frames with the astronomical SSOs by the new Lemur software of the Collection Light Technology (CoLiTec) project [50].

6. Acknowledgements

The research was supported by the Ukrainian project of fundamental scientific research “Development of computational methods for detecting objects with near-zero and locally constant motion by optical-electronic devices” #0124U000259 in 2024-2026 years.

7. References

- [1] S. Khlamov, I. Tabakova, T. Trunova, and Z. Deineko, Machine Vision for Astronomical Images Using the Canny Edge Detector, CEUR Workshop Proceedings, vol. 3384, pp. 1–10, 2022.
- [2] Š. Parimucha, et al., CoLiTecVS – A new tool for an automated reduction of photometric observations, Contributions of the Astronomical Observatory Skalnaté Pleso, vol. 49, issue 2, pp. 151-153, 2019.
- [3] V. G. Godunova, A. O. Simon, Y. S. Markus, et al., Photometric and colorimetric studies of target objects using small and medium-size telescopes, Contributions of the Astronomical Observatory Skalnaté Pleso, vol. 54, issue 2, pp. 205-212, 2024. doi: 10.31577/CAOSP.2024.54.2.205.
- [4] S. Khlamov, et al., Automated data mining of the reference stars from astronomical CCD frames, CEUR Workshop Proceedings, vol.3668,pp.83–97, 2024.
- [5] K. D. Borne, Scientific data mining in astronomy, Next Generation of Data Mining, Chapman and Hall/CRC, pp. 115-138, 2008.
- [6] I. B. Vavilova, Y. S. Yatskiv, L. K. Pakuliak, et al., UkrVO astroinformatics software and web-services, Proceedings of the International Astronomical Union, vol. 12, issue S325, pp. 361-366, 2016. doi: 10.1017/S1743921317001661.
- [7] V. Akhmetov, et al., Fast coordinate cross-match tool for large astronomical catalogue, Advances in Intelligent Systems and Computing, vol. 871, pp. 3–16, 2019. doi: 10.1007/978-3-030-01069-0_1.
- [8] G. Adam, P. Kontaxis, L. Doulos, E.-N. Madias, C. Bouroussis, and F. Topalis, Embedded Microcontroller with a CCD Camera as a Digital Lighting Control System, Electronics, vol. 8, issue 1, 2019. doi: 10.3390/electronics8010033.
- [9] D. Oszkiewicz, et al., Spins and shapes of basaltic asteroids and the missing mantle problem, Icarus, vol. 397, 115520, 2023. doi: 10.1016/j.icarus.2023.115520.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

- [10] V. Troianskyi, P. Kankiewicz, and D. Oszkiewicz, Dynamical evolution of basaltic asteroids outside the Vesta family in the inner main belt, *Astronomy and Astrophysics*, vol. 672, A97, 2023. doi: 10.1051/0004-6361/202245678.
- [11] V. Akhmetov, et al., Cloud computing analysis of Indian ASAT test on March 27, 2019, *IEEE International Scientific-Practical Conference: Problems of Infocommunications Science and Technology*, pp. 315–318, 2019. doi: 10.1109/PICST47496.2019.9061243.
- [12] E. L. Lehmann, J. P. Romano, and G. Casella, *Testing statistical hypotheses*, vol. 3, New York: Springer, 2005.
- [13] V. Troianskyi, V. Kashuba, O. Bazyey, et al., First reported observation of asteroids 2017 AB8, 2017 QX33, and 2017 RV12, *Contributions of the Astronomical Observatory Skalnaté Pleso*, vol. 53, pp. 5-15, 2023. doi: 10.31577/caosp.2023.53.2.5.
- [14] V. Savanevych, et al., Formation of a typical form of an object image in a series of digital frames, *Eastern-European Journal of Enterprise Technologies*, vol. 6, issue 2-120, pp. 51–59, 2022. doi: 10.15587/1729-4061.2022.266988.
- [15] W. Burger, and M. Burge, *Principles of digital image processing: fundamental techniques*, New York, NY: Springer, 2009.
- [16] V. Savanevych, et al., Mathematical methods for an accurate navigation of the robotic telescopes, *Mathematics*, vol. 11, issue 10, 2246, 2023. doi: 10.3390/math11102246.
- [17] T. Ando, *Bayesian model selection and statistical modeling*, CRC Press, 2010.
- [18] V. Vlasenko, et al., Devising a procedure for the brightness alignment of astronomical frames background by a high frequency filtration to improve accuracy of the brightness estimation of objects, *Eastern-European Journal of Enterprise Technologies*, vol. 2, issue 2-128, pp. 31–38, 2024. doi: 10.15587/1729-4061.2024.301327.
- [19] S. Khlamov, et al., Development of computational method for matched filtration with analytic profile of the blurred digital image, *Eastern-European Journal of Enterprise Technologies*, vol. 5, issue 4-119, pp. 24–32, 2022. doi: 10.15587/1729-4061.2022.265309.
- [20] M. Dadkhah, et al., Methodology of wavelet analysis in research of dynamics of phishing attacks, *International Journal of Advanced Intelligence Paradigms*, vol. 12(3-4), pp. 220-238, 2019. doi: 10.1504/IJAIP.2019.098561.
- [21] L. Kirichenko, A.S.A. Alghawli, T. Radivilova, Generalized approach to analysis of multifractal properties from short time series, *International Journal of Advanced Computer Science and Applications*, vol. 11, issue 5, pp. 183–198, 2020. doi: 10.14569/IJACSA.2020.0110527.
- [22] V. Savanevych, et al., CoLiTecVS software for the automated reduction of photometric observations in CCD-frames, *Astronomy and Computing*, vol. 40 (100605), 15 p., 2022. doi: 10.1016/j.ascom.2022.100605.
- [23] S. Khlamov, et al., Development of the matched filtration of a blurred digital image using its typical form. *Eastern-European Journal of Enterprise Technologies*, vol. 1, issue 9 (121), pp. 62-71, 2023. doi: 10.15587/1729-4061.2023.273674.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

- [24] C. A. Politsch, et al., Trend filtering–I. A modern statistical tool for time-domain astronomy and astronomical spectroscopy, *MNRAS*, vol. 492, issue 3, pp. 4005–4018, 2020. doi: 10.1093/mnras/staa106.
- [25] R. Klette, *Concise computer vision. An Introduction into Theory and Algorithms*, London: Springer, 233, 2014. doi: 10.1007/978-1-4471-6320-6.
- [26] S. Khlamov, I. Tabakova, T. Trunova, Recognition of the astronomical images using the Sobel filter. In *Proceedings of the International Conference on Systems, Signals, and Image Processing*, 4 p., 2022. doi: 10.1109/IWSSIP55020.2022.9854425.
- [27] Y. Bodyanskiy, S. Popov, F. Brodetskyi, and O. Chala, Adaptive Least-Squares Support Vector Machine and its Combined Learning-Selflearning in Image Recognition Task. In *Proceedings of the IEEE 17th International Conference on Computer Sciences and Information Technologies*, 2022. doi: 10.1109/csit56902.2022.10000518.
- [28] R. Dhanalakshmi, et al., Onboard Pointing Error Detection and Estimation of Observation Satellite Data Using Extended Kalman Filter, *Computational Intelligence and Neuroscience*, 2022, pp. 1–8. doi: 10.1155/2022/4340897.
- [29] V. Savanevych, et al., Selection of the reference stars for astrometric reduction of CCD-frames, *Advances in Intelligent Systems and Computing*, vol. 1080, pp. 881–895, 2020. doi: 10.1007/978-3-030-33695-0_57.
- [30] M. Lösler, C. Eschelbach, and S. Riepl, A modified approach for automated reference point determination of SLR and VLBI telescopes, *Technisches Messen*, vol. 85 (10), pp. 616–626, 2018. doi: 10.1515/teme-2018-0053.
- [31] W. Shan, Y. Yi, J. Qiu, and A. Yin, Robust Median Filtering Forensics Using Image Deblocking and Filtered Residual Fusion, *IEEE Access*, vol. 7, pp. 17174–17183, 2019. doi: 10.1109/access.2019.2894981.
- [32] L. Kirichenko, P. Zinchenko, and T. Radivilova, Classification of time realizations using machine learning recognition of recurrence plots, *Advances in Intelligent Systems and Computing*, vol. 1246, pp. 687–696, 2021. doi: 10.1007/978-3-030-54215-3_44.
- [33] S. Khlamov, et al., The astronomical object recognition and its near-zero motion detection in series of images by in situ modeling, *Proceedings of the 29th IEEE International Conference on Systems, Signals, and Image Processing, IWSSIP 2022, Sofia, Bulgaria, June 1st – 3rd, 4 p.*, 2022. doi: 10.1109/IWSSIP55020.2022.9854475.
- [34] I. Kudzej, et al., CoLiTecVS – A new tool for the automated reduction of photometric observations, *Astronomische Nachrichten*, vol. 340, pp. 68–70, 2019. doi: 10.1002/asna.201913562.
- [35] D. Oszkiewicz, et al., Spin rates of V-type asteroids, *Astronomy & Astrophysics*, vol. 643, A117, 2020. doi: 10.1051/0004-6361/202038062.
- [36] Hu Xuanyu, C. K. Shum, and M. Bevis, A triaxial reference ellipsoid for the Earth, *Journal of Geodesy*, vol. 97(4), 29, 2023. doi: 10.1007/s00190-023-01717-1.
- [37] S. Khlamov, et al., Machine vision for astronomical images using the modern image processing algorithms implemented in the CoLiTec software, *Measurements*

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

and Instrumentation for Machine Vision, Chapter 12: CRC Press, Taylor & Francis Group, pp. 269-310, 2024. doi: 10.1201/9781003343783-12.

[38] H. Khudov, I. Ruban, O. Makoveichuk, H. Pevtsov, V. Khudov, I. Khizhnyak, S. Fryz, V. Podlipaiev, Y. Polonskyi, R. Khudov, Development of methods for determining the contours of objects for a complex structured color image based on the ant colony optimization algorithm, EUREKA, Physics and Engineering, vol. 2020, issue 1, pp. 34–47, 2020. doi: 10.21303/2461-4262.2020.001108.

[39] S. Khlamov, et al., Development of computational method for detection of the object's near-zero apparent motion on the series of CCD–frames, EEJET, vol. 2, issue 9(80), pp. 41-48, 2016. doi: 10.15587/1729-4061.2016.65999.

[40] S. Khlamov, et al., Big astronomical datasets and discovery of new celestial bodies in the Solar System in automated mode by the CoLiTec software, Knowledge Discovery in Big Data from Astronomy and Earth Observation, Astrogeoinformatics, pp. 331–345, 2020. doi: 10.1016/B978-0-12-819154-5.00030-8.

[41] V. Savanevych, et al., A new method based on the subpixel Gaussian model for accurate estimation of asteroid coordinates, MNRAS, vol. 451, issue 3, pp. 3287–3298, 2015. doi: 10.1093/mnras/stv1124.

[42] L. Mykhailova, et al., Method of maximum likelihood estimation of compact group objects location on CCD-frame, Eastern-European Journal of Enterprise Technologies, vol. 5, issue 4, pp. 16-22, 2014. doi:10.15587/1729-4061.2014.28028.

[43] V. Savanevych, et al., Comparative analysis of the positional accuracy of CCD measurements of small bodies in the solar system software CoLiTec and Astrometrica, Kinematics and Physics of Celestial Bodies, vol. 31, issue 6, pp. 302–313, 2015. doi: 10.3103/S0884591315060045.

[44] S. Kashuba, M. Tsvetkov, N. Bazyey, E. Isaeva, and V. Golovnia, The Simeiz plate collection of the ODESSA astronomical observatory, Proceedings of the 11th Bulgarian-Serbian Astronomical Conference, pp. 207-216, 2018.

[45] V. Kudak, V. Epishev, V. Perig, and I. Neybauer, Determining the orientation and spin period of TOPEX/Poseidon satellite by a photometric method, Astrophysical Bulletin, vol. 72, issue 3, pp. 340-348, 2017. doi: 10.1134/S1990341317030233.

[46] T. Li, D. DePoy, J. Marshall, et al., Monitoring the atmospheric throughput at Cerro Tololo Inter-American Observatory with aTmCam, Ground-based and Airborne Instrumentation for Astronomy V, vol. 9147, pp. 2194–2205, 2014.

[47] S. Rattanasoon, E. Semenko, D. Mkrtichian, and S. Poshychinda, Spectroscopic Devices for Asteroseismology With Small Telescopes in NARIT, arXiv -> astro-ph, vol. 2307.03985, 5 p., 2023. doi: 10.48550/arXiv.2307.03985.

[48] V. Shvedun, et al., Statistical modelling for determination of perspective number of advertising legislation violations, Actual Problems of Economics, vol. 184, issue 10, pp. 389-396, 2016.

[49] V. Troianskyi, V. Godunova, A. Serebryanskiy, et al., Optical observations of the potentially hazardous asteroid (4660) Nereus at opposition 2021, Icarus, vol. 420, 116146, 2024. doi: 10.1016/j.icarus.2024.116146.

[50] S. Khlamov, et al., Data Mining of the Astronomical Images by the CoLiTec Software, CEUR Workshop Proceedings, vol. 3171, pp. 1043–1055, 2022.

ОТРИМАННЯ ДАНИХ ПЕРВИННИХ ОРБИТ ОБ'ЄКТІВ
СОНЯЧНОЇ СИСТЕМИ ЗА ДОПОМОГОЮ ПРОГРАМНОГО
ЗАБЕЗПЕЧЕННЯ COLITEC ТА МЕТОДУ VÄISÄLÄ

Ph.D. В. Троянський ORCID: 0000-0002-5899-2300

*Одеський національний університет імені І. І. Мечникова, Україна
E-mail: v.troianskyi@onu.edu.ua*

Dr.Sci. О. Базей ORCID: 0000-0001-6886-4575

*Одеський національний університет імені І. І. Мечникова, Україна
E-mail: o.bazyey@onu.edu.ua*

Ph.D. Г. Охотко ORCID: 0009-0002-1403-4298

*Одеський національний університет імені І. І. Мечникова, Україна
E-mail: hannaohotko@gmail.com*

Ph.D. С. Хламов 0000-0001-9434-1081

*Харківський національний університет радіоелектроніки, Україна
E-mail: sergii.khlamov@gmail.com*

***Анотація.** Розділ присвячено конвєсеру обробки даних первинних орбіт і виявлення нових об'єктів Сонячної системи за допомогою програмного забезпечення CoLiTec і класичного методу Вяйсяля. Першим кроком такого конвєсера обробки є виконання послідовних астрономічних спостережень і класичного астрометричного редукування даних. Він реалізований як комбінація загальних математичних алгоритмів і методів обробки астрономічних кадрів, інкапсульованих у програмне забезпечення CoLiTec. Він містить зворотний медіанний фільтр, астрономічне калібрування з використанням калібрувальних майстер-кадрів (bias, dark, flat, dark-flat), виявлення астрономічних об'єктів і їх траєкторій у серії кадрів та інші дуже корисні та важливі функції. Після цього розраховуються особливі параметри орбіти об'єкта (пряме сходження і схилення) в певний час. Коли ми отримуємо принаймні два спостереження одного і того ж досліджуваного об'єкта в різні моменти, можна застосувати класичний алгоритм Вяйсяля. Для цього розраховується первинна орбіта з двох найближчих спостережень. Потім обчислюються геоцентричні прямокутні координати та відповідні геоцентричні компоненти швидкості. Це дає нам можливість визначати кеплерівські елементи орбіти досліджуваного об'єкта в будь-який час, який нас цікавить. Розроблений алгоритм реалізовано у вигляді конвєсера обробки, що включає комбінацію програмного забезпечення CoLiTec та створеного інструменту з інкапсуляцією методу Вяйсяля. Практично перевірено створений конвєсер обробки даних первинних орбіт і відкриття нових об'єктів Сонячної системи за допомогою програмного забезпечення CoLiTec і класичного методу Вяйсяля. З його допомогою вперше повідомляється про кілька нових астероїдів і знайдено кілька втрачених малих тіл Сонячної системи на Київській кометній станції та в обсерваторії Одеса – Маяки.*

***Ключові слова:** Інтелектуальний аналіз даних, конвєсер обробки, астрономічні спостереження, програмне забезпечення CoLiTec, метод Вяйсяля, обробка зображень, калібрування зображення, астрометричне зменшення, фотометричне зменшення, виявлення об'єктів, позиційні координати, визначення орбіти, об'єкти Сонячної системи*

**ADVANCES
IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES**

UDC 004.623

**ARTIFICIAL INTELLIGENCE IN THE DIAGNOSIS, PROGNOSIS
AND TREATMENT OF DIABETIC NEOVASCULAR GLAUCOMA**

Dr.Sci. V. Vychuzhanin ORCID: 0000-0002-6302-1832

Odessa Polytechnic National University, Ukraine

E-mail: vychuzhanin.o.v@op.edu.ua

Ph.D. O. Guzun ORCID: 0009-0003-6873-8503

*ISI "The Filatov Institute of Eye Diseases and Tissue Therapy of the National
Academy of Medical Sciences of Ukraine", Ukraine*

E-mail: olga.v.guzun@gmail.com

Ph.D. M. Rudnichenko ORCID: 0000-0002-7343-8076

Odessa Polytechnic National University, Ukraine

E-mail: nickolay.rud@gmail.com

Ph.D. O. Zadorozhnyy ORCID: 0000-0003-0125-2456

*ISI "The Filatov Institute of Eye Diseases and Tissue Therapy of the National
Academy of Medical Sciences of Ukraine", Ukraine*

E-mail: zadoroleg2@gmail.com

Ph.D. A.Korol ORCID: 0000-0003-0516-308X

*ISI "The Filatov Institute of Eye Diseases and Tissue Therapy of the National
Academy of Medical Sciences of Ukraine", Ukraine*

E-mail: andrii.r.korol@gmail.com

Abstract. *This work is focused on key aspects of the diagnosis, prognosis and treatment of neovascular glaucoma of diabetic origin based on machine learning approaches and, in particular, various architectures artificial neural models. An analysis of the relevance, priority provisions and advantages of using machine learning methods is carried out, the existing approaches used in modern literature in the context of the topic under study are considered, the specifics of their integration into the process of diagnostic analysis of the feature space of an aggregated and labeled by the authors data set on patients with visual problems are described, in particular, those suffering from neovascular glaucoma of diabetic origin. A correlation analysis of input features was carried out, 3 different models of artificial neural networks were built, trained and tested, metrics for assessing the accuracy of their work were experimentally calculated and studied, and statistical indicators were determined, including errors and losses, characterizing their generalizing ability. Analysis of the results obtained from the studies made it possible to identify the prevailing input features and evaluate their impact on the target output variable and the overall significance in the feature space of the data set, as well as to establish the most suitable models for data analysis in terms of their accuracy and speed. The conducted research made it possible to establish the fact of a greater degree deep learning artificial neural networks models fully connected adaptability for the analyzed data set.*

Keywords. *Artificial intelligence, neovascular glaucoma, diagnosis eye treatment, neural networks, data analysis, data mining, machine learning*

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

1. Introduction

Currently, the volumes of heterogeneous information collected during the examination of patients in various fields of medicine are constantly increasing [1]. This is due to the tendency to integrate various technical means and software systems for diagnosing human body organs diseases, especially vision organs, which make it possible to measure and process numerous quantitative and qualitative parameters characterizing the nature, stage and disease complexity. The development of artificial intelligence (AI) technology in medical decision making allows for the simultaneous analysis of an infinite variables number. AI technologies provide improving patient care in medical decision making and require physicians and computer scientists to have a successful mutual understanding of both technology and medical practice. Recently, thanks to AI methods, significant advances have been made in the diagnosis of ophthalmic pathologies.

With their help, data from visual fields, optic nerve structure (for example, obtained using optical coherence tomography (OCT), biomechanical ocular properties and their combination are successfully analyzed and classified to determine the severity of the disease, its progression and/or referral for specialized treatment. Diagnostic search algorithms for patients with glaucoma have undergone further changes, becoming more and more complex, and to improve existing methodologies it is necessary to use more reliable classification diseases signs.

A significant contribution in this direction is made by modern methods and models for assessing and predicting the effectiveness of patient treatment, actively developed and implemented by specialists in the field of prevention and eye pathologies diagnosis. It should be noted that in the process of inflammation assessing indicators and intraocular circulation in patients collected during statistical data examination, an important aspect of the procedure for their analysis is indicators diagnostic significance [2]. This is relevant both for identifying and formalizing key factors that have the greatest impact on the visual organs integral state, and for developing and implementing preventive measures and developing protocols ophthalmic diseases effective treatment.

Due to the lack of clearly identified patterns and correlations in the feature space of aggregated diagnostic data for the patients' vision organs as well as due to the high degree of uncertainty in mutual influence, carrying out the processes of assessing and analyzing data in a manual format is difficult and labor-intensive. Therefore, it is rational to use modern methods of data mining, in particular machine learning (ML) algorithms, in order to automate the process of searching for hidden patterns in data and assessing the level of feature space diagnostic significance, which is especially justified in the presence of large data volumes [3]. This allows us to provide solutions to various applied problems in the field of ophthalmology. In particular, it helps to increase the efficiency of the decision support process for assessing the patient's condition and the use of targeted treatments for diabetic neovascular glaucoma [4] through the use of ML models to automate data research and search for individual signs correlations with each other. There are significant

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

results from the use of ML in the analysis of such pathological eye conditions as diabetic retinopathy, age-related macular degeneration, macular edema, glaucoma, cataracts, etc. In this case, color fundus photographs, images obtained during fluorescein angiography and autofluorescence, OCT scans, fields of view [5, 6, 7].

The defining characteristic of ML algorithms is the quality of their predictions, which improves with experience. The more data provided, the better the forecasting model. In this context, difficulties arise due to various factors, including [8]:

- insufficiently high generalization ability of classical ML models;
- absence of memory effect in models;
- insufficient adaptability of models to data, taking into account the specifics under consideration;
- the need to compile ML models ensembles to ensure a higher degree of accuracy of the forecast values they generate;
- time costs for preliminary data scaling and preprocessing.

In this regard, a perspective way is to use more advanced, modern and efficient deep ML models, which are artificial neural networks (ANN) of various architectures, topologies and hierarchically interconnected. An important aspect in the problem we are considering is the study of different ML models among themselves to experimentally identify an estimate of the most appropriate hyperparameters values, which affect the output metrics for assessing used models quality [9]. In this context, an approach based on deep learning and ANN makes it possible to more effectively solve classification and regression problems, taking into account the specifics of the application area under consideration, as well as to form various hybrid models that can have greater generalization ability and be more flexible in comparison with classical ML approaches, eliminate the imbalance of the feature space, perform the functions of data normalization and reduce the likelihood of overtraining models through the introduction of regularization methods [1].

An additional important aspect is the ability to minimize the risk of generating contradictory results from ANN models, for example, by integrating bagging and boosting techniques when creating model's ensembles. In this regard, ANN using is more appropriate within the framework of the topic under consideration.

2. Analysis existing researches

In the medical field, there is an active use of various approaches, most often based on statistical methods and ML models for the analysis and evaluation of experimentally obtained results of diagnosis and various diseases treatment, including vision organs.

Thus, the authors [10] adapt ML learning algorithms to solve the classification problem, achieving significant results of both high accuracy and completeness on the collected dataset of ophthalmological indicators.

However, the data analyzed by the authors is often not complete and contains signs of synthesized subsamples, which complicates the procedure for assessing metric indicators. In [11], the authors use fully connected ANN models, comparing

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

their work with each other and existing methods for classifying ML data, which is appropriate to demonstrate the capabilities and performance of these models in the context of their deployment in real diagnostic software and hardware tools for data analysis and evaluation. The effectiveness of using ML was also established by the authors [12] in studies in the field of treating respiratory system evaluating methods when analyzing the significance of individual signs and diseases course intensity indicators. According to a number of authors [13, 14], the use of methods for preventive intelligence medical data analysis in the context of assessing statistical indicators and correlations between individual data sets features allows the formation of an effective consistent data basis, thus organizing the process of automatic dimensionality reduction. As follows from the works [15, 16] on the use of ML in practice, the most effective are algorithms united in committees, this allows for models balancing and error values averaging for various metrics.

Thus, analyzing the research results in the reviewed authors works [10-16], it should be noted that more often they consider the possibility of using statistical approaches, as well as ML and ANN models, primarily to solve classification and regression problems in a heterogeneous feature space. However, outside the scope of research, questions remain related to assessing the individual medical indicators diagnostic significance, identifying correlations between input signs and assessing their specific weight values in the context of considering ophthalmological disease problems in patients with diabetic neovascular glaucoma.

The relevance of such studies is undoubted, due to the increasing disability of patients with this pathology throughout the world. In this regard, this work goal is to create and study different ANN models with generalization abilities and architecture for assessing the significance of features based on the collected data set on diagnostic indicators of inflammation and intraocular circulation in patients with diabetic neovascular glaucoma.

3. Collected data set description

The created set of the most significant target input and output features with medical interpretation was selected as a data set for analysis in applying ML process.

A retrospective cohort study of 127 patients (127 eyes) with a painful form of neovascular glaucoma (NVG) of diabetic origin was conducted at the Institute of Eye Diseases and Tissue Therapy named after V.P. Filatov NAMS of Ukraine. The study protocol complied with the principles of the Declaration of Helsinki and was approved by the local institute's bioethical committee. Written informed consent was obtained from all study participants.

The average age of patients is 65.0 years (62-68). The patients had uncontrolled intraocular pressure - $IOP \geq 30$ mm Hg, and also had ocular pain syndrome. The main criterion for assessing the success of treatment was control of IOP and achieving its reduction by 20% from the initial value after 12 months of observation and maintaining best-corrected visual acuity (BCVA) - "success of treatment".

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

The preoperative visit (V0) was carried out on the eve of transscleral (TSC) cyclophotocoagulation (CPC), which was performed according to standard techniques. The laser power ranged from 850 to 1500 mW (Me 1100 mW), exposure time was 1.5-2 seconds, and laser coagulates average number was 22.

In all patients, the need for repeat CFC TSC was determined at each postoperative visit. The criterion for repeated laser treatment was maintaining high IOP values. Preoperative laboratory parameters were determined: neutrophils (N), lymphocytes (L), platelets (Throm), monocytes (M), glycosylated hemoglobin (HbA1c, %), volumetric intraocular circulation (RQ, %) according to rheophthalmography. The systemic immune inflammation index ($SII = \text{Throm} \times [N/L]$) and systemic inflammation response index ($SIRI = N \times [M/L]$) were calculated. The SIRI and SII scores were further divided into quartiles, and the RQ score into quintiles. The data has been imported, divided into input and output characteristics. The target variable is the indicator “success of treatment”, which is a binary attribute. A fragment of the generated dataset is shown in Fig. 1. The results of related correlation analysis of the most significant features are shown in Fig. 2.

Name	Type	Missing	Statistics		
complications after CPT	Integer	0	0	1	0.591
LYM (109/L)	Real	0	Min 1.500	Max 2.400	Average 1.657
SIRI	Real	0	Min 0.460	Max 1.150	Average 0.727
SIRI kvartils	Integer	0	Min 1	Max 4	Average 2.244
SII	Real	0	Min 338	Max 673.900	Average 474.002
SII kvartils	Integer	0	Min 1	Max 4	Average 2.394
RQ critical - 0	Integer	0	Min 0	Max 1	Average 0.551
RQ V0	Real	0	Min 1.400	Max 5.650	Average 3.168
Success VOT	Polynomial	0	Less false (44)	More true (63)	Values true (63), false (44)

Figure 1. Fragment of the input data set for analysis

There is some imbalance in the output class values, which is not critical for research, and therefore the use of synthetic balancing methods is not advisable due to introducing additional noise risk into the data. As part of the reconnaissance data analysis, a correlation analysis of the feature space was performed in order to identify obvious patterns between individual input variables.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

Attribut...	sex	age	HbA1	laserc...	Caite...	Laser ...	VOVOT	GZ VO	com...	LYM L...	SIRI	SIRI ...	SII	SII kv...	RQ cr...	RQ VO	Success...
sex	1	-0.048	0.021	0.206	-0.066	0.069	0.102	0.131	-0.078	0.014	0.016	0.048	-0.024	-0.009	-0.097	0.148	-0.026
age	-0.048	1	-0.273	-0.241	-0.018	-0.021	-0.041	-0.295	0.103	-0.202	-0.156	-0.103	-0.074	-0.081	0.183	0.285	-0.115
HbA1	0.021	-0.273	1	-0.189	0.306	0.363	0.573	-0.219	0.355	-0.149	0.815	0.758	0.774	0.633	-0.620	-0.156	0.751
lasercou...	0.206	-0.241	-0.189	1	0.004	-0.191	-0.193	0.348	-0.163	0.133	-0.163	-0.203	-0.263	-0.263	0.082	-0.110	-0.230
Cauderz...	-0.066	-0.018	0.306	0.004	1	-0.093	0.141	-0.153	0.193	-0.040	0.316	0.301	0.356	0.377	-0.203	-0.187	0.304
Laserf81...	0.069	-0.021	0.363	-0.191	-0.093	1	0.251	-0.066	0.209	-0.144	0.360	0.409	0.410	0.365	-0.213	0.046	0.332
VO VOT	0.102	-0.041	0.573	-0.193	0.141	0.251	1	-0.494	0.504	-0.115	0.643	0.590	0.657	0.563	-0.430	-0.123	0.611
GZ VO	0.131	-0.295	-0.219	0.349	-0.153	-0.066	-0.494	1	-0.574	0.107	-0.385	-0.397	-0.379	-0.334	0.279	0.018	-0.344
complica...	-0.078	0.103	0.355	-0.163	0.193	0.209	0.594	-0.574	1	-0.148	0.536	0.495	0.510	0.408	-0.397	-0.086	0.472
LYM (10...	0.014	-0.202	-0.149	0.133	-0.040	-0.144	-0.115	0.107	-0.148	1	-0.259	-0.281	-0.265	-0.307	0.025	-0.034	-0.183
SIRI	0.016	-0.156	0.815	-0.163	0.316	0.360	0.643	-0.385	0.536	-0.259	1	0.954	0.917	0.813	-0.744	-0.138	0.874
SIRI kvar...	0.048	-0.103	0.758	-0.203	0.301	0.409	0.590	-0.397	0.465	-0.281	0.954	1	0.874	0.806	-0.683	-0.061	0.822
SII	-0.024	-0.074	0.774	-0.209	0.356	0.410	0.657	-0.379	0.510	-0.265	0.917	0.874	1	0.893	-0.682	-0.047	0.876
SII kvartils	-0.009	-0.081	0.633	-0.263	0.377	0.365	0.563	-0.334	0.408	-0.307	0.813	0.896	0.893	1	-0.533	-0.001	0.736
RQ crtic...	-0.097	0.183	-0.620	0.062	-0.203	-0.213	-0.430	0.279	-0.397	0.025	-0.744	-0.683	-0.682	-0.533	1	0.287	-0.807
RO VO	0.148	0.285	-0.156	-0.110	-0.187	0.046	-0.123	0.018	-0.086	-0.034	-0.138	-0.061	-0.047	-0.001	0.287	1	-0.175
Success...	-0.026	-0.115	0.751	-0.230	0.304	0.332	0.611	-0.344	0.472	-0.183	0.874	0.822	0.876	0.796	-0.807	-0.175	1

Figure 2. Related correlation analysis of the most significant features

How can we note the indicators SIRI, SIRI quartiles, SII, SII quartiles have a high correlation with each other and with another input feature HbA1, which can

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

introduce additional noise into the operation of models, and therefore it is necessary to take into account the nature of the influence of these features on the output target variable.

The correlation analysis showed a high positive relationship between the success of treatment and the indicators HbA1c ($r = 0.751$), SII ($r = 0.876$), SIRI quartiles ($r = 0.874$), IOP V0 ($r = 0.611$) and a high negative relationship with the RQ quintiles indicator ($r = -0.807$).

4. Development of artificial neural network models

We construct a computational process for constructing and studying ANN models to assess the accuracy of their training and classification. To do this, we use the Rapidminer system and blocks for importing a data set from a *.csv file, setting a target variable, and a subsystem for dividing the sample into test and validation. In order to conduct a systemic study and determine the ANN model type influence nature used on the final classification accuracy, assessed by different metrics, it is necessary to create several ANN models with different architectures.

In this regard, we use 3 types of ANN models: single perceptron (SP), multilayer perceptron (MP) and deep multilayer neural network (DNN).

In RapidMiner, ANN modeling can be implemented using the Neural Net operator, which allows for the creation, training, and evaluation of neural networks. Here's an overview of how ANN modeling works in RapidMiner:

Key Concepts of ANN in RapidMiner:

1. **Neurons and Layers.** Developed neural network models are consist of interconnected neurons, arranged in layers: an input layer, one or more hidden layers, and an output layer. Neurons in one layer are connected to neurons in the next, with each connection having a weight that is learned during the training process.

2. **Activation Functions.** Each neuron in a hidden layer applies an activation function to the weighted sum of its inputs to introduce non-linearity, which helps the model capture complex relationships. We've used Sigmoid functions and ReLU.

The structure of the developed process for creating and modeling ANN operation is shown in the figure 3. All blocks are unitary commands aimed at processing data and performing processes for modeling the operation of ANN.

Training and test data are divided among themselves in the proportion of 75% to 25%, respectively. The structure of the Validation block of the model is shown at fig.4.

Also, we used backpropagation learning algorithm. We build ANN training process on the base of backpropagation algorithm, where the network adjusts the weights of connections based on the error between predicted and actual outputs.

This is done iteratively over the training data to minimize the error, usually measured using a loss function (e.g., mean squared error for regression). During training, data is fed into the network, and the model adjusts weights to minimize prediction error. This is repeated over several iterations or epochs.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

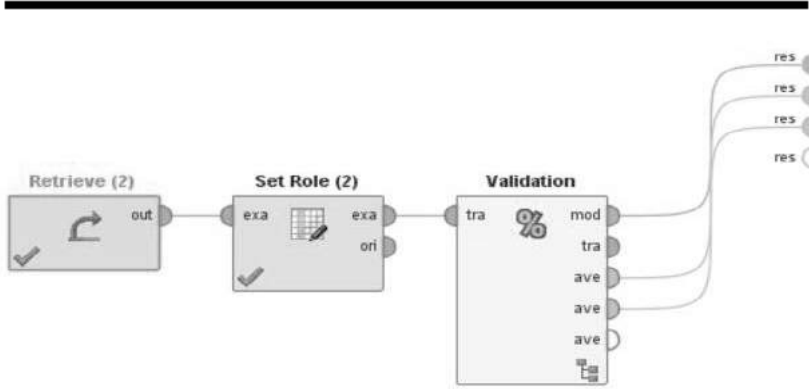


Figure 3. The general structure of the developed process for creating and modeling the operation of an ANN

Hyperparameters like learning rate, momentum, and number of hidden layers are critical in determining the success of the model.

During to our research in RapidMiner, model combination tools (also called ensemble techniques) are used to combine the predictions of multiple models to improve the overall performance.

These techniques aim to reduce errors, improve accuracy, and provide more robust predictions by leveraging the strengths of individual models.

We also provide a distinct module for confusion matrix calculation. It help us to provide different additional types of logical model's estimation, because of:

1. Correctly Identified Classes. True Positives (TP) t_p . These are instances where the ANN model correctly predicts the positive class. True Negatives (TN)

t_n . These are instances where the model correctly predicts the negative class. TPs and TNs indicate the correct predictions made by the model, and their sum reflects the model's accuracy on correctly classified instances.

2. Misclassified Instances. False Positives (FP) f_p . These occur when the model incorrectly predicts a positive class when it should have predicted a negative one. In binary classification, this is known as a Type I error. False Negatives (FN)

f_n . These occur when the model incorrectly predicts a negative class when the true label is positive. This is referred to as a Type II error. FPs and FNs indicate the errors made by the model. The distribution of these errors helps in identifying where the model is going wrong (e.g., if it's more prone to false alarms or missing positive cases).

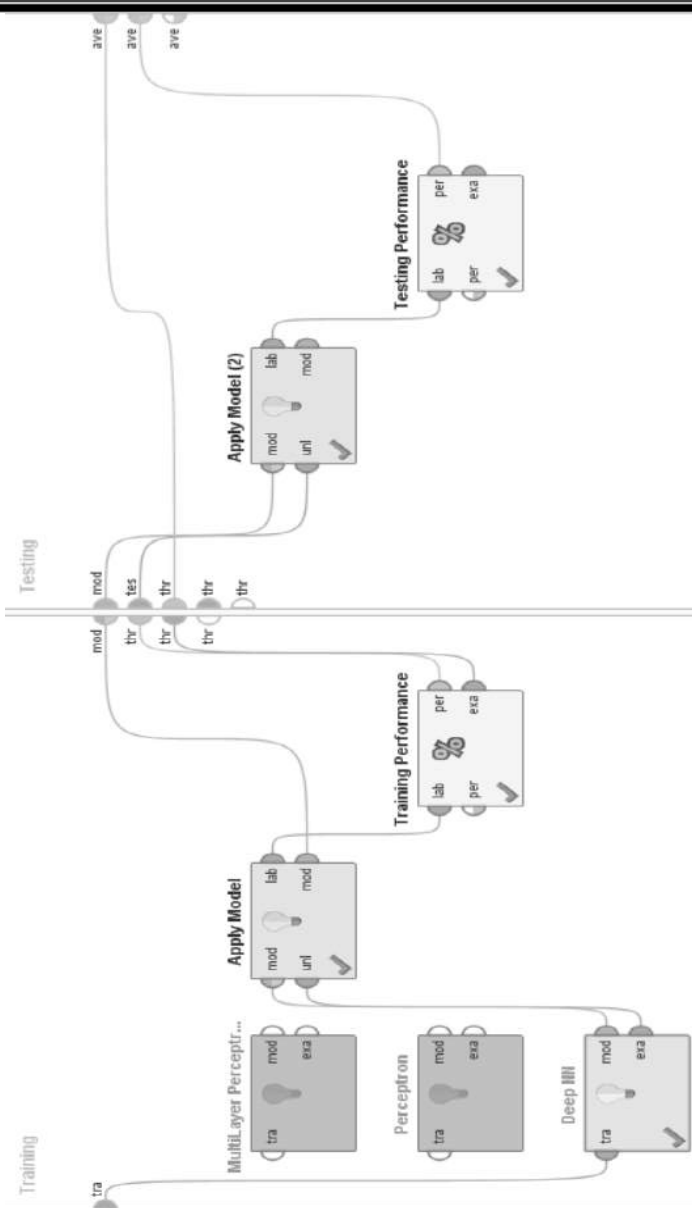


Figure 4. The structure of the Validation block of the model

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

3. Class Imbalance. Class Distribution. It is essential to consider the distribution of the classes when constructing the confusion matrix, especially in datasets where the classes are imbalanced (i.e., one class appears much more frequently than the other). In imbalanced datasets, accuracy alone can be misleading. For example, in a dataset with 90% negative and 10% positive examples, predicting every instance as negative would give a high accuracy but would fail on the positive class. The confusion matrix provides a more nuanced view of how the model is performing across different classes. As part of the process of studying the operation of the developed software, an assessment of the classification accuracy of the ANN models was carried out. ACCURACY was used as a numerical characteristic for assessing the operation of the software – a reliability metric that allows assessing the accuracy of classification, i.e. determining the proportion of correctly classified examples.

$$Accuracy = \frac{t_p + t_n}{t_p + f_p + f_n + t_n}$$

5. Experiments and results

10 computational experiments were carried out with different sets of parameters (hidden layers number, activation functions, learning rate coefficients, error rates). The average obtained metrics values for assessing model's accuracy are shown in the table below. In particular, for a single perceptron, the value of the learning rate coefficient varied from 0.05 to 0.3. For a multilayer perceptron, 2 hidden layers of 5 and 3 neurons were created, respectively. For the deep ANN, 50 hidden layers were created. The results of obtained ANN model's metrics evaluation to the first experiment are given in Table 1. The confusion matrices for each of the created neural network models for the training and test samples are shown in the following (Fig.5-7). Visualization of the results of comparing estimates of accuracy and error metrics for the created ANN models of the first experiment is shown in Fig.8.

As we can see (Fig. 8), the least accurate classification results on both the training (about 84%) and training set were shown by the SP model (about 87%), which is due to its simplified architecture, the absence of hidden layers and a number of hyperparameters. affecting model's final accuracy.

accuracy: 86.90%			
	true true	true false	class precision
pred. true	50	6	89.29%
pred. false	5	23	82.14%
class recall	90.91%	79.31%	

accuracy: 83.72%			
	true true	true false	class precision
pred. true	22	1	95.65%
pred. false	6	14	70.00%
class recall	78.57%	93.33%	

Figure 5. Confusion of training and test sample matrices for the Single Perceptron model

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

Table 3

The results of obtained ANN model's metrics evaluation to the first experiment

Metric name	Metric values of ANN models					
	Single Perceptron (SP)		Multilayer Perceptron (MP)		Deep NN (DNN)	
	Training set	Test sample	Training set	Test sample	Training set	Test sample
Accuracy	86.90%	83.72%	100.00%	95.35%	100.00%	97.67%
Classification error	13.10%	16.28%	0.00%	4.65%	0.00%	2.33%
Kappa	0.708	0.667	1.000	0.898	1.000	0.948
Weighted mean recall	85.11%	85.95%	100.00%	94.88%	100.00%	96.67%
Weighted mean precision	85.71%	82.83%	100.00%	94.88%	100.00%	98.28%
Spearman rho	0.708	0.667	1.000	0.898	1.000	0.949
Kendall tau	0.708	0.667	1.000	0.898	1.000	0.949
Absolute error	0.131 +/- 0.337	0.163 +/- 0.369	0.004 +/- 0.013	0.038 +/- 0.171	0.029 +/- 0.070	0.036 +/- 0.150
Relative error	13.10% +/- 33.73%	16.28% +/- 6.92%	0.37% +/- 1.33%	3.78% +/- 17.14%	2.85% +/- 6.99%	3.57% +/- 14.99%
Squared error	0.131 +/- 0.337	16.28% +/- 6.92%	0.001 +/- 0.001	0.031 +/- 0.157	0.006 +/- 0.020	0.024 +/- 0.143
Correlation	0.708	0.667	1.000	0.898	1.000	0.949
Logistic loss	0.363	0.375	0.314	0.327	0.293	0.305

accuracy: 100.00%			
	true true	true false	class precision
pred. true	55	0	100.00%
pred. false	0	29	100.00%
class recall	100.00%	100.00%	

accuracy: 95.35%			
	true true	true false	class precision
pred. true	27	1	96.43%
pred. false	1	14	93.33%
class recall	96.43%	93.33%	

Figure 6. Confusion of training and test sample matrices for the Multilayer Perceptron model

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

accuracy: 100.00%			
	true true	true false	class precision
pred. true	55	0	100.00%
pred. false	0	29	100.00%
class recall	100.00%	100.00%	

accuracy: 97.67%			
	true true	true false	class precision
pred. true	28	1	96.55%
pred. false	0	14	100.00%
class recall	100.00%	93.33%	

Figure 7. Confusion of training and test sample matrices for the Deep NN model

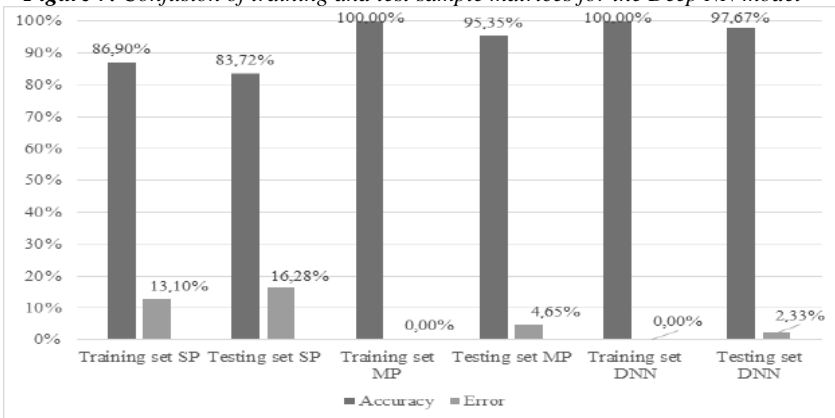


Figure 8. Visualization of the results of comparing estimates of accuracy and error metrics for the created ANN models of the first experiment

The MP and DNN models showed approximately the same results for metric evaluations on the training subset of data, however, the accuracy of DNN was 2.3% higher on the test subset, which may be due to a more complex model structure and a larger number of computational iterations.

An additional experiment was aimed at reducing the dimension of input features. A unique identifier, calculated values of SIRI quartiles, SII, HbA1c, RQ quintiles, IOP V0 were used as input features; the output feature is “success of treatment”. Results of calculating weighting coefficients for input parameters of the data set for the first set of experiments are shown in Fig.9. As we can see, the values are scaled

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

to the range $\{0,1\}$, with occupies the smallest value – SII, and the largest – RQ critical -0.

attribute	weight	attribute	weight
id	0.626	complications after CPT	0.241
sex	0.430	LYM (109/L)	0.684
age	0.604	SIRI	0.019
HbA1	0.100	SIRI kvartils	0.030
lasercougul (1-yes)	0.662	SII	0
Cauterization	0.302	SII kvartils	0.043
Laser 810 power	0.280	RQ critical - 0	1
V0 VOT	0.140	RQ V0	0.533
GZ V0	0.801	Success VOT	0.065

Figure 9. Results of calculating weighting coefficients for input parameters of the data set for the first set of experiments

Results of calculating weighting coefficients for initial input parameters of the data set for the second set of experiments are shown in Fig.10.

As can be seen, the spread of values is quite significant, which is associated with stochastic processes in the formation of weighting coefficients of initial data in the process of initializing the ANN models within the framework of the experimental studies conducted when launching the Rapidminer working environment.

Attribute	Weight
ID	497.739
SIRI kvar...	-804.910
SII	80.686
RQ critic...	771.697
Success...	1482.795
VOT V5	-4124.037

Figure 10. Results of calculating weighting coefficients for initial input parameters of the data set for the second set of experiments

Research modelling was performed on the created three ANN models with the same parameters. The results of evaluating the metrics of the obtained NN models for the second experiment are given in Table 2.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

Table 2

Results of evaluation of metrics of the obtained ANN models for the second experiment

Metric name	Metric values of ANN models					
	Single Perceptron (SP)		Multilayer Perceptron (MP)		Deep NN (DNN)	
	Training set	Test sample	Training set	Test sample	Training set	Test sample
Accuracy	6.90%	3.81%	100.00%	93.02%	100.00%	90.70%
Classification error	2.56%	6.19%	0.00%	6.98%	0.00%	9.30%
Kappa	.355	.487	1.000	0.822	1.000	0.769
Weighted mean recall	2.31%	0.42%	100.00%	90.05%	100.00%	88.44%
Weighted mean precision	7.97%	4.89%	100.00%	92.33%	100.00%	88.44%
Spearman rho	.400	.550	1.000	0.824	1.000	0.769
Kendall tau	.400	.550	1.000	0.824	1.000	0.769
Absolute error	.326	+/- .262	+/ 0.009	+/- 0.049	0.029 +/- 0.070	0.112
	.469	.440	0.017	0.153		+/- 0.21
Relative error	2.56%	+/- 6.19%	+/ 0.94%	+/- 4.91%	2.85% +/- 6.99%	11.18%
	6.86%	3.97%	1.65%	15.26%		+/- 21.13%
Squared error	.326	+/- .262	+/ 0.001	+/- 0.026	0.006 +/- 0.020	0.057
	.469	.440	0.000	0.094		+/- 0.163
Corellation	.400	.550	1.000	0.824	1.000	0.769
Logistic loss	.437	.413	0.316	0.329	0,293	0.349

The nature of the obtained results differs somewhat from the previously calculated metric values for the better, however, due to the presence of noise effects, the values are not ideal. Adjacent correlation analysis of the most significant features of experiment 2 is shown in Fig.11.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

As we can see, a number of features have a significant correlation with each other, which may be an additional reason for the presence of noise effects during training and testing of models. Visualization of the results of comparing estimates of accuracy and error metrics for the created ANN models for the second experiment is shown in Fig.12.

In the third experiment, gender was excluded from the original sample. This reduces noise effects because this feature does not carry a significant semantic load in the context of data analysis. Results of calculating weighting coefficients for initial input parameters of the data set for the third set of experiments are shown in Fig.13.

Attribut...	SIRI kva...	SII	RQ criti...	Succes...	VOT V5	Succes...
SIRI kvar...	1	0.874	-0.683	-0.822	0.423	-0.163
SII	0.874	1	-0.682	-0.876	0.415	-0.165
RQ critic...	-0.683	-0.682	1	0.807	-0.250	-0.006
Success...	-0.822	-0.876	0.807	1	-0.376	0.130
VOTV5	0.423	0.415	-0.250	-0.376	1	-0.781
Success...	-0.163	-0.165	-0.006	0.130	-0.781	1

Figure 11. Adjacent correlation analysis of the most significant features of experiment 2

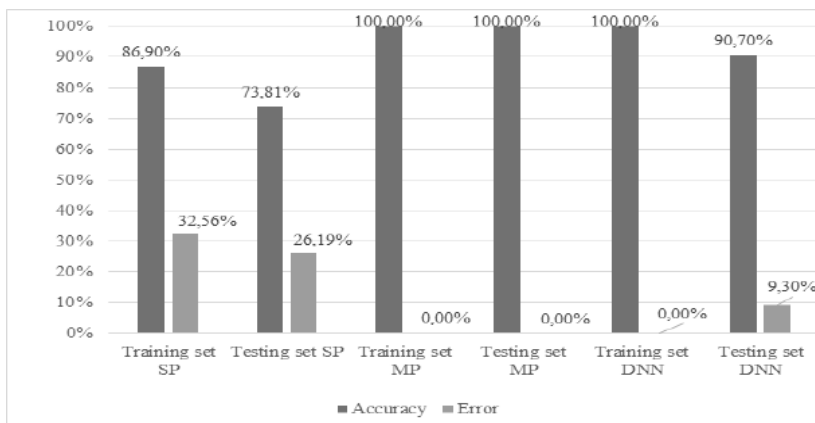


Figure 12. Visualization of the results of comparing estimates of accuracy and error metrics for the created ANN models for the second experiment

The results of evaluation of the metrics of the obtained NN models for the third experiment are given in Table 3.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

Attribute	Weight	Attribute	Weight
id	3412.931	complica...	453.048
age	-9980.359	LYM (10...	-512.371
HbA1	-402.500	SIRI	243.611
lasercou...	-366.595	SIRI kvar...	967.704
Cauteriz...	-4811.274	SII	1441.607
Laser 81...	-73.848	SII kvartil...	-245.604
V0 VOT	-3350.753	RQ critic...	-1097.827
GZ V0	-27.132	RQ V0	-1436.026

Figure 13. Results of calculating weighting coefficients for initial input parameters of the data set for the third set of experiments

The final values of the weighting coefficients of the most significant features determined by DNN are shown in Fig.14.

attribute	weight
ID	0
SIRI kvar...	0.481
SII	0.595
RQ critic...	0.592
Success...	1
VOT V5	0.643
Success...	0.806

Figure 14. The final values of the weighting coefficients of the most significant features determined by DNN

Visualization of the results of comparing estimates of accuracy and error metrics for the created ANN models for the third experiment is shown in Fig.15. As a result of ANN constructing significant input parameters were established that most influence the effectiveness of treatment: SIRI quartiles, SII, HbA1c and RQ quintiles. During inflammation, leukocytes accumulate in the lesion and the speed of local blood flow decreases. Impaired retinal microcirculation is observed in patients with type 2 diabetes mellitus (T2DM) without clinically significant diabetic retinopathy [17].

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

Table 3

Results of evaluation of metrics of the obtained ANN models for the third experiment

Metric name	Metric values of ANN models					
	Single Perceptron (SP)		Multilayer Perceptron (MP)		Single Perceptron (SP)	
	Training set	Metric name	Training set	Metric name	Training set	Metric name
Accuracy	89.29%	95.35%	100.00%	97.67%	98.81%	97.67%
Classification error	10.71%	4.65%	0.00%	2.33%	1.19%	2.33%
Kappa	0.769	0.898	1.000	0.948	0.974	0.948
Weighted mean recall	89.37%	94.88%	100.00%	96.67%	99.09%	96.67%
Weighted mean precision	87.74%	94.88%	100.00%	98.28%	98.33%	98.28%
Spearman rho	0.771	0.898	1.000	0.949	0.974	0.949
Kendall tau	0.771	0.898	1.000	0.949	0.974	0.949
Absolute error	0.107	+/- 0.047	0.005	+/- 0.024	0.034	+/- 0.037
	0.309	+/- 0.211	0.016	+/- 0.151	0.101	+/- 0.147
Relative error	10.71%	+/- 4.65%	0.47%	+/- 2.39%	3.41%	+/- 3.70%
	30.93%	+/- 21.06%	1.57%	+/- 15.06%	10.11%	+/- 14.69%
Squared error	0.107	+/- 0.047	0.000	+/- 0.023	0.011	+/- 0.023
	0.309	+/- 0.211	0.001	+/- 0.151	0.058	+/- 0.140
Corellation	0.771	0.898	1.000	0.949	0.974	0.949
Logistic loss	0.354	0.331	0.315	0.322	0.324	0.326

Altered blood flow in patients with type 2 diabetes contributes to macrovascular (peripheral vascular disease and coronary artery disease) and microvascular (diabetic retinopathy and diabetic nephropathy) complications. Our results confirm that higher values of SIRI, SII, HbA1c and RQ indicate the severity of the disease and determine the need for diabetes mellitus stabilization [4], additional anti-inflammatory and anti-

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

ischemic treatment in patients with painful NVG of diabetic origin to improve treatment prognosis.

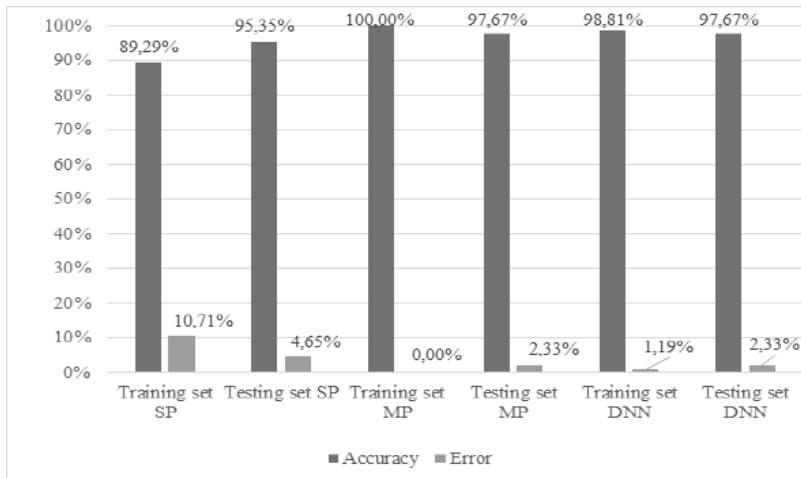


Figure 15. Visualization of the results of comparing estimates of accuracy and error metrics for the created ANN models for the third experiment

6. Conclusion

The conducted research made it possible to establish a higher adaptability of deep learning models, in particular deep fully connected ANN models, for the analyzed data set.

The SP model demonstrates unstable accuracy on the training and test samples in different experiments, which may be due to shortcomings in determining the weight values of features at different iterations, as well as limitations in generalization ability.

The MP model is more stable in all experiments, demonstrating high accuracy and completeness; its construction speed is 25% higher than the SP model. Presumably, the accuracy of this model can be increased through a more efficient organization model hyperparameter values automating selection process. The DNN model is the most accurate, but its training process is the most resource-intensive and takes almost 4 times longer than the SP model.

A promising direction for further research is the search for optimizing the ANN training process in order to minimize training and testing errors, as well as increase the generalization ability of models in general. It has been established that the most significant diagnostic features of the collected dataset in the context of the problems

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

under consideration are the indicator of glycosylated hemoglobin HbA1c of the volumetric intraocular circulation (RQ), the systemic inflammatory response index (SIRI) and the systemic inflammation index (SII).

The data obtained allow us to conclude that the use of neural networks to predict the effectiveness of treatment is justified and timely. By taking into account and stabilizing blood sugar, as well as adjusting indicators of inflammation and microcirculation in patients with diabetic neovascular glaucoma, it is possible to ensure a timely significant reduction in intraocular pressure, maintain visual acuity, and therefore the quality of life of patients.

The data obtained allow us to conclude that the use of different ANN to predict the effectiveness of transcleral cyclophotocoagulation is justified. Timely prescribed treatment of identified changes in glycolized hemoglobin (HbA1c), volumetric intraocular circulation (RQ), systemic inflammatory response index (SIRI) and systemic inflammation index (SII) against the background of transcleral cyclophotocoagulation can provide a significant reduction in intraocular pressure of at least 20%, maintaining visual acuity and patients life quality with painful diabetic neovascular glaucoma.

7. References

- [1] V. Vychuzhanin, N. Rudnichenko, Z. Sagova, M. Smieszek, V. V. Cherniavskiy, A. I. Golovan, M. V. Volodarets, Analysis and structuring diagnostic large volume data of technical condition of complex equipment in transport. IOP Conference Series: Materials Science and Engineering, Volume 776, 24th Slovak-Polish International Scientific Conference on Machine Modelling and Simulations - MMS 2019, 3-6 September 2019, Liptovský Ján, Slovakia, 2019 pp.1-11. DOI:10.1088/1757-899X/776/1/012049.
- [2] N. Rudnichenko, V. Vychuzhanin, I. Petrov, D. Shibaev, Decision Support System for the Machine Learning Methods Selection in Big Data Mining, in: Proceedings of The Third International Workshop on Computer Modeling and Intelligent Systems (CMIS-2020), CEUR-WS, 2608, 2020, pp. 872-885.
- [3] M. Alloghani, D. Al-Jumeily, J. Mustafina, A. Hussain, A.J. Aljaaf, A systematic review on supervised and unsupervised machine learning algorithms for data. Supervised and Unsupervised Learning for Data Science, Unsupervised and Semi-supervised Learning, Springer International Publishing, Cham (2014) 3-21. DOI: 0.1007/978-3-030-22475-2_1.
- [4] O. Guzun, O. Zadorozhnyy, L. Velychko, O. Bogdanova, L. Dumbrăveanu, V. Cușnir, A. Korol, The effect of the intercellular adhesion molecule-1 and glycated haemoglobin on the management of diabetic neovascular glaucoma, Romanian Journal of Ophthalmology, 68 2 (2024) 135-142. DOI:10.22336/rjo.2024.25.
- [5] J.De. Fauw, J.R. Ledsam, B. Romera-Paredes, Clinically applicable deep learning for diagnosis and referral in retinal disease, Nature Medicine, 24 9 (2018) 1342–1350. DOI: 10.1038/s41591-018-0107-6.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

- [6] B. Al-Bander, W. Al-Nuaimy, B.M. Williams, Y. Zheng, Multiscale sequential convolutional neural networks for simultaneous detection of fovea and optic disc, *Biomed Signal Process Control*, 40 (2018) 91–101. DOI: 10.1016/j.bspc.2017.09.008.
- [7] B.J. Antony, S. Maetschke, R. Garnavi, Automated summarisation of SDOCT volumes using deep learning: Transfer learning vs de novo trained networks, *PLoS ONE*, 14 5 (2019). DOI: 10.1371/journal.pone.0203726.
- [8] J. Bertomeu, Machine learning improves accounting: discussion, implementation and research opportunities, *Review of Accounting Studies*, 25 3 (2020) 1135-1155. DOI:10.1007/s11142-020-09554-9
- [9] M. Solanki, Ms. Sharma, A Review of Data Mining Techniques and Its Applications, *International Journal of Innovative Research in Computer Science & Technology*, 122 (2021) 100-104. DOI:10.55524/ijircst.2021.9.6.23.
- [10] S. Sheshkal, M. Gundersen, M. Riegler, Ø. Utheim, K. Gundersen, H. Hammer, Classifying Dry Eye Disease Patients from Healthy Controls Using Machine Learning and Metabolomics Data (2024).
- [11] A. Abdullah, A. Aldhabab, H. Abboodi, Review of Eye Diseases Detection and Classification Using Deep Learning Techniques, *BIO Web of Conferences*, 97 (2024). DOI:10.1051/bioconf/20249700012.
- [12] A. Selim, M. Barz, O. Bhatti, H. Alam Tusfiqur, D. Sonntag, A review of machine learning in scanpath analysis for passive gaze-based interaction, *Frontiers in Artificial Intelligence*, 7 (2024). DOI:10.3389/frai.2024.1391745.
- [13] J. Van Eijgen, V. Schuhmann, E.-L. Fingerroos, M. Renier, H. Burchert, J. Kröpfl, A. Craenenbroeck, V. Cornelissen, K. Gugleta, I. Stalmans, H. Hanssen, High-intensity interval training in patients with glaucoma (HIT-GLAUCOMA): protocol for a multicenter randomized controlled exercise trial, *Frontiers in Physiology*, 15 (2024). DOI:1349313. 10.3389/fphys.2024.1349313.
- [14] C.-H. Moon, Ah-Jun Lee, H.-Y. Jeon, E.-B. Kim, K.-S. Ha, Therapeutic effect of ultra-long-lasting human C-peptide delivery against hyperglycemia-induced neovascularization in diabetic retinopathy, *Theranostics*, 13 (2023) 2424-2438. DOI:10.7150/thno.81714.
- [15] E. Tokuç, M. Eksi, R. Kayar, S. Demir, R. Topaktaş, Y. Bastug, M. Akyuz, M. Ozturk, Inflammation indexes and machine-learning algorithm in predicting urethroplasty success, *Investigative and Clinical Urology*, 65 (2024) 240. DOI: 10.4111/icu.20230302.
- [16] A. Abujaber, Y. Imam, I. Albalkhi, S. Yaseen, A. Nashwan, N. Akhtar, Utilizing machine learning to facilitate the early diagnosis of posterior circulation stroke, *BMC Neurology*, 24 (2024) 1-12. DOI:10.1186/s12883-024-03638-8.
- [17] V. Cankurtaran, M. Inanc, K. Tekin, F. Turgut, Retinal Microcirculation in Predicting Diabetic Nephropathy in Type 2 Diabetic Patients without Retinopathy, *Ophthalmologica*, 243 4 (2020) 271-279. DOI: 10.1159/000504943.

**ШТУЧНИЙ ІНТЕЛЕКТ В ДІАГНОСТИЦІ, ПРОГНОЗІ ТА
ЛІКУВАННІ ДІАБЕТИЧНОЇ НЕОВАСКУЛЯРНОЇ ГЛАУКОМИ**

Dr.Sci. В. Вичужанін ORCID: 0000-0002-6302-1832

Національний університет «Одеська політехніка», Україна

E-mail: vychuzhanin.o.v@op.edu.ua

Ph.D. О. Гузун ORCID: 0009-0003-6873-8503

*ІДУ «Інститут очних хвороб і тканинної терапії ім. Філатова НАМН
України», Україна*

E-mail: olga.v.guzun@gmail.com

Ph.D. М. Рудниченко ORCID: 0000-0002-7343-8076

Національний університет «Одеська політехніка», Україна

E-mail: nickolay.rud@gmail.com

Ph.D. О. Задорожний ORCID: 0000-0003-0125-2456

*ІДУ «Інститут очних хвороб і тканинної терапії ім. Філатова НАМН
України», Україна*

E-mail: zadoroleg2@gmail.com

Ph.D. А.Король ORCID: 0000-0003-0516-308X

*ІДУ «Інститут очних хвороб і тканинної терапії ім. Філатова НАМН
України», Україна*

E-mail: andrii.r.korol@gmail.com

Анотація. Ця робота зосереджена на ключових аспектах діагностики, прогнозу та лікування неоваскулярної глаукоми діабетичного походження на основі підходів машинного навчання та, зокрема, різних архітектур штучних нейронних моделей. Проведено аналіз актуальності, пріоритетних положень і переваг використання методів машинного навчання, розглянуто існуючі підходи, які використовуються в сучасній літературі в контексті досліджуваної теми, особливості їх інтеграції в процес діагностичного аналізу. Описано простір ознак агрегованого та позначеного авторами набору даних про пацієнтів із проблемами зору, зокрема тих, хто страждає на неоваскулярну глаукому діабетичного походження. Проведено кореляційний аналіз вхідних ознак, побудовано, навчено та протестовано 3 різні моделі штучних нейронних мереж, експериментально розраховано та досліджено метрики для оцінки точності їх роботи, визначено статистичні показники, у тому числі похибки та втрати, що характеризують їх узагальнюючу здатність. Аналіз результатів, отриманих у ході досліджень, дав змогу визначити переважаючі вхідні характеристики та оцінити їхній вплив на цільову вихідну змінну та загальну значимість у просторі ознак набору даних, а також встановити найбільш прийнятні моделі для даних аналізу з точки зору їх точності та швидкості. Проведене дослідження дозволило встановити факт повної адаптованості моделей глибокого навчання штучних нейронних мереж до аналізованого набору даних.

Ключові слова. Штучний інтелект, неоваскулярна глаукома, діагностика лікування очей, нейронні мережі, аналіз даних, аналіз даних, машинне навчання

**ІНТЕЛЕКТУАЛЬНА СИСТЕМА АНАЛІЗУ ТА ДЕТЕКЦІЇ
ТЕКСТОВОГО БОТ-КОНТЕНТУ ВЕЛИКОГО ОБСЯГУ У
СОЦІАЛЬНИХ МЕРЕЖАХ**

Ph.D. М. Рудніченко ORCID: 0000-0002-7343-8076

*Національний університет «Одеська Політехніка», Україна
E-mail: nickolay.rud@gmail.com*

Ph.D. Н. Шибасва ORCID: 0000-0002-7869-9953

*Національний університет «Одеська Політехніка», Україна
E-mail: nati.sh@gmail.com*

Ph.D. Т. Отрадська ORCID: 0000-0002-5808-5647

*Одеський коледж комп'ютерних технологій «СЕРВЕР», Україна
E-mail: tv_61@ukr.net*

Д. Шведов ORCID: 0009-0002-4823-8782

*Національний університет «Одеська Політехніка», Україна
E-mail: frumle@ukr.net*

Ph.D. І. Шпінарева ORCID: 0000-0001-9208-4923

*Національний університет «Одеська Політехніка», Україна
E-mail: iryna.shpinareva@onu.edu.ua*

Dr.Sci. І. Петров ORCID: 0000-0002-8740-6198

*Національний університет «Одеська Політехніка», Україна
E-mail: firmp@gmail.com*

Abstract. У роботі розглядаються різні аспекти розробки інтелектуальної системи аналізу та обробки великих обсягів неоднорідних текстів природною мовою для завдання виявлення ботів у соціальних мережах із використанням методів глибокого перенесення навчання, зокрема великих мовних моделей. Наведено детальний аналіз специфічних характеристик та ключових аспектів структурування, обробки та аналізу текстового контенту, обґрунтовано актуальність проблеми та проведено огляд існуючих підходів у науковій літературі. У роботі підкреслено переваги та потенційні можливості використання штучних нейронних мереж і машинного навчання для автоматизації аналізу текстів користувачів соціальних мереж. Надано опис набору даних, обраного для дослідження, обґрунтовано вибір мовних моделей на основі штучних нейронних мереж та пояснено використання перенесення навчання для адаптації цих моделей до завдання виявлення ботів. Описано технічні засоби та сервіси, що використовуються для реалізації функціоналу розробленого веб-додатку, а також створено об'єктно-орієнтовані моделі системи за допомогою UML, включаючи діаграми прецедентів та компонентів. Окреслено функціональні можливості програмного забезпечення, прототипи сторінок та графічний інтерфейс користувача. У роботі представлені результати експериментальних досліджень обраних мовних

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

моделей на розширеному наборі даних, перевірених у режимах як з текстовими поясненнями, так і без них. Проаналізовано продуктивність адаптованих нейронних моделей на певному етапі, визначено особливості їхньої роботи та запропоновано перспективні напрями для подальших досліджень і розробок для вирішення виявлених проблем.

***Ключові слова:** інтелектуальний аналіз даних, класифікація тексту, соціальні мережі, аналіз тексту, обробка природної мови, розробка програмного забезпечення, виявлення ботів, великі дані*

1. Вступ

У сучасному інформаційному суспільстві Інтернет можна назвати невід'ємною частиною бізнесу, що дозволяє будь-якій компанії здійснювати ділові комунікації з такими цільовими групами, як клієнти, торгові посередники (канали збуту), PR-сфера, постачальники, конкуренти, чинні та потенційні співробітники [1].

Під час проведення подібних комунікацій генеруються, обробляються і зберігаються великі обсяги різноманітних даних, зокрема мультимедійні файли (зображення, відео), і навіть який завжди чітко структурований текстовий контент [2]. В даному контексті слід зазначити, що однією з головних тенденцій розвитку Інтернету останніх років є стрімке зростання популярності соціальних мереж (SN), які все частіше та активніше використовуються в маркетингових цілях, зокрема для просування того чи іншого товару, послуги, експерта, лідера думок, програмних додатків та сервісів та ін.

У цих умовах використання SN як джерела отримання даних та формування інформаційної бази по клієнтам є доцільною та важливою [3].

Для сучасних SN можна виділити такі характерні ефекти та властивості, які важливо враховувати при їх використанні для вирішення завдань бізнесу:

- наявність власних думок користувачів, що беруть участь у системі; зміна думок членів SN під впливом інших;
- різна значущість (пріоритетність або вага) думок одних користувачів для інших через їх рівень експертизи;
- змінюється ступінь схильності членів SN до впливу між собою;
- наявність непрямого впливу чи залежностей між користувачами у всьому ланцюзі наявних соціальних контактів; існування експертів, тобто. «лідерів думок» у певній тематиці;
- наявність деякого порога чутливості до зміни у лексиці оточуючих;
- локалізація створених груп за ознаками (за інтересами, з близькими думками, об'єднаних за соціальними чи гендерними ознаками);
- облік факторів "соціальної кореляції";
- існування зовнішніх факторів впливу та сторонніх агентів (ЗМІ, продавці чи виробники);
- вплив SN на динаміку думок у віртуальному співтоваристві;
- можливість утворення коаліцій чи команд, груп за інтересами;

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

– ігрову або інтерактивну взаємодію користувачів в інтерактивному режимі [4-6].

При цьому слід зазначити, що в даний час все більшої актуальності набувають проблеми захисту інформації та протидії інформаційним загрозам у різних системах обміну даними, у тому числі і в SN, контент у яких формується різними способами та методами, від ручного написання тематичних текстів до їх синтетичної генерації на основі застосування різних інтелектуальних технологій та засобів [7]. Фактично на практиці часто зустрічаються ситуації, коли потрібно розпочати листування з іншими користувачами SN з метою проведення консалтингу, обміну думками або оцінки характеру та якості контенту, що публікується [8].

Через те, що наведені вище процеси не можуть бути повноцінно автоматизовані і часто виконуються вручну, внаслідок чого є ресурсомісткими і дорогими для бізнесу в таких випадках потрібно гарантувати коректність інформації, що отримується, її цільовий характер і мінімізувати ризики отримання некоректних даних.

У зв'язку з цим актуальним завданням є ідентифікація та виявлення за прямими і непрямыми поведінковими, лінгвістичними та семантичними ознаками автоматизованих програм (ботів), що ховаються під профілями користувача, що здійснюють публікацію недостовірних та свідомо неправдивих відомостей, що прагнуть обманним шляхом отримати особисті номери телефонів, скани документів, номери платіжних реквізитів, кредитних та дебетових карток та ін.), а також сприяють дестабілізації настроїв у суспільстві SN, що призводить до негативних наслідків для бізнесу при просуванні товарів та послуг [9].

Бот або віртуальний помічник (ВП) у широкому сенсі є спеціалізованим програмним забезпеченням, здатним здійснювати симуляцію дій реального користувача, зокрема генерувати текстовий контент [10]. Зокрема, у разі управління обліковим записом користувача за допомогою застосування такого ПЗ в автоматизованому режимі вважається, що даний процес реалізується ботом. У випадку, коли обліковий запис керується частково програмою та частково людиною, застосовується термін «кіборг». На практиці розрізняють прості боти, що діють директивно та виконують набір чітко заданих команд, а також за допомогою функцій самонавчання [11].

Боти мають ряд істотних переваг у порівнянні зі звичайними обліковими програмними додатками, наприклад, їх простіше встановити, не потрібно займати для зберігання даних пам'ять пристрою, посилання на отримання доступу до бота легко поширювати. Фактична зручність від використання ботів полягає у підтримці можливостей доставки повідомлень у зручні для отримання користувачем місця, наприклад, особисті повідомлення в SN, месенджерах.

ВП у ряді випадків застосовуються в діалогових системах для різних прикладних цілей, у тому числі для обслуговування клієнтів, агрегації даних та інформації. Боти уможливають спілкування компаній із замовниками в

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

індивідуальному інтерактивному режимі, що не вимагає залучення до цього процесу співробітників.

Боти можуть бути адаптовані для завдань автоматизації рекламування або надання облікових сервісів, від замовлення квитків на заходи, букінгу та бронювання місць у готелях, виконання порівняльного аналізу товарів та послуг за заданими критеріями. Можливим аспектом їх використання може бути автоматизація виконання різних рутинних операцій з великою кількістю клієнтів у банківському секторі, торгівлі [8].

Боти починають застосовуватися і в рамках державного сектору з метою реєстрації звернень громадян до міських служб, проведення обробки запитів по комунальному господарству, що надходять від людей, оплаті рахунків та відправці нагадування про необхідність внесення показань лічильників.

В даний час боти в SN класифікуються за різними ознаками та типами (рис.1.6), розглянемо найбільш популярні їх типи, до яких належать:

1. Соціальні боти – це спеціалізовані програми, використовувані насамперед для імітації процесу живої поведінки людини у SN. Тобто. соціальні роботи наслідують людську поведінку для акцентування уваги користувачів на заданій інформації. На практиці подібні роботи використовуються як для позитивних завдань (консультування користувачів, підтримка у проведенні опитувань, публікація контенту за розкладом, просування брендів або конструктивних ідей у SN, привернення уваги користувачів до соціальних проблем чи інших тематиків), так і для негативних завдань (виявлення та розкрадання персональних даних користувачів шляхом поширення недостовірної інформації у процесі імітації легітимних користувачів). Політики можуть використовувати подібний тип ботів для спілкування зі своєю цільовою аудиторією та отримання зворотного зв'язку, компанії застосовують їх як віртуальні агенти з обслуговування клієнтів.

2. Технічні роботи – різновид програми, що застосовуються для виконання одноманітних дій в SN, як правило з метою підвищення числа позитивних відгуків (накручування лайків), підвищення рівня ранжування інформації в стрічці новин, і додавання простих коментарів з метою подальшого репоста. Даний тип робіт реалізують функцію соціалізації для інших користувачів або робіт в SN шляхом додавання їх у відповідні тематичні списки з метою підвищення рівня довіри до них у активній спільноті

3. Бойові боти характеризуються призначенням щодо відкладених (спланованих у часі за розкладом) різних активних дій, пов'язаних з обробкою облікових записів користувачів SN або публікацією цільового контенту. Як правило, дані боти використовуються для негативних завдань, вони можуть бути тривало не активними, активізуюся в заданий момент і отримуючи доступ до персональних даних користувача в момент початку інформаційної операції використовуються, наприклад, для публікації негативних відгуків або коментарів [10].

4. Тролі представляють найбільш агресивний та негативний тип ботів у SN. Даний тип ґрунтується на застосуванні різних семантичних та лексичних наборів даних, що є деякою подобою словників і містять текстові набори

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

різних ключових слів за заданою тематикою. За словниками роботи знаходять необхідні цільові публікації в постах або стрічках SN, публікують ворожі та образливі коментарі користувача, тим самим провокуючи не конструктивні та асоціальні суперечки між членами віртуального співтовариства, формуючи негативний інформаційний фон та поширюючи деструктивний інформаційний.

5. Дезінформатори є окремим гібридним видом ботів-тролів та соціальних ботів для виконання негативних завдань з імітації діяльності користувачів у SN, входять у довіру співтовариства, після чого плавно публікують заданий шкідливий або хибний контент для інформаційного впливу на користувачів. У випадках їх успішної діяльності сформована дезінформація лавиноподібно поширюються як у рамках SN, так і поза нею, зокрема у ЗМІ.

6. Боти-спамери застосовуються в SN для поширення контенту не несе користі, зокрема це може бути публікація застарілих та не актуальних відомостей. Метою цього типу шкідливих ботів є ускладнення сприйняття користувачами публікованого контенту, внесення шуму чи засмічення хештегів, тобто. спамери призначені виключно для виконання зловмисних дій. Популярними діями даного типу роботів є поширення інформаційного чи персонального контенту серед користувачів без дозволу правовласниками.

7. Впливові боти - це тип ботів, які здійснюють інформаційні дискусії щодо обраних тенденцій або тематик у розділах SN для просування та популяризації заданих тем. Частково їх принцип роботи ґрунтується на ботах дезінформаторів, при цьому їх складніше виявити. Цей тип роботів зазвичай генерують повідомлення шляхом повторного використання чужого контенту з незначним рерайтом вмісту або створюють авторські повідомлення за допомогою певного семантичного набору правил. Оскільки впливові облікові записи мають одну зі своїх цілей щодо поширення контенту на максимальну кількість людей, тому вони намагаються надіслати найбільшу кількість запитів у друзі до розповсюдження контенту. Вплив конкретного користувача в SN залежить від його рівня популярності та довіри в мережі, іноді цей критерій оцінюється як кількість вхідних запитів або отриманих повідомлень. Основне завдання подібних ботів полягає у зміні думки або відношення користувача з конкретної тематики або продукту [11].

Останнім часом, починаючи з фази появи COVID-19, ситуація з проявом негативної активності з боку ботів значно загострилася. Ризики використання ботів пов'язані з різними аспектами інформаційної безпеки, що найчастіше зустрічаються такі негативні аспекти їх використання на практиці:

1. Використання не ефективних налаштованих та функціонуючих ботів у службах підтримки клієнтів може призвести до втрат у бізнесі та подальшого банкрутства компанії. Слід зазначити, що рівень довіри до компанії знижується у разі, коли в роботі робота спостерігається надмірна кількість безглузвих питань, відсутність емоційного співчуття та конкретних відповідей на питання, а також неможливість підтримки процесу вирішення складних складових проблем. Все це призводить до того, що клієнти почуваються обдуреними.

2. Використання ботів для завдань збору даних (парсингу) із сторонніх ресурсів. Загрози від використання роботів даному ракурсі полягають у

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

крадіжці унікального контенту з ресурсу з метою подальшої його публікації без посилань на джерело. Це призводить до того, що рівень авторитетності ресурсу-джерела в пошуковій видачі знижується, призводячи до скорочення цільової аудиторії, рівня продажу та обсягів рекламних доходів. У тому числі збирання даних використовується для автоматизації відстеження цін на товари у конкурентів для подальшого демпінгу та відсікання клієнтської бази або для перепродажу товарів з націнкою. Можливі ризики створення хибних замовлень з метою завантаження логістичних ресурсів збільшення витрат компаній конкурентів і забезпечення тимчасової недоступності товарів замовлення іншими користувачами [8].

3. Накручування показників. Боти вносять шумові дані в статистику та аналітику бізнес-завдань компанії, впливаючи на показники конверсії, кількість лідів, параметри виври продажів, що веде до нерациональних рішень та зайвих маркетингових витрат. У контексті SN некоректні дані можуть бути внесені до спільноти або групи під час проведення онлайн-голосувань, де використовувані боти можуть штучно завищувати різні показники для просування своїх цілей чи людей.

4. Автоматизація проведення DDoS-атак (класу "відмова в обслуговуванні"), які сфокусовані на вплив за обчислювальними системами (веб-серверами та серверами додатків, іноді це також можуть бути канали зв'язку) для створення ситуації, в якій дані системи та сервіси стають недоступним користувачам. Технічно DDoS-атаки виражаються у формі одночасної (паралельної) відправки на адресу певного веб-сайту або сервісу великої кількості запитів на читання даних з безлічі розподілених комп'ютерів у мережі Інтернет. Процес впливу зумовлений тим, що велика кількість (десятки і сотні тисяч) запитів з різних комп'ютерів (керованих ботами) за адресою певного сервера (сервісу) призводить до фізичної неможливості їх оперативної обробки, тобто. може бути переповнені обсяги виділеної для обробки даних пам'яті або смуга пропускання каналу зв'язку не зможе забезпечити проходження запитів на сервер

І в першому, і в другому випадках, користувачі не зможуть отримати доступ до такого сервісу або до інших веб-сайтів (на вкладених доменах, зокрема) через звернення через канал зв'язку. Метою проведення DDoS-атак є отримання матеріальної вигоди за допомогою виконання здирицтва за припинення таких атак, або досягнення необхідних політичних інтересів.

Найбільш активним використовуваним методом ефективних DDoS-атак є метод створення ботнетів, які є заражені вірусним ПЗ комп'ютери, що містять у своєму складі відповідні програмні закладки для реалізації потрібної реакції.

У більш широкому значенні ботнетом називається мережа автоматизованих комп'ютерних роботів. Кожному роботі в цій мережі надається свій набір цільових завдань, які повинні виконуватися автоматично за певними подіями або умовами. У зв'язку з тим, що мережа ботів складається з їх наборів – контролер (керівна ланка системи) може динамічно виконувати різні шкідливі завдання, у тому числі розповсюдження небажаного рекламного, хибного чи вірусного контенту, надсилання запитів користувачам із соціального графа

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

(переліку друзів) користувачів SN з метою отримання коштів та заклику до інших дій [12].

2. Постановка проблеми та аналіз існуючих підходів та публікацій

Останні досягнення в мовних моделях можна пояснити переважно методами глибокого навчання, прогресом у нейронних архітектурах, таких як трансформери, розширеними обчислювальними можливостями та доступністю навчальних даних, отриманих з Інтернету. Ці розробки призвели до революційної трансформації, дозволивши створити LLM, здатні наближати продуктивність людського рівня за певними тестами оцінки [9, 16].

LLM, особливо попередньо підготовлені види даних моделей, згідно з рядом досліджень [17] здатні надати широкі можливості для розуміння, аналізу, оцінки та генерації текстового контенту широкому діапазоні завдань.

У зв'язку з цим попит на LLM виріс, у тому числі через зростаючу потребу в машинах для виконання складних мовних завдань, таких як переклад, резюмування, пошук інформації та розмовна взаємодія. LLM досягають цієї майстерності шляхом самостійного навчання на великих наборах текстових даних [18].

Після точного налаштування (тюнінгу) виконання завдань з аналізу різномірних текстів великих обсягів LLM демонструють істотне підвищення продуктивності, часом [19] перевищуючи ефективність моделей, навчених повністю з нуля.

Ці риси мовних моделей сприяють застосуванню LLM при їх навчанні на великих наборах даних, що дозволяє відзначити той факт, що масштабування розмірів самих моделей і обсягів використовуваних для навчання і тестування наборів даних призводить до подальшого вдосконалення їх узагальнюючої здатності.

LLM також починають часто використовуватись у бізнесі. Наприклад LLM можливо використовувати для менеджменту бізнес-процесів, зокрема виконання таких процесів: видобуток імперативних моделей процесів з текстових описів, видобуток декларативних моделей процесів з текстових описів, та оцінка придатності завдань процесу з текстових описів для роботизованої автоматизації процесів. Вони показали, що без масштабної конфігурації чи *prompt-engineering* LLM працюють порівняно або краще, ніж існуючі рішення. Це дослідження є аргументом на користь того, що має сенс порівнювати різні LLM задля обрання найкращих з них для бізнес-задач.

LLM часто базуються на архітектурі глибоких нейронних мереж, які застосовують архітектуру трансформерів. Трансформери - це клас моделей глибокого навчання для роботи з послідовностями чи множинами даних, ці моделі засновані на механізмі самоуваги. Цей механізм дозволяє моделі акцентувати увагу на конкретних елементах послідовності залежно від інших елементів та краще розуміти зв'язки між словами. Вони ефективним чином вловлюють складні контекстуальні зв'язки в тексті, що робить їх основою

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

багатьох найсучасніших програм NLP. Їхня архітектура дозволяє виконувати паралельну обробку, що робить їх високоефективними та масштабованими для різних завдань, окрім обробки мови, таких як розпізнавання зображень і навчання з підкріпленням. Важливими аспектами трансформерів є [9]:

1. Механізм самоуважності. Цей динамічний механізм дає змогу моделі фіксувати довгострокові залежності та асоціації між словами в послідовності.

2. Увага кількох голів. Замість того, щоб покладатися на єдиний механізм уваги, трансформери використовують кілька “голів уваги”, що працюють паралельно. Кожна головка спеціалізується на фіксуванні різних взаємозв’язків у даних, а їхні результати об’єднуються, щоб охопити широкий спектр інформації.

3. Складені шарів. Трансформери зазвичай складаються з кількох ідентичних слоїв, складених послідовно. Кожен шар удосконалює представлення, отримані від його попереднього, дозволяючи моделі охоплювати дедалі складніші та абстрактні характеристики.

4. Вихідний рівень у завданнях класифікації вихідний рівень генерує ймовірності класу, тоді як у завданнях генерації послідовності він послідовно створює вихідну послідовність.

5. Навчання: Трансформери навчаються за допомогою алгоритмів зворотного поширення та оптимізації, таких як ADAM. Специфічні для завдання функції втрат, такі як перехресна ентропія для класифікації, зведені до мінімуму під час навчання. Попереднє навчання великим мовним корпусам, як це видно в таких моделях, як BERT і GPT, стало ключовим фактором їх успіху.

Ця комбінація характеристик обумовлює успіх LLM на основі трансформерів, але при використанні даного механізму існують також і недоліки. Деякими з них є наступні [10]:

1. Обчислювальна складність. Навчання та використання трансформерів може бути витратним процесом, особливо для великих моделей, таких як GPT-3. Це може бути основною перешкодою для їх розгортання в реальних програмах, особливо для невеликих організацій і окремих осіб, які можуть не мати доступу до необхідних потужних обчислювальних ресурсів.

2. Перенавчання. Моделі трансформерів можуть бути легко перенавчені, особливо якщо дані невеликі або недостатньо різноманітні. Це може призвести до низької продуктивності узагальнення раніше невідомих даних. Це може відобразитися у значній зміні результату роботи трансформера при незначній зміні опрацьованого речення без зміни його сенсу.

3. Довгострокові залежності. У моделей трансформерів можуть виникнути труднощі з моделюванням довгострокових залежностей у послідовностях, особливо в ситуаціях, коли залежності охоплюють кілька токенів. Це також залежить від методу позиційного енкодування.

4. Прихильність уваги. Моделі даного типу покладаються на механізми уваги, щоб визначити, які частини вхідної послідовності є найбільш релевантними. Однак іноді ці механізми можуть бути прихильні до деяких значень більш за інші, що призводить до неоптимальних результатів.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

5. Можливість інтерпретації. Такі моделі можуть бути складними для інтерпретації та розуміння, оскільки вони не мають чітких проміжних представлень, які можна інтерпретувати, як ті, що виробляються деякими іншими архітектурами нейронних мереж.

Також слід відвести увагу на те, що великі мовні мережі за своєю архітектурою не моделюють чітких логічних зв'язків у реченні. Механізм самоуваги надає реальні числа як позначення уваги до елементів речення, що є механізмом нечіткої логіки, та не завжди буде ідеальним методом моделювання мови.

Аналізуючи характеристики LLM, та недоліки їх найпопулярнішої архітектури, зроблено висновок, що велика складність імплементацій трансформерів, а також характеристики та недоліки найпопулярнішої архітектури (трансформери), обґрунтовують створення платформи для експериментування над та порівняння не тільки існуючих архітектурних рішень LLM, а що й забезпечує можливість експериментувати над іншими майбутніми архітектурами BMM, та експериментувати з використанням майбутніх допоміжних методик задля покращення результатів роботи LLM. Слід зазначити, що згідно з рядом досліджень [20] на якість результатів LLM впливає не лише подання прикладів виконання завдання у запитів, але й те, як саме завдання було описано природною мовою в запиті.

Важливою частиною роботи з LLM є інжиніринг запитів (фрагменти текстових запитів, що надсилаються на вхід моделі, які формалізують завдання, яке LLM має виконати, з урахуванням додаткових правил, підказок, прикладів та змістового контексту) для підвищення ефективності та точності їх використання. Даний процес, на думку авторів [21], заснований на послідовному виконанні процедур зміни та оптимізації вхідних запитів для підвищення цільового результату, згенерованого LLM для прикладних завдань.

Важливим аспектом у цьому випадку є те, що підсумкова якість роботи моделі може значно змінюватись в залежності від того, як саме був сформований запит, навіть у тому випадку, коли два різні запити мають однакову сутність та мету, але різні процедури формування.

Як результат роботи подібної моделі ANN можна сформувати широкий розподіл ймовірностей можливих токенів, що є продовженням текстових речень. Вибір кінцевого токена для моделі часто визначається за допомогою виконання етапів вибірки даних та її тюнінгу, у цьому випадку важливу роль відіграє підбір значень гіперпараметрів, які можуть впливати на компроміс між різноманітністю та точністю згенерованого тексту [22].

Все це може бути корисним при оцінці текстових постів користувачів в SN для аналізу їх профілів щодо наявності аномальної поведінки і виявлення ботів.

Як результат роботи LLM отримується розподіл ймовірностей можливих токенів - продовжень речень. Вибір кінцевого токена часто визначається за допомогою процесу вибірки, де гіперпараметри відіграють ключову роль. Ці гіперпараметри можуть впливати на компроміс між різноманітністю та точністю згенерованого тексту [21].

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

Гіперпараметри, такі як "temperature", використовуються для контролю рівня випадковості у виводі LLM. Вище значення температури призводить до більш різноманітних, але потенційно менш зв'язних відповідей, оскільки модель досліджує ширший діапазон можливостей. І навпаки, нижче значення температури робить вихід більш детермінованим, сприяючи точності та узгодженості за рахунок різноманітності. Це створює додатковий аспект у порівнянні LLM, бо різні комбінації гіперпараметрів можуть призвести до різної якості результатів роботи LLM [22]. Це особливо стосується пропріетарних моделей, бо компанії які їх надають частіше не дозволяють переглянути отриманий розподіл ймовірностей токенів, тому для оцінки якості моделі з різними гіперпараметрами знадобиться проводити експериментування з різними параметрами, на відміну від можливого аналізу отриманого розподілу ймовірностей при використанні відкритих LLM. Слід зазначити, що одним із ключових недоліків поширених типів архітектур LLM, наприклад, трансформерів, є неможливість моделювати чітку логіку виконання запиту та схильність моделей до фактичних помилок на великих текстових промптах [11,17,19]. Для боротьби з подібними проблемами активно розробляються та досліджуються різні методи підвищення точності та якості роботи LLM під різні змістові контексти.

Прикладом підходу, що використовується, наприклад, є підключення реляційних або не реляційних баз даних як джерела актуальної інформації та символічної пам'яті, що спрощує моделям процес обробки даних.

У цьому випадку, поєднуючи метод ланцюжка знань та БД, можна надати BMM можливість доступу до фактичної та символічної інформації, отриманої або збереженої за потребою [17].

Таким чином, аналізуючи існуючі праці з дослідження даної тематики, незважаючи на виявлені складності використання LMM та їх недоліки, слід відзначити актуальність та доцільність розробки та використання таких моделей для завдань аналізу текстових даних, зокрема, у контексті виявлення ботів у SN.

Метою роботи є розробка та дослідження інтелектуальної системи аналізу та детекції текстового бот-контенту великого обсягу у соціальних мережах на базі застосування глибинного навчання та LLM підходу.

3. Розробка концепції проекту

Для реалізації та застосування функціоналу моделей ANN у рамках аналізованої проблематики необхідно знайти або створити набори тестових даних значного обсягу. Як основу вирішено використовувати існуючі фрагменти наборів даних, що знаходяться у відкритому доступі, провівши їх попередню обробку, очищення, а також агрегувати ряд адаптованих вибірок для надання даних більшого балансування та різноманітності. Для завдання виявлення ботів у SN, яку доцільно звести до завдання класифікації використано набір даних "PAN19 Author Profiling" [23]. Цей набір даних був

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

створений з метою допомогти визначити онлайн-ботів користувачів. Набір даних включає по 100 публікацій різних користувачів у соціальній мережі Twitter, а також індикатор того, чи є даний користувач ботом. Набір даних є збалансованим. Для оцінки адекватності та точності LLM за цим набором даних доцільним є використання метрик бінарної класифікації, такі як accuracy, recall, precision, f1. Для проведення експериментів над популярними та новими LLM необхідно забезпечити доступ до їхнього функціоналу за допомогою підключення доступних API. Провівши аналіз доступних варіантів встановлено, що:

- Для пропріетарних моделей доступ надається найчастіше завдяки спеціально розробленим для них API під завдання генерації тексту.

- Для open-source моделей можна отримати доступ завдяки публічним репозиторіям та реалізованим драйверам підтримки їхнього залучення в роботу.

- Для самостійної розробки мовних моделей необхідно створити свій або використовувати існуючий фреймворк тренування та активації LLM.

В рамках цього дослідження прийнято рішення використовувати такі моделі LLM (адаптувавши їх під наше завдання): GPT2, Bloomz-1b1 та Mistral-7B. GPT2. У порівнянні з найновішими моделями GPT2 має значно менше параметрів та значно меншу здатність розуміти текст. Але через невеликий розмір моделі було вирішено використовувати GPT2 як базовий "нульовий" рівень якості при порівнянні з іншими моделями, тому що її результат роботи можна швидко обчислити, що сприяє реалізації концепції порівняльного тестування моделей. Bloomz-1b1.

Це open-source LLM приймає близько 1.1 мільярд параметрів, що відносно мало в порівнянні з іншими моделями. Це зменшує її потенціал до розуміння тексту, але її використання дозволить виміряти наскільки гнучкими завдання виявлення ботів в SN можуть бути LLM при відносно малій кількості параметрів. Також це дозволить проводити локальні експерименти відносно швидко.

Дана модель спочатку навчена для аналізу семантичних інструкцій у тексті, що доводить її доцільність при аналізі текстових постів розмовної стилістики. Mistral-7B. Модель з відкритим кодом розроблена MistralAI. модель, розроблена на вирішення завдань NLP з високим рівнем продуктивності. На думку авторів [24], Mistral 7B перевершує Llama 2 13B за всіма оціночними показниками, модель використовує увагу до згрупованих запитів для більш швидкої генерації, у поєднанні з увагою до ковзних вікон для ефективної обробки послідовностей довільної довжини зі зниженою швидкістю генерації. Використання даної моделі дозволить більш репрезентувати сферу розробки LLM з відкритим кодом, в даному випадку представляється модель більшого розміру, ніж bloomz-1b1 і з можливістю вказувати інструкції. Для адаптації моделей даної задачі пропонується використовувати концепцію індуктивного типу transfer learning (TL) з елементами кросмодальності [11, 17, 25].

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

Якщо $f_{w,s} : X \rightarrow Y$ буде попередньо навченою моделлю на вихідному наборі даних D_s де $w_s \in \mathcal{R}^D$ позначає D -вимірний ваговий вектор попередньо підготовленої LLM. Враховуючи цільовий набір даних D_t , метод тонкого налаштування мінімізує стандартний негативний логарифм правдоподібності $L_t(w) = \sum_{i=1}^{N_t} \log p_w(\frac{y_t^i}{x_t^i})$ за допомогою стохастичного градієнтного спуску $w(t+1) = w(t) - \eta \nabla_w L_t(w)$, $w_0 = w_s$, де η це розмір кроку і $\nabla_w L_t(w)$ позначає стохастичну оцінку градієнта втрат з використанням міні-пакета даних.

Таким чином, точне налаштування є оцінкою максимальної правдоподібності, на якій зосереджено логарифмічний пріоритет W_s .

Використовуючи наведені вище передбачені моделі, ми скорочуємо час навчання тренуючи тільки останній шар моделей зі значно меншою кількістю змінних. Це пов'язано з тим, що якщо не "заморозити" змінні попередньої моделі, то в процесі навчання на новому наборі даних значення змінних будуть змінюватися (останній шар буде заповнений випадковими значеннями), у зв'язку з цим моделі можуть допускати великі помилки при аналізі тексту, що, у свою чергу, спричинить сильні зміни вихідних ваг у передбачуваній моделі.

Перевагою доступу до вибраних моделей LLM за допомогою вибраного API є підтримка використання обчислювальних можливостей компанії, що надає доступ до LLM, але недоліком цього є різні URL-адреси та формати запитів до API залежно від політики та обмежень, що накладаються компанією, що надає доступ до LLM.

Це ускладнює проведення досліджень, т.к. необхідно реалізувати методи здійснення різних форматів запиту.

Для вирішення цієї проблеми було вирішено використати сервіс OpenRouter. Цей сервіс дозволяє виконувати запити до пропрітарних LLM, використовуючи єдиний інтерфейс, незалежно від конкретної моделі та компанії, що надає доступ до неї.

Для обраних open-source моделей було вирішено адаптувати публічний репозиторій для отримання натренованих LLM та датасетів для них – "Huggingface", а також бібліотеку, розроблену цим сервісом, "transformers".

Завдяки даному репозиторію, можливо вести індексування найпопулярніших LLM з часом, за допомогою "transformers" забезпечується можливість локального запуску більшості моделей безпосередньо з репозиторію завдяки спеціальному програмному інтерфейсу для їх використання.

На основі концепції проекту створено діаграму варіантів використання, результат наведено на рис. 1. Технічна сторона виконання досліджень

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

вибраних LLM моделей реалізована у вигляді клієнт-серверної веб-додатки зі спрощеним графічним інтерфейсом користувача.

Для впровадження основної функціональності розробленого проекту обрано мову програмування Python версії 3.7.12, що дозволяє використовувати зручні колекції даних та інтегрувати бібліотеки з обробки та аналізу текстових даних. Для впровадження ряду функціональних можливостей у рамках веб-програми необхідно створити інтерактивну взаємодію між користувачем та веб-сторінкою, з цією метою використана мова програмування JavaScript. Для побудови каркасу веб-застосування та покращення роботи з БД вирішено використовувати фреймворк Django.

Для зберігання даних прийнято рішення використовувати реляційну БД PostgreSQL, створена БД з 4 таблиць для зберігання метаданих про моделі, результати експериментів, набори гіперпараметрів і датасетів.

Для забезпечення більш простого управління залежностями та версіями, можливості запускати пропонувану платформу на багатьох платформах та логічного розподілу архітектури системи вирішено використовувати Docker та Kubernetes.

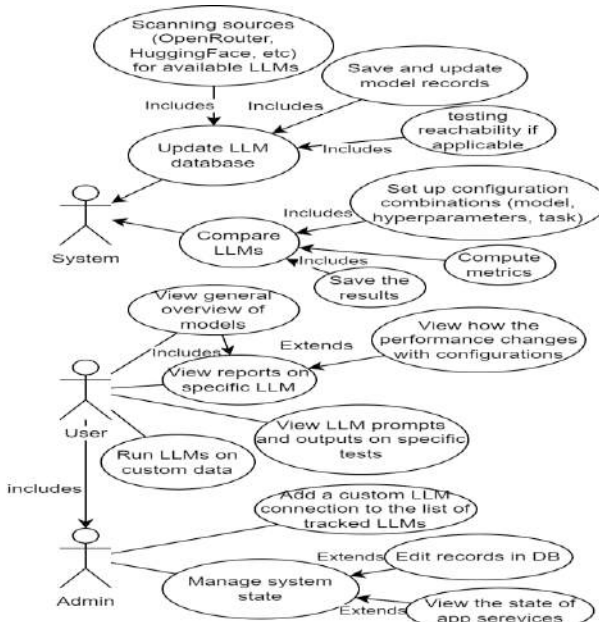


Рисунок 1. Діаграма варіантів створеного проекту системи

Особливістю програмної імплементації проекту є широкий перелік конфігурацій задачі аналізу текстових постів для виявлення ботів у SN,

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

інтеграція з платформою X для отримання доступу до даних відкритих постів та для автоматизації оцінки LLM, а також функціонал автоматичного трекінгу моделей у відкритих репозиторіях, що обумовлено раніше описаною зміною їх якості із різними версіями.

Веб-додаток використовується таким чином: користувач взаємодіє із системою через веб-додаток, він може вибрати різні роути, кожен з яких надає функціонал, необхідний для задоволення функцій користувача.

Процес експериментування проводиться автоматично, система вибирає комбінації LMM, конфігурацій і завдань, у яких слід провести експерименти, зберігаючи отримані результати таблиці БД. Адміністратор - користувач, який проводить хостинг розробленої платформи для проведення експериментів у ручному режимі, задаючи конфігурації, використовуючи та тестуючи новітні моделі та методи, вносячи модифікації в методології проведення експериментів, а також редагуючи відкритий код розробленого веб-додатку.

Діаграма компонентів системи, задіяних у процесі розгортання, наведена на рис.2. Кластер складається з наступних елементів (кожен вузол – окрема віртуальна чи реальна машина):

1. Вузол управління. На цьому вузлі виконуються завдання, пов'язані з оркестрацією завдань, передачею повідомлень та управління кластером. Саме він розміщує елемент управління кластером kubernetes (“Control Plane”), сервер брокера повідомлень Kafka для комунікації даними та повідомленнями між окремими аплікаціями в кластері, та сервер оркестрації робіт Apache Airflow для виконання завдань з трекінгу та оцінки мовних моделей. Оскільки цей вузол є найважливішим у кластері, вирішено не розміщувати на ньому тільки той код, який взято з довірених бібліотек (Kubernetes, Kafka, Apache Airflow).

2. Вузол постійних БД. На цьому сайті розміщуються сервери баз даних, необхідні для кластера. Розміщуючи їх на окремій машині, дозволить оптимізувати цей вузол під постійне збереження даних.

3. Вузол веб-сервера. На цьому вузлі знаходиться веб-сервер для взаємодії користувачів із системою, а також метод створення повідомлень Kafka (це необхідно для функціоналу, де користувач вимагає виконання генерації деякою моделлю).

4. Вузол трекінгу та оцінки мовних моделей. На цьому вузлі розміщуються контейнери та методи виконання трекінгів мовних моделей та їх оцінки. До того ж, ці методи запускаються виконавцем завдань Airflow, якщо оркестратор вирішує їх запустити, і вузол також розміщує метод створення повідомлень Kafka (це необхідно для функціонала, де потрібно запросити створення тексту).

5. Вузол запуску мовних моделей. На вузлі розміщуються методи генерації тексту мовними моделями, а також метод отримання повідомлень Kafka про генерацію тексту.

6. Інтернет. Кластеру необхідно мати доступ до Інтернету для обслуговування запитів користувачів, знаходження та трекінгу мовних моделей, а також посилання на API запитів на генерацію тексту для оцінки моделей.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

7. Хост. Вузлу керування кластера необхідно мати доступ до хост-машини, з якої він отримуватиме команди з керування сервером.

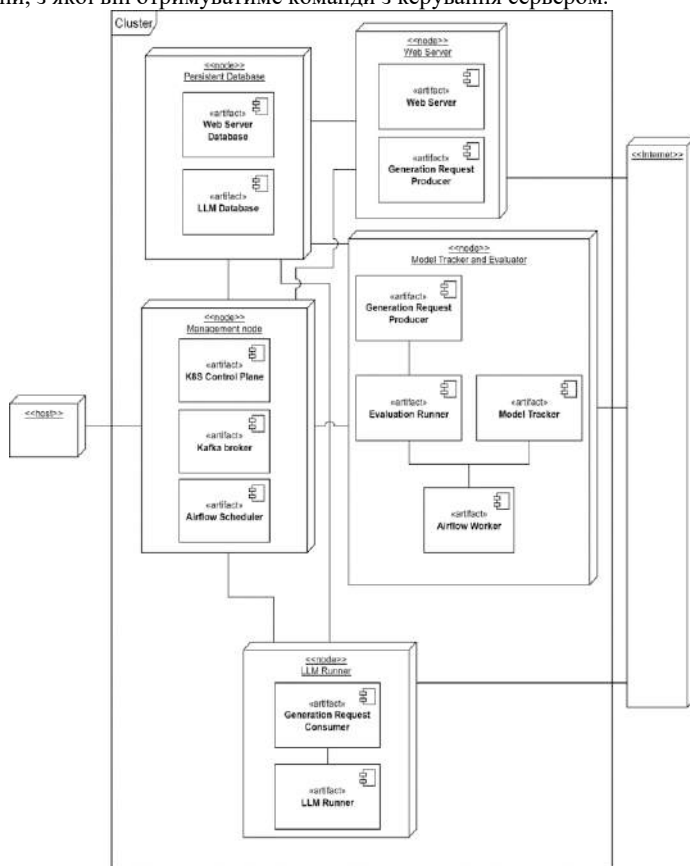


Рисунок 2. *Діаграма послідовності дій системи*

Для створення системи було вирішено в першу чергу реалізувати 4 головні сторінки, що відповідають функціональним вимогам: сторінка з навігацією, сторінка з переглядом метрик конкретної LLM на задачах аналізу тексту, сторінка з переглядом відповідей LLM щодо набору постів для задачі класифікації, сторінка з можливістю внесення користувачем даних щодо завдання та отримання результатів роботи LLM. Дані сторінки дозволять отримати ключові результати оцінки роботи моделей і відповідатимуть за більшу кількість інформації, яку можна відобразити у звітах. За цими вимогами було розроблено мокап інтерфейсу (рис.3, 4). Для збереження та управління даними вирішено розробити базу даних (БД) на базі використання NoSQL підходу, який на відміну від реляційної бази, є дозволить мати більшу

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

гнучкість стосовно структури БД під час розробки, що допоможе у випадку зміни вимог та структури проєкту. У якості СУБД було обрано MongoDB через її велику популярність та наявність документального матеріалу.

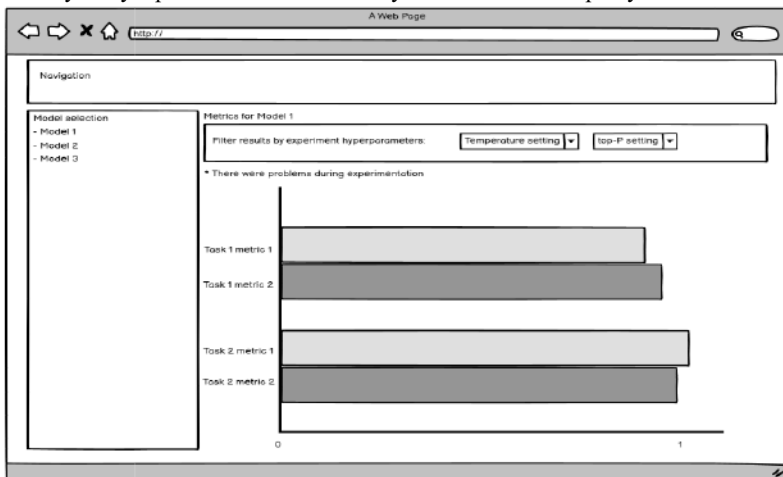


Рисунок 3. Прототип інтерфейсу головної сторінки системи

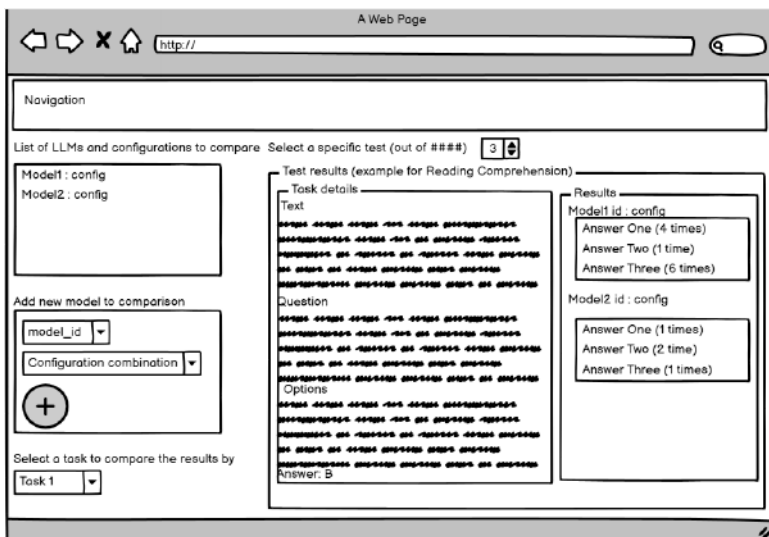


Рисунок 4. Прототип інтерфейсу сторінки з переглядом результатів роботи LLM на тестах

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

Структура бази даних для запропонованої платформи та їх евалуації зображена на діаграмі (рис.5).

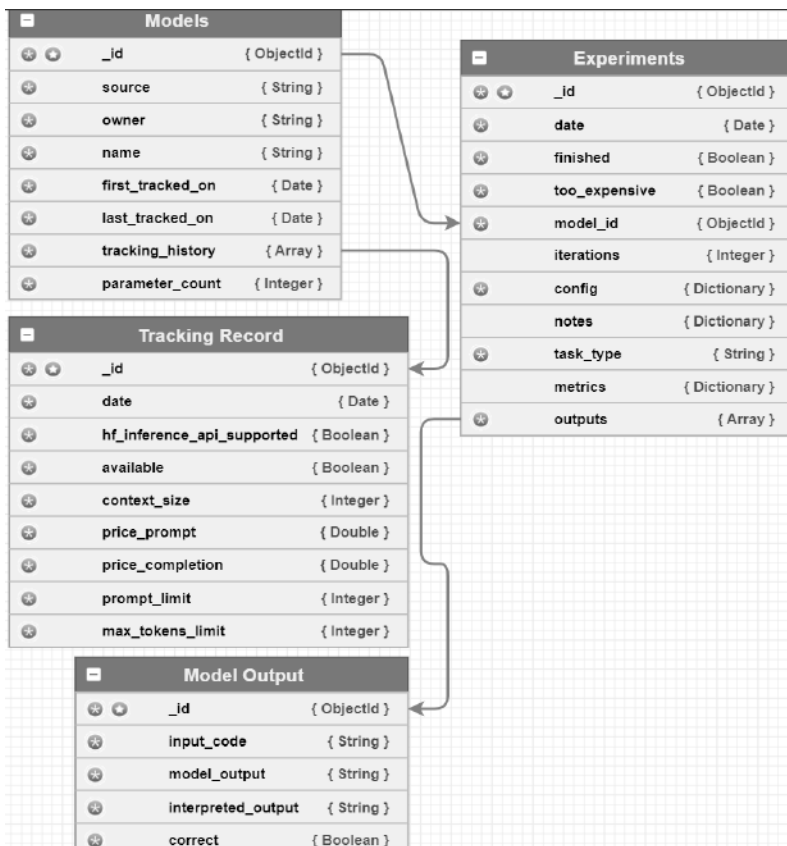


Рисунок 5. Структура колекцій створеної БД

Структура бази даних розподілена на дані частини, починаючи з колекції моделей, яка складається з наступних полів не зважаючи “_id”:

1. Source - джерело з якого є доступ до мовної моделі. Цей параметр необхідний для визначення того, яким саме методом буде виконана генерація тексту..

2. Owner - компанія чи користувач, який надає доступ до моделі

3. Name - назва моделі.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

4. `First_tracked_on` - дата, коли система вперше здійснила перший трекінг моделі.

5. `Last_tracked_on` - дата, коли система вперше здійснила останній трекінг моделі.

6. `Tracking_history` - масив об'єктів з записами о трекінгу моделі.

Об'єкти записів трекінгу:

1. `Date` - дата створення запису трекінгу.

2. `Hf_inference_api_supported` - чи підтримує модель використання API Huggingface для генерації тексту (має сенс лише у випадку коли джерелом є huggingface).

3. `Available` - чи є доступ до моделі узагалі.

4. `Context_size` - максимальний розмір контексту який підтримує модель.

Запис експерименту:

1. `Date` - дата початку експерименту.

2. `Finished` - чиє експеримент завершеним.

3. `Too_expensive` - чи був експеримент завершений через перевищення ліміту на ціну генерації.

4. `Model_id` - ID мовної моделі, над якою був проведений даний експеримент.

5. `Iterations` - На даний момент не використовується. Може бути використаний для позначення кількості ітерацій над набором даних, у тому випадку де це релевантно.

6. `Config` - словник, визначаючий конфігурацію яка була використана для генерації тексту.

7. `Notes` - словник, не використаний на даний момент, але може бути використаний для позначення спеціальних заміток.

8. `Task_type` - позначає тип задачі над якою був проведений відповідний експеримент.

9. `Metrics` - словник з метриками, які оцінюють якість моделі в завершеному експерименті.

10. `Outputs` - масив з детальними результатами роботи усіх мовних моделей.

Запис результату роботи моделі:

1. `Input_code` - код, який ідентифікує який саме запис з якого набору даних був використаний для генерації отриманого тексту.

2. `Model_output` - текст, який був згенерований моделлю.

3. `Interpreted_output` - те, як згенерований текст був інтерпретований при оцінці моделі (наприклад, згенерований текст "(A)" в задачі на вибір варіанту відповіді буде інтерпретовано як "A").

4. `Correct` - чи збігається інтерпретований результат з очікуваним в даному тесті, якщо це актуально.

Потрібно врахувати те, що в обраній NoSQL базі даних ("MongoDB") об'єкти записів трекінгу, експериментів та виводів моделей можуть бути як окремими колекціями, так і частинами іншого об'єкта (наприклад, записи трекінгу можуть бути частинами запису мовної моделі).

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

На даний момент, для гнучкості розробки було вирішено створити дві окремі колекції - моделей та експериментів, з вбудованими записами трекінгу та виводів моделей.

Проект структурований за каталогами так:

- `experiment_running`, що містить програмну логіку імплементації процесу запуску моделей LLM;

- `frontendapp`, містить реалізацію процесів завантаження та відображення даних в інтерфейсі користувача за різними роутами через RESTAPI запити. Містить підкаталоги `migrations` та `templates` для зберігання скриптів виконання міграції даних у БД та html сторінок розмітки уявлень;

- `lpprofrontend`, містить програмну логіку роботи сервісних функцій фреймворку Django для базового функціоналу роутингу та спільної роботи адміністративної панелі;

- `model_running`, імплементує ключовий програмний функціонал забезпечення процесів побудови моделей LLM, завантаження наборів даних та їх розбиття на навчальну та тестову підвиборки, лематизацію та токенизацію, нормалізацію даних, формування окремих промптів, функції зворотного виклику для обробки та збереження метрик оцінки моделей LLM при десері побудові;

- `model_tracking`, реалізує функціонал відстеження змін у метриках формованих моделей;

- `mongodb`, містить конфігурацію побудови схеми БД для зберігання даних про LLM.

Деталізована структура файлів у пакетах проекту системи наведена на рис.6.

Окремо слід зазначити, що базова бізнес логіка роботи системи з управління потоками та рендерингом даних у рамках запуску веб-дodatка знаходиться в каталозі `frontendapp`, у тому числі файли, що генеруються при ініціалізації проекту: `admin.py`, призначений для адміністративних функцій, зокрема для процедури реєстрації моделей, які використовуються в інтерфейсі адміністратора; `apps.py`, визначає базову конфігурацію програми та не стандартні параметри її запуску; `models.py`, зберігає визначення моделей, які описують дані, що використовуються в додатку; `tests.py`, описує модульні тести програми, моки, стаби та заглушки; `views.py` визначає функції, які отримують запити користувачів, обробляючи їх і повертаючи результат через сервер.

Запуск файлу здійснюється в командному рядку через менеджер пакетів `pip`. Перераховані залежності, що використовуються для шаблонізації (`jinjia2`), інтеграції коду (`Jupyter core`, `ipython` та ін.), підключення та взаємодії з БД (`pyMongo`, `sqlparse` та ін.), обробки даних, об'єктів та результатів роботи ІНС (`keras`, `tensorboard`, `torch`, `huggingface` та ін), підтримки асинхронних запитів та автоматизації розгортання проекту (`async-timeout`, `executing`, `ruyaml` та ін), аналізу та виведення даних (`numPy`, `pandas`, `matplotlib` та ін), а також бібліотеки утилітарної спрямованості (`кешування`, `асинхронність`) та ін).

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES



Рисунок 6. Деталізована структура файлів у пакетах проекту системи

В рамках проекту сформовано механізм автоматичної експериментальної оцінки LLM, та у даному розділі було описано одну ітерацію даного алгоритму. Його метою є оцінка LLM на деякій задачі, та збереження метрик у

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

базі даних. При розробці алгоритму, було визначено декілька факторів, які необхідно врахувати: 1. Необхідно проводити експериментування на кожній LLM періодично, бо, як було зазначено раніше, LLM можуть бути оновлені з часом. Це особливо стосується пропрієтарних LLM, про оновлення яких компанія-розробник може не об'являти. 2. Необхідно підготувати запити до LLM (комбінація інструкцій та тексту стосовно конкретної задачі) відповідно до особливостей LLM. Наприклад, деякі моделі оптимізовані до виконання інструкцій у запиті, якщо ці інструкції були виділені певним чином. Через це, при складанні запитів для експерименту, необхідно враховувати особливості певної моделі та відповідним чином складати запит. 3. Необхідно розраховувати ціну. 4. Необхідно враховувати те, що різні LLM мають різні методи їх виконання. Тобто, мала open-source LLM може бути завантажена та використана локально, тоді як більша LLM може бути використана через спеціальний сервіс, а пропрієтарні LLM можуть бути використані лише через деякі спеціалізовані API. Через це, необхідно обирати метод доступу в залежності від LLM. 5. Необхідно розраховувати вартість виконання експерименту, та звіряти її з допустимою ціною.

4. Дослідження роботи системи

У таблиці 1 представлені метрики для завдання визначення ботів в SN відповідно до історії їх публікацій на базі TL адаптованих LLM GPT2, bloomz-1b1, mistral-7b і без нього (в останньому випадку результати були в 3-4 рази гірше в порівнянні з адаптованим варіантом). Були проведені експерименти з двома типами запиту ("prompt type") - тип запиту "with explanation" у якому є пояснення щодо того, які публікації зазвичай роблять боти (рекламні пости, повторювані пости, посилання на новини, або надто монотонні пости), та запит "without explanation" у якому немає даного пояснення. Розмір доповненого набору даних складає 6760000 записів. Аналізуючи отримані результати, можна зробити висновок, що різні LLM мають значно різну якість незалежно від їх розміру. Наприклад, за метрикою Recall видно, що bloomz-1b1 відзначає користувачів як бот частіше ніж інші, тому її не має сенсу використовувати на практиці, тоді як модель mistral-7b, яка має той же розмір, виявила значно більшу точність (більше 0.9) як класифікатор ботів. Також mistral-7b за метриками відповідає кращим результатам, ніж gpt2 і bloomz-1b1, при цьому майже в 7 разів більше bloomz-1b1. Аналізуючи метрики BMM, що найбільш якісно впоралися з даним завданням (mistral-7b і bloomz-1b1), зроблено висновок, що точне знаходження ботів в онлайн-мережах завдяки LLM можливо проводити, проте для цього потрібно тонке налаштування та передобробка даних для отримання більшого ступеня адекватності та узагальнюючої здатності моделі, при цьому чутливість використаних LLM до ряду гіперпараметрів у разі проведених експериментів невелика. Тобто, під час формування моделей попередньо слід перевірити дані узгодженість. На додаток наголосимо на тому, що наявність у запиті пояснення того, якими

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

завичай є публікації від аккаунтів-ботів, негативно вплинула на якість LLM усім метрикам. Тому зроблено висновок, що при інжинірингу запитів слід враховувати те, що новий змінений формат запити може погіршити якість LLM, навіть якщо він має додану інформацію з наміром поліпшити якість моделі, тому необхідно проводити окрему процедуру оцінки нових форматів запити. Ітерація показників візуалізації на моделі GPT2 наведена на рис.7.

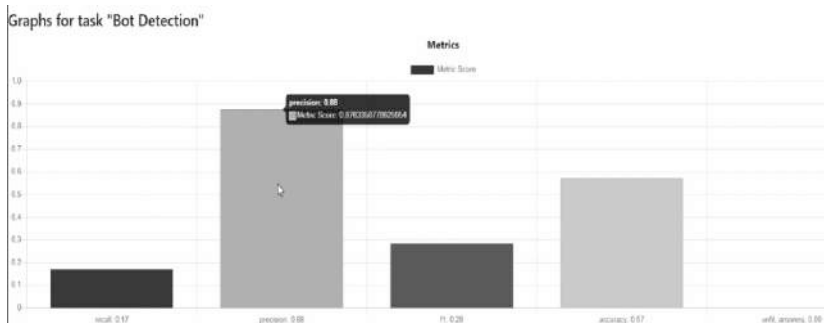


Рисунок 7. Ітерація показників візуалізації на моделі GPT2

Таблиця 4

Результати метрики LLM щодо завдання ідентифікації ботів у SN

LMM	Prompt Type	Recall	Precision	F1	Accuracy	Unfit Answers
gpt2	Without Explanation	0,87	0,66	0,22	0,75	15
gpt2	With Explanation	0,84	0,64	0,26	0,73	10
bloom z-1b1	Without Explanation	0,79	0,79	0,31	0,7	25
bloom z-1b1	With Explanation	0,77	0,78	0,28	0,72	23
mistral -7b	Without Explanation	0,95	0,9	0,14	0,92	2
mistral -7b	With Explanation	0,93	0,87	0,12	0,91	3

На рис.8 наведено результат перегляду фрагмента постів одного з користувачів (записів датасета), коли модель видає різні класи в залежності від довжини та змістовності запити.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

User's post history (user ID = 104eee2839f69f59af377fec70eaf7b):

- IT Security Analyst: IT Security Analyst – Berkshire – Permanent – SOC, Threat, vulnerability, SIEM, risk, malware Outsource UKs cyber team have an exciting opportunity for an IT Security Analyst to join an organisation that are currently insourcing... <https://t.co/sKOc98Plad>
- CRM Developer (Dynamics): I have an immediate requirement for a Dynamics CRM Developer to join my client on an initial 6 month contract (Outside of IR35) . You will be working on a major Dynamics 365 project for a leading organisation based in... <https://t.co/NEwKWpVe15> <https://t.co/mTipJar3V4>
- The election overseer for critical Palm Beach County says there is no way the recount for 3 races will be finished by Thursday's deadline: The election overseer for a critical county in Florida confirmed to CNN on Sunday what observers in both parties... <https://t.co/aXmntXQhBN> <https://t.co/Vol9MzVkpQ>
- Software Engineer – C++ / C# / UML: Software Engineer – C++ / C# / UML – Various Levels Commutable from Uxbridge / Slough / Watford / High Wycombe / Staines / Twickenham A market leading Global manufacturer is seeking to recruit a Software Engineer to... <https://t.co/wA0S8fmqZU>
<https://t.co/RmSKLPX8ME>

Рисунок 8. Приклад публікації бота, зібраний у набір даних

Користувач, текст якого наведено вище, на самому місці є ботом, часто публікує пости - вакансії на роботу та пости на ІТ тематику. Можливо припустити, що даний користувач є роботом іншої компанії для рекрутингу нових співробітників і не має негативного ефекту в рамках SN, т.к. контролюється співробітниками організації. Модель GPT2 класифікувала даний користувач як бота з впевненістю на 77%, bloomz-1b1 з 88%, mistral-7b з 94%. У цьому прикладі можна наглядно дослідити правильність роботи моделі LLM за класифікацією тексту користувача як належного боту. Це можна пояснити тим, що завдання формалізації в запиті описує публікації постів від ботів як такі, які містять явну рекламу (у тому числі посилань), повторювані та близькі за контекстом фрази в поштах, заголовки новин у різних реєстрах з використанням високореlevantних анкорів або занадто звучать. монотонно, без визнань зміни тональності тексту. Слідкуйте також за тим, щоб більша частина публікацій відзначила пости від даного користувача звучати більш енергійно.

5. Висновки

У результаті проведених досліджень виконано застосування та адаптація існуючих більших мовних моделей для обробки та інтелектуального аналізу різноманітних текстових більших обсягів при виявленні ботів у соціальних мережах. Розроблене веб-прикладення дозволяє підключати, вибирати, відстежувати оновлення в API та адаптувати вибрані LLM для вхідних наборів даних, автоматизуючи всі етапи аналізу даних в окремих пайплайнах за допомогою AirFlow та інших технологій. Адаптовані на базі TL моделі GPT2, bloomz-1b1, mistral-7b в цілому успішно справляються із задачами виявлення ботів у SN за їх текстовим постами, найбільша точність досягається моделлю mistral-7b без функції видачі пояснень. Виходячи з отриманих результатів дослідження, можна зробити висновок про те, що наявність додаткових

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

пояснень при аналізі агрегованих різнорідних текстів користувачів, обсяг яких перевищує довжину окремого місяця, часто накладає додаткові обмеження на роботу ANN, обмежуючи їх узагальнюючу здатність. У разі відсутності даного параметра робота моделі ANN є більш середньозв'язаною, однак цей ефект може бути пов'язаний зі специфікою використовуваного набору даних.

У подальшому раціональним шляхом дослідження є емпіричний пошук ступенів впливу даного параметра на робочу модель і виявлення його відносного значення в довільній формі з урахуванням підходу TL.

6. Література

- [1] N. Rudnichenko, V. Vychuzhanin, N. Shibaeva, I. Petrov, T. Otradska, Intelligent Data Clustering System for Searching Hidden Regularities in Financial Transactions, in: 11-th International Conference «Information Control Systems & Technologies» (ICST-2023) CEUR-WS, 3513, 2023, pp. 163-176.
- [2] V. Vychuzhanin, N. Rudnichenko, Z. Sagova, M. Smieszek, V. V. Cherniavskiy, A. I. Golovan, M. V. Volodarets, Analysis and structuring diagnostic large volume data of technical condition of complex equipment in transport. IOP Conference Series: Materials Science and Engineering, Volume 776, 24th Slovak-Polish International Scientific Conference on Machine Modelling and Simulations - MMS 2019, 3-6 September 2019, Liptovský Ján, Slovakia, 2019 pp.1-11. DOI:10.1088/1757-899X/776/1/012049.
- [3] N. Rudnichenko, V. Vychuzhanin, I. Petrov, D. Shibaev, Decision Support System for the Machine Learning Methods Selection in Big Data Mining, in: Proceedings of The Third International Workshop on Computer Modeling and Intelligent Systems (CMIS-2020), CEUR-WS, 2608, 2020, pp. 872-885.
- [4] C. Segalina, D. Cheng, M. Cristani, Social profiling through image understanding: Personality inference using convolutional neural networks, Computer Vision and Image Understanding 156 (2017) 34–50.
- [5] F. Liu, Zh. Li, Ch. Yang, D. Gong, H. Lu, F. Liu, SEGCN: a subgraph encoding based graph convolutional network model for social bot detection, Scientific Reports 14 (2024). DOI: 10.1038/s41598-024-54809-z.
- [6] M. Zhou, W. Feng, Y. Zhu, D. Zhang, D. Yuxiao, J. Tang, Semi-Supervised Social Bot Detection with Initial Residual Relation Attention Networks, Machine Learning and Knowledge Discovery in Databases: Applied Data Science and Demo Track (2023) 207-224. DOI: 10.1007/978-3-031-43427-3_13.
- [7] S. Gera, A. Sinha, T-Bot: AI-based social media bot detection model for trend-centric twitter network, Social Network Analysis and Mining 12 (2022). DOI: 10.1007/s13278-022-00897-6.
- [8] Z. Ellaky, F. Benabbou, S. Ouahabi, N. Sael, A Survey of Spam Bots Detection in Online Social Networks, in: Conference: 2021 International Conference on Digital Age & Technological Advances for Sustainable Development (ICDATA), 2021, pp. 58-65. DOI: 10.1109/ICDATA52997.2021.00021.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

- [9] N. Sadeghi, N. Riahi, Comparison of the effect of the generative model on the performance of deep neural networks and transformer in contextual social bot detection (2023). DOI: 10.21203/rs.3.rs-2556040/v1.
- [10] E. Kheir, R. Daouadi, R. Rebaï, I. Amous, Bot Detection on Online Social Networks Using Deep Forest. Artificial Intelligence Methods in Intelligent Algorithms (2019) 307-315. DOI: 10.1007/978-3-030-19810-7_30.
- [11] S. Pulipati, Malicious Social Bots Detection in Online Social Networks with Using Ensemble Model 14 2510 (2022). DOI:10.9756/INT-JECSE/V14I2.232.
- [12] P. Pham, L. Nguyen, B. Vo, U. Yun, Bot2Vec: A general approach of intra-community oriented representation learning for bot detection in different types of social networks. Information Systems 103 (2021). DOI:10.1016/j.is.2021.101771.
- [13] M. Duddu, D. Mahesh, Detection of Social Bots in Twitter Network, in: Proceedings of International Joint Conference on Advances in Computational Intelligence, 2023, pp.655-668. DOI:10.1007/978-981-99-1435-7_53.
- [14] M. Mendoza, E. Providel, M.L. Santos, S. Valenzuela, Detection and impact estimation of social bots in the Chilean Twitter network, Scientific reports 14 6525 (2024). DOI:10.1038/s41598-024-57227-3.
- [15] N. Rudnichenko, V. Vychuzhanin, T. Otradskeya, I. Petrov, I. Shpinareva, Hybrid Intelligent System for Recognizing Biometric Personal Data, in: Proceedings of the 3rd International Workshop on Computational & Information Technologies for Risk-Informed Systems (CITRisk 2022) the co-located with XXII International scientific and technical conference on Information Technologies in Education and Management (ITEM 2022), CEUR-WS, 3422, 2023. pp. 74-85.
- [16] M. Zhou, D. Zhang, W. Dan, G. Yuandong, Y. Yangli-ao, T.J. Dong, LGB: Language Model and Graph Neural Network-Driven Social Bot Detection (2024). DOI: 10.48550/arXiv.2406.08762
- [17] S. Ozdemir. Quick Start Guide to Large Language Models: Strategies and Best Practices for Using ChatGPT and Other LLMs (2023).
- [18] A. Wang, SuperGLUE: A Stickier Benchmark for General-Purpose Language Understanding Systems (2019). DOI:10.48550/arXiv.1905.00537
- [19] J. Devlin, BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding, Google AI Language 4 (2018) 29. DOI:10.48550/arXiv.1810.04805
- [20] H. A. Naveed, Comprehensive Overview of Large Language Models (2023).
- [21] M. Grohs, Large Language Models can accomplish Business Process Management Tasks (2023). DOI:10.48550/arXiv.2307.09923
- [22] R.E. Turner, An Introduction to Transformers (2023). DOI:10.48550/arXiv.2304.10557
- [23] Data set for bot user classification. URL: <https://zenodo.org/records/3692340>
- [24] T. Wolf Transformers: State-of-the-Art Natural Language Processing, in: Proceedings of the 2020 Conference on Empirical Methods in Natural Language Processing: System Demonstrations, 2020, pp.38-45.
- [25] M. Sanghoon, H. In, J. Wonik, C.M. Jae, R. Jisu, S. K. Dae, K. Kee-Eung, J. Changwook, PAC-Net: A Model Pruning Approach to Inductive Transfer Learning, in: Proceedings of the 39th International Conference on Machine Learning, PMLR 162, 2022. DOI:10.48550/arXiv.2206.05703

**ADVANCES
IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES**

**AN INTELLIGENT SYSTEM FOR ANALYZING AND DETECTING
TEXT BOT CONTENT OF GREAT IMPORTANCE IN SOCIAL
NETWORKS**

Ph.D. M. Rudnichenko ORCID: 0000-0002-7343-8076

Odesa Polytechnic National University, Ukraine

E-mail: nickolay.rud@gmail.com

Ph.D. N. Shibaeva ORCID: 0000-0002-7869-9953

Odesa Polytechnic National University, Ukraine

E-mail: nati.sh@gmail.com

Ph.D. T. Otradska ORCID: 0000-0002-5808-5647

Odesa College of Computer Technologies "SERVER", Ukraine

E-mail: tv_61@ukr.net

D. Shvedov ORCID: 0009-0002-4823-8782

Odesa Polytechnic National University, Ukraine

E-mail: frumle@ukr.net

Ph.D. I. Shpinareva ORCID: 0000-0001-9208-4923

Odesa Polytechnic National University, Ukraine

E-mail: iryna.shpinareva@onu.edu.ua

Dr.Sci. I. Petrov ORCID: 0000-0002-8740-6198

Odesa Polytechnic National University, Ukraine

E-mail: firmn@gmail.com

Abstract. *The paper addresses the challenges of analyzing and processing large volumes of heterogeneous natural language texts for the task of detecting bots on social networks using deep transfer learning methods, specifically large language models. It provides a detailed analysis of the specific characteristics and key aspects of structuring, processing, and analyzing text content, substantiates the relevance of the problem, and reviews existing approaches in the scientific literature. The paper highlights the advantages and potential applications of artificial neural networks and machine learning for automating the analysis of social network user posts. A description of the dataset selected for research is provided, along with a justification for the choice of artificial neural network language models, and an explanation of the use of transfer learning to adapt these models for bot detection. The technical tools and services employed to implement the functionality of the developed web application are described, and object-oriented models of the system are developed using UML, including use case and component diagrams. The software functionality, prototype pages, and graphical user interface are also outlined. The paper presents experimental results of the selected language models on an extended dataset, tested in modes both with and without text explanations. It analyzes the performance of adapted neural network models at a given stage, identifies the specifics of their operation, and suggests promising directions for further research and development to address the identified issues.*

Keywords: *Intelligent data analysis, text classification, social networks, text analysis, natural language processing, software development, bot detection, big data*

**ІНТЕЛЕКТУАЛЬНИЙ МЕТОД ВИЯВЛЕННЯ ЦІЛЬОВИХ
ОБ'ЄКТІВ ПРЕДМЕТНОЇ ОБЛАСТІ ЗА ПОКАЗНИКАМИ
СЕМАНТИЧНОЇ ЗВ'ЯЗНОСТІ ДЛЯ КЛАСИФІКАЦІЇ
ТЕКСТОВОЇ ІНФОРМАЦІЇ**

Ph.D. О. Мазурець ORCID: 0000-0002-8900-0650

Хмельницький національний університет, Україна

E-mail: exe.chong@gmail.com

P. Віт ORCID: 0009-0009-6958-4730

Хмельницький національний університет, Україна

E-mail: vit.roman.vit@gmail.com

***Анотація.** Розглянуто інтелектуальний метод виявлення цільових об'єктів предметної області за показниками семантичної зв'язності, який призначений для автоматизації процесу ідентифікації ключових елементів у великих масивах текстових даних. Розроблений метод відрізняється від існуючих урахуванням ключових слів та іменникових сутностей предметної області, що дало змогу підвищити точність виявлення цільових об'єктів предметної області внаслідок врахування іменникових сутностей. Проведені дослідження встановили, що знайдені за створеним методом цільові об'єкти спроможні виконувати подальшу задачу класифікації, демонструючи на матриці евклідових відстаней групування текстів однієї категорії та збільшення відстані ортогональної їй. Для прикладної реалізації створеного інтелектуального методу виявлення цільових об'єктів предметної області, було сформовано модель сучасної української мови, що побудована шляхом об'єднання значимих для передачі сенсу відомих частотних словників. Для створення коректної моделі сучасної української мови було використано частотні словники існуючих корпусів української мови, які сукупно охоплюють як різні сфери діяльності та типи контенту, так і різні області спілкування, враховуючи спілкування в Інтернет. Шляхом об'єднання за частотними показниками словників цих корпусів української мови було одержано вектор слів, який для покращення спроможності класифікації був відфільтрований за іменниковою групою та обмежений кількісно. Проведені дослідження дали можливість стверджувати про можливість використання створеної моделі сучасної української мови для ефективного вирішення задач аналізу текстового контенту одиниць інтернет-спілкування та його класифікації за різними ознаками.*

***Ключові слова:** цільові об'єкти предметної області, класифікація текстів, модель української мови, частотні словники, вектор слів, семантична зв'язність*

1. Вступ та постановка проблеми

За відсутності гарантій забезпечення вчасного й повноцінного процесу навчання, підвищення кваліфікації чи контролю рівня поточних знань фахівців сфери безпеки та медицини у зв'язку з складними епідеміологічними, екологічними й соціальними умовами, в сучасному світі зростає роль комп'ютерних засобів перевірки рівня знань [1, 2]. Одним із основних способів контролю рівня знань залишається комп'ютерне тестування [3]. Особливо перспективним є впровадження технологій адаптивного тестування, за яких складність чи інші властивості тестових завдань змінюються залежно від правильності попередніх відповідей [4]. Методи виявлення цільових об'єктів у предметній області є критично важливими для ефективного аналізу та обробки великих обсягів інформації. В умовах зростаючої складності даних, які охоплюють різноманітні предметні області, необхідність розробки та вдосконалення методів автоматизованого виявлення цільових об'єктів стає все більш актуальною [1]. Це особливо важливо в таких сферах, як штучний інтелект, а саме системи обробки природної мови та інформаційний пошук [2]. Відсутність надійних та ефективних методів виявлення цільових об'єктів може призвести до втрати важливої інформації, зниження точності прийняття рішень та збільшення витрат на аналіз даних. Враховуючи швидкий розвиток технологій та постійне зростання обсягів інформації, дослідження методів виявлення цільових об'єктів набуває особливої ваги. Виявлення цільових об'єктів у заданій предметній області передбачає застосування спеціальних алгоритмів та методів, спрямованих на ідентифікацію та класифікацію елементів, які мають ключове значення для аналізу конкретної задачі [3]. У роботі цільові об'єкти будуть шукатись у текстових даних, а під терміном «цільові об'єкти» буде матись на увазі сукупність множини ключових слів та множини NER з групуванням шляхом лематизації [4]. Виявлення цільових об'єктів у системах NLP, зокрема розпізнавання іменованих сутностей, відіграє важливу роль у багатьох завданнях аналізу тексту та обробки інформації. Основна мета NER полягає в ідентифікації і класифікації значущих елементів тексту, таких як імена людей, назви організацій, географічні назви, дати та інші сутності, які мають специфічне значення для конкретного контексту. Це завдання є ключовим для ряду практичних задач, таких як інформаційний пошук, машинний переклад, обробка юридичних документів та аналіз даних у соціальних медіа. Одним із перспективних напрямків для задачі виявлення цільових об'єктів є використання методів машинного навчання, які дозволяють автоматично адаптуватися до особливостей даних та поліпшувати точність виявлення об'єктів з часом [5].

З проведеного аналізу, запропоновано автоматизувати виявлення цільових об'єктів предметної області з використанням підходів машинного навчання. В даній праці наведено розроблений авторами комплексний підхід до побудови моделі сучасної української мови, у рамках якої стане можлива гіперплощинна класифікація контенту для задач автоматизації виявлення цільових об'єктів

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

предметної області, що сприятиме значному підвищенню ефективності та точності ідентифікації релевантних об'єктів у великих обсягах даних.

2. Аналіз останніх досліджень та публікацій

Проблему виявлення цільових об'єктів предметної області варто розглядати у контексті пошуку іменованих сутностей та пошуку ключових слів [6]. Даними задачами широко займаються науковці як по всьому світу, так і в Україні. Модель отримання ключових слів загального призначення, що призначена для роботи з групами документів різних розмірів і читабельності, а також наявності міток ключових слів запропонована у [7]. Для отримання кращого вибору ключових слів використано модель логістичної регресії з найменшим стисненням і регуляризацією оператора вибору. Заснована на класифікації структура такого підходу забезпечує виявлення слів, які чітко характеризують цю групу документів у порівнянні з групами порівняння, що підвищує репрезентативність вилучених ключових слів.

У роботі [8] були проведені експерименти на різних мовах, що показують, що зображення доповнюють моделі обробки природної мови (включаючи BERT), навчені без зовнішнього попереднього навчання. Дослідження класифікації текстів були зосереджені на статтях з Вікіпедії, оскільки зображення зазвичай доповнюють текст і сторінка Вікіпедії може бути написана різними мовами. У статті [9] досліджують онлайн-розмови: їх перебіг, аргументи й як вони вирішуються. Експеримент проводився на основі функцій, використовуючи модель логістичної регресії від Scikit-learn. У роботі [10] було проведено виділення емоційних настроїв та класифікація їх полярності. У публікації були проведені експерименти з 8-и наборами даних англійською мовою. Результати показують, що продуктивність сучасних моделей для передбачення полярних зворотів мови погана, і це перешкоджає використанню цієї інформації на практиці.

Щодо задачі NER, у [11] запропоновано підхід до оптимізації завдання розпізнавання іменованих сутностей шляхом використання попередньо навчених мовних моделей для автоматичного дослідження слів, пов'язаних з віртуальними мітками, що представляють категорії сутностей. Метод передбачає розробку міток через встановлення зв'язків між початковими словами міток і відповідними словами сутності на основі розподілу даних, отриманих з попередньо навченої мовної моделі. Завдяки цьому покращується семантичне представлення слів міток, що в результаті підвищує точність моделі в ідентифікації конкретних сутностей. Крім того, завдання NER переналаштовується у формат text2text, що дозволяє краще використовувати знання мовної моделі та оптимізує процес вилучення інформації.

Отже, зважаючи на проведені дослідження, поставлена задача виявлення цільових об'єктів предметної області за показниками семантичної зв'язності є актуальною для сучасної української мови. Ця задача вимагає формування моделі української мови, для чого перспективним є використання векторної моделі, у якій ознаками будуть слугувати статистичні міри, які

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

використовуються для оцінки важливості слова в контексті повідомлення, яке в свою чергу є частиною колекції повідомлень або корпусу (TF-IDF, BM25, Yake, дисперсійна оцінка тощо).

3. Постановка задачі

Метою роботи є розробка моделі сучасної української мови, у рамках якої стане можлива гіперплощина класифікація текстів для виявлення цільових об'єктів предметної області за показниками семантичної зв'язності.

Основним результатом роботи є створений інтелектуальний метод виявлення цільових об'єктів предметної області за показниками семантичної зв'язності для класифікації текстової інформації з використанням розробленої моделі сучасної української мови, який відрізняється від існуючих урахуванням ключових слів та іменникових сутностей предметної області, що дало змогу підвищити точність виявлення цільових об'єктів предметної області внаслідок врахування іменникових сутностей.

4. Метод виявлення цільових об'єктів предметної області

Інтелектуальний метод виявлення цільових об'єктів предметної області за показниками семантичної зв'язності для класифікації текстової інформації призначений для автоматизації процесу ідентифікації ключових елементів у великих масивах текстових даних, спрямований на підвищення точності та ефективності аналізу текстової інформації. Цей метод використовує алгоритми машинного навчання для адаптивного розпізнавання об'єктів, враховуючи специфіку предметної області, що дозволяє значно скоротити час обробки даних і знизити ризик упущення важливої інформації. Схема та кроки методу наведені на рис. 1.

Вхідними даними методу є досліджуваний текст та попередньо оброблений збалансований корпус текстів досліджуваної предметної області.

Першим етапом є підготовка досліджуваного тексту для аналізу, який включає в себе токенізацію, лематизацію та видалення стоп-слів.

Наступним етапом є пошук ключових слів різними методами, такими як TF-IDF, TF, YAKE! та методом дисперсної оцінки. Кожним перерахованим методом відбувається формування множини ключових слів.

На третьому етапі здійснюється виявлення цільових об'єктів, яке включає в себе декілька кроків. Схематично виявлення цільових об'єктів зображено на рис. 2. Цільові об'єкти є об'єднаною множиною ключових слів знайденими різними методами без повторів та множиною NER що згруповані шляхом лематизації. Наведені етапи є основними у роботі запропонованого інтелектуального методу виявлення цільових об'єктів предметної області за показниками семантичної зв'язності для класифікації текстової інформації з використанням моделі сучасної української мови.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

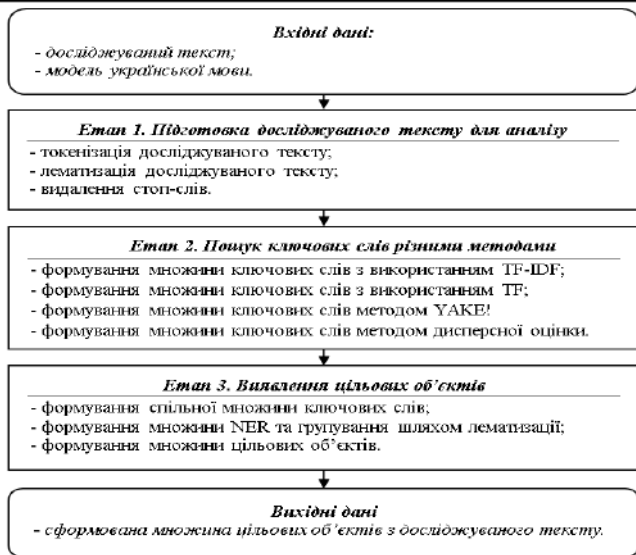


Рисунок 1. Етапи роботи методу виявлення цільових об'єктів предметної області за показниками семантичної зв'язності

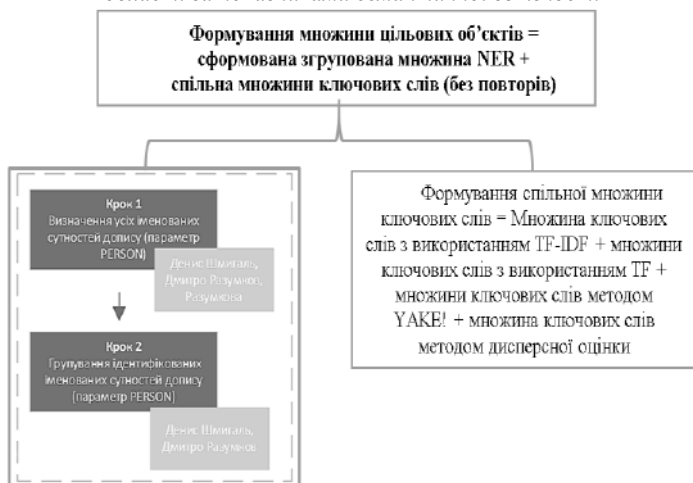


Рисунок 2. Приклад виконання етапу формування цільових об'єктів методу виявлення цільових об'єктів предметної області

Цей метод призначений для автоматизації процесу ідентифікації ключових елементів у великих масивах текстових даних й відрізняється від існуючих урахуванням ключових слів та іменникових сутностей предметної області, що

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

дало змогу підвищити точність виявлення цільових об'єктів предметної області внаслідок врахування іменникових сутностей.

5. Модель сучасної української мови

Модель сучасної української мови забезпечує гіперплощинну класифікацію текстів для її подальшого використання методом виявлення цільових об'єктів предметної області за показниками семантичної зв'язності. Схема запропонованого підходу до побудови моделі для контент-аналізу україномовного сегменту Інтернет-спілкування зображена на рисунку 3. Запропонований підхід до побудови моделі для контент-аналізу україномовного сегменту Інтернет-спілкування, яка формується для її використання в методі виявлення цільових об'єктів предметної області за показниками семантичної зв'язності, на першому кроці передбачає побудову вектора ключових слів, для чого послідовно виконуються вибір частотних словників української мови, об'єднання цих словників і подальше обмеження кількості ключових слів шляхом відкидання стоп-слів та рідковживаних слів.

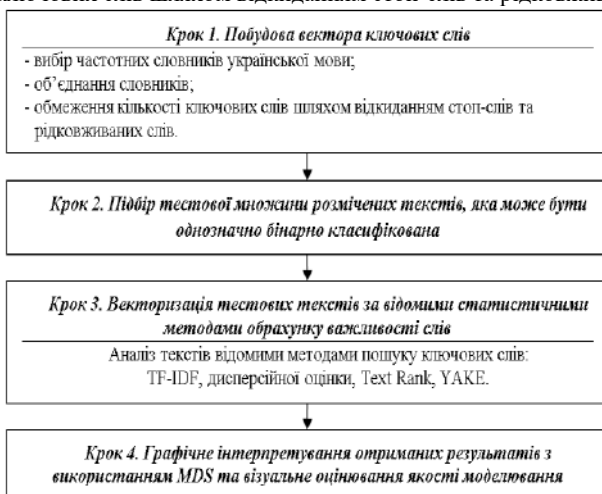


Рисунок 3. *Схема підходу до створення моделі сучасної української мови для методу виявлення цільових об'єктів предметної області*

Першим кроком підходу є побудова вектору ключових слів для передачі сенсу при комунікації у мережі Інтернет. Враховуючи зазначену особливість (використання для спілкування суржиків, деформованих слів та ненормативної лексики), побудова вектору ключових слів є окремою підзадачею. Оскільки мова йде про специфічну флективну українську мову, це мають бути не просто ключові слова зі статей, а це повинен бути збалансований набір даних. Тому в роботі були використані частотні словники української мови [12-16]

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

$(\overline{W}_j = \{\overline{w}_1, \overline{w}_2, \dots, \overline{w}_n\}, j = \overline{1..n})$, де j – порядковий номер словника, n – кількість словників. Де кожен словник представляє собою відповідний набір слів $\overline{w} = \{\text{слово}_1, \text{слово}_2, \dots, \text{слово}_n\}, i = \overline{1..n}$, де n – кількість слів у словнику. У дослідженні з кожного частотного словника видалялися слова, які на думку авторів, не суттєво впливатимуть на модель (слова притаманні дуже великій кількості текстів (стоп-слова які мають службове значення та використовуються для зв'язування слів у тексті), надто рідковживані слова тощо). Тобто \overline{W}_j містять тільки відібрані слова. Вектор ключових слів \overline{Word} буде об'єднанням таких частотних словників:

$$\overline{Word} = \bigcup_{i=1}^n \overline{W}_i \quad (1)$$

На другому кроці при побудові моделі для контент-аналізу україномовного сегменту Інтернет-спілкування виконується підбір тестової множини розмічених текстів, яка може бути однозначно бінарно класифікована. Основним змістом кроку є вибір текстів, які підлягають ідеальній класифікації, коли однозначно можна зробити висновок щодо належності обраного тексту конкретній категорії. Формується множина текстів D , у якій кожен текст $d \in D$ може відповідати конкретній категорії $c \in C$, де C – множина категорій. У даному випадку буде використана бінарна класифікація, оскільки наша мета – виявлення текстів з негативною забарвленістю контенту як категорії.

Третій крок передбачає векторизацію тестових текстів за відомими статистичними методами обрахунку важливості слів, тобто аналіз текстів відомими методами пошуку ключових слів, до яких належать TF-IDF, дисперсійна оцінка, Text Rank, YAKE. Тобто, кожен текстовий документ векторизується відомими методами пошуку ключових слів.

На етапі препроцесінгу, кожен текстовий документ $d_i \in D$, де i – кількість документів у колекції, перетворюється у вектор слів. Після цього за допомогою кожного з методів пошуку ключових слів формується відповідний вектор оцінок входжень ключових слів \overline{Wd}_i , які є у векторі \overline{Word} р_i.

Для формування оцінок пропонується використати відомі методи пошуку ключових слів TF-IDF [17], дисперсійної оцінки [18], Text Rank [19, 20, 21], YAKE [22]. Класично TF-IDF подається наступним чином:

$$TF - IDF(t, d, D) = TF(t, d) \times IDF(t, d, D) \quad (2)$$

та є вагою терміну t документа d корпусу D , а $TF(t, d)$ є значенням частоти терміну t в документі d .

Дисперсійна оцінка подається як оцінка важливості кожного слова в досліджуваному тексті, що проводиться з використанням методу дисперсійного оцінювання. Цей метод є оцінкою дискримінантної сили слів і дозволяє

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

відділити із загальної множини слів широкого вжитку в тексті слова, що розташовані рівномірно. Відповідно з [18], якщо деяке слово A в тексті, що складається з N слів, позначене як A_k^n , де індекс k – номер появи даного слова в тесті, а n – його позиція в тексті, то інтервалом між послідовними появами слова при таких позначеннях буде величина

$$\Delta A_k^m = A_{k+1}^m - A_k^n = m - n, \quad (3)$$

де на ітерації m і позиції n в тексті знаходиться слово A , яке зустрілось $k+1$ -ий і k -ий рази. Таким чином, дисперсійна оцінка розраховується за формулою

$$\sigma = \sqrt{(\Delta A^2) - (\Delta A)^2} / (\Delta A), \quad (4)$$

де (ΔA) – середнє значення послідовності $\Delta A_1, \Delta A_2, \dots, \Delta A_k$. K – кількість появи слова A в тексті.

Метод Text Rank призначений для моделювання тексту як неорієнтованого зваженого графа $G=(V,E,W)$, у якому ключові слова-кандидати розглядаються як набір вузлів V , а взаємозв'язок між двома словами розглядається як ребро в E . W представляє частоту появ по відношенню до E [19, 20]. Для ітераційного обчислення ваг вузлів використовується:

$$WS(V_i) = (1 - d) + d * \sum_{V_j \in \ln(V_i)} \frac{w_{i,j}}{\sum_{V_k \in \text{Out}(V_j)} w_{jk}} WS(V_j) \quad (5)$$

де d є коефіцієнтом амортизації ітераційного обчислення та може приймати значення 0,85 за замовчуванням [19]. $\ln(V_i)$ є набором вузлів, що вказують на V_i , $\text{Out}(V_j)$ є набором вузлів, на які вказує V_j . Формула (5) показує, що вага вузла V_i залежить від ваги ребра від V_j до V_i (on the edge weight from) та суми ваг ребер від вузла V_j до інших вузлів.

Алгоритм YAKE складається з 4 кроків: попередня обробка та генерація термінів-кандидатів; визначення особливості термінів; підрахунок балів за термін; асоціація подібних термінів [22]. На першому етапі виконується поділ на рівні речення, які в подальшому розбиваються на терміни. На етапі визначення особливості термінів кожен термін оцінюється завдяки використанню спеціальних функцій [22]. На етапі підрахунку балів за термін використовується нижченаведена формула:

$$S(t) = (Trel * Tposition) / Tcase + ((Tnorm / Trel) + (Tsentence / Trel)), \quad (6)$$

де $Tcase$ – важливість використання великих літер і скорочень, $Tposition$ – більше значення надається словам, які присутні на початку документа, $Tnorm$ – частота слів, $Trel$ – перевіряє різноманітність контексту, у якому зустрічається це слово, $Tsentence$ – функція визначає, як часто слово-кандидат зустрічається з різними реченнями.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

Вищий бал отримують слова, які часто зустрічаються в різних реченнях. Останнім етапом є об'єднання значень оцінок морфологічно подібних слів. Мінімальні бали одержують кращі ключові слова.

На *четвертому кроці* виконується графічне інтерпретування отриманих результатів з використанням MDS та візуальне оцінювання якості моделювання [23]. Важливим вмістом етапу інтерпретації отриманих результатів є вибір критерію якості моделювання за візуальною аналітикою [24, 25]. Для можливості оцінки якості отриманих моделей для задач класифікації пропонується використовувати метод Multidimensional scaling MDS [6, 19]. Це один з методів пониження розмірності векторного простору. Метою методу є пониження розмірності до такої яку можливо візуалізувати (3 чи 2-мірної). Критерієм для пониження розмірності виступає, наприклад, Евклідова відстань між векторами. Тобто розв'язуючи оптимізаційну задачу знаходять відображення $R^n \rightarrow R^2$ що дає можливим отримати двовимірний графік взаємного розташування точок-векторів та візуально оцінити якість моделі для задачі класифікації.

Запропоновано візуальні критерії для оцінки якості візуального моделювання (рисунки 4-6).

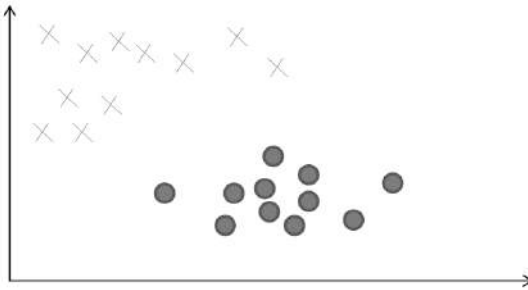


Рисунок 4. Приклад високого рівня якості моделі для задачі класифікації

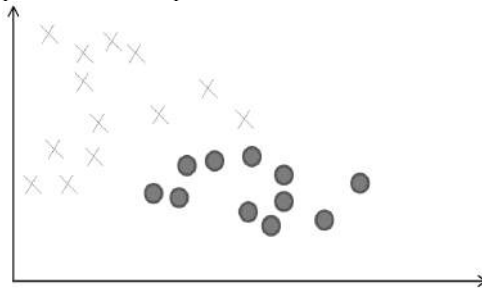


Рисунок 5. Приклад прийняттого рівня якості моделі для задачі класифікації

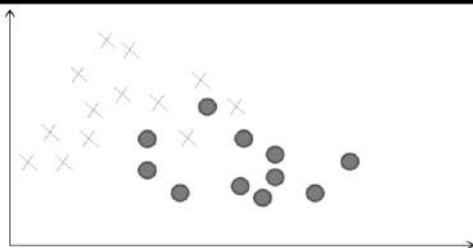


Рисунок 6. Приклад незадовільного рівня якості моделі для задачі класифікації
Критерій 1 – Високий рівень моделі для класифікації текстів. На рисунку 4 видно, що два класи чітко розділені між собою, що свідчить про коректність запропонованої моделі.

Критерій 2 – Прийнятний рівень моделі для класифікації текстів. На рисунку 5 видно, що два класи стикаються між собою. При такому показнику можна вважати модель працездатною, проте вона потребуватиме додаткового експертного висновка для підтвердження класифікації.

Критерій 3 – Незадовільний рівень моделі для класифікації текстів. На рисунку 6 видно, що два класи майже не розділені між собою, відстань між ними незначна, а місцями зустрічається перетин. При такому показнику модель не можна вважати працездатною, вона потребує доопрацювання.

Наведені критерії пропонується застосувати для перевірки якості запропонованої моделі сучасної української мови. Модель вважатимемо коректною, якщо значення результатів буде знаходитись в межах між першим та другим критеріями.

6. Підготовка навчальних вибірок даних

Підготовка навчальних вибірок даних для створення моделі сучасної української мови для методу виявлення цільових об'єктів предметної області є окремою складовою дослідження.

Для побудови моделі та її валідації (спроможності класифікувати тексти спілкування у Інтернеті) було використано такі корпуси української мови з частотними словниками та розміченими за категоріями текстами:

1. *БрУК* – збалансований корпус-мільйонник сучасної мови. Відкритий, збалансований за жанрами корпус сучасної української мови обсягом 1 млн слововживань. Корпус побудований на засадах, що були покладені в основу відомого корпусу англійської мови Brown. [12]. Також до складу цього корпусу входить словник VESUM (URL: <https://r2u.org.ua/vesum/>), який містить слова-покручі, ненормативну лексику, суржик, що є невід'ємною частиною побутової української мови.

2. *Корпус української мови MOVA.info*. Призначений для пошуку лексем та словоформ в українських текстах певного стилю (для окремих частин корпусу також можливий пошук морфем, морфемних і синтаксичних структур) [13]. У даній роботі використовувався для побудови вектора ключових слів.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

3. *UA-GEC*: перший анотований GEC-корпус української мови. Це колекція текстів, написаних звичайними людьми: есеї, дописи в блогах та соцмережах, відгуки, листи тощо. Ці тексти містять граматичні, стилістичні та орфографічні помилки, що максимально наближають їх до повсякденної мови [14].

4. *Ukrainian News Collection*. Українські новини – це колекція з понад 150 тисяч новинних статей, зібраних з понад 20 новинних ресурсів. Зразки наборів даних поділяються на 5 категорій: політика, спорт, новини, бізнес, технології. Набір даних надано некомерційною студентською організацією FIdo.ai (дослідницький відділ машинного навчання FIdo Національного університету «Києво-Могилянська академія») для дослідницьких цілей в області аналізу даних (класифікація, кластеризація, виділення ключових слів тощо) [15].

5. *Український веб-корпус Лейпцизького університету*. Корпус текстів української мови. Містить частотні словники. Словники побудовані на базі Вікіпедії, новинних сайтів, вебдокументів. Можна завантажити в різних обсягах токенів (слів): 10 000, 30 000, 100 000, 300 000, 1000 000 [16].

6. *Карпати буд каркас*. Набір статей де зібрані інформація про перебіг будівництва, новини сучасної архітектури, технології. Складається з понад 200 текстів в середньому по 500 слів (<https://karpatybud.com.ua/statti/>).

7. *Блог садівника*. Сайт, що містить понад 200 текстів розмірністю близько 500 слів кожен, присвячених тематиці садівництва (<https://agromarket.net/ua/news/>).

Така кількість джерел обумовлена тим, що сучасної українська мова охоплює багато сфер життєдіяльності.

Тому взявши тільки один з корпусів для дослідження не зможемо охопити весь лексичний запас мови. Кожен із взятих корпусів здатен передавати сенс сучасної української мови, тому для побудови вектору ключових слів *Word* було використано наведені джерела.

7. Прикладне застосування для дослідження ефективності методу виявлення цільових об'єктів предметної області

Для валідації запропонованого інтелектуального методу виявлення цільових об'єктів предметної області за показниками семантичної зв'язності для класифікації текстової інформації з використанням розробленої моделі сучасної української мови, було розроблено програмний застосунок мовою C# для перетворення текстового контенту файлів із тестової вибірки у множину цільових об'єктів предметної області [1]. Головне вікно розробленого застосунку зображено на рисунку 7.

Застосунок дозволяє задавати наступні параметри:

- 1) шлях до файлу, що містить ключові терміни;
- 2) обирати метод оцінки термінів в текстовому контенті;
- 3) обирати корпуси текстів які будуть оброблятися. В результаті роботи застосунку отримується файл який містить цифрове представлення кожного тексту із обраних корпусів.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

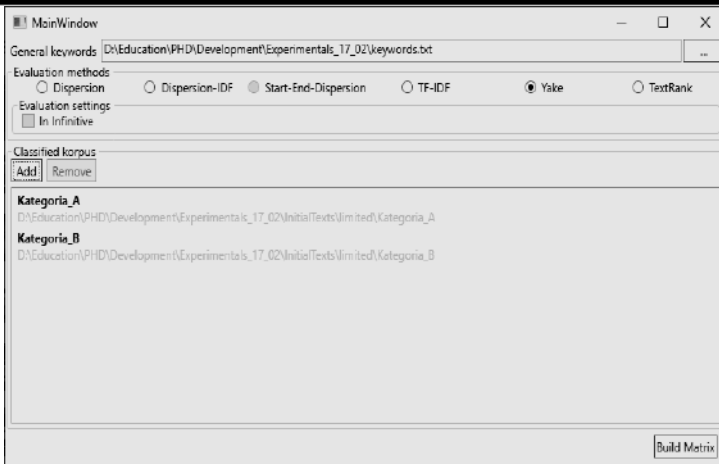


Рисунок 7. Експериментальний застосунок для пошуку ключових слів альтернативними методами й перетворення текстового контенту в цифрове подання

Параметри середовища аналізу текстових даних. Отриманий файл передається на обробку програмному застосунку розробленого на мові програмування Python із застосуванням бібліотеки Manifold. Даний застосунок зчитує дані із отриманого на вхід файлу із попереднього етапу та обробляє отримані дані за допомогою методу MDS із бібліотеки Manifold. Результат отриманий з методу MDS візуалізується на графічному інтерфейсі.

8. Результати експерименту та дискусія

Для дослідження ефективності запропонованого методу було створено окреме консольне програмне забезпечення мовою Python, яке передбачає використання отриманого списку цільових об'єктів для досліджуваних текстів, та словників для окреслених тем «Карпати буд каркас» та «Блог садівника». Відповідно, знайдені цільові об'єкти були переведені у векторне представлення розміром 1500 (як розмір словника) методом One-Hot Encoding.

Надалі було перевірено Евклідові відстані між текстами одного спрямування (5 текстів категорії «Карпати буд каркас» та 5 текстів «Блог садівника»), а також були обраховані Евклідові відстані між векторами протилежних категорій. Дані експерименту наведено в таблиці 1.

Матриця відстаней таблиці 1 та рисунку 8 демонструють чітке розділення текстів на дві основні групи з різним змістом.

Перша група текстів (1–5), що належать категорії «Карпати буд каркас» має тісніші зв'язки між собою, аналогічно як друга група (6–10) також має менші внутрішні відстані (категорія «Блог садівника»), але водночас має великі відстані до текстів з першої групи, що свідчить про те, що ці групи належать до

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

різних тематик. Тексти всередині кожної групи мають невеликі відстані, що свідчить про їхню тематичну схожість.

Таблиця 1

Евклідові відстані між текстами (№1-10) одного спрямування

	№1	№2	№3	№4	№5	№6	№7	№8	№9	№10
№1	0	10.3	11.2	9.75	14.7	25.7	23.4	28.6	29.6	24.7
№2	10.3	0	15.7	17.1	16.4	30.2 1	24.5	26.3	23.3 4	26.5
№3	11.2	15.7	0	9.4	8.89	27.6	24.9	23.8	25.7	27.1
№4	9.75	17.1	9.4	0	5.47	32.4	30.7	26.1	27.6	23.6
№5	14.7	16.4	8.89	5.47	0	19.4	23.4 5	26.1 2	28.4	24.7
№6	25.7	30.2 1	27.6	32.4	19.4	0	9.78	6.99	9.1	14.3
№7	23.4	24.5	24.9	30.7	23.4 5	9.78	0	11.9	12.4 5	7.98
№8	28.6	26.3	23.8	26.1	26.1 2	6.99	11.9	0	6.33	8.91
№9	29.6	23.3 4	25.7	27.6	28.4	9.1	12.4 5	6.33	0	13.5
№10	24.7	26.5	27.1	23.6	24.7	14.3	7.98	8.91	13.5	0

Результати отримані з таблиці проілюстровані графіком на рисунку 8.

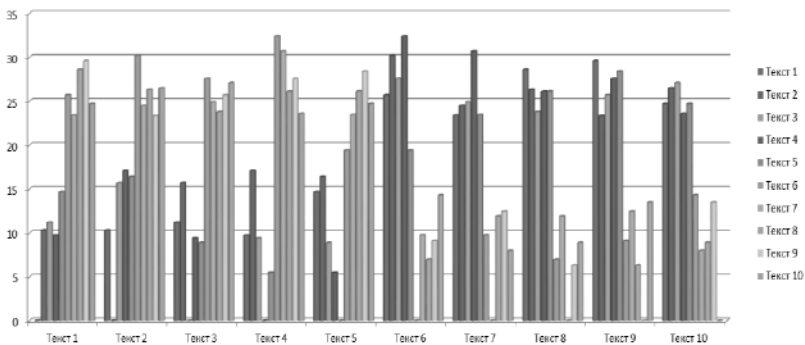


Рисунок 8. Евклідові відстані між тестовими текстами двох категорій

При побудові мовної моделі основою пропонованого узагальненого вектору *Word* є словник MOVA.info [13], оскільки він найближче підходить для задач класифікації інтернет-контенту з додаванням слів інших словників. Для досягнення поставленої задачі було також проведено фільтрацію за іменниками, оскільки отриманий словник мав різні частини мови та був неоднорідним. Отриманий таким чином вектор складається з 1500 слів.

Довжина вектору слів моделі для векторизації україномовного сегменту Інтернет у 1500 одиниць була встановлена за результатом досліджень. Наприклад, на рисунку 9 наведено візуалізацію бінарної класифікації описаної

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

множини текстів методом TF-IDF за довжини вектора у 3000 слів, а на рисунку 10 наведено візуалізацію бінарної класифікації описаної множини текстів методом TF-IDF за довжини вектору у 2000 слів. Дослідження встановили, що найкраща здатність до роздільності при класифікації текстів спостерігається при довжині вектора слів рівній 1500 одиниць.

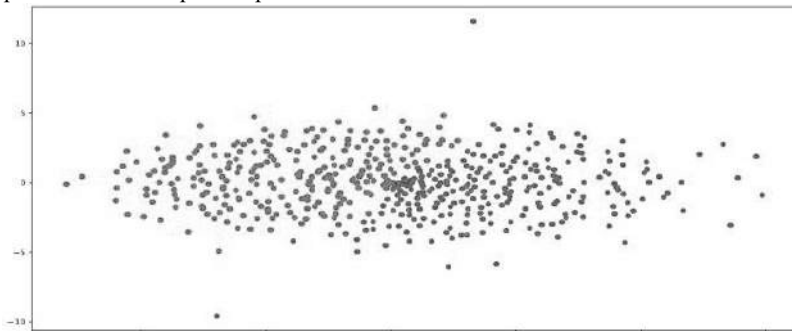


Рисунок 9. Візуалізація бінарної класифікації текстів методом TF-IDF за довжини вектора у 3000 слів

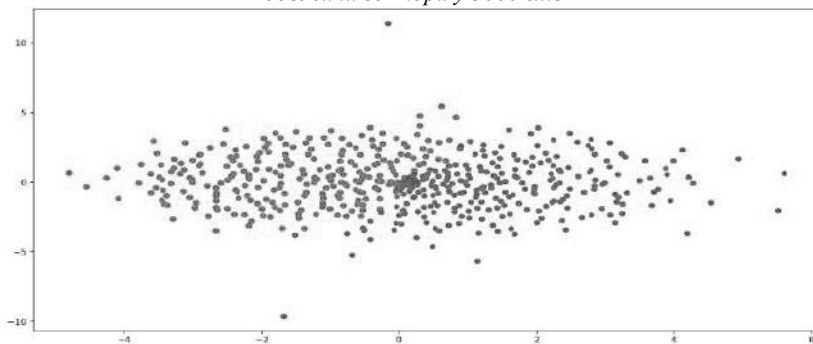


Рисунок 10. Візуалізація бінарної класифікації текстів методом TF-IDF за довжини вектора у 2000 слів

Для проведення експериментальних досліджень були зібрані тексти двох категорій: будівництво (<https://karpatybud.com.ua/statti/>) та садівництво (<https://agro-market.net/ua/news/>). Ці зібрання містять по 200 текстів кожен, в середньому довжиною в 500 слів кожен текст. Оскільки у завданнях дослідження метою є бінарна класифікація, то використати дві категорії достатньо для валідації запропонованої моделі та проведення експериментальних досліджень.

Результат 1. В результаті валідації якості моделі побутового лексику Україномовного сегменту Інтернет за використання методу TF-IDF були отримані результати, зображені на рисунку 11. Результат можна оцінити як незадовільний, оскільки категорії деяких текстів було визначено помилково, а

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

область поділу/розмежування є нечіткою. Це пояснюється характерними рисами цього методу, які полягають у його високій чутливості до підбору текстів альтернативних категорій. Оскільки альтернативні категорії можуть бути поза межами використаних класів для класифікації, що особливо чутливо для текстів побутової тематики, то це може приводити до випадків неправильної класифікації текстів.

Результат 2. Отримані за використання методу дисперсійного оцінювання результати валідації якості моделі побутового лексику проілюстровані на рисунку 12. Результат можна оцінити як прийнятний, оскільки є тексти, які містяться на межі класів. Метод дисперсійного оцінювання для ефективного обрахунку значень семантичної важливості слів потребує якомога більшої кількості появ значущих слів в окремих текстах. Побутове спілкування характеризується фрагментарним використанням значущих слів у невеликій кількості, тому в деяких випадках незадовільні статистичні показники унікальних слів тексту не забезпечують достатньої роздільності значень показників, актуальних для класифікації.

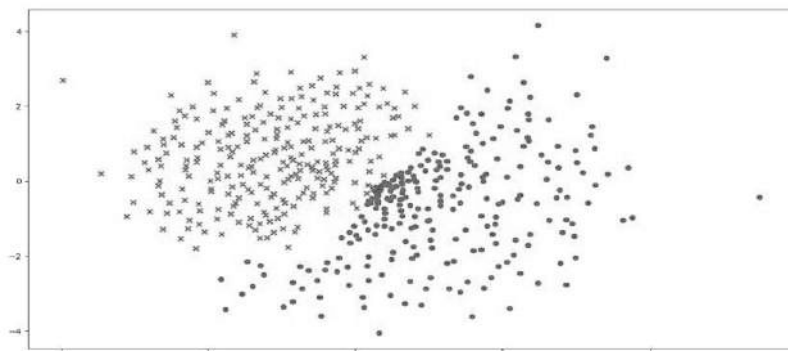


Рисунок 11. Валідація якості моделі за методом TF-IDF

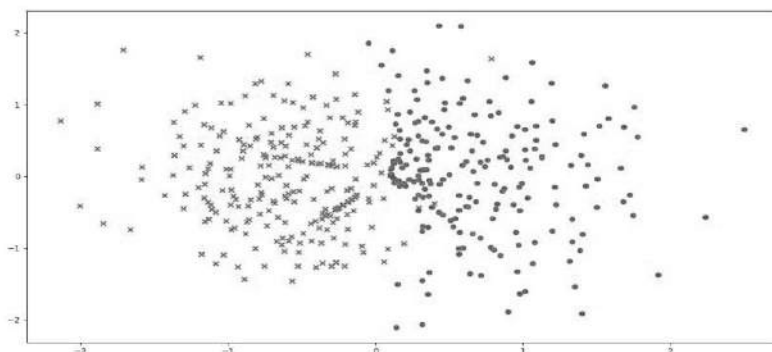


Рисунок 12. Валідація якості моделі за методом дисперсійного оцінювання

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

Результат 3. Отримані за використання методу Text Rank результати проілюстровані на рисунку 13. Якість результату можна оцінити як високу, оскільки обидві категорії мають чітке розділення. Метод Text Rank для обрахунку значень семантичної важливості слів використовує не тільки власне позиції слів у тексті, а й взаємозв'язки між словами та взаємозв'язок частот появ слів по відношенню до взаємозв'язків між словами.

Це дозволяє приймати до уваги більшу за інші методи кількість параметрів тексту, в той час як тематики побутового спілкування не дозволяють одержувати у великій кількості первинні показники для оцінювання. Тому даний метод виявив достатньо високу ефективність роздільності текстів за категоріями.

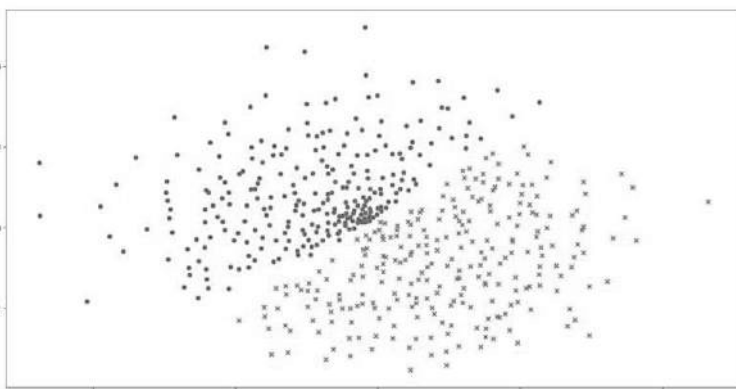


Рисунок 13. Валідація якості моделі за методом Text Rank

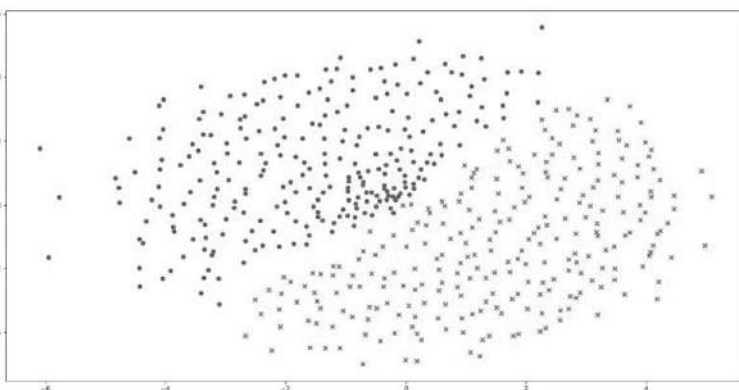


Рисунок 14. Валідація якості моделі за методом YAKE

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

Результат 4. За використання методу YAKE були отримані результати класифікації текстів, зображені на рисунку 14. Такі результати можна інтерпретувати як між високим та задовільним. Категорії розділені, проте чіткої межі немає. Цей метод враховує ряд важливих показників тексту, таких як частота слів, різноманітність контексту появ слова та частота появ слів у різних реченнях. Проте характерні особливості побутового спілкування не дозволяють методу використати його характерні переваги. До таких переваг належать врахування використання великих літер і скорочень, присутність слів на початку тексту. Також, при збільшенні числа кількості текстів можливості методу YAKE знижуються і його застосування може призвести до нечіткої класифікації. Тому цей метод, ефективний для текстів іншого характеру, таких як наукової статті, в випадку аналізу текстів з побутового спілкування виявив менш задовільний результат.

Результат 5. За отриманими різними методами числовими значеннями для вектору слів які відповідають важливості кожного з них для задачі класифікації, був проведений аналіз, шляхом їх перетину для різних методів. В результаті наведеного отримана множина слів яка є загальною для методів що розглядалися. Об'єм множини склав біля 500 слів.

Отримані слова можна вважати достатніми для моделювання задачі класифікації за наборами текстів, що розглядалися. В подальшому, отриманий таким чином набір можливо використати як базовий для формування векторної моделі. Формування моделі може проходити шляхом доповнення базової множини слів словами що притаманні конкретним задачам, що розглядатимуться: виявлення суїцидних настроїв [26], буллінгу [27], негативного емоційного забарвлення текстів [28], негативного контенту тощо.

З отриманих результатів валідації моделі побутового лексику Україномовного сегменту Інтернет видно, що класифікація текстів побутового характеру є найбільш ефективною за використанням методу пошуку ключових слів Text Rank. Подальші дослідження направлені на вдосконалення та модифікацію вже описаних підходів шляхом перевірок припущень, використання для векторизації текстів композиції методів тощо. Також подальші дослідження будуть спрямовані на удосконалення загального вектору слів сучасної побутової української мови та розв'язання задач визначення негативного забарвлення текстових повідомлень в сегменті інтернет-спілкування.

9. Висновки

Було розглянуто поточний стан наукового напрямку виявлення цільових об'єктів предметної області, та на основі опрацьованого матеріалу запропоновано власний інтелектуальний метод виявлення цільових об'єктів предметної області за показниками семантичної зв'язності для класифікації текстової інформації, який призначений для автоматизації процесу ідентифікації ключових елементів у великих масивах текстових даних,

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

спрямований на підвищення точності та ефективності аналізу текстової інформації.

Запропонований метод показав, що знайдені цільові об'єкти предметних областей спроможні виконувати подальшу задачу класифікації, демонструючи на метриці Евклідових відстаней групування текстів однієї категорії та збільшення відстані ортогональної їй. Супутнім результатом реалізації методу є розробка моделі сучасної української мови, у рамках якої можлива гіперплощина класифікація текстів для виявлення цільових об'єктів предметної області за показниками семантичної зв'язності. Тож було запропоновано модель сучасної української мови, що побудована шляхом об'єднання значимих для передачі сенсу відомих частотних словників.

Модель має використовуватись для аналізу контенту Україномовного сегменту Інтернет, який характеризується використанням граматично й синтаксично хибних, але в побутовому спілкування розповсюджених слів, враховуючи нецензурні; тому існуючі сучасні частотні словники не покривають у повній мірі вказаний сегмент. Для створення коректної моделі сучасної української мови було використано частотні словники існуючих корпусів української мови, які сукупно охоплюють як різні сфери діяльності та типи контенту, так і різні області спілкування, враховуючи спілкування в Інтернет. Шляхом об'єднання за частотними показниками словників цих корпусів української мови було одержано вектор слів, який для покращення спроможності класифікації був відфільтрований за іменниковою групою та обмежений кількісно.

Для валідації запропонованої моделі було взято дві ортогональних множини текстів розмірністю понад 200 у кожній. Кожен текст був векторизований одним із чотирьох запропонованих методів пошуку ключових слів (TF-IDF, дисперсійної оцінки, Text Rank, YAKE) за ключовими словами та був віднесений до заданої категорії. Для забезпечення можливості оцінки якості отриманих моделей був використаний метод MDS та запропоновані критерії для інтерпретації отриманих результатів за трьохрівневою шкалою. Це дозволило визначити метод пошуку ключових слів, який найкраще підходить для використання з запропонованою моделлю сучасної української побутової мови. Проведені дослідження визначили наступні результати:

1. Встановлено, що найкраща здатність до роздільності при класифікації текстів з використанням запропонованої моделі сучасної української побутової мови спостерігається при довжині вектора слів рівній 1500 одиниць, це визначає оптимальну розмірність моделі.

2. За результатом тестової класифікації понад 400 текстів, з використанням візуальної верифікації результатів класифікації методом MDS було визначено, що метод пошуку ключових слів Text Rank найкраще підходить для використання з запропонованою моделлю сучасної української побутової мови.

3. Підтверджено, що метод візуальної аналітики MDS є ефективним і достатнім інструментом для візуальної верифікації результатів класифікації цифрових текстів за різними категоріями, до яких належать як тематичні класи, так і категорії емоційного забарвлення тестів.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

Наведене дає можливість стверджувати про можливість використання створеної моделі сучасної української мови для вирішення задач аналізу текстового контенту одиниць інтернет-спілкування та його класифікації за різними ознаками. У подальших дослідженнях планується вдосконалення наведених підходів до векторизації з перевіркою припущень використання композицій методів тощо. Також є потреба спрямувати дослідження на удосконалення загального вектору слів української мови та розв'язання задач визначення негативного забарвлення текстових повідомлень під час інтернет-спілкування.

Характерною рисою розглянутого підходу є його висока ефективність при роботі з сучасною українською мовою як характерного представника флективних мов. З огляду на особливості підходу, він виявиться ефективним також для аналітичних мов, зокрема англійської. Це підвищує цінність підходу для роботи з країномовним контентом побутового спілкування, оскільки в ньому часто присутні як запозичення англійські слова та власні назви. Ефективність підходу для аглютинативних мов таких як угорська вбачається нижчою, оскільки ідентифікація формантів та робота з ними дещо відрізняється від роботи з флексіями флективних мов і потребує окремих рішень. Наведене формує окремий напрямок подальших досліджень по роботі з текстами побутового спілкування, що мають змішаний багатомовний контент.

Основним результатом роботи є створений інтелектуальний метод виявлення цільових об'єктів предметної області за показниками семантичної зв'язності для класифікації текстової інформації з використанням розробленої моделі сучасної української мови, який відрізняється від існуючих урахуванням ключових слів та іменникових сутностей предметної області, що дало змогу підвищити точність виявлення цільових об'єктів предметної області внаслідок врахування іменникових сутностей. Подальші дослідження будуть спрямовані на розширення кількості категорій та експерименти із іншими метриками оцінки знайдених цільових об'єктів, у порівнянні їх із відомими великими мовними моделями, на кшталт GPT, Gemini тощо.

10. Література

- [1] Mazurets O., Sobko O., Vit R., Pasternak V. Practical Approach for Detection by Deep Learning of Target Objects of Subject Area Based on Semantic Connectivity Indicators in Audio Database. Proceedings of XXIV International Scientific and Practical Conference «Modern Scientific Challenges are the Driving Force of the Development of Scientific Research». May 22-24, 2024. Bruges, Belgium. 2024. Pp. 91-96.
- [2] Залуцька О.О., Молчанова М.О., Віт Р.В., Мазурець О.В. Конфігурування нейронної мережі для класифікації емоційної тональності текстової інформації за показниками семантичної зв'язності. Збірник наукових праць за матеріалами XV Всеукраїнської науково-практичної конференції «Актуальні проблеми комп'ютерних наук АПКН-2023». Хмельницький, 2023. с. 102-107.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

- [3] Mazurets O., Uspenska K., Vit R., Tyschenko O. Intelligent System for Determining the Object Attributes Values by Neural Networks Means by Graphic Images in Databases. Current Trends in the Development of Scientific Research in Today's Conditions. Proceedings of XXV International scientific and practical conference. May 29-31, 2024. Florence, Italy. 2024. Pp. 86-91.
- [4] Молчанова М.О., Мазурець О.В., Собко О.В., Віт Р.В., Назаров В.В. Алгоритм виявлення аб'юзивного вмісту в україномовному аудіоконтенті для імплементації в об'єктно-орієнтовану інформаційну систему. Науковий журнал «Вісник Хмельницького національного університету» серія: Технічні науки. Хмельницький, 2024. №1 (331). С. 101-106.
- [5] Slobodzian V., Molchanova M., Kovalchuk O., Sobko O., Mazurets O., Barmak O., Krak I. An Approach Based on the Visualization Model for the Ukrainian Web Content Classification. 2022 12th International Conference on Advanced Computer Information Technologies, ACIT 2022. 2022. pp. 400-405.
- [6] Krak Y., Barmak O., Mazurets O. The practice implementation of the information technology for automated definition of semantic terms sets in the content of educational materials. CEUR Workshop Proceedings. 2018. vol. 2139. pp. 245–254.
- [7] Shin H., Lee H. J., Cho S. General-use unsupervised keyword extraction model for keyword analysis. Expert Systems with Applications. Volume 233, 2023.
- [8] Ma Ch., Shen A., Yoshikawa H., Iwakura T., Beck D., Baldwin T. On the (In)Effectiveness of Images for Text Classification. Proceedings of the 16th Conference of the European Chapter of the Association for Computational Linguistics. Association for Computational Linguistics. 2021. pp. 42-48.
- [9] Ghosh D., Shrivastava R., Muresan S. «Laughing at you or with you»: The Role of Sarcasm in Shaping the Disagreement Space. 2021.
- [10] Barnes J., Øvrelid L., Veldal E. If you've got it, flaunt it: Making the most of fine-grained sentiment annotations. Proceedings of the 16th Conference of the European Chapter of the Association for Computational Linguistics. Association for Computational Linguistics. 2021. pp. 49–62.
- [11] Chen X., Zhang, Z. Lu X. Named Entity Recognition via Unified Information Extraction Framework. 2024 4th International Conference on Computer Communication and Artificial Intelligence (CCAI). Xi'an, China. 2024. pp. 308-313.
- [12] Corpus of Modern Ukrainian Language (BRUK). URL: <https://r2u.org.ua/corpus>.
- [13] MOVA.info: about the Ukrainian language, linguistics and more. URL: <http://www.mova.info/>.
- [14] UA-GEC: the first annotated GEC-corpus of the Ukrainian language. URL: <https://ua-gec-dataset.grammarly.ai/>.
- [15] Ukrainian News is a collection. URL: https://github.com/fido-ai/ua-datasets/tree/main/ua_datasets/src/text_classification.
- [16] Deutscher Wortschatz. Corpora Ukrainian. URL: https://wortschatz.uni-leipzig.de/en/download/Ukrainian#ukr_mixed_2014.
- [17] Jiang Zh., Gao Bo, He Y., Han Y., Doyle P., Zhu Q. Text Classification Using Novel Term Weighting Scheme-Based Improved TF-IDF for Internet Media Reports. Mathematical Problems in Engineerin. 2021.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

- [18] Krak I., Barmak O., Mazurets O. The practice investigation of the information technology efficiency for automated definition of terms in the semantic content of educational materials. CEUR Workshop Proceedings. 2016. vol.1631. pp. 237–245.
- [19] Kazemi A., P´erez-Rosas V., Mihalcea R. Biased TextRank: Unsupervised Graph-Based Content Extraction, Proceedings of the 28th International Conference on Computational Linguistics, Barcelona, Spain (Online), 2020. pp. 1642–1652.
- [20] Huang Zh., Xie Zh. A patent keywords extraction method using TextRank model with prior public knowledge, Complex Intell. Syst. 2021.
- [21] Zhang M., Li X., Yue Sh., Yang L. An Empirical Study of TextRank for Keyword Extraction, IEEE Access, Volume 8. 2020.
- [22] Campos R., Mangaravite V., Pasquali A., Jorge A., Nunes C., Jatowt A. YAKE! Keyword extraction from single documents using multiple local features. Information Sciences. Volume 509. 2020. pp. 257–289.
- [23] Manziuk E.A. Barmak O.V., Krak Iu.V., Pasichnyk O.A., Radiuk P.M., Mazurets O.V. Semantic alignment of ontologies meaningful categories with the generalization of descriptive structures. Problems in programming. 2023. Vol. 3-4. Pp. 355-363.
- [24] Тимуш О.Ю. Шпичко А.В., Мазурець О.В. Дослідження ефективності інформаційної технології тематичного сортування текстових повідомлень. Збірник наукових праць за матеріалами XI всеукраїнської науково-практичної конференції «Актуальні проблеми комп’ютерних наук АПКН-2019». Хмельницький, 2019. Т.1. С.207-212.
- [25] Molchanova M., Mazurets O., Sobko O., Boiarchuk I. Object-Oriented Approach for Ethnic Enmity Detection in Text Messages by NLP. Proceedings of XXI International Scientific and Practical Conference «Scientific Achievements and Innovations as a Way to Success». Vilnius, Lithuania. 2024. Pp. 73-77.
- [26] Sobko O., Mazurets O., Didur V., Chervonchuk I. Recurrent Neural Network Model Architecture for Detecting a Tendency to Atypical Behavior Of Individuals by Text Posts. Theoretical and Practical Aspects of Modern Research. Proceedings of XXVI International scientific and practical conference. June 5-7, 2024. International Scientific Unity. Ottawa, Canada. 2024. Pp. 113-117.
- [27] Залуцька О.О., Молчанова М.О., Мазурець О.В., Мельник О.І., Скрипник Т.К. Метод інтелектуального аналізу емоційної тональності текстової інформації для визначення поведінкових намірів нейромережевими засобами. Науковий журнал «Вісник Хмельницького національного університету» серія: Технічні науки. Хмельницький, 2023. №5 (325). Т.1. С. 67-73.
- [28] Молчанова М.О., Мазурець О.В., Собко О.В., Кліменко В.І., Андрощук В.І. Метод нейромережевого виявлення кібербулінгу з використанням хмарних сервісів та об’єктно-орієнтованої моделі. Науковий журнал «Вісник Хмельницького національного університету» серія: Технічні науки. Хмельницький, 2024. №2 (333). С. 200-206.

**INTELLIGENT METHOD FOR IDENTIFYING TARGET OBJECTS
OF THE SUBJECT AREA BASED ON SEMANTIC CONNECTIVITY
INDICATORS FOR TEXT INFORMATION CLASSIFICATION**

Ph.D. **O. Mazurets** ORCID: 0000-0002-8900-0650

Khmelnyskyi National University, Ukraine

E-mail: exe.chong@gmail.com

R. Vit ORCID: 0009-0009-6958-4730

Khmelnyskyi National University, Ukraine

E-mail: vit.roman.vit@gmail.com

Abstract: The intelligent method for identifying target objects of subject area based on indicators of semantic connectivity was considered, which is designed to automate the process of identifying key elements in large arrays of text data. The developed method differs from the existing ones by taking into account keywords and noun entities of the subject area, which made it possible to increase the accuracy of detection of target objects of the subject area due to the consideration of noun entities. The conducted studies established that the target objects found by the created method are able to perform the further task of classification, demonstrating on the metric of Euclidean distances the grouping of texts of the same category and the increase of the distance orthogonal to it.

For the applied implementation of created intellectual method for identifying target objects of subject area, the model of modern Ukrainian language was formed, which was built by combining known frequency dictionaries that are significant for conveying meaning. To create the correct model of modern Ukrainian language, frequency dictionaries of existing corpora of the Ukrainian language were used, which collectively cover both different fields of activity and types of content, as well as different areas of communication, taking into account communication on the Internet. By combining the dictionaries of these corpora of the Ukrainian language according to frequency indicators, a vector of words was obtained, which was filtered by noun group and quantitatively limited in order to improve the ability of classification. The conducted research made it possible to assert the possibility of using the created model of modern Ukrainian language to effectively solve the problems of analyzing the text content of Internet communication units and classifying it according to various characteristics.

Keywords: target objects of subject area, texts classification, Ukrainian language model, frequency dictionaries, words vector, semantic connectivity

**МЕТОД ВИЯВЛЕННЯ ТА КЛАСИФІКАЦІЇ ТЕХНІК
ПРОПАГАНДИ У ТЕКСТОВОМУ КОНТЕНТІ ЗАСОБАМИ
ШТУЧНОГО ІНТЕЛЕКТУ**

М. Молчанова ORCID: 0000-0001-9810-936X

Хмельницький національний університет, Україна

E-mail: m.o.molchanova@gmail.com

***Анотація.** Робота присвячена створенню та апробації методу нейромережевого виявлення техніки пропаганди за маркерами з візуальною аналітикою, що дозволяє перетворювати вхідні дані у вигляді тексту для аналізу та моделей керованого машинного навчання у вихідні дані, що містять числові оцінки присутності кожного пропагандистського прийому та розміченого тексту з візуальною аналітикою присутності виявлених пропагандистських маркерів. Було проведено дослідження, яке дозволяє виявити 17 основних пропагандистських прийомів. У дослідженні порівнювалися 3 підходи, які найчастіше використовуються: традиційний підхід машинного навчання, підхід на основі рекурентних нейронних мереж і підхід на основі трансформаторних моделей. Найвищих результатів досяг підхід на основі моделі трансформатора, який використовує механізми самоуваженості, які дозволяють кожному елементу послідовності безпосередньо взаємодіяти з усіма іншими елементами. Це забезпечує ефективне захоплення довготривалих залежностей, що характерно для пропагандистських технік. Такий підхід дозволив виявити методи пропаганди з точністю до 0,96.*

***Ключові слова:** BERT, RNN, методи пропаганди, виявлення пропаганди, пропагандистські маркери, візуальна аналітика*

1. Вступ

Пропаганда, замаскована під звичайні новини, поширюється вже багато десятиліть, але сучасна цифрова ера додатково створює умови для її більш швидкого, масового та ефективного поширення [1].

Створюються нові методи генерації текстів, які дедалі частіше мало відрізняються від створених людиною [2], що призводить до стрімкого зростання кількості контенту. Тому це все підкреслює важливість створення автоматизованих методів для виявлення пропагандистських маніпуляцій, які допоможуть користувачам отримувати інформацію більш усвідомлено.

Метою дослідження є підвищення точності виявлення методів пропаганди шляхом розробки методу виявлення методів пропаганди за маркерами на основі набору моделей машинного навчання, окремо для кожного методу пропаганди, навчених на модифікованих маркованих даних.

Основні внески дослідження можна підсумувати так:

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

– Розроблено підхід до підготовки навчальних даних, що дозволяє проводити навчання моделей машинного навчання для окремих технік пропаганди;

– Запропоновано метод виявлення прийомів пропаганди, що дозволяє знаходити силу прояву кожного з 17-и прийомів пропаганди, а також візуально інтерпретувати отриманий результат з використанням моделі LIME.

– Експериментально продемонстровано ефективність використання нейромережових моделей-трансформерів в порівнянні з рекурентними моделями та Traditional machine learning approaches

В цій роботі, далі представлено огляд пов'язаних робіт у сфері виявлення прийомів пропаганди згідно двох складових дослідження, зокрема аналіз наявних шляхів до вирішення проблеми виявлення пропаганди та аналіз моделей машинного навчання для виявлення прийомів пропаганди. Третій розділ паперу містить схему та кроки методу нейромережового виявлення технік пропаганди за маркерами. Четвертий розділ присвячений опису плану експерименту виявлення технік пропаганди за маркерами та підготовці датасету. П'ятий розділ містить результати експерименту, їх аналітику та обговорення.

2. Аналіз останніх досліджень та публікацій

Наявні шляхи вирішення проблеми виявлення пропаганди. Проблема виявлення пропаганди залишається актуальною, адже і досі з'являються нові способи впливу на користувачів для поширення пропагандистських повідомлень. З огляду на це, виникає потреба у постійному моніторингу нових способів створення пропагандистського вмісту та вдосконалення методів їх ідентифікації, що є важливою задачею забезпечення інформаційної безпеки та протидії дезінформації. Тому науковці працюють над виявленням нових маркерів та нових прийомів пропаганди, а також над покращенням існуючих підходів для її виявлення.

Досліджено основні методи аналізу газетних текстів для виявлення маніпулятивних технологій, що допомагає застеретти від дезінформації та пропаганди [1]. Представлено новий набір еталонних даних чеською мовою для навчання та оцінки сучасних і майбутніх методів розпізнавання 18 маніпулятивних прийомів, таких як нагнітання страху, релятивізація та навішування ярликів. Показано, що поєднання контент-аналізу з запропонованим стильовим аналізом підвищує точність виявлення 15 з 17 оцінених маніпулятивних технік від 0.05% до 1.46%. Метод перевірено на пропагандистській базі QCRI. Подальші дослідження будуть зосереджені на додаванні нових стилеметричних характеристик, вдосконаленні існуючих методів та використанні методів доповнення даних для боротьби з дисбалансом етикеток. Також планується перейти до дрібнозернистої класифікації на рівні проміжків часу, а не на рівні документа в цілому.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

У ще одному дослідженні представлено багатомовний набір даних про пропаганду та проведено експеримент для дослідження маркерів, за якими людські анотатори та алгоритми класифікації відрізняють пропагандистські статті від непропагандистських на певну тему [3]. Показано, що перебільшення, зменшення описовості та відсутність адекватних джерел часто зустрічаються у пропагандистській пресі. Аналізатор VAGO підтвердив, що використання невизначених маркерів значно корелює з цими особливостями. Виявлено, що моделі машинного навчання ефективні для виявлення пропаганди на певну тему, але потребують покращення щодо пояснюваності та узагальнення на інші теми. Подальші роботи зосередяться на вдосконаленні аналізу, розробці багатомовних моделей та покращенні інструментів пояснюваності. Також планується введення нових міток для уточнення анотацій та ідентифікації більшої кількості стилістичних особливостей.

Застосування моделі MVPROP, що використовує багатомірні контекстні вбудовування, дозволяє покращити точність виявлення пропаганди. Експерименти показали, що модель може бути перенесена на новинні статті [4]. Для тестування представлено TWEETSPIN, набір даних із твітами, що містить слабкі анотації тонких пропагандистських технік, і модель MVPROP для їх виявлення. TWEETSPIN включає лише ідентифікатори твітів, що відповідає умовам використання Twitter, і містить потенційно образливі та ворожі висловлювання. Основним обмеженням є слабкі анотації через великий масштаб даних. У майбутньому планується дослідження виявлення пропаганди на рівні окремих фрагментів.

Дослідники застосували мовну модель RoBERTa для виявлення пропагандистських технік у новинних статтях [5]. Модель оцінювалась за допомогою референсного набору даних для завдання SemEval-2020 Task 11, демонструючи здатність виявляти складні техніки пропаганди і перевершуючи базову модель з показником F1-score у 60.2%. У той час, як [6] аналізувались можливості використання великих мовних моделей (LLMs), зокрема моделі GPT-3.5-Turbo від OpenAI, для виявлення ознак пропаганди в новинних статтях. Використовуючи технологію, що лежить в основі ChatGPT, дослідники аналізували тексти для визначення присутності різних технік пропаганди, визначених у попередній роботі [7]. Розроблено ретельно уточнений запит, який поєднується зі статтями з мережі Russia Today (RT) та датасету SemEval-2020 Task 11, щоб визначити наявність пропагандистських методик. Дослідження показало, що технологія LLM може давати розумні висновки про пропаганду, хоча точність виявлення складає всього 25.12% за датасетом SemEval-2022. Однак вона демонструє потенціал як інструмент для виявлення пропаганди для кінцевих користувачів, таких як медіа споживачі та журналісти.

Як підтверджено у роботах вище, пропаганда характеризується прийомами, за які відповідають певні маркери, які притаманні використовуваним прийомам. У роботі увага буде зосереджена на виявленні 17 known прийомів пропаганди, детально описаних в [8]. А саме: «Appeal to fear-prejudice», «Causal Oversimplification», «Doubt», «Exaggeration», «Flag-Waving», «Labeling»,

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

«Loaded Language», «Minimisation», «Name Calling», «Repetition», «Appeal to Authority», «Black and White Fallacy», «Reductio ad Hitlerum», «Red Herring», «Slogans», «Thought terminating Cliches», «Whataboutism».

Моделі машинного навчання для виявлення прийомів пропаганди. У рамках дослідження будуть використані 3 підходи щодо моделей машинного навчання:

- Традиційний підхід на основі машинного навчання.
- Підхід на основі рекурентних реймереж.
- Підхід на основі моделей-трансформерів.

Традиційний підхід на основі машинного навчання охоплює декілька методів і алгоритмів, призначених для розв'язання різноманітних завдань прогнозування, класифікації та кластеризації даних, в тому числі і для виявлення прийомів пропаганди. Лінійна регресія використовується для моделювання лінійних залежностей між вхідними функціями (ознаками) і цільовими значеннями, а також є одним з найпростіших методів регресійного аналізу і часто використовується для прогнозування числових значень. Метод опорних векторів (SVM) шукає оптимальну гіперплощину, яка найкращим чином розділяє два класи точок даних у просторі ознак. Він часто використовується для задач класифікації, особливо коли дані мають складну структуру [9]. Навчання на основі байєсових мереж ґрунтується на байєсівській ймовірнісній моделі, де кожна змінна розглядається як випадкова, і використовуються правила байєсівського висновку для побудови моделі. Також серед традиційні підходів машинного навчання для виявлення прийомів пропаганди використовується логістична регресія, k-NN, алгоритми кластеризації, наприклад, k-means. У роботі [10] автори наводять результати дослідження кілька моделей класифікації, включаючи мультиноміальний наївний метод Байєса, SVM, логістичну регресію та K-найближчих сусідів. У статті [11] автори представили два альтернативні методи (BERT та SVM) автоматичного визначення прокремлівської пропаганди в газетних статтях і дописах у Telegram.

Підхід до виявлення пропаганди на основі рекурентних нейронних мереж використовується для аналізу послідовних даних, зокрема текстів, що часто зустрічаються у соціальних мережах. Рекурентні нейронні мережі, Long Short-Term Memory (LSTM) і Gated Recurrent Unit (GRU) це різновиди архітектур рекурентних нейронних мереж, кожна з яких має свої особливості і застосування у вирішенні різних завдань у машинному навчанні, зокрема виявленні пропаганди в соціальних мережах. RNN є базовою архітектурою, яка здатна обробляти послідовні дані, зберігаючи інформацію у вигляді внутрішнього стану (пам'яті), який оновлюється при кожному новому вході [12]. LSTM – це розширена версія RNN, яка включає додаткові механізми, такі як ворота забування, ворота оновлення та ворота виходу. GRU являється спрощеною версією LSTM, яка має менше внутрішніх компонент. GRU вважається менш обчислювально витратною архітектурою порівняно з LSTM [13]. Результати дослідження ідентифікації пропаганди на платформі Twitter

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

під час пандемії COVID-19 авторів [14] показали, що запропонована пропагандистська ідентифікація на основі LSTM показала кращі результати, ніж інші розглянуті у роботі методи машинного навчання. За допомогою запропонованого підходу на основі LSTM досягається точність 77,15%. А у статті [15] автори використовують техніки глибокого навчання Bi-LSTM і Bi-GRU з методами SVM із слабким контролем забезпечили. Даний підхід забезпечив точність 90% у виявленні пропагандистських новин. Автори стверджують, що такий підхід є дуже ефективним і дієвим для нерозмічених даних.

Підхід на основі моделей-трансформерів передбачає використання таких архітектур нейромереж як BERT, RoBERTa, DistilBERT, GPT тощо [16]. BERT є однією з найвідоміших архітектур трансформерів, розроблена Google. BERT здатний досягти вражаючих результатів у завданнях обробки природної мови (NLP) завдяки здатності до контекстної обробки слів і здібності до підготовки звичайних моделей для багатьох NLP-завдань [17]. RoBERTa – це оптимізований підхід до BERT, який покращує навчання і результати моделі на різних NLP-завданнях шляхом застосування різних оптимізаційних стратегій [18]. DistilBERT вважається легковаговою версією BERT, яка зберігає сутність оригінальної моделі, зменшуючи кількість параметрів і зберігаючи високу продуктивність на різних NLP-завданнях. GPT – це родина моделей трансформерів, розроблених OpenAI. Даний підхід застосовують у дослідженні для класифікації пропаганди [19]. Автори використовують три моделі глибокого навчання, CNN, LSTM, Bi-LSTM і чотири моделі на основі трансформаторів, а саме багатомовні BERT, Distil-BERT, Hindi-BERT і Hindi-TPU-Electra. Експериментальні результати вказують на те, що багатомовні моделі BERT і Hindi-BERT забезпечують найкращу продуктивність із найвищим показником F1 84% за даними проведеного експериментального дослідження. Також у дослідженні [20] досліджується продуктивність BERT і RoBERTa, DeBERTa з комбінацією різних методів збільшення даних для виявлення пропагандистських текстів. Автори змогли досягти F1 micro 60% на тестовому наборі, використовуючи ансамбль моделей BERT, RoBERTa та DeBERTa.

Отже, наведені підходи знаходять своє застосування у завданні виявлення прийомів пропаганди.

3. Метод виявлення та класифікації технік пропаганди

Для реалізації методу виявлення та класифікації технік пропаганди за маркерами пропонується створити 17 моделей машинного навчання, кожна з яких буде відповідати за визначений прийом пропаганди. Такий підхід (рисунок 1) дозволить навчити моделі машинного навчання таким чином, щоб у них змогли вибудуватись залежності, притаманні конкретним видам пропаганди.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

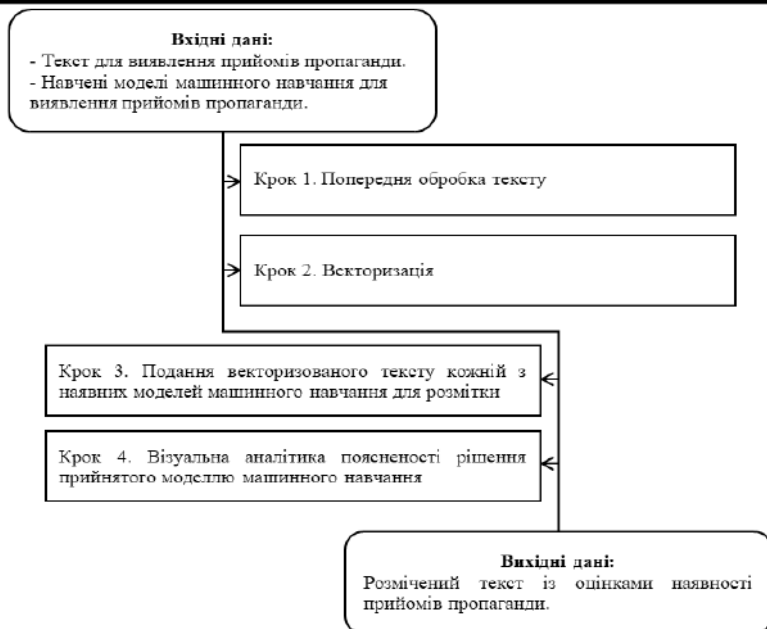


Рисунок 1. Кроки методу виявлення та класифікації технік пропаганди

В загальному, схема методу для виявлення прийомів пропаганди наведена на рисунку 1. Метод дозволяє перетворювати вхідні дані у вигляді тексту для аналізу та навчених моделей машинного навчання у вихідні дані, які містять числові оцінки наявності кожного з прийомів пропаганди та розмічений текст з візуальною аналітикою присутності детектованих маркерів пропаганди.

Вхідними даними методу виявлення прийомів пропаганди є текст для виявлення прийомів пропаганди та навчені моделі машинного навчання для виявлення прийомів пропаганди.

Попередня обробка тексту включає видалення розділових знаків та стоп-слів, хоча і розділові знаки, розміщені певним чином, також можуть впливати на наявність пропаганди [22]. Асоціація споріднених слів була виконана шляхом лематизації, яка показує кращі результати, ніж стемінг. Для лематизації була використана відповідна стандартна бібліотека Pyton. Однак, в рамках даного дослідження такий вплив досліджуватись не буде.

Наступним кроком є векторизація тексту після попередньої обробки. Векторизоване представлення подається на вхід кожній навченій моделі машинного навчання, яка виконує передбачення наявності для кожного прийому пропаганди та його сили прояву. Більш детально крок 3 наведено на рисунку 2.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

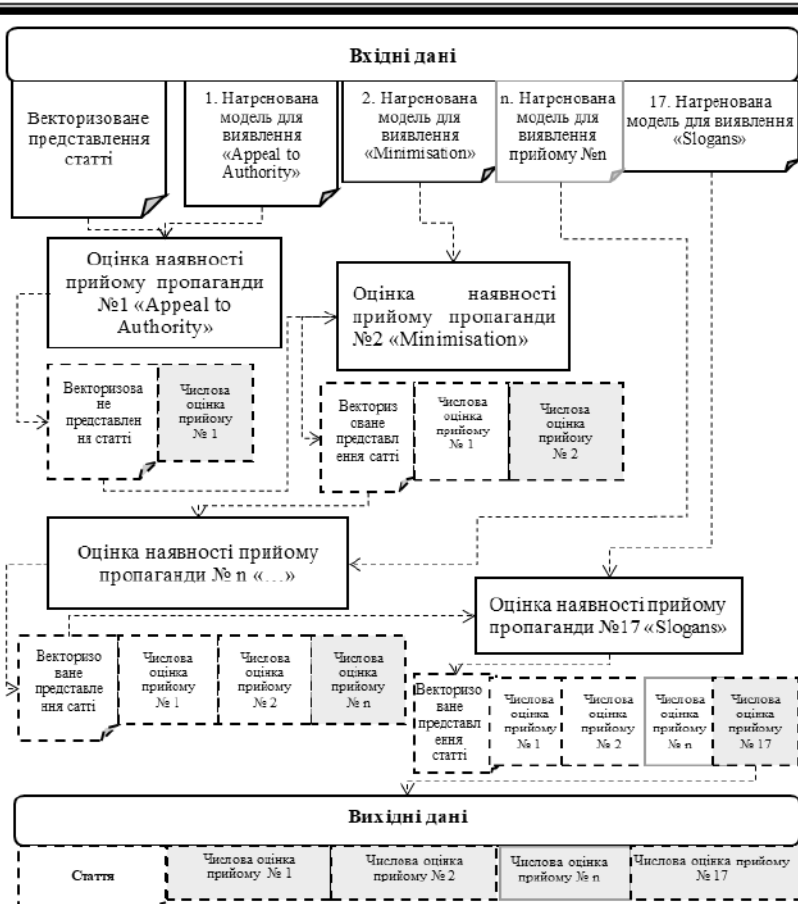


Рисунок 2. Деталізація кроку подання векторизованого тексту кожній з моделей машинного навчання для розмітки

Останнім етапом є проведення візуальної аналітики для поясненості рішення прийнятого кожною моделлю машинного навчання. Візуальна аналітика використовується із застосуванням методу Лайма, що є методом для інтерпретації прогнозів моделей машинного навчання, що розроблений для того, щоб пояснювати індивідуальні прогнози складних моделей [23]. LIME наближає будь-яку модель машинного навчання чорної скриньки до локальної, інтерпретованої моделі для пояснення кожного окремого прогнозу. LIME дозволяє зрозуміти, які частини вхідних даних вплинули на рішення моделі.

Вхідними даними кроку подання векторизованого тексту кожній з наявних моделей машинного навчання для розмітки є векторизоване представлення

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

статті та натреновані 17 моделей машинного навчання. Моделі по черзі оцінюють векторизоване представлення текстового контенту для аналізу на предмет наявності кожного з 17-и прийомів пропаганди. Вихідними даними є числові оцінки сили проявів прийомів пропаганди, що притаманні поданому векторному представленню тексту.

Таким чином, було створено метод нейромережевого виявлення технік пропаганди за маркерами, що дозволяє перетворювати вхідні дані у вигляді тексту для аналізу та навчених моделей машинного навчання у вихідні дані, які містять числові оцінки наявності кожного з прийомів пропаганди та розмічений текст з visual analytic присутності детектованих маркерів пропаганди.

4. Експеримент

У ході проведення експерименту досліджувалось використання 3-х підходів до навчання моделей для виявлення прийомів пропаганди:

- Традиційний підхід на основі машинного навчання.
- Підхід на основі рекурентних нейромереж.
- Підхід на основі моделей-трансформерів.

У рамках традиційного підходу на основі машинного навчання досліджувалось виявлення прийомів пропаганди з використанням моделей регресії, SVM, Random Forest та Naive Bayes. Для прийомів «Appeal to Authority», «Black and White Fallacy», «Reductio ad Hitlerum», «Red Herring», «Slogans», «Thought Terminating Cliches» та «Whataboutism» також буде проведено дослідження із застосуванням SMOTE балансування та без нього.

Підхід на основі рекурентних нейромереж включає в себе порівняння 3-х видів архітектур: RNN, LSTM та GRU.

Підхід на основі моделей-трансформерів включає в себе порівняння BERT-подібних моделей: RoBERTa, BERT, ELECTRA.

Для проведення експерименту було створено програмне забезпечення на мові програмування Python, з використанням бібліотек для машинного навчання Sklearn [24], Tensorflow [25], LimeTextExplainer [26], NumPy [27], Pandas [28]. Програмне забезпечення складається із консольного застосунку для навчання моделей машинного навчання, консольного застосунку для виявлення технік пропаганди за маркерами та веб-модуля для візуальної аналітики оцінювання прийнятих результатів обраною моделлю машинного навчання з її оцінками.

Для навчання моделей машинного навчання, що будуть виконувати функції виявлення прийомів пропаганди, буде використано набір даних «emnlp_trans_uk_dataset», що є перекладеним набором даних «emnlp_en_dataset» з відповідністю розмітки на українській мові, взятий з Kaggle-змагань «Disinformation Detection Challenge» [29] з посиланням на «Analysis Project».

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

Команда «Analysis Project» [30] провела аналіз текстів, виявивши всі фрагменти, які містять пропагандистські прийоми, а також їх тип. Розподіл статей за довжиною у символах наведено на рисунку 3.

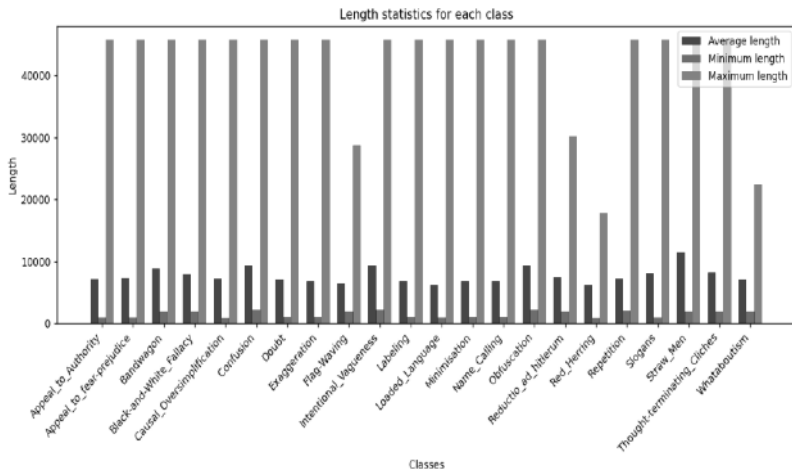


Рисунок 3. Статистика за довжиною у символах по прийомам пропаганди

Зокрема, ними створено корпус новинних статей, анотованих вручну на рівні фрагментів за допомогою вісімнадцяти пропагандистських прийомів. Набір даних налічує 788 статей.

Як видно з графіку на рисунку 3, для більшості прийомів пропаганди довжина текстів де вони представлені особливої ролі не грають. Однак, «Flag Waving», «Red Herring», «Reductio ad hitlerum» та «Whataboutism» все ж мають меншу максимальну довжину в текстах, де вони представлені.

Для тренування моделей машинного навчання даний датасет було модифіковано таким чином, щоб текст що містить кожен прийом пропаганди був розміщений в окремому каталозі. Після такого перерозподілу було виведено статистику наявних текстів, що репрезентують прийоми пропаганди. Статистика наведена на рисунку 4. Як видно з рисунку 4 деякі прийоми пропаганди, такі як «Bandwagon», «Confusion», «Intentional Vagueness», «Obfuscation» та «Straw Men» представлені у критично низькій кількості (менше 20 тестів), тому для них окремі класифікатори створені не будуть, ці дані будуть об'єднані у категорію «Інші прийоми пропаганди», однак таким чином, щоб у наявному наборі не були присутні інші прийоми, відмінні від п'яти перерахованих. До прийомів пропаганди, що представлені менш ніж у 100 документах, однак більше ніж 20 буде застосовано SMOTE-балансування під час навчання класифікаторів [31]. До таких категорій належать: «Appeal to

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

Authority», «Black and White Fallacy», «Reductio ad hitlerum», «Red Herring», «Slogans», «Thought terminating Cliches» та «Whataboutism».

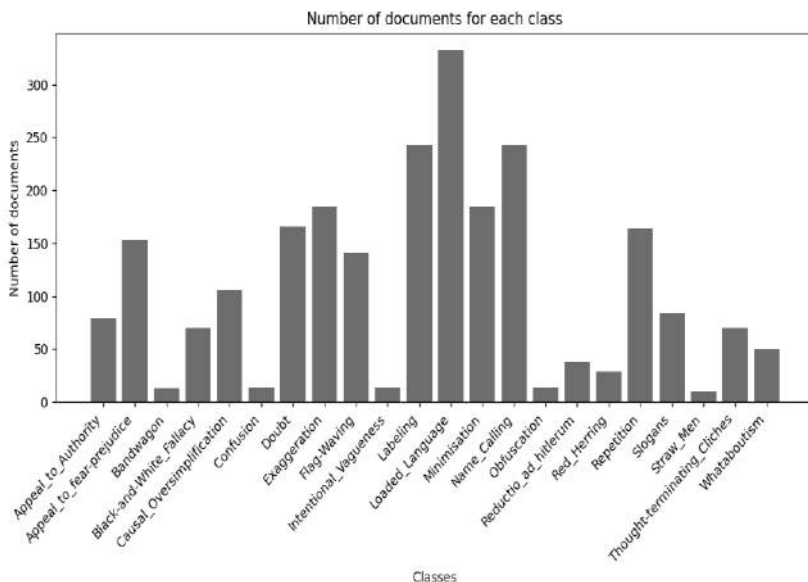


Рисунок 4. Статистика по кількості текстів, що представляють прийоми пропаганди, *шт.*



Рисунок 5. Приклад балансування при формуванні набору даних для навчання та тестування моделі виявлення прийому «Appeal to fear-prejudice»

Із розглянутого вище набору даних для кожної з 17 типових моделей машинного навчання буде сформовано власний дочірній набір текстів, що буде задовольняти такі вимоги:

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

- мати тексти з визначеним прийомом пропаганди;
- у протипагу використовувати набір «Інші прийоми пропаганди» доповнений текстами без пропаганди та текстами, що представляють інші прийоми пропаганди, відмінні від цільового виду.

Приклад формування набору даних для виявлення прийому «Appeal to fear-prejudice» наведено на рисунку 5.

Отже, у дослідженні буде використано 18 класів: 17 цільових, що є репрезентативними по кількості та відповідають 17 визначеним прийомам пропаганди та 5 об'єднаних в категорію «Інші прийоми пропаганди».

5. Результати та дискусія

Результати дослідження для Traditional machine learning approaches для прийомів «Appeal to Authority», «Black and White Fallacy», «Reductio ad hitlerum», «Red Herring», «Slogans», «Thought terminating Cliches» та «Whataboutism» без використання SMOTE балансування за метрикою точності наведено в Таблиці 1.

Таблиця 1

Традиційний підхід на основі машинного навчання для виявлення прийомів пропаганди до SMOTE балансування за метрикою Accuracy

Techniques of propaganda	Regression	SVM	Random Forest	Naive Bayes
Appeal to Authority	0.57	0.63	0.55	0.64
Black and White Fallacy	0.55	0.64	0.51	0.58
Reductio ad hitlerum	0.68	0.56	0.61	0.59
Red Herring	0.61	0.61	0.59	0.61
Slogans	0.62	0.63	0.56	0.62
Thought terminating Cliches	0.59	0.58	0.63	0.58
Whataboutism	0.62	0.65	0.59	0.57

Як видно з таблиці 1, точність виявлення прийомів пропаганди коливається від 0.51 до 0.68, що є доволі низьким показником.

Наступним етапом для даних прийомів пропаганди було застосовано SMOTE балансування, збільшивши таким чином кількість навчальних зразків до рівня не менше 100. Результат експерименту наведено у таблиці 2.

Як видно з таблиці 2, застосування SMOTE балансування дало позитивні результати для більшості прийомів пропаганди, однак для «Slogans» результат покращення не дав.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

Це пов'язано з тим, що кількість навчальних зразків близька до граничної і є достатньою для навчання запропонованих версій машинного навчання.

Таблиця 2

Традиційний підхід на основі машинного навчання для виявлення прийомів пропаганди зі SMOTE балансування за метрикою Accuracy

Techniques of propaganda	Regression	SVM	Random Forest	Naive Bayes
Appeal to Authority	0.59	0.67	0.54	0.60
Black and White Fallacy	0.61	0.62	0.55	0.64
Reductio ad hitlerum	0.69	0.63	0.62	0.58
Red Herring	0.69	0.64	0.58	0.61
Slogans	0.62	0.63	0.56	0.62
Thought terminating Cliches	0.62	0.68	0.62	0.61
Whataboutism	0.64	0.66	0.58	0.56

Для решти прийомів SMOTE балансування не застосовувалося, та результати застосування традиційного підходу машинного навчання наведено у таблиці 3.

Таблиця 3

Традиційний підхід на основі машинного навчання для виявлення прийомів пропаганди без SMOTE балансування за метрикою Accuracy

Techniques of propaganda	Regression	SVM	Random Forest	Naive Bayes
Appeal to fear-prejudice	0.62	0.61	0.55	0.59
Causal Oversimplification	0.58	0.62	0.59	0.55
Doubt	0.6	0.58	0.63	0.59
Exaggeration	0.61	0.63	0.61	0.53
Flag-Waving	0.62	0.61	0.64	0.6
Labeling	0.67	0.62	0.61	0.61
Loaded Language	0.6	0.59	0.6	0.58
Minimisation	0.62	0.61	0.61	0.60
Name Calling	0.55	0.59	0.57	0.61
Repetition	0.69	0.7	0.61	0.55

Результати з таблиці 3 також коливаються від 0.6 до 0.67, що має схожий результат із застосуванням SMOTE балансування (таблиця 2). Однак отримані результати також не є задовільними. Ілюстрація експерименту щодо застосування традиційного підходу машинного навчання наведено на рисунку 6.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

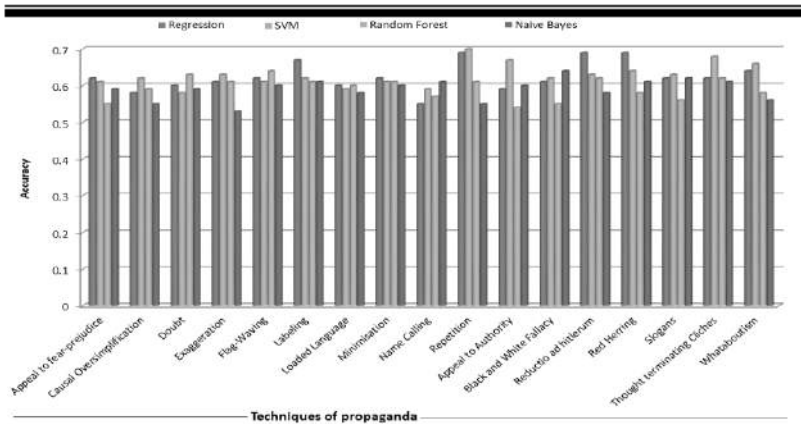


Рисунок 6. Порівняння точності моделей для традиційного підходу машинного навчання

Таблиця 4

Підхід на основі рекурентних неймереж для виявлення прийомів пропаганди за метрикою Accuracy

Techniques of propaganda	RNN	LSTM	GRU
Appeal to fear-prejudice	0.69	0.69	0.71
Causal Oversimplification	0.73	0.71	0.76
Doubt	0.75	0.7	0.74
Exaggeration	0.64	0.72	0.75
Flag-Waving	0.69	0.7	0.79
Labeling	0.69	0.73	0.8
Loaded Language	0.71	0.7	0.68
Minimisation	0.78	0.78	0.74
Name Calling	0.76	0.74	0.76
Repetition	0.74	0.75	0.76
Appeal to Authority	0.71	0.72	0.73
Black and White Fallacy	0.7	0.68	0.72
Reductio ad hitlerum	0.75	0.68	0.71
Red Herring	0.65	0.72	0.70
Slogans	0.74	0.68	0.75
Thought terminating Cliches	0.63	0.66	0.65
Whataboutism	0.67	0.69	0.69

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

Наступним експериментом проводилось дослідження застосування An approach based on recurrent rail networks, що включало в себе порівняння використань 3-х видів архітектур: RNN, LSTM та GRU. Дані експерименту без використання SMOTE балансування наведено у таблиці 4.

Як видно з даних таблиці 4, результати для усіх прийомів пропаганди окрім Thought terminating Cliches, є вищими та знаходяться у діапазоні від 0.66 до 0.8. Однак до даного прийому пропаганди буде в подальшому застосовано SMOTE балансування, що можливо дозволить покращити показник. Наступним експериментом буде використання SMOTE балансування до навчання нейромережних моделей для «Appeal to Authority», «Black and White Fallacy», «Reductio ad hitlerum», «Red Herring», «Slogans», «Thought terminating Cliches» та «Whataboutism». Із таблиці 5 видно, що SMOTE балансування дає позитивний ефект на точність виявлення прийомів пропаганди. Не вдалося покращити виявлення прийому «Reductio ad hitlerum», де результати до SMOTE балансування були на 0.01 вище, а також «Appeal to Authority» та «Black and White Fallacy» залишились на тому ж рівні, що і до виконання балансування. На рисунку 7 показано порівняння найвищих отриманих показників точності для рекурентних нейромережних моделей.

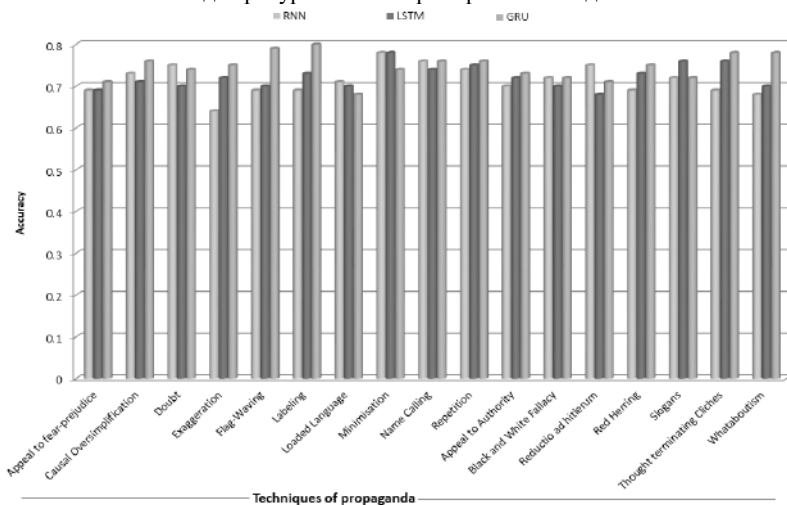


Рисунок 7. Порівняння точності моделей для підходу на основі рекурентних нейронних мереж

Останнім етапом дослідження є використання підходу на основі використання моделей-трансформерів, що включає в себе порівняння BERT-подібних моделей: RoBERTa, BERT, ELECTRA. Були використані попередньо натреновані моделі з ресурсу Hugging Face [32], які було донавчені вищеописаним способом протягом 3-х епох навчання. Отримані результати без використання SMOTE балансування наведені у таблиці 6.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

Таблиця 5

Підхід на основі рекурентних неймереж для виявлення прийомів пропаганди за метрикою Accuracy із SMOTE балансуванням

Techniques of propaganda	RNN	LSTM	GRU
Appeal to Authority	0.7	0.72	0.73
Black and White Fallacy	0.72	0.7	0.72
Reductio ad hitlerum	0.73	0.74	0.74
Red Herring	0.69	0.73	0.75
Slogans	0.72	0.76	0.72
Thought terminating Cliches	0.69	0.76	0.78
Whataboutism	0.68	0.7	0.78

Таблиця 6

Підхід на основі неймереж-трансформерів для виявлення прийомів пропаганди за метрикою Accuracy

Techniques of propaganda	bert-base-multilingual-cased	roberta-base	ukr-electra-base
Appeal to fear-prejudice	0.81	0.8	0.87
Causal Oversimplification	0.78	0.79	0.82
Doubt	0.93	0.9	0.87
Exaggeration	0.8	0.8	0.8
Flag-Waving	0.92	0.9	0.89
Labeling	0.96	0.94	0.96
Loaded Language	0.93	0.97	0.94
Minimisation	0.89	0.86	0.9
Name Calling	0.92	0.92	0.91
Repetition	0.93	0.94	0.94
Appeal to Authority	0.87	0.89	0.88
Black and White Fallacy	0.89	0.91	0.88
Reductio ad hitlerum	0.85	0.87	0.86
Red Herring	0.67	0.8	0.78
Slogans	0.84	0.86	0.83
Thought terminating Cliches	0.8	0.73	0.79
Whataboutism	0.79	0.78	0.78

Із даних таблиці 6 видно, що BERT-подібні неймережеві архітектури значно краще виявляють прийоми пропаганди, порівняно з рекурентними та традиційним підходами до навчання. Це пояснюється тим, що такі архітектури

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

є контекстно-орієнтованими, що є важливим аспектом для виявлення прийомів пропаганди. Застосування SMOTE балансування дозволило підвищити точність виявлення «Red Herring» нейромережевою моделлю ukr-electra-base до 0.89, а також «Whataboutism» до 0.83 з використанням bert-base-multilingual-cased. Порівняння найвищих оцінок за метрикою точності для 3-х розглянутих підходів наведено на рисунку 8.

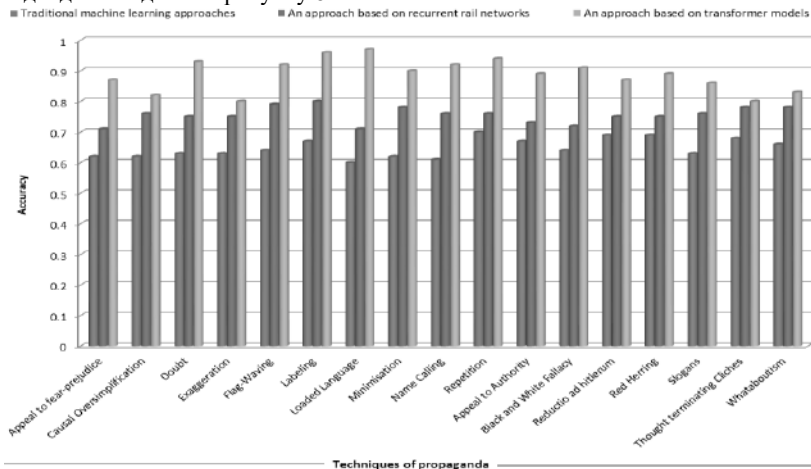


Рисунок 8. Порівняння точності моделей альтернативних підходів для виявлення технік пропаганди

Як видно з рисунку 8, традиційний підхід на основі машинного навчання очікувано показав гірші результати, оскільки він не вмів бачити контекст, що є важливим для виявлення технік пропаганди. Рекурентні нейромережеві моделі хоч і показали результати вищі від традиційного підходу, однак все ще мають проблеми з обробкою довгих залежностей. Найвищі результати з проведеного експерименту виявились у підході на основі моделей-трансформерів, це пояснюється використовуваними механізмами самоуваги, які дозволяють кожному елементу послідовності безпосередньо взаємодіяти з усіма іншими елементами. Це дозволяє ефективно захоплювати довготривалі залежності, що характерно для проявів технік пропаганди. Отримані результати забезпечили виявлення різних пропагандистських прийомів з мінімальною точністю 79,03% (мінімальні значення точності отримані для методики «Whataboutism»), що краще за відомі аналоги [8] щодо виявлення пропаганди незалежно від використовуваних методик. Порівняно з відомими аналогами [7] підвищилась точність виявлення різних пропагандистських прийомів:

- для техніки «Appeal to Authority», точність виявлення зросла на 9.81% (існуючий метод 77.27%, розроблений метод 87.08%);
- для техніки «Causal Oversimplification», точність виявлення зросла на 11.99% (існуючий метод 70.1%, розроблений метод 82.09%);

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

- для техніки «Doubt», точність виявлення зросла на 75.32% (існуючий метод 17.78%, розроблений метод 93.1%);
- для техніки «Exaggeration», точність виявлення зросла на 26.04% (існуючий метод 54.17%, розроблений метод 80.21%);
- для техніки «Flag-Waving», точність виявлення зросла на 27.65% (існуючий метод 64.52%, розроблений метод 92.17%);
- для техніки «Labeling», точність виявлення зросла на 48.57% (існуючий метод 47.43%, розроблений метод 96.0%);
- для техніки «Loaded Language», точність виявлення зросла на 42.9% (існуючий метод 54.17%, розроблений метод 97.07%);
- для техніки «Name Calling», точність виявлення зросла на 44.6% (існуючий метод 47.43%, розроблений метод 92.03%);
- для техніки «Repetition», точність виявлення зросла на 58.11% (існуючий метод 35.98%, розроблений метод 94.09%);
- для техніки «Appeal to Authority», точність виявлення зросла на 11.84% (існуючий метод 77.18%, розроблений метод 89.02%);
- для техніки «Black and White Fallacy», точність виявлення зросла на 36.68% (існуючий метод 54.55%, developed method 91.23%);
- для техніки «Reductio ad hitlerum», точність виявлення зросла на 62.31% (існуючий метод 25.0%, розроблений метод 87.31%);
- для техніки «Red Herring», точність виявлення зросла на 41.07% (існуючий метод 39.22%, розроблений метод 80.29%);
- для техніки «Slogans», точність виявлення зросла на 10.54% (існуючий метод 75.5%, розроблений метод 86.04%);
- для техніки «Thought terminating Cliches», точність виявлення зросла на 26.74% (існуючий метод 53.57%, розроблений метод 80.31%);
- для техніки «Whataboutism», точність виявлення зросла на 39.81% (існуючий метод 39.22%, розроблений метод 79.03%).

Приклад візуальної поясненості [33, 34] щодо виявлення прийому пропаганди «Repetition» наведено на рисунку 9 (використано оригінальний текст повсякденною українською мовою із збереженням орфографії та помилок). Як видно з рисунку 9, є багаторазові повторення фраз на кшталт «економічні мігранти», «мусульманський», «Орбан» того. З означення виду пропаганди «Repetition», це є «повторення того самого повідомлення знову і знову, щоб глядачі зрештою прийняли це». Отже, запропонований метод дозволяє ефективно виявляти прийоми пропаганди, та має перевагу у точності в порівнянні із запропонованими моделями що використовують підхід багатокласової класифікації.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

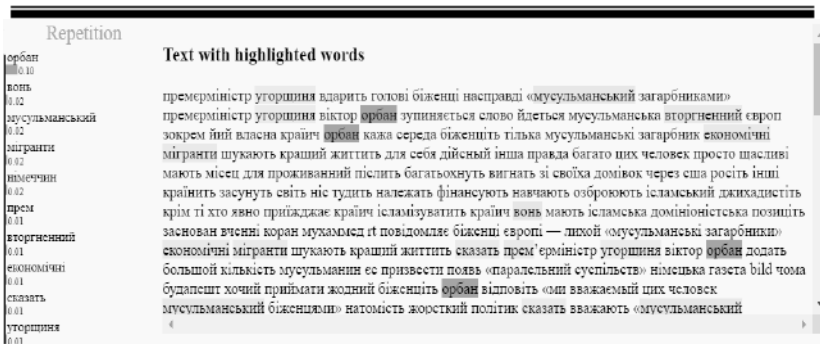


Рисунок 9. Візуальна аналітика щодо виявлення прийому пропаганди «Repetition» розробленим програмним забезпеченням

Експерименти, представлені в статті, проводилися з використанням різних можливостей бібліотеки SKLearn. У цій роботі представлені максимальні результати, яких вдалося досягти авторам емпіричним шляхом. Питання конфігурації та вибору гіперпараметрів є окремою проблемою, яка виходить за рамки питань, що розглядаються.

6. Висновки

Створено метод виявлення та класифікації технік пропаганди у текстовому контенті засобами штучного інтелекту, що дозволяє перетворювати вхідні дані у вигляді тексту для аналізу та навчених моделей машинного навчання у вихідні дані, які містять числові оцінки наявності кожного з прийомів пропаганди та розмічений текст з візуальною аналітикою присутності детектованих маркерів пропаганди. Було проведено дослідження, що дозволяє визначати 17 основних прийомів пропаганди, таких як: «Appeal to fear-prejudice», «Causal Oversimplification», «Doubt», «Exaggeration», «Flag-Waving», «Labeling», «Loaded Language», «Minimisation», «Name Calling», «Repetition», «Appeal to Authority», «Black and White Fallacy», «Reductio ad hitlerum», «Red Herring», «Slogans», «Thought terminating Cliches», «Whataboutism».

У рамках дослідження було порівняно 3 найчастіше застосовувані підходи: традиційний підхід машинного навчання, підхід на основі рекурентних нейронних мереж та підхід на основі трансформерних моделей. Традиційні підходи машинного навчання очікувано показали гірші результати, оскільки вони не здатні враховувати контекст, що є важливим для виявлення технік пропаганди. Досягнута точність для традиційного підходу становила від 0.60 до 0.67. Рекурентні нейромережі, хоча й перевершили традиційні підходи, все ж мають труднощі з обробкою довгих залежностей. Для цього підходу було досягнуто точності від 0.66 до 0.80. Найвищі результати були досягнуті підходом на основі трансформерних моделей, завдяки використанню механізмів самоуваги, які дозволяють кожному елементу послідовності безпосередньо взаємодіяти з усіма іншими елементами. Це забезпечує

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

ефективне захоплення довготривалих залежностей, що є характерним для технік пропаганди. Даний підхід дозволив виявляти техніки пропаганди з точністю до 0.96. Отримані результати забезпечили виявлення різних пропагандистських прийомів з мінімальною точністю 79,03% (мінімальні значення точності отримані для методики «Whataboutism»), що краще за відомі аналоги [8] щодо виявлення пропаганди незалежно від використовуваних методик. Порівняно з відомими аналогами [7] покращилась точність виявлення різноманітних прийомів пропаганди: за методикою «Appeal to Authority» точність виявлення зросла на 9,81%, за методикою «Причинне спрощення» — на 11,99%, за методикою «Causal Oversimplification» точність виявлення зросла на 75,32% для методики «Doubt», точність виявлення зросла на 26,04% для техніки «Exaggeration», точність виявлення зросла на 27,65% для техніки «Flag-Waving», точність виявлення зросла на 48,57% для «Labeling» методики, точність виявлення зросла на 42,9% для методики «Loaded Language», точність виявлення зросла на 44,6% для техніки «Name Calling», точність виявлення зросла на 58,11% для техніки «Repetition», точність виявлення зросла на 11,84% для техніки «Appeal to Authority», точність виявлення зросла на 36,68% для техніки «Black and White Fallacy», точність виявлення зросла на 62,31% для техніки «Reductio ad hitlerum», точність виявлення зросла на 41,07% для «Red Herring», точність виявлення зросла на 10,54% для техніки «Slogans», точність виявлення зросла на 26,74% для техніки «Thought terminating Cliches», точність виявлення зросла на 39,81% для техніки «Whataboutism».

Подальші дослідження будуть спрямовані на розширення датасету для навчання та пошуку додаткових міток у текстах, що характеризують прийоми пропаганди, таких як наявність булінгу, емоційна тональність тощо, що дозволить зробити більш поясненим рішення моделі машинного навчання та дозволить зробити більш точним виявлення прийомів.

7. Література

- [1] A. Horak, R. Sabol, O. Herman, V. Baisa, Recognition of propaganda techniques in newspaper texts: Fusion of content and style analysis, *Expert Systems with Applications*, Volume 251, 202. doi:10.1016/j.eswa.2024.124085.
- [2] A. Bhattacharjee, H. Liu, Fighting Fire with Fire: Can ChatGPT Detect AI-generated Text? *SIGKDD Explor. Newsl.*, 25, pp. 14–21, 2023. doi:10.1145/3655103.3655106.
- [3] G. Faye, B. Icard, M. Casanova, J. Chanson, F. Maine, F. Bancilhon, G. Gadek, G. Gravier, P. Egre, Exposing propaganda: an analysis of stylistic cues comparing human annotations and machine classification, in: *Proceedings of the Third Workshop on Understanding Implicit and Underspecified Language*, pp. 62–72, Malta, Association for Computational Linguistics.
- [4] P. Vijayaraghavan, S. Vosoughi, TWEETSPIN: Fine-grained Propaganda Detection in Social Media Using Multi-View Representations, in: *Proceedings of the 2022 Conference of the North American Chapter of the Association for*

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

Computational Linguistics, pp. 3433–3448, Seattle, United States, Association for Computational Linguistics.

[5] M. Abdullah, O. Altit, R. Obiedat, Detecting Propaganda Techniques in English News Articles using Pre-trained Transformers, in: 2022 13th International Conference on Information and Communication Systems (ICICS), Irbid, Jordan, 2022, pp. 301-308. doi: 10.1109/ICICS55353.2022.9811117.

[6] D.G. Jones, Detecting Propaganda in News Articles Using Large Language Models, Eng OA, 2(1), 2024, pp. 1-12. URL: <https://www.opastpublishers.com/peer-review/detecting-propaganda-in-news-articles-using-large-language-models-6952.html>.

[7] G. D. S. Martino, A. Barron-Cedeno, H. Wachsmuth, R. Petrov, P. Nakov, SemEval-2020 Task 11: Detection of Propaganda Techniques in News Articles, in: Proceedings of the Fourteenth Workshop on Semantic Evaluation, pp. 1377–1414, Barcelona (online), International Committee for Computational Linguistics.

[8] G. Martino, S. Yu, A. Barron-Cedeno, R. Petrov, P. Nakov, Fine-Grained Analysis of Propaganda in News Article, in: Proceedings of the 2019 Conference on Empirical Methods in Natural Language Processing and the 9th International Joint Conference on Natural Language Processing (EMNLP-IJCNLP), pp. 5640-5650, 2019. doi:10.18653/v1/D19-1565.

[9] Analytics Vidhya, Guide on Support Vector Machine (SVM) Algorithm, 2024. URL: <https://www.analyticsvidhya.com/blog/2021/10/support-vector-machinessvm-a-complete-guide-for-beginners/>.

[10] S. Mann, D. Yadav, D. Rathee, Identification of Racial Propaganda in Tweets Using Sentimental Analysis Models: A Comparative Study, in: Swaroop, A., Kansal, V., Fortino, G., Hassanien, A.E. (eds) Proceedings of Fourth Doctoral Symposium on Computational Intelligence. DoSCI 2023. Lecture Notes in Networks and Systems, vol 726, Springer, Singapore. doi: 0.1007/978-981-99-3716-5_28.

[11] L. Syed, A. Alsaeedi, L. A. Alhuri, H. R. Aljohani, Hybrid weakly supervised learning with deep learning technique for detection of fake news from cyber propaganda, Array, Volume 19, 2023. doi:10.1016/j.array.2023.100309.

[12] Krak I., Zalutka O., Molchanova M., Mazurets O., Bahrii R., Sobko O., Barmak O. Abusive Speech Detection Method for Ukrainian Language Used Recurrent Neural Network. CEUR Workshop Proceedings, 2023, vol. 3387, pp. 16-28. URL: <https://ceur-ws.org/Vol-3688/paper2.pdf>.

[13] Geeks for geeks, What is LSTM – Long Short Term Memory, 2024. URL: <https://www.geeksforgeeks.org/deep-learning-introduction-to-long-short-term-memory/>.

[14] A.M.U.D. Khanday, Q.R. Khan, S.T. Rabani, M.A. Wani, M. ELAffendi, Propaganda Identification on Twitter Platform During COVID-19 Pandemic Using LSTM, in: Abd El-Latif, A.A., Maleh, Y., Mazurczyk, W., ELAffendi, M., I. Alkanhal, M. (eds) Advances in Cybersecurity, Cybercrimes, and Smart Emerging

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

Technologies, CCSET 2022, Engineering Cyber-Physical Systems and Critical Infrastructures, vol 4. Springer, Cham. doi:10.1007/978-3-031-21101-0_24.

[15] Dev, Large Language Models: Comparing Gen 1 Models (GPT, BERT, T5 and More), 2024. URL: <https://dev.to/admantium/large-language-models-comparing-gen-1-models-gpt-bert-t5-and-more-74h>.

[16] Hugging Face, BERT, 2024. URL: https://huggingface.co/docs/transformers/model_doc/bert.

[17] Zalutska O., Molchanova M., Sobko O., Mazurets O., Pasichnyk O., Barmak O., Krak I. Method for Sentiment Analysis of Ukrainian-Language Reviews in E-Commerce Using RoBERTa Neural Network. CEUR Workshop Proceedings, 2023, vol. 3387, pp. 344-356. URL: <https://ceur-ws.org/Vol-3387/paper26.pdf>

[18] Hugging Face, DistilBERT, 2024. URL: <https://huggingface.co/distilbert/distilbert-base-uncased>.

[19] D. Chaudhari, A. V. Pawar, Empowering Propaganda Detection in Resource-Restrained Languages: A Transformer-Based Framework for Classifying Hindi News Articles, Big Data and Cognitive Computing, 2023, 7(4):175. doi:10.3390/bdcc7040175.

[20] A. Malak, D. Abujaber, A. Al-Qarqaz, R. Abbott, M. Hadzikadic, Combating propaganda texts using transfer learning, IAES International Journal of Artificial Intelligence (IJ-AI). Volume 12, pp. 956-965, 2023. doi: 10.11591/ijai.v12.i2.pp956-965

[21] A. Malak, D. Abujaber, A. Al-Qarqaz, R. Abbott, M. Hadzikadic, Combating propaganda texts using transfer learning, IAES International Journal of Artificial Intelligence (IJ-AI). Volume 12, pp. 956-965, 2023. doi: 10.11591/ijai.v12.i2.pp956-965.

[22] I. Krak, O. Barmak, O. Mazurets, The practice investigation of the information technology efficiency for automated definition of terms in the semantic content of educational materials. CEUR Workshop Proceedings, 2016, vol.1631, pp. 237–245. doi:10.15407/pp2016.02-03.237.

[23] C3.ai, What is Local Interpretable Model-Agnostic Explanations (LIME)?, 2024. URL: <https://c3.ai/glossary/data-science/lime-local-interpretable-model-agnostic-explanations/>.

[24] Scikit-learn, Machine Learning in Python, 2024. URL: <https://scikit-learn.org/stable/>.

[25] Tensorflow, An end-to-end platform for machine learning. Machine Learning in Python, 2024. URL: <https://www.tensorflow.org>.

[26] GitHub, Lime, 2024. URL: <https://github.com/marcotcr/lime>.

[27] Numpy, The fundamental package for scientific computing with Python, 2024. URL: <https://numpy.org>.

[28] Pandas, Pandas, 2024. URL: <https://pandas.pydata.org>.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

- [29] Kaggle, Disinformation Detection Challenge, 2024. URL: https://www.kaggle.com/competitions/disinformation-detection-challenge/data?select=emnlp_trans_uk_dataset.
- [30] Propaganda, Propaganda Analysis Project, 2024. URL: <https://propaganda.qcri.org/index.html>.
- [31] Y. Elor, H. Averbuch-Elor, To SMOTE, or not to SMOTE. URL: <https://arxiv.org/abs/2201.08528>.
- [32] Hugging Face, The AI community building the future, 2024. URL: <https://huggingface.co/>.
- [33] V. Slobodzian, M. Molchanova, O. Kovalchuk, O. Sobko, O. Mazurets, O. Barmak, I. Krak. An Approach Based on the Visualization Model for the Ukrainian Web Content Classification. 2022 12th International Conference on Advanced Computer Information Technologies, ACIT 2022. 2022. pp. 400-405. doi: 10.1109/ACIT54803.2022.9913162
- [34] O. Kovalchuk, V. Slobodzian, O. Sobko, M. Molchanova, O. Mazurets, O. Barmak, I. Krak, N. Savina. Visual Analytics-Based Method for Sentiment Analysis of COVID-19 Ukrainian Tweets. Book Chapter. Lecture Notes on Data Engineering and Communications Technologies. 2023. Vol. 149. pp. 591–607. doi: 10.1007/978-3-031-16203-9_33

METHOD FOR DETECTING AND CLASSIFYING PROPAGANDA TECHNIQUES IN TEXTUAL CONTENT USING ARTIFICIAL INTELLIGENCE

M. Molchanova ORCID: 0000-0001-9810-936X

Khmelnytskyi National University, Ukraine

E-mail: m.o.molchanova@gmail.com

Abstract. *The paper is devoted to the creation and approbation of the method for neural network detecting propaganda techniques by markers with visual analytic, which allows converting input data in the form of text for analysis and supervised machine learning models into output data containing numerical estimates of the presence of each propaganda technique and marked-up text with visual analytical presence of detected propaganda markers. Research was conducted that allows us to detect 17 main propaganda techniques. The study compared the 3 most commonly used approaches: a traditional machine learning approach, an approach based on recurrent neural networks, and an approach based on transformer models. The highest results were achieved by the transformer model approach, which uses self-attention mechanisms that allow each element of the sequence to interact directly with all other elements. This ensures efficient capture of long-term dependencies, which is typical for propaganda techniques. This approach allowed us to detect propaganda techniques with an accuracy of 0.96.*

Keywords: *BERT, RNN, propaganda techniques, detecting propaganda, propaganda markers, visual analytics*

**МЕТОД ІНТЕЛЕКТУАЛЬНОГО ВИЯВЛЕННЯ
КІБЕРЗАЛЯКУВАНЬ У ТЕКСТОВОМУ КОНТЕНТІ**

О. Собко ORCID: 0000-0001-5371-5788

*Хмельницький національний університет, Україна
E-mail: olena.sobko.ua@gmail.com*

***Анотація.** Дослідження присвячене створенню та апробації методу інтелектуального виявлення кіберзалякувань в текстовому контенті. Метод здатний оцінювати за введеною текстовою інформацією рівень кіберзалякувань з використанням рекурентної нейронної мережі. Виявлення кіберзалякувань передбачає використання комбінованого підходу, що поєднує використання словника слів мови ворожнечі та нейромережевий підхід для визначення наявності кіберзалякувань. Запропонований метод дозволяє встановити наявність кіберзалякувань у тексті та визначити числову оцінку рівня прояву кіберзалякувань для подальшого моніторингу комунікаційного процесу, попередження шкідливого впливу та вжиття необхідних заходів з боку модераторів чи автоматизованої модерації контенту відповідними системами управління контентом.*

Було використано тришарову архітектуру з Embedding Layer, LSTM Layer та Dense Layer із сигмоїдною функцією активації. Навчена за розробленим методом модель RNN була в подальшому протестована й виявила показники ефективності: точність 0.96, Recall 0.959 та F1 0.957. Як метод, так і модель враховують контекст, тон висловлювань та наявність мови ворожнечі. Це свідчить про те, що результати аналізу відповідають сучасним підходам до виявлення кіберзалякування, підвищуючи їх достовірність.

Метод інтелектуального виявлення кіберзалякувань у текстовому контенті було протестовано на створеному програмному забезпеченні, й встановлено, що метод має високу ефективність виявлення кіберзалякувань у текстовому контенті. Згідно проведених прикладних досліджень, метод має оцінку точності ідентифікації кіберзалякувань понад 90%, однак оцінка наявності кіберзалякувань може бути суб'єктивною і сприйняття контенту може різнитися від особи до особи. Для покращення результату можна доповнювати словник виразів мови ворожнечі. Також метод має обмеження, працюючи з текстами довжиною від 3 до 500 слів.

***Ключові слова:** кіберзалякування, інтелектуальний аналіз текстів, мова ворожнечі, нейронної мережі, класифікація кіберзалякувань.*

1. Вступ та постановка проблеми

Кіберзалякування, або інтернет-агресія, являє собою новітню форму насильства, що здійснюється у віртуальному просторі. Зловмисник використовує різні онлайн-комунікаційні канали, такі як соціальні мережі,

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

електронна пошта або месенджери, з метою психологічного тиску, нанесення шкоди або приниження особистості [1]. Це тривала і повторювана маніпулятивна дія, спрямована на окремих осіб або групи з метою створення почуття страху, гніву або приниження. Основним завданням кіберзалякування є завдання психічної або емоційної шкоди його жертвам [2].

Серед типових прикладів кіберзалякування можна навести наступні ситуації:

- поширення неправдивої інформації або публікація компрометуючих матеріалів щодо особи в соціальних мережах;
- надсилання образливих повідомлень чи погроз, спрямованих на приниження або завдання шкоди через сервіси обміну повідомленнями;
- видавання себе за іншу особу з метою введення в оману та надсилання повідомлень третім сторонам від її імені.

Значущою відмінністю кіберзалякування є наявність цифрових слідів, таких як повідомлення та публікації, які можуть слугувати доказами та сприяти припиненню агресії. Незважаючи на те, що кіберзалякування і традиційні форми залякувань можуть перетинатися, перший залишає конкретні електронні свідчення.

Законодавче регулювання кіберзалякувань є порівняно новим явищем і ще не прийняте в усіх країнах. У зв'язку з цим багато держав використовують для боротьби з кіберзалякуваннями інші правові норми, зокрема, закони про захист від домагань. На рисунку 1 подана інформація про кількість судових справ, пов'язаних з різними формами цькування. Загалом було розглянуто 335 справ. Основна частина справ (271 або 80,9%) стосується традиційних залякувань. Інша частина (61 справа або 18,2%) пов'язана із застосуванням засобів електронних комунікацій. Лише 3 справи (0,9%) належать до категорії неназваних зловмисних дій або некласифікованих випадків залякувань [3].

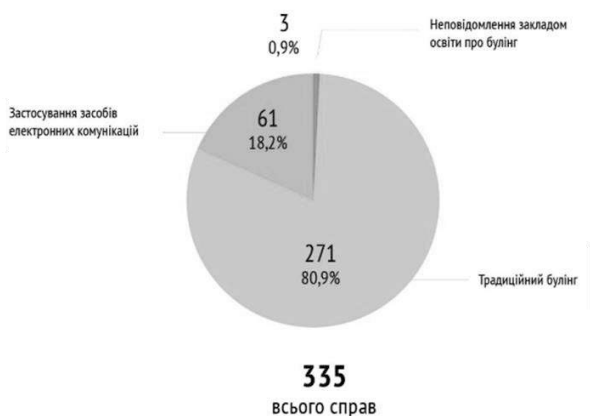


Рисунок 1. Статистика судових справ щодо цькування

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

На рисунку 2, більш детально подано типи зловживань, що включають використання цифрових технологій [3]. Найбільша кількість справ стосується публікації та поширення фото чи відеоматеріалів (16 справ). На другому місці розташовані справи, пов'язані з погрозами чи переслідуванням через електронну пошту чи месенджери (12 справ). Інші види зловживань включають створення фейкових сторінок (6 справ), злом акаунтів або блокування доступу (4 справи), поширення чуток (3 справи), шантаж (3 справи), а також погрози з боку невідомих осіб у соціальних мережах чи месенджерах (1 справа).

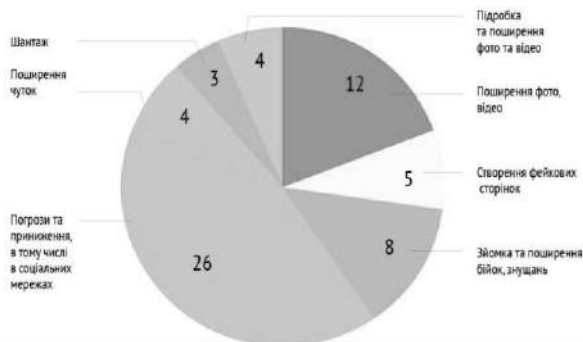


Рисунок 2. Кількість судових справ за проявами залякувань з використанням засобів електронних комунікацій

Останні дослідження [4] показують, що кіберзалякування часто включають мову ворожнечі (hate speech), яка є важливим компонентом цього явища. У кіберзалякуванні агресивні та образливі висловлювання часто спрямовані на дискримінацію за ознаками раси, статі, релігії, сексуальної орієнтації тощо. Наприклад, дослідження за допомогою технології BERT та інших методів машинного навчання показують, що розпізнавання мови ворожнечі є ключовим завданням у виявленні кіберзалякувань у текстовому контенті, особливо на платформах соціальних мереж, таких як Twitter. Актуальність розробки методу інтелектуального виявлення кіберзалякувань у текстовому контенті зумовлена поширенням агресивної поведінки в онлайн-середовищі та її впливом на психологічний стан жертв [5]. Як свідчить статистика судових справ, значна частка інцидентів цькування вже переміщується у цифровий простір, де нападники використовують електронні засоби комунікації для переслідувань, погроз і приниження. Ці дані вказують на те, що майже п'ята частина випадків булінгу відбувається саме через використання таких технологій, як соціальні мережі, месенджери або електронна пошта. Незважаючи на те, що кількість справ про традиційний булінг залишається високою, випадки кіберзалякування, зокрема розповсюдження зловмисного контенту, створення фейкових акаунтів, шантаж та поширення неправдивої інформації, становлять серйозну проблему. Оскільки ця форма агресії залишає цифровий слід, розробка інтелектуальних

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

систем, здатних автоматично ідентифікувати кіберзалякування в текстовому контенті, є важливою для швидкого реагування і запобігання подальшій ескалації конфлікту. Такий метод дозволить ефективніше виявляти прояви агресії, мінімізувати емоційні наслідки для жертв і слугуватиме інструментом для забезпечення безпеки в онлайн-просторі.

2. Аналіз останніх досліджень та публікацій

Задача виявлення кіберзалякування у текстовому контенті залишається вкрай актуальною через зростаючу кількість шкідливих взаємодій на платформах соціальних мереж, особливо серед молоді. У дослідженнях останніх років науковці зробили значний прогрес у цій галузі, використовуючи алгоритми машинного навчання та обробки природної мови (NLP).

У статті [6] розглядається проблема кіберзалякувань, яка набула актуальності через зростання залежності суспільства від онлайн-платформ внаслідок пандемії. Автори акцентують увагу на тому, що існуючі алгоритми виявлення кіберзалякувань часто класифікують дружні жарти як образливі, оскільки використовують лише бінарну класифікацію на основі ключових слів, що містять образи. Відсутність аналізу контексту та недоступність відкритих навчальних даних ускладнює точне навчання моделей. Саме тому дослідження зосереджується на врахуванні контексту як важливого параметра для класифікації онлайн-повідомлень. Використаний набір даних був анотований на основі п'яти параметрів, що враховують контекст онлайн-розмов. У роботі застосовуються різні алгоритми машинного навчання, такі як SVM (метод опорних векторів), випадковий ліс (random forest), AdaBoost і багатопартийний перцептрон (MLP), до вибірки даних про кіберзалякування, отриманих із Twitter. Найкращі результати показав алгоритм SVM, на якому було виконано рандомізований перезапис, що привело до значного підвищення середнього значення F1-міри, перевищивши базовий показник. Відомий підхід [7] до виявлення кіберзалякувань в соціальних мережах за допомогою ансамблевого навчання на основі стекування. Основна увага приділяється використанню глибоких нейронних мереж (DNNs) та модифікованої моделі BERT (BERT-M) для аналізу даних із Twitter. Зібраний набір даних було попередньо оброблено для видалення нерелевантної інформації. Основним засобом класифікації у представленому підході став стековий ансамбль моделей, який продемонстрував високі показники ефективності. Для валідації моделей були використані загальноприйнятні метрики оцінки, і запропонований стековий підхід досягнув F1-міри 0.964, точності 0.950, і повноти 0.92.

У статті [8] розглянуто методи виявлення кіберзалякувань. Використано шість наборів даних із Facebook, Twitter та Instagram, а також спеціально розроблений арабський лексикон кіберзалякувань. Перед класифікацією було здійснено попередню обробку тексту, зокрема очищення даних, і застосовано методи вбудовування слів для обробки природної мови. У дослідженні оцінювали різноманітні алгоритми машинного та глибинного навчання: найкращий базис, метод опорних векторів, нейронні мережі та інші. Проведено

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

детальний порівняльний аналіз, який показав, що гібридні моделі мають перевагу над окремими алгоритмами. Представлено гібридну глибинну модель зі стекуванням вбудовування слів, яка продемонструвала покращену здатність до вилучення ознак та точну класифікацію текстів, зокрема в різних мовних контекстах.

Незважаючи на значний прогрес у дослідженнях в області виявлення кіберзалякувань, ця тема залишається актуальною через постійно зростаючу кількість цифрового контенту та змінюваний характер онлайн-комунікацій. Нові форми комунікації, соціальні мережі та анонімність користувачів створюють сприятливі умови для кіберзалякувань, що ускладнює їх автоматичне виявлення.

3. Постановка задачі

Метою роботи є розробка методу інтелектуального виявлення кіберзалякувань у текстовому контенті, що поєднує використання словника слів, що притаманні мові ворожнечі, та нейромережевого підходу для визначення наявності кіберзалякування у текстовому контенті.

4. Метод інтелектуального виявлення кіберзалякувань у текстовому контенті

Для виявлення кіберзалякувань у текстовому контенті, а також з метою забезпечення надійності результату при визначенні рівня кіберзалякувань буде використано нейронну мережу для визначення кіберзалякувань та підхід словника для перевірки наявності елементів мови ненависті.

Вхідними даними методу є: попередньо навчена модель виявлення кіберзалякування RNN, текстовий контент для аналізу, словник ключових виразів мови ненависті, яка притаманна кіберзалякуванням. Текстовий контент соціальних мереж для аналізу характеризуються деякими особливостями [9], основні з них:

- невелика довжина (часто мають обмеження на кількість символів, що спричиняє стислості тексту та вимагає ясного та лаконічного висловлення думок);
- інформальність (зазвичай, інформація подана у неформальному характері, і може містити скорочення, нестандартну лексику);
- використання мультимедіа (тексти можуть включати гіфки, емодзі тощо);
- діалогічний характер (соціальні мережі мають розгалужену структуру, що сприяє взаємодії між користувачами та створенню діалогів).

Це все робить обробку короткого контенту специфічною, відмінною від загальних методів для роботи з текстами. Узагальнена схема пропонованого методу проілюстрована на рисунку 3.

Кроком 1 є нейромережева оцінка оцінка кіберзалякувань в тексті, що відбувається на основі попередньо натренованої моделі RNN. Результатом виконання кроку є числова оцінка кіберзалякувань в текстовому контенті в

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

проміжку від 0 до 1, де 0 – текст не містить кіберзалякування, 1 – містить кіберзалякування.



Рисунок 3. Кроки методу інтелектуального виявлення кіберзалякувань у текстовому контенті

Крок 2 відбувається паралельно з першим, і полягає в оцінці частоти (TF) появи мови ворожнечі, яка буде визначатись при порівнянні вмісту текстового повідомлення із словником «Hatebase». Оцінка частоти появи мови ворожнечі буде розраховуватись за формулою:

$$TF = \frac{O_w}{TotalCount} \quad (1)$$

де O_w – кількість слів мови ворожнечі, що містяться у словнику, $TotalCount$ – загальна кількість слів у досліджуваному текстовому контенті. Результатом виконання кроку є числова оцінка концентрації складових мови ворожнечі.

На кроці 3 здійснюється обрахунок оцінки кіберзалякування текстового контенту за виявленим кіберзалякуванням неймережею та концентрацією виразів мови ворожнечі. Числова оцінка кіберзалякування текстового контенту буде розраховуватись за формулою:

$$CyberbullyingLevel = \frac{k \cdot TF + (1 - k)(1 - CybBullVal)}{2} \quad (2)$$

де TF – числова оцінка концентрації виразів мови ворожнечі, $CybBullVal$ – неймережева оцінка кіберзалякування контенту, k – коефіцієнт порогу

чутливості слів мови ворожнечі на загальний рівень виявлення мови ворожнечі. Підбирається згідно до політики досліджуваного соціального сервісу.

Відповідно, вихідними даними методу інтелектуального виявлення кіберзалякувань у текстовому контенті за допомогою рекурентної нейронної мережі є числова оцінка кіберзалякування текстового контенту.

5. Підготовка навчальних вибірок даних

У якості експериментальних даних для реалізації методу виявлення кіберзалякувань за допомогою рекурентної нейронної мережі буде використано «Cyberbullying Data for Multi-Label Classification», «Cyberbullying Tweets», «Cyberbullying Dataset» «A Comprehensive Dataset for Automated Cyberbullying Detection», (для навчання RNN), а також «Hatebase» (для ідентифікації мови ненависті).

Датасет «Cyberbullying Data for Multi-Label Classification» [10], доступний на Kaggle, призначений для багатоміткової класифікації текстів з соціальних мереж. Він включає 47 тисяч твітів, що належать до 6 різних категорій кіберзалякувань: стать, вік, етнічність, релігія, ознаки інвалідності та зовнішній вигляд. Цей датасет допомагає ідентифікувати різні форми кіберзалякувань на основі текстів і класифікувати їх за кількома параметрами одночасно. Дані попередньо оброблені, включаючи очистку текстів від зайвої інформації, що робить цей набір готовим для використання в моделях машинного навчання та глибинного навчання.

Датасет «Cyberbullying Tweets», доступний на Kaggle [11], містить твіттерпости, які використовуються для дослідження та моделювання виявлення кіберзалякувань. Цей набір даних включає твіти, мічені за категоріями, пов'язаними з кіберзалякуваннями, що дозволяє проводити багатокласову класифікацію. Він призначений для тренування моделей машинного та глибинного навчання з метою ідентифікації образливих повідомлень або ворожих висловлювань.

Датасет «Cyberbullying Dataset», доступний на Kaggle [12], містить твіти, які використовуються для тренування моделей виявлення кіберзалякування. Цей датасет був створений для аналізу образливого контенту в соціальних мережах, дозволяючи проводити класифікацію текстів на основі того, чи містять вони ознаки кіберзалякувань.

Для автоматичного виявлення кіберзалякувань дослідники створюють набори даних, що включають слова та фрази, які часто використовуються для агресії в інтернеті. Наприклад, датасет від дослідників [13] містить не лише агресивні тексти, але й включає чотири аспекти кіберзалякувань, такі як повторюваність, намір заподіяння шкоди та агресивність.

«Hatebase» [14] – це платформа, яка спеціалізується на зборі та систематизації термінів, пов'язаних з мовою ненависті. Вона була створена для боротьби з дискримінацією, ненавистю та насильством, що виражаються через мову, в контексті як онлайн, так і офлайн. Платформа містить великий обсяг даних, включаючи терміни, фрази та сленг, що можуть використовуватися для

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

дискримінаційних висловлювань проти різних груп людей, включаючи расові, етнічні, релігійні та інші меншини. Платформа підтримує багатомовність, що дозволяє користувачам аналізувати ненависть у різних культурних контекстах. «Hatebase» надає можливість систематизувати дані за різними категоріями ненависті, такими як расова чи сексуальна, що полегшує дослідження. Інструменти аналітики на платформі допомагають розуміти, де і як використовуються ненавистницькі висловлювання, що може бути корисним для розробки стратегій протидії цим явищам. Дані платформи «Hatebase» буде використаний у якості даних для числової оцінки рівня кіберзалякувань у текстовому контенті.

Складові дані для запропонованого методу наведено на рисунку 4.

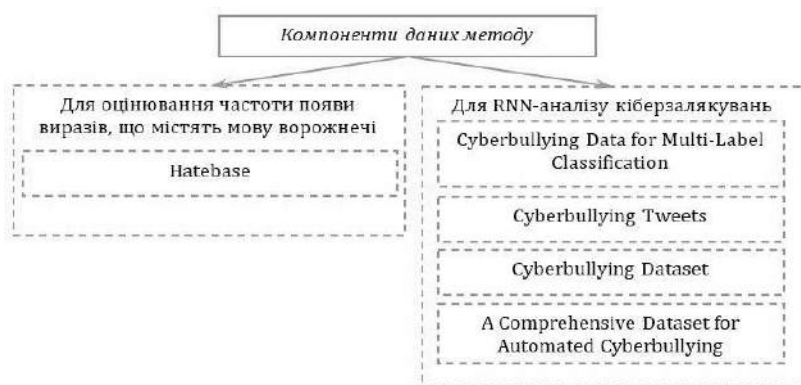


Рисунок 4. Складові набору даних методу інтелектуального виявлення кіберзалякувань у текстовому контенті

Вищеописаний набір даних буде використано з метою реалізації методу інтелектуального виявлення кіберзалякувань у текстовому контенті, що буде спроможний визначати за уведеною текстовою інформацією рівень наявності кіберзалякувань.

6. Формування навченої моделі RNN для виявлення кіберзалякувань у текстовому контенті

Оскільки одними з вхідних даних методу виявлення кіберзалякувань у текстовому контенті є навчена модель, виникає потреба її отримання. Схема виявлення кіберзалякування у текстовому контенті нейромережевою моделлю показана на рисунку 5.

Схема ілюструє процес виявлення кіберзалякування в текстових даних за допомогою RNN. Процес починається з визначення вхідних даних, які

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

складаються з векторизатора, навченої моделі, що спеціалізується на виявленні кіберзалякування, та текстового зразка, що підлягає аналізу.

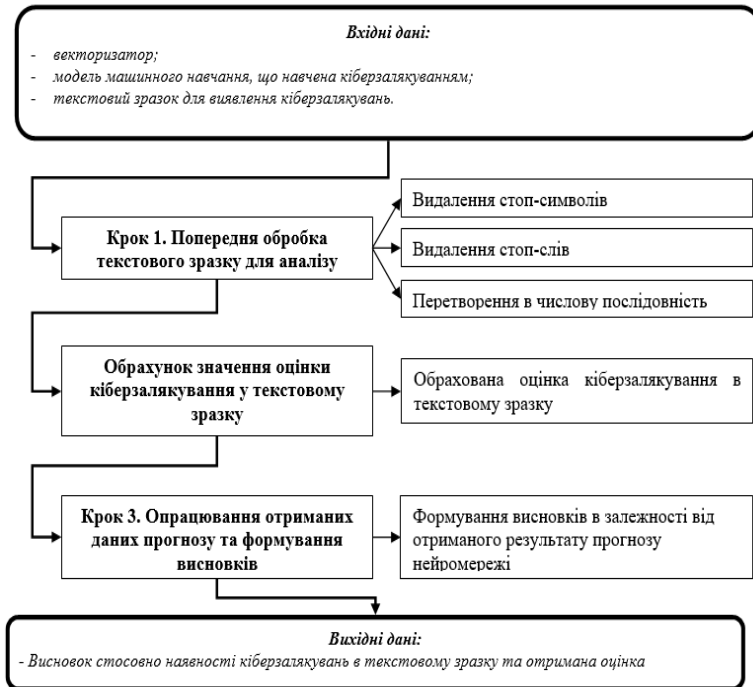


Рисунок 5. *Схема виявлення кіберзалякування у текстовому контенті нейромережевою моделлю*

Першим кроком цього процесу є попередня обробка текстового зразка для аналізу. Крок є важливим, оскільки забезпечує чистоту та правильне форматування вхідних даних, що робить їх придатними для подальшого аналізу. У процесі попередньої обробки видаляються стоп-символи, які є непотрібними символами, що не додають значення тексту, а також видаляються стоп-слова, які є часто вживаними словами, що можуть не нести суттєвої інформації, наприклад, «і», «те» чи «е». Після цього текст перетворюється на числове представлення, що необхідно для роботи алгоритмів машинного навчання. Такого роду перетворення дозволяє представити текстовий зміст у форматі, який кількісно описує інформацію та робить її підлягаючою статистичному аналізу. На наступному кроці модель оцінює значення індикаторів кіберзалякування в текстовому зразку. Це передбачає порівняння обробленого тексту з попередньо визначеними метриками, які характеризують випадки кіберзалякування. Вихідні даними моделі є оцінка кіберзалякування в тексті, який відображає ймовірність або присутність шкідливого контенту.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

Останній крок зосереджується на обробці отриманих даних прогнозу та формуванні висновків. На основі результатів аналізу модель генерує висновки, які відображають ймовірність присутності кіберзаялювання в текстовому зразку. Цей прогноз служить основою для подальшої інтерпретації та прийняття рішень стосовно аналізованого контенту.

В результаті всього цього процесу формується визначення наявності кіберзаялювання в аналізованому тексті, а також оптимальна оцінка, що вказує на ступінь або інтенсивність виявленого кіберзаялювання.

Тренування нейромережевої моделі відбувається за алгоритмом, зображеним на рисунку 6.



Рисунок 6. Етапи формування навченої моделі аналізу тональності RNN для виявлення образливого мовлення

Відповідно, вхідними даними для підбору моделі є розмічений датасет, що використовується для навчання нейромережі та оцінки його ефективності. Рівень присутності кіберзаялювань у текстовому контенті буде визначатись з числового проміжку від 0 до 1, де 0 – відсутність кіберзаялювань, 1 – присутність кіберзаялювань.

Першим етапом є поділ датасету на навчальну та тестову вибірки. Було прийнято рішення поділити датасет у пропорції 60 на 40, де 60 % це навчальна вибірка, а 40 % – тестова. Наступним етапом був підбір архітектури нейромережі. Було прийнято рішення використовувати тришарову архітектуру з Embedding Layer, LSTM Layer та Dense Layer із сигмоїдною функцією активації. Наступним етапом було навчання нейромережі з вищеописаною архітектурою. Етап навчання проводився спільно з етапом подальшого оцінювання моделі на основі таких метрик, як: accuracy, recall, f1 та матриці сплутування [15]. Accuracy визначається як відношення кількості правильно

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

класифікованих прикладів до загальної кількості прикладів [16]. Recall визначається як відношення кількості правильно класифікованих позитивних прикладів до загальної кількості позитивних прикладів. F1-score обчислюється як гармонічне середнє між точністю і повнотою [17].

На рисунках 7-10 наведено ілюстрацію сплутувань зразків неймережевими моделями. Зелений колір – істинно позитивні, червоний – істинно негативні, жовтий – хибно позитивні і синій – хибно негативні.

Таблиця 1

Параметри навчання RNN та результати

Параметри навчання	Моделі						
	V1	V2	V3	V4	V5	V6	V7
Кількість епох навчання	20	20	20	20	10	10	10
Batch size	128	64	32	16	64	32	16
Результати							
Час навчання (sec)	257	343	503	921	183	255	442
Accuracy	0.951	0.951	0.957	0.949	0.96	0.956	0.947
Recall	0.963	0.968	0.948	0.936	0.959	0.943	0.978
F ₁	0.959	0.961	0.956	0.95	0.957	0.956	0.960
True positive	0.96	0.97	0.95	0.94	0.96	0.94	0.98
True negative	0.96	0.96	0.97	0.97	0.97	0.98	0.95
False positive	0.036	0.037	0.028	0.026	0.035	0.02	0.047
False negative	0.037	0.032	0.05	0.06	0.04	0.06	0.022

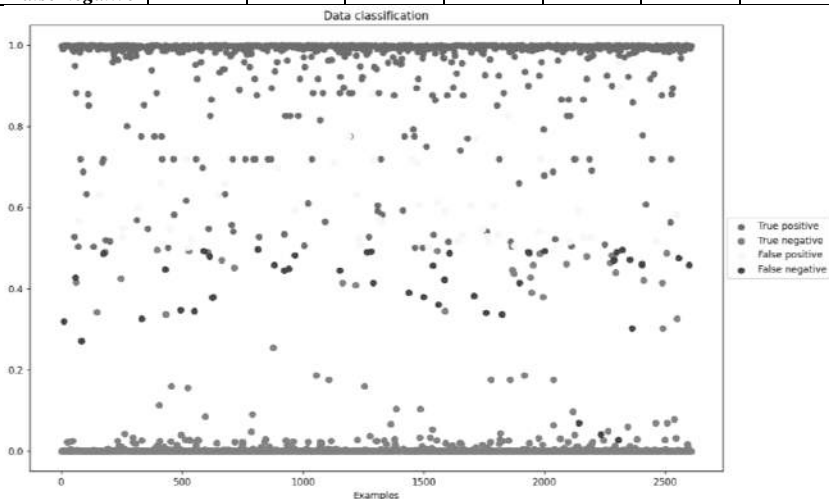


Рисунок 7. Класифікація текстового контенту моделлю V1

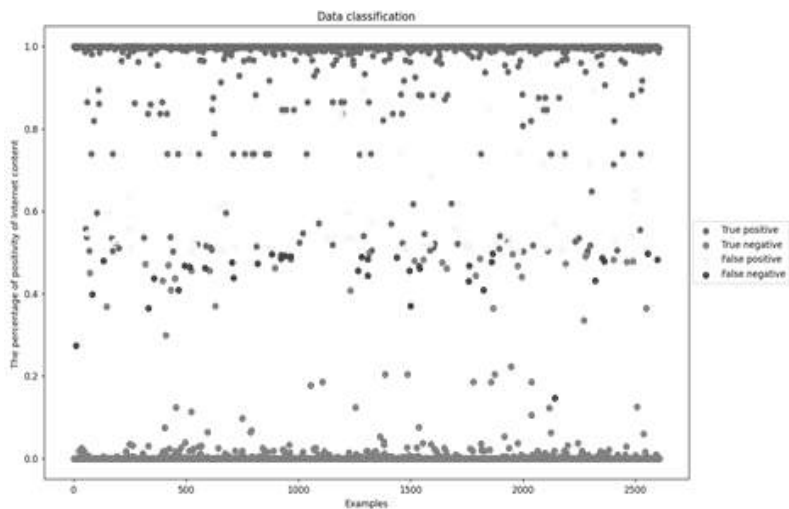


Рисунок 8. Класифікація текстового контенту моделлю V2

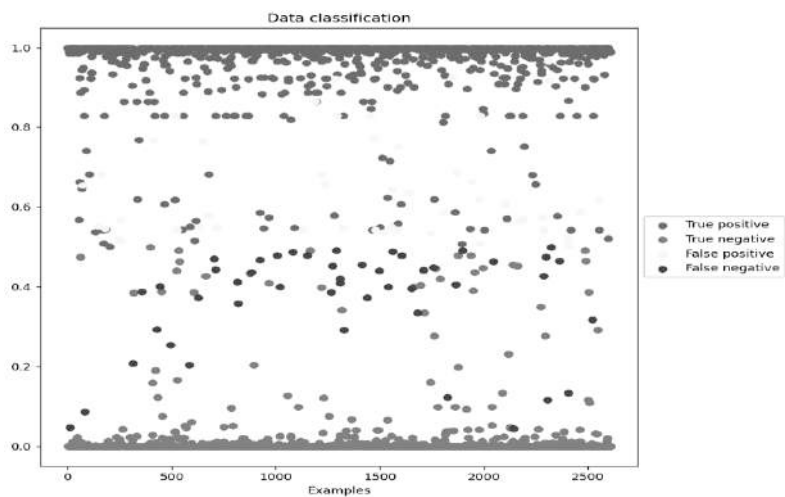


Рисунок 9. Класифікація текстового контенту моделлю V5

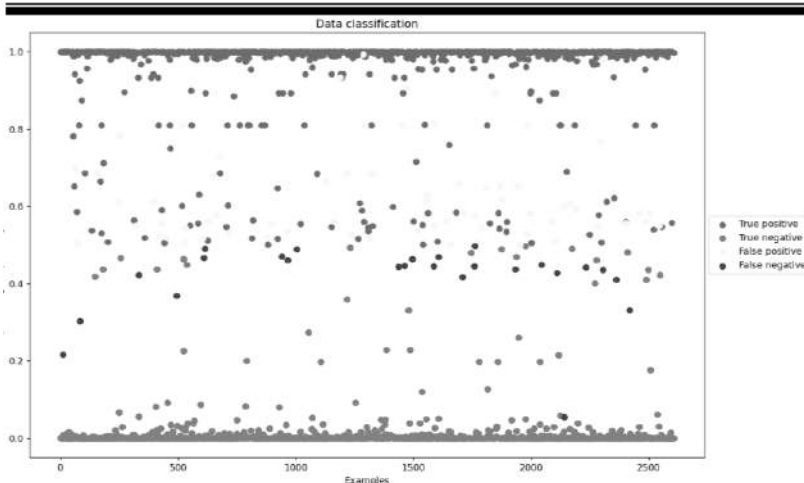


Рисунок 10. Класифікація відгуків моделлю V7

Для процесу навчання досліджувались такі вхідні параметри: Batch size, кількість епох. Кількість епох навчання показує, скільки разів модель підлягає навчанню. Batch size показує кількість навчальних прикладів, що використовуються в межах однієї ітерації навчання нейромережі. Дуже важко відразу визначити, який ідеальний розмір партії для потреб конкретної задачі [18], тому даний параметр буде підібрано експериментальним шляхом. Статистика метрик за проведеним навчанням наведена у таблиці 1.

Як видно з рисунків 7-10, в цілому, всі моделі справляються із поставленою задачею, але зважаючи на мету дослідження, було прийнято рішення у подальшому використовувати модель V5, яка має найвищий показник Ассигасу. Хоча і модель V7 має досить високі показники Recall та F1, проте виходячи з мети, більш важливим є більш точна ідентифікація саме позитивних зразків.

7. Дослідження ефективності запропонованого методу

Для дослідження ефективності методу виявлення кіберзалякувань за допомогою рекурентної нейронної мережі було створено відповідну програмну реалізацію. Для розробки було використано засоби мови Python, для інтерфейсу користувача було використано бібліотеку «wx» [19]. Для навчання та подальшого використання нейронної мережі використовувалась бібліотека «Sklearn» [20]. Приклад ідентифікації контенту проілюстровано на рисунку 11. Для того, щоб проаналізувати текстовий контент на наявність кіберзалякувань необхідно у верхній частині вікна розташоване текстове поле з підписом «Текст для аналізу» ввести або вставити вміст, який потрібно оцінити на наявність ознак кіберзалякування.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

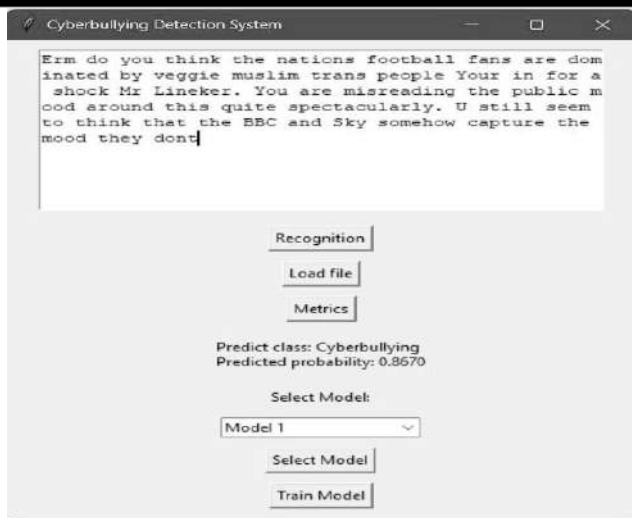


Рисунок 11. Приклад ідентифікації контенту як «контент з кіберзалякуванням»

Після введення тексту треба натиснути кнопку «Розпізнавання», що активує алгоритм виявлення для обробки введеного тексту. Програма оцінить текст і надасть прогноз щодо наявності кіберзалякування, а також ймовірність, що вказує на ступінь присутності кіберзалякування у вхідному текстовому контенті. Якщо потрібно навчити модель на основі нових даних, слід натиснути кнопку «Навчити модель», що відкриє нове вікно, яке надасть можливість налаштувати параметри нейромережі. Функція вибору моделі дає змогу обрати конкретну модель для аналізу, що може бути корисним у різних сценаріях використання програми. Після виконання всіх необхідних дій результати з'являться в нижній частині інтерфейсу, де відобразяться клас прогнозу та відповідна ймовірність.

У проілюстрованих прикладах для тестування текстового контенту були взяті два текстових зразки, які слугують прикладами для виявлення кіберзалякувань. Перший зразок: «Original: *Erm do you think the nations football fans are dominated by veggie muslim trans people Your in for a shock Mr Lineker. You are misreading the public mood around this quite spectacularly. U still seem to think that the BBC and Sky somehow capture the mood they dont* / Переклад українською: *Емм, як ви думаєте, серед футбольних уболівальників домінують вегетаріанці-мусульмани-трансгендери? Ви в шоці, пане Лінекер? Ви досить вражаюче неправильно розумієте суспільні настрої навколо цього. Здається, ви все ще думаєте, що BBC і Sky якимось чином вловлюють настрої, яким вони не можуть». Цей коментар був охарактеризований нейромережею як той, що містить кіберзалякування з оцінкою 0.8670.*

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

Другий текстовий зразок: «Original: *In today's digital age, it's essential to foster a culture of respect and support online. Social media platforms can be powerful tools for connection, allowing us to share our thoughts, celebrate our achievements, and uplift one another.* / Переклад українською: *У сучасну епоху цифрових технологій дуже важливо розвивати культуру поваги та підтримки в Інтернеті. Платформи соціальних медіа можуть бути потужними інструментами для спілкування, дозволяючи нам ділитися своїми думками, відзначати наші досягнення та підбадьорювати один одного.*». Нейромережа класифікувала текстовий зразок, як той, що не має кіберзалякування з показником 0.028.

Таким чином, ці два коментарі демонструють різні рівні кіберзалякування та мови ворожнечі, що важливо для ефективного виявлення кіберзалякувань в текстовому контенті.

8. Результати експерименту та дискусія

Було розроблено та практично реалізовано метод інтелектуального виявлення кіберзалякувань у текстовому контенті за допомогою рекурентної нейронної мережі, що містить у собі комбінований підхід: мережа RNN для визначення числової оцінки наявності кіберзалякувань у текстовому контенті та підхід числової оцінки концентрації мови ворожнечі на основі «Hatebase». Значення метрик для навчених версій нейромереж при 20-и епохах і різних розмірах батча наведено на рисунку 12. Значення метрик для навчених версій нейромереж при 10-и епохах і різних розмірах батча наведено на рисунку 13. Як видно з наведених діаграм, показники не опускаються метрик не опускаються нижче 94%, отже нейронна мережа показує на всіх моделях високі показники до визначення присутності кіберзалякувань у текстовому контенті.

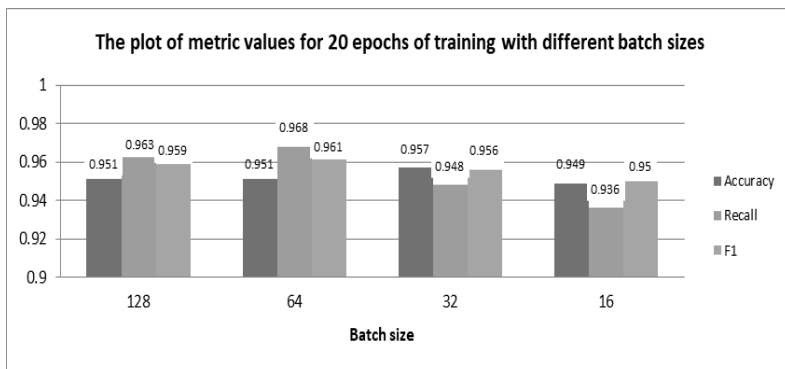


Рисунок 12. Значення метрик для визначення кіберзалякувань у текстовому контенті RNN для 20-и епох

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

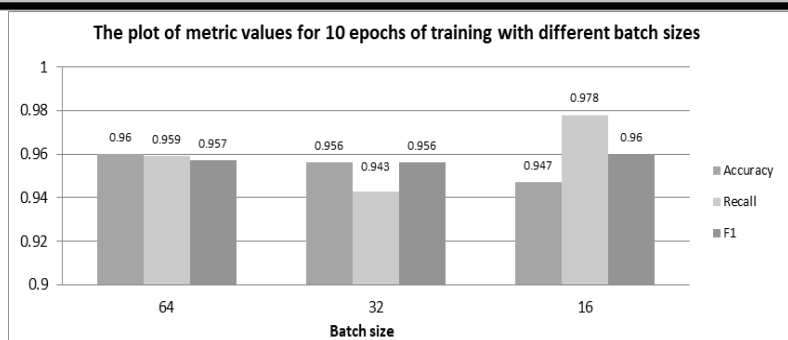


Рисунок 13. Значення метрик для визначення кіберзалежувань у текстовому контенті RNN для 10-и epoch

У рамках проведення дослідження було зібрано 50 коментарів, які не входять у навчальні та тестові дані з соціальних мереж «Facebook» та «Instagram», які було оцінено експертами на 2 категорії: «з кіберзалежуванням» та «без кіберзалежувань». З них за оцінкою експертів, 32 коментарі мали маркер «без кіберзалежувань» та 18 «з кіберзалежуванням». З проведеного тестування розробленим методом, 30 текстових зразків є з кіберзалежуванням, а 20 – без кіберзалежування.

Однак, спірні текстові зразки, що були охарактеризовані попереднім експертом як «з кіберзалежуванням», а розробленим методом, як «без кіберзалежування» було запропоновано оцінити ще 3-м експертам, і у першому випадку 2-є з 3-х їх теж віднесли до «без кіберзалежування». Текст був наступним: «Original: *Honestly, I can't believe how clueless some people are. It's like they just don't get it. Maybe if you actually paid attention, you'd understand why everyone is frustrated with you. Do you even care about what others think? It seems like you just enjoy making things difficult for everyone around you. Just saying.* / Український переклад: *Чесно, я не можу повірити, як деякі люди можуть бути такими нездатними. Здається, вони просто не розуміють. Може, якби ти справді звертав увагу, ти б зрозумів, чому всі незадоволені тобою. Тобі взагалі цікаво, що думають інші? Схоже, ти просто отримуєш задоволення від того, що ускладнює життя всім навколо. Просто кажу*». Оцінка даного коментаря розробленим методом склала 0.37, при пороговому значення 0.4. Це повідомлення містить елементи критики та розчарування, але не містить явних образ або загроз, мови ворожнечі, що ускладнює його класифікацію як чітке кіберзалежування.

Порогові значення для визначення кіберзалежувань в текстовому контенті є важливими для аналізу даних, оскільки вони впливають на точність і чутливість моделей виявлення. Загальноприйнятим є те, що оптимальні порогові значення можуть варіюватися від 0.4 до 0.7, залежно від контексту та застосованих підходів до виявлення кіберзалежувань. Зокрема, оцінка 0.4 часто розглядається як мінімальний поріг для виявлення образливого контенту, що

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

значення дозволяє класифікувати коментарі, що містять потенційно небезпечні висловлювання, як такі, що потребують подальшого аналізу, водночас виключаючи деякі менш агресивні повідомлення. Важливо, щоб порогове значення забезпечувало достатній рівень чутливості, що дозволяє виявляти численні випадки кіберзалякувань, які в іншому випадку могли б залишитися непоміченими. Крім того, використання порогового значення 0.4 забезпечує можливість швидкого виявлення небезпечних висловлювань, що є критично важливим для оперативного реагування на ситуації кіберзалякувань. Нижчі порогові значення здатні виявляти значну частину випадків кіберзалякувань, що є важливим для модерації контенту [21].

Також результати з прикладами використання методу наведені на рисунку 14.

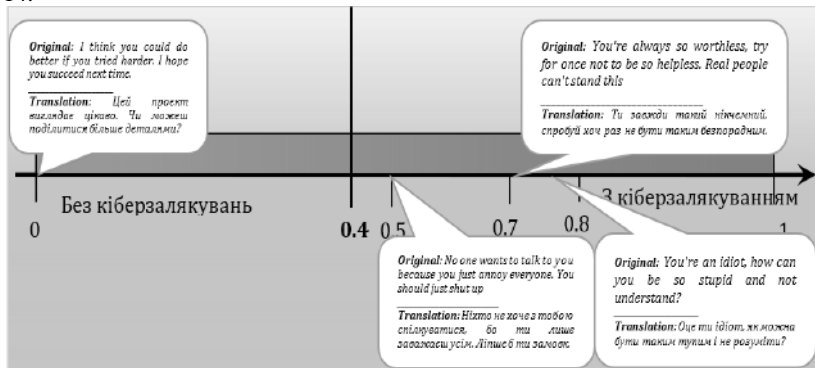


Рисунок 14. Результат прикладного використання методу

Для порівняння, ці ж коментарі були подані для оцінки чату GPT, де він дав оцінки, наведені на рисунку 15.

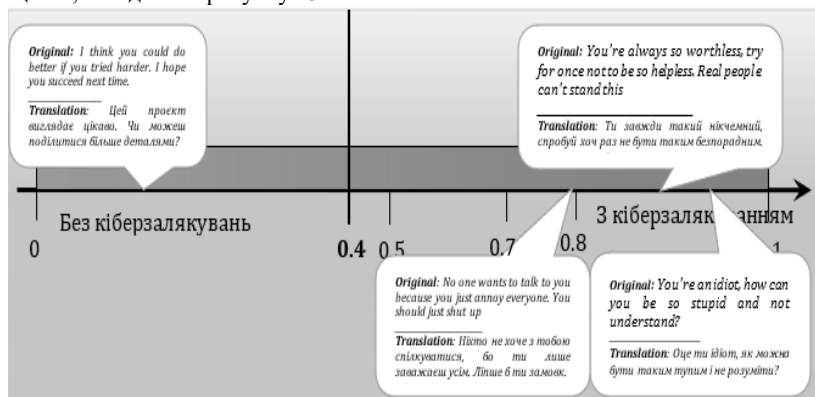


Рисунок 15. Оцінка тексту мовною моделлю ChatGPT

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

При цьому, ChatGPT визначив наступне обґрунтування своїм оцінкам:

Текст 1: «*I think you could do better if you tried harder. I hope you succeed next time.*» – оцінка 0.2. Цей коментар має позитивний підхід, пропонуючи підтримку, хоча може бути сприйнятий як критичний. Однак у ньому відсутнє пряме приниження чи образи, тому загальна оцінка кіберзалежування залишається низькою.

Текст 2: «*You're always so worthless, try for once not to be so helpless. Real people can't stand this.*» – оцінка 0.9. У цьому коментарі є явне приниження і негативне висловлювання про людину, що підвищує оцінку кіберзалежування. Слова "worthless" та "helpless" є образливими, що свідчить про ненависть.

Текст 3: «*No one wants to talk to you because you just annoy everyone. You should just shut up.*» – оцінка 0.8. Цей коментар також містить ненависть і приниження. Він не лише висловлює негативні почуття, а й закликає мовчати, що підкреслює деструктивний характер повідомлення.

Текст 4: «*You're an idiot, how can you be so stupid and not understand?*» – оцінка 0.95. Цей коментар містить дуже сильні образи і ненависть, безпосередньо принижуючи особу, що є явним прикладом кіберзалежування.

Оцінка наявності кіберзалежування, отримана шляхом застосування розробленого методу, відображає результати, що не суперечать оцінкам, отриманим за допомогою моделі, такої як ChatGPT. Обидва підходи використовують схожі критерії для аналізу коментарів, що свідчить про прийнятність отриманих результатів. Зокрема, як метод, так і модель враховують контекст, тон висловлювань та наявність мови ворожнечі. Це свідчить про те, що результати аналізу відповідають сучасним підходам до виявлення кіберзалежування, підвищуючи їх достовірність. Таким чином, можна стверджувати, що застосований метод надає об'єктивні та коректні оцінки, які можуть бути використані для подальших досліджень у цій галузі.

9. Висновки

Було розглянуто сучасний стан напряму виявлення кіберзалежувань у текстовому контенті, й відповідно до проведеного аналізу були виділені основні підходи до вирішення задачі виявлення кіберзалежувань, серед яких є: аналіз тональності, виявлення мови ворожнечі (підхід словника) та використання машинного навчання. Було прийнято рішення використати комбінований підхід на базі виявлення кіберзалежування та виявленні мови ворожнечі (підхід словника), яка підсилювала б оцінку кіберзалежування при його наявності. Також сформовано відповідний набір даних, що складався з датасетів «Cyberbullying Data for Multi-Label Classification», «Cyberbullying Tweets», «Cyberbullying Dataset» «A Comprehensive Dataset for Automated Cyberbullying Detection» (для навчання RNN), а також «Hatebase» (для ідентифікації мови ненависті). На твіті було накладено фільтрацію, було видалено твіти що склались менше ніж з 3-х слів. Для навчання RNN було прийнято рішення поділити датасет у пропорції 60/40, де 60 % це навчальна вибірка, а 40 % тестова. Навчена модель RNN, що була в подальшому

використана для аналізу тональності, мала точність 0.96, а Recall та F1 мали показники 0.959 та 0.957 відповідно. Метод інтелектуального виявлення кіберзалякувань у текстовому контенті було протестовано на створеному програмному забезпеченні, та з проведеного дослідження показано що метод має високу ефективність виявлення кіберзалякувань у текстовому контенті. Запропонований метод дозволяє оцінити рівень присутності кіберзалякувань у текстовому контенті для його подальшого моніторингу, попередження шкідливого впливу та вжиття необхідних заходів з боку модераторів чи автоматизованих систем управління контентом. Згідно проведених досліджень, метод має оцінку точності ідентифікації понад 90 %, однак, оцінка наявності кіберзалякувань може бути суб'єктивною, і сприйняття контенту може різнитися від особи до особи. Однак, для покращення результату необхідно доповнити словник виразів мови ворожнечі. Також запропонований метод має ряд обмежень: працює з текстовим контентом довжиною від 3 до 500 слів.

Подальші дослідження можуть бути спрямовані на прикладне застосування, що може бути корисним інструментом для оцінки рівню кіберзалякувань у текстовому контенті, який публікується в соціальних мережах, та для запобігання поширенню шкідливої чи образливої інформації.

10. Література

- [1] Молчанова М.О., Мазурець О.В., Собко О.В., Кліменко В.І., Андрощук В.І. Метод нейромережевого виявлення кібербулінгу з використанням хмарних сервісів та об'єктно-орієнтованої моделі. Науковий журнал «Вісник Хмельницького національного університету» серія: Технічні науки. Хмельницький, 2024. №2 (333). С. 200-206.
- [2] Молчанова М.О., Мазурець О.В., Собко О.В., Віт Р.В., Назаров В.В. Алгоритм виявлення аб'юзивного вмісту в україномовному аудіоконтенті для імплементації в об'єктно-орієнтовану інформаційну систему. Науковий журнал «Вісник Хмельницького національного університету» серія: Технічні науки. Хмельницький, 2024. №1 (331). С. 101-106.
- [3] Департамент ГО «Докудейз». URL: https://cyber.bullyingstop.org.ua/storage/media-archives/cyberbuling_виправл15-10_compressed.pdf
- [4] Nouas S., Boumahdi F., Madani A., Berrhail F. Cyberbullying: A BERT Bi-LSTM Solution for Hate Speech Detection. Proceedings of the International Conference on Applied Cybersecurity (ACS) 2023. ACS 2023. Lecture Notes in Networks and Systems, vol 760. Springer, Cham.
- [5] Sobko O., Mazurets O., Didur V., Chervonchuk I. Recurrent Neural Network Model Architecture for Detecting a Tendency to Atypical Behavior Of Individuals by Text Posts. Theoretical and Practical Aspects of Modern Research. Proceedings of XXVI International scientific and practical conference. June 5-7, 2024. International Scientific Unity. Ottawa, Canada. 2024. Pp. 113-117.
- [6] Dhingra N., Chawla S., Saini, O. An Improved Detection of Cyberbullying on Social Media Using Randomized Sampling. Int Journal of Bullying Prevention (2023).

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

- [7] Muneer A., Alwadain, A., Ragab M.G. Alqushaibi A. Cyberbullying Detection on Social Media Using Stacking Ensemble Learning and Enhanced BERT. *Information* 2023, 14, 467.
- [8] Daraghmi E.-Y., Qadan S., Daraghmi Y.-A., Yousuf R., Cheikhrouhou O., Baz M. From Text to Insight: An Integrated CNN-BiLSTM-GRU Model for Arabic Cyberbullying Detection. *IEEE Access*. 2024. vol. 12, pp. 103504-103519.
- [9] Slobodzin V., Molchanova M., Kovalchuk O., Sobko O., Mazurets O., Barmak O., Krak I. An Approach Based on the Visualization Model for the Ukrainian Web Content Classification. *2022 12th International Conference on Advanced Computer Information Technologies, ACIT 2022*. 2022. pp. 400-405.
- [10] CyberBullying Detection Dataset. URL: <https://www.kaggle.com/datasets/sayankr007/cyber-bullying-data-for-multi-label-classification>
- [11] Cyberbullying Tweets. URL: <https://www.kaggle.com/datasets/soorajtomar/cyberbullying-tweets>
- [12] Cyberbullying Dataset. URL: <https://www.kaggle.com/datasets/saurabhshahane/cyberbullying-dataset>
- [13] A Comprehensive Dataset for Automated Cyberbullying Detection. URL: <https://data.mendeley.com/datasets/wmx9jj2htd/2dataset> .
- [14] Hatebase. URL: <https://hatebase.org> .
- [15] Y. Krak Y., O. Barmak O., O. Mazurets O.. The practice implementation of the information technology for automated definition of semantic terms sets in the content of educational materials, *CEUR Workshop Proceedings*, 2018, vol. 2139, pp. 245-254.
- [16] Hartmann M., Heitmann Ch., Siebert Ch., Schamp, More than a Feeling: Accuracy and Application of Sentiment Analysis, *International Journal of Research in Marketing*, Volume 40, Issue 1, 2023, pp. 75-87.
- [17] Scikit-learn, `sklearn.metrics.f1_score`. URL: https://scikit-learn.org/stable/modules/generated/sklearn.metrics.f1_score.html
- [18] Medium, How does Batch Size impact your model learning. URL: <https://medium.com/geekculture/how-does-batch-size-impact-your-model-learning-2dd34d9fb1fa>.
- [19] wxPython. URL: <https://wxpython.org/index.html>.
- [20] Scikit-learn. Machine Learning in Python. URL: <https://scikit-learn.org/stable/>.
- [21] Залуцька О.О., Молчанова М.О., Мазурець О.В., Мельник О.І., Скрипник Т.К. Метод інтелектуального аналізу емоційної тональності текстової інформації для визначення поведінкових намірів нейромережевими засобами. *Науковий журнал «Вісник Хмельницького національного університету» серія: Технічні науки. Хмельницький, 2023. №5 (325). Т.1. С. 67-73.*

**METHOD FOR INTELLIGENT DETECTION OF
CYBERBULLYING IN THE TEXT CONTENT**

O. Sobko ORCID: 0000-0001-5371-5788

Khmelnytskyi National University, Ukraine

E-mail: olenasobko.ua@gmail.com

***Abstract.** Research is devoted to creation and testing of method for intelligent detection of the cyberbullying in text content. The method is able to estimate the level of cyberbullying based on the entered text information using a recurrent neural network. The detection of cyberbullying involves the use of combined approach, that combines the use of hate speech words dictionary and neural network approach to determine the cyberbullying presence. The proposed method allows establishing the presence of cyberbullying in the text and determining numerical assessment of the level of cyberbullying, for further monitoring of communication process, prevention of harmful effects and taking necessary measures by moderators or automated content moderation by relevant content management systems.*

Three-layer architecture with Embedding Layer, LSTM Layer and Dense Layer was used. The RNN model, trained according to the developed method, was further tested and found performance indicators: accuracy 0.96, recall 0.959 and F1 0.957. Both the method and the model take into account the context, the tone of statements and the presence of hate speech. This indicates that the results of the analysis correspond to modern approaches to the detection of cyberbullying, increasing their credibility.

The method for intelligent detection of the cyberbullying in text content was tested on the created software, and it was established that the method has high efficiency of detecting cyberbullying in text content. According to applied studies, the method has an accuracy rating of over 90% for identifying cyberbullying, however, the assessment of the presence of cyberbullying can be subjective and the perception of content can vary from person to person. Method has limitations: it working with texts from 3 to 500 words long.

***Keywords:** cyberbullying, text mining, hate speech, neural network, classification of cyberbullying.*

UDC 004.896

**HIERARCHICAL CLASSIFICATION OF UKRAINIAN
TECHNICAL TEXTS USING TREE-BASED MODELS:
APPLICATIONS IN THE AUTOMOTIVE INDUSTRY**

S. Mashtalir ORCID: 0000-0002-0917-6622

Kharkiv National University of Radio Electronics

E-mail: sergii.mashtalir@nure.ua

O. Nikolenko ORCID: 0000-0002-6422-7824

Uzhhorod National University

E-mail: oleksandr.nikolenko@uzhnu.edu.ua

Abstract. *Hierarchical classifiers play a crucial role in addressing complex classification tasks by breaking them down into smaller, more manageable sub-tasks. This paper focuses on the technical Ukrainian texts hierarchical classification, specifically the classification of repair works and spare parts used in automobile maintenance and servicing. We tackle the challenges posed by multilingual data inputs – specifically Ukrainian, Russian, and their hybrid – and the lack of standard data cleaning models for the Ukrainian language. We developed a novel classification algorithm, which employs TF-IDF vectorization with unigrams and bigrams, keyword selection, and cosine similarity for classification. Also this paper describes a method for training and evaluating a hierarchical classification model using parameter tuning for each node in a tree structure. The training process involves initializing weights for tokens in the class tree nodes and input strings, followed by iterative parameter tuning to optimize classification accuracy. Initial weights are assigned based on predefined rules, and the iterative process adjusts these weights to achieve optimal performance. The paper also addresses the challenge of interpreting multiple confidence scores from the classification process, proposing a machine learning approach to calculate a unified confidence score. This score helps assess the classification reliability, particularly for unlabeled data, by transforming input values, generating polynomial parameters, and using logarithmic transformations and scaling. The classifier is fine-tuned using hyperparameter optimization techniques, and the final model provides a robust confidence score for classification tasks, enabling the verification and classification results optimization across large datasets. Our experimental results demonstrate significant improvements in classification performance. Overall classification accuracy nearly doubled after training, reaching 92.38%. This research not only advances the theoretical framework of hierarchical classifiers but also provides practical solutions for processing large-scale, unlabeled datasets in the automotive industry. The developed methodology can enhance various applications, including automated customer support systems, predictive maintenance, and decision-making processes for stakeholders like insurance companies and service centers. Future work will extend this approach to more complex tasks, such as extracting and classifying information from extensive text sources like telephone call transcriptions.*

Keywords: *NLP, tree-based classification, machine learning, data analysis, applied intelligent systems.*

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

1. Introduction and literature review

The field of tree-based data classification has gained increasing prominence due to its capacity to efficiently manage and categorize data with inherent hierarchical structures. This capability is essential for applications across diverse disciplines, such as phylogenetic tree analysis in biology [1], file system organization in computer science [2], and document categorization in information retrieval [3]. The primary strength of tree-based classification lies in its ability to structure data hierarchically, which facilitates efficient retrieval, analysis, and interpretation.

In tree-based classification models, each node within a tree represents a category or class, with branches to child nodes denoting subcategories. The classification process involves assigning data points to appropriate nodes based on their attributes, following a set of predefined rules or models that guide their placement. While various methodologies – such as Decision Trees [4], Random Forests [5], Gradient Boosted Trees [6], and Hierarchical Clustering [7] – have been extensively developed and optimized for numerical and formal categorical attributes, a significant gap exists in their application to Natural Language Processing (NLP).

Although some progress has been made in applying tree-based classification to NLP tasks like fake news detection [8], document clustering using summarization [9], and classification using Discriminative-Semantic Features [10], there is still a lack of robust frameworks for categorizing textual data into predefined hierarchical classes, particularly for less-resourced languages and specialized technical terminologies. Text mining remains a critical area of research due to its potential to produce concise textual representations of complex physical or technical phenomena. As scientific fields evolve and more sophisticated deep learning tools become available, the need for effective big data text analysis has expanded to various applications, such as medical diagnostics [11], where labeling algorithms can parse large-scale textual datasets, and information extraction in noisy environments [12].

Despite the wealth of data available, NLP systems still grapple with issues related to data incompleteness and errors [13, 14]. Inaccurate or incomplete training data can lead to biased or erroneous model outputs, affecting the reliability of NLP applications. Addressing these issues requires the development of more robust data curation and cleaning processes. However, many existing approaches do not account for the unique characteristics of specific languages, relying instead on generic toolkits that limit their efficacy in multilingual or domain-specific contexts.

Consequently, research into NLP methods that incorporate language-specific features has gained considerable interest. Such methods have not only improved human-computer interactions but also broadened the applicability of NLP in various domains. Despite recent advancements, challenges persist, particularly in processing specialized scientific and technical texts that employ complex, domain-specific terminologies. Developing NLP models that can accurately interpret and generate content in these contexts demands further research, including domain-specific fine-tuning and the construction of specialized lexicons. Furthermore, NLP models and libraries are disproportionately developed for major languages, leaving many languages underrepresented and limiting the accessibility of these technologies [15, 16]. The problem is further compounded in multilingual settings, where shared

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

linguistic roots and overlapping vocabulary complicate accurate language processing [17]. Developing robust multilingual NLP models remains active research area.

This study consolidates our previous research on addressing a complex Natural Language Processing (NLP) challenge, focusing on the classification of automotive repair parts and labor descriptions [18-20]. The data utilized for this research was derived from a Garage Management System (GMS).. The dataset is notable for its high variability, containing errors, technical abbreviations, and domain-specific jargon, with entries predominantly in Ukrainian and Russian, and occasionally a blend of the two, known as "Surzhik." Additionally, annotated data is available in the form of a hierarchical classifier for automotive service jobs in both languages.

The primary objective is to categorize each labor entity into predefined categories. To achieve this, we establish a comprehensive data cleansing and preprocessing pipeline, including tokenization (see Figure 1 and [21]), to convert raw text into a structured format suitable for classification. An essential step in this process is vocabulary normalization, which is crucial for managing computational resources and processing time [17]. This paper investigates tree-based classification methodologies for textual data, exploring theoretical foundations, algorithms, and applications, with a particular emphasis on classifying automotive service descriptions. Such methodologies are invaluable for automating processes within the automotive industry, ranging from quality monitoring in service centers to centralizing vehicle issue data for stakeholders like insurance companies and manufacturers.

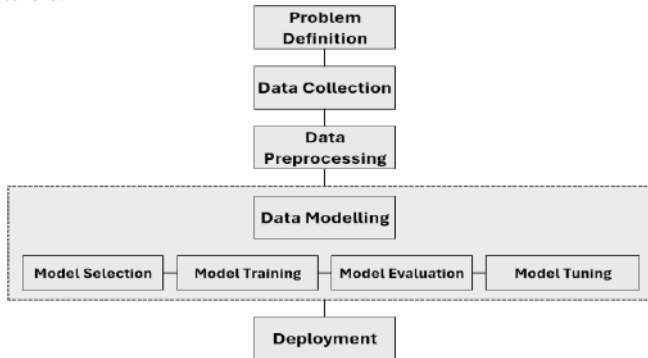


Figure 1. Typical data science process

The classification of automotive labor entities falls under the broader category of unstructured data processing, a challenging area that requires a blend of natural language processing expertise and advanced data science techniques [22]. Given the hierarchical nature of the task directory, this problem is framed as a supervised machine learning task, facilitating the development and evaluation of classification models. As illustrated in Figure 1, typical data science workflows are divided into distinct phases: Problem Definition, Data Collection, Data Preprocessing, Data Modeling (encompassing Model Selection, Model Training, Model Evaluation, and

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

Model Tuning), and Deployment. These phases will be elaborated upon in subsequent sections of the paper.

2. Problem definition and data collection

Automotive sector issues

This work focuses on the technical Ukrainian texts hierarchical classification. The primary issue addressed in the study is the classification of repair works and spare parts used in the automobiles' maintenance and servicing.

This problem's significance cannot be overstated. Out of approximately 1.5 billion vehicles globally, only 20% have detailed, centrally collected, stored, and analyzed repair information [23] and [24]. This data pertains primarily to new vehicles, up to four years old, which are serviced at authorized service centers. Automotive manufacturers utilize specialized software in the original equipment service centers (OES), where all repairs and spare parts are accurately classified. This allows for the collection of precise statistical data on the individual components and assemblies reliability, their operational characteristics, warranty cases, and more [25]. Unfortunately, once a vehicle leaves the official service network, its subsequent repair and maintenance history becomes fragmented and often lost. Non-authorized service centers lack a unified classifier for repairs and spare parts, let alone a single information system. Furthermore, there are thousands of such systems worldwide, each with different languages and data formats. In Ukraine alone, dozens of similar programs are used. Figure 2 illustrates the automotive fleet structure and highlights the data problem concerning repairs.



Figure 2. Global car park structure

Repair data is valuable not only to automotive manufacturers but also to various other sectors. For example, insurance companies can benefit from this data to determine repair costs and residual vehicle values. Similarly, service centers and even car owners would find it beneficial to have information not only about the current repair costs but also about future expenses related to repair and maintenance.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

Data collection and data structure

Our research utilized anonymous data from an online garage management system, covering five years and 500 service stations, yielding over 1 million work records and 1.2 million spare parts records annually. Additionally, customer calls recorded via IP telephony and transcribed into text data contributed to a substantial dataset with hundreds of thousands of texts and tens of millions of data rows. Training and test sets were randomly drawn and manually labeled. The general objective is to develop an algorithm for extracting and further classifying texts using given tree-based classes sets. For this purpose, we have 4 types of datasets:

1. **Classes** – two distinct trees for works (180 entries) and parts (1,600 entries).
2. **Training** – the class trees, augmented with manually labeled data (6,000 entries).
3. **Test** – additional labeled dataset (11,000 entries).
4. **Operational or Input Data** – tens of millions of entries.

Let us examine these types in greater detail.

Car repair works are organized in a three-level tree structure as shown in the data extract in Table 1.

Table 1

Repair works classes data tree extract

ID	Parent ID	UA	EN
1000	0	Діагностичні роботи	Diagnostic work
1100	1000	Діагностика	Diagnostics
1101	1100	Ручна діагностика	Manual diagnostics
1102	1100	Комп'ютерна діагностика	Computer diagnostics
1200	1000	Тестування	Testing
2000	0	Загальні роботи	General works
2100	2000	Заміна	Replacement

Car components are classified within a hierarchical four-level tree structure. The classification begins with the most general component types, such as mechanical and body parts, oils and fluids, wheels and tires. These broad categories are then divided into their corresponding systems, including filters, power transmission, braking, suspension, steering, engine, cooling, electric and electronic systems. Within each system, the classification is further refined into specific components. For example, the suspension is divided into subcategories such as damping, arms, wheel hubs, bearings, etc. Finally, the lowest classification tier consists of specific spare parts detailed lists, such as shock absorbers, struts, coil and leaf springs. The car parts data tree extract is presented in Table 2. The training and test datasets comprise combined repair works and parts lists. For example, an entry might be "Pneumatic damping diagnostics on shock-tester". These lists have been manually labeled specifically for this study. Operational data consists of arbitrary text, which may include information from garage management systems (GMS), phone calls transcriptions, messages from messengers, etc. The objective is to determine whether the input text contains

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

information related to car repairs and to correctly assign it to one of the predefined classes for works and parts.

Table 2

Car parts classes data tree extract

ID	PARENT ID	UA	EN
1000000	0	Механічні деталі	Mechanical parts
1070000	1000000	Амортизація	Suspension damping
1070100	1070000	Амортизатори і стійки	Shock absorbers & struts
1070101	1070100	Амортизатори підвіски	Shock absorbers
1070102	1070100	Стойки підвіски	Struts
1070105	1070100	Пневмо-амортизатори	Pneumatic shocks
1070300	1070000	Опори амортизаторів	Strut mountings

Classification Success Criteria

A classification is deemed successful if:

1. No less than 90% of car repair works are identified and extracted from the incoming unlabeled texts
2. Of these, no less than 90% of works and parts are correctly assigned to their appropriate classes.

For example, the text "Pneumatic damping diagnostics on shock-tester" should be accurately classified into class 1102 for works and 1070105 for parts

For this study purposes, we simplify the task by assuming that the input text contains information about works and components. Therefore, only the second criterion of successful classification is considered. The task of extracting relevant information about repair works and automotive parts from arbitrary text will be addressed in future studies.

In summary, this work aims to address the critical issue of technical texts hierarchical classification, focusing on the automotive industry. By improving the classification and analysis of repair and maintenance data, we can enhance this information's reliability and accessibility for multiple stakeholders, ultimately contributing to better decision-making and resource management in the automotive sector.

3. Data preprocessing

Classical NLP preprocessing pipeline contains some preliminary (sentence segmentation, word tokenization), frequent (stop word removal, stemming and lemmatization, removing digits/punctuation, lowercasing) and other steps (normalization, language detection, code mixing, transliteration) [17, 21].

In our data preprocessing pipeline, certain modifications were necessitated due to the origin of the data. Specifically, some conventional steps such as sentence segmentation were deemed unnecessary.

Conversely, we introduced additional procedures tailored to the dataset's characteristics, which included language detection, specific Cyrillic characters

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

approach, the disassembling of compounded words and handling of specific shortcuts and abbreviations.

Language Identification

Language identification is accomplished through the utilization of two distinct approaches:

1. **Identification of Specific Characters:** This approach involves the recognition of language-specific characters, such as "i," "ї," "є," and "r" for Ukrainian, as well as "ы," "ь," "э," and "ё" for Russian.

2. **Word Counting in Dictionaries:** A complementary method relies on counting the occurrences of words found in both Ukrainian and Russian dictionaries, as detailed in the "Lemmatization" chapter.

Following the language identification process, all data undergo translation into Ukrainian. This translation is facilitated by two custom correspondence dictionaries, which are elaborated upon in the chapters titled "Translation of Tokens from Russian to Ukrainian" and "Synonyms".

Text Lines Normalization

Text line normalization encompassed a series of standardization procedures. These encompassed segregating numbers and punctuation symbols with spaces, uniformly converting all characters to lowercase, substituting backslashes ("\") with regular forward slashes ("/"), and replacing underscores ("_") with spaces. Additionally, our specific task demanded the normalization of various types of apostrophes into a singular format. This process also extended to the treatment of certain Cyrillic characters, such as transforming "r" to "r" and "ё" to "e". Furthermore, prior to the removal of stop words and special characters, common abbreviations featuring slashes or hyphens were substituted with their expanded counterparts, a feature particularly relevant to the context of garage repair texts (e.g., "к-т" denoting "комплект" (kit), "д/м" signifying "демонтаж / монтаж" (mounting / dismounting) and "о/р" representing "охлаждающая рідина" (cooling fluid) among others). Subsequently, all special characters, with the exception of the apostrophe, which holds linguistic significance in the Ukrainian language, and designated stop words were eliminated from the text.

Stopwords

Our compilation of stopwords comprised a comprehensive set, encompassing both Ukrainian and Russian languages. Notably, certain stopwords present in the general set were excluded, given their relevance to our classification task. For instance, "ТО," an abbreviation for "технічне обслуговування" (technical maintenance), and "ніж," which could be interpreted as a noun (knife) and is pertinent to our directory, were retained. Conversely, additional stopwords were introduced that did not significantly contribute to the subsequent classification process. These included brand names of cars or parts, terms such as "auto," "automobile," "automotive," "service," and other highly generic words devoid of distinctive characteristics relevant to individual entities.

Translation Of Tokens From Russian To Ukrainian

Since we possess detailed classifiers containing Ukrainian and Russian versions of names, and since most names share an identical number and order of words in

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

both versions, we were able to automatically construct a correspondence dictionary between Russian and Ukrainian words.

For each name in the dictionary, we iteratively compare Ukrainian and Russian name versions.

1. Split both versions into token lists.
2. If the lengths of the token lists are equal, iterate through the tokens and increment a "counter" by 1 for each corresponding Ukrainian-Russian token pair. If the number of tokens in the names is not the same, add the missing tokens to the "omitted" category, which is then manually checked. We also skip tokens that are identical in both versions.

3. We obtain correspondence dictionaries where each Russian token corresponds to Ukrainian tokens that were found in the same position in the sentence, along with the number of such occurrences. We select the translation option that occurred most frequently as the most likely correct one. Consequently, we have a dictionary where each Russian token can be matched to its Ukrainian equivalent.

4. Additional steps included manual verification of token translations that differed significantly according to the Jaro-Winkler metric [26], as well as the addition of translations for omitted names with differing token counts.

Tokenization of "Concatenated" Tokens (with Missing Spaces)

The algorithm takes as input a unique set of tokens derived from the data we intend to classify subsequently. It searches for concatenated tokens within this set. For each input token:

1. Check whether it starts or ends with a token known to us.
2. If so, separate it and add it to the "parts" list.
3. Repeat steps 1-2 until we traverse the sorted list of known tokens.
4. Anything that remains unprocessed is added to the list of parts. Remove all parts that are absent from the set of known tokens.
5. If, after this process, more than one part is obtained, identify it as a concatenated token. Add both the original concatenated token and its decomposition to a "dictionary" of token decompositions, which is used later to replace such tokens in input strings.

This token concatenation search is relatively basic in nature, as it can only break tokens that start or end with reference tokens without typographical errors. In the worst-case scenario, a token may not only be concatenated but also contain errors within its constituent parts, in which case the algorithm will fail to identify it. However, concatenated tokens themselves are relatively infrequent, and concatenated tokens with errors are even rarer. Developing a more complex algorithm to address such cases would entail significant computational costs. Therefore, we have chosen to implement this straightforward approach.

Spelling Correction

Spelling errors are identified within tokens that do not exist in reference dictionaries; otherwise, they are considered correct and skipped. Essentially, this process entails the search for the most similar words among those present in the token sets from reference dictionaries, including all their inflected forms found in

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

Ukrainian and Russian noun and adjective dictionaries. For input, we receive a unique set of tokens from the data that we plan to classify subsequently. Typographical errors are sought within this set. The error detection occurs in two stages.

1. In the first stage, search for the nearest match for tokens that differ by no more than 2 characters from existing tokens. The match is found using the Jaro-Winkler [27] similarity function and is accepted if the similarity value exceeds a predefined threshold. The Jaro-Winkler metric assigns greater weight to token "prefixes" (letters at the beginning of the token).

2. In the second stage, the match is also sought using the same function but without a limit on the maximum of 2 character differences, hence, the threshold value is higher compared to the first stage. Therefore, in the first stage, we tolerate lower "similarity," as long as the token differs from existing ones by no more than 2 characters, while in the second stage, greater dissimilarity is allowed, but the similarity value requirement is higher.

In essence, during the first stage, the distance function allows for smaller "similarity," but tokens must differ from existing ones by no more than 2 characters. In the second stage, greater differences (more than 2 characters) are allowed, but the similarity requirement is stricter.

Motivation For Choosing The Jaro-Winkler Metric

The Jaro-Winkler Measure is a measure of *similarity / distance* between two text sequences. It uses the prefix scaling factor p , which provides a higher score to sequences that match at the beginning up to a specified prefix length l . The higher the Jaro-Winkler similarity measure, the more similar the two text sequences are. The score is normalized such that 0 indicates no similarity, and 1 indicates a perfect match. *Similarity* and *distance* are inversely related, and their correspondence is established by the formula $distance = 1 - similarity$. The Jaro-Winkler Measure is a modification of the Jaro measure.

The Jaro similarity sim_j of two text strings s_1 and s_2 is determined by the formula (1):

$$sim_j = \begin{cases} 0 & \text{if } m = 0 \\ \frac{1}{3} \left(\frac{m}{|s_1|} + \frac{m}{|s_2|} + \frac{m-t}{m} \right) & \text{if } m > 0 \end{cases}, \quad (1)$$

where: $|s_i|$ – length of string s_i
 m – number of matching characters
 t – number of transpositions.

Two characters from s_1 and s_2 are considered a match if they are identical and located no more than p positions apart. If no matches are found, the algorithm stops and returns a *similarity* score of 0. If matches are found, the number of transpositions is then calculated. A transposition occurs when a corresponding (matching) character is not in its correct position, and the number of corresponding characters not in their correct position, divided by 2, yields the number of transpositions.

The Jaro-Winkler similarity sim_{jw} of two text strings s_1 and s_2 is determined by the formula (2):

**ADVANCES
IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES**

$$sim_{jw} = sim_j + lp (1 - sim_j), \tag{2}$$

where: sim_j – Jaro similarity of text strings s_1 and s_2

l – length of the common prefix at the beginning of the string, maximum of 4 characters

p – a constant scaling coefficient that adjusts the estimate in the direction of increasing values in the presence of a common prefix: the standard value is 0.1.

By substituting formula (1) into the Jaro-Winkler similarity expression, we obtain formula (3):

$$sim_j = \begin{cases} 0 & \text{if } m = 0 \\ \frac{1}{3} \left(\frac{m}{|s_1|} + \frac{m}{|s_2|} + \frac{m-t}{m} \right) + lp \left(1 - \frac{1}{3} \left(\frac{m}{|s_1|} + \frac{m}{|s_2|} + \frac{m-t}{m} \right) \right) & \text{if } m > 0 \end{cases} \tag{3}$$

There are many distance metrics, among others Levenshtein Distance, Indel (Insertion-Deletion) Distance, Hamming Distance.

Levenshtein Distance. The minimum number of single-character operations (insertions, deletions, and substitutions) required to transform one text string into another [28]:

- Insertion: автообиль → автомобиль
- Deletion: автомиобиль → автомобиль
- Substitution: автомоьиль → автомобиль

According to Levenshtein pair of редуктор → редуктор**н**ий has a distance of 3 (3 insertions) and pair of ремкомпл**е**кт → ремкомпл**е**кт has a distance of 2 (2 substitutions).

Indel (Insertion-Deletion) Distance. The minimum number of insertions and deletions of characters required to transform one text string into another. Substitutions are not allowed, but each substitution can be accomplished by a pair of a deletion and an insertion, making this distance equivalent to the Levenshtein distance with a substitution weight of 2.

Hamming Distance. The number of positions where two strings of equal length differ. It represents the minimum number of substitutions required to transform one string into another and can only be applied to sequences of equal length.

Jaro-Winkler Metric is more complex than simple distance algorithms based on counting basic character operations. It provides a real value between 0 and 1, making the distance values more informative and suitable for comparison and sorting. Additionally, it gives more significance to prefixes, which is a useful property when dealing with "typo searching". Spelling correction is used not for spelling errors only but as well for words with variations in their endings, sharing a common prefix. Giving more weight to prefixes increases the chances of correctly identifying such "typos". Table 3 shows comparative example using the Levenshtein distance and Jaro-Winkler metric, with short and long words. Differences in short sequences are more significant than in long sequences.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

Therefore, the metric's value must depend not only on the number of basic operations but also on the length of the sequences, allowing for more accurate word comparisons.

Table 3

Levenshtein distance and Jaro-Winkler Metric Comparison

COMPARABLE STRINGS	LEVENSHTEIN DISTANCE	JARO-WINKLER METRIC
КОЖУХ – КОЖУХА	1	0.966
САЙЛЕНТЬЛОК – САЙЛЕНТЬЛОКА	1	0.983
КОЖУХ – КОЛЕСА	4	0.577
САЙЛЕНТЬЛОК – САЙЛЕНТЬЛОКІВ	4	0.951

The Levenshtein metric erroneously yields equivalent distances for the latter two comparisons, which stands in contradiction to the substantial dissimilarity in the lengths of the respective sequences. In stark contrast, the Jaro-Winkler metric aptly delineates the similarities among pairs 1, 2, and 4 while appropriately highlighting the substantial dissimilarity within pair 3.

Lemmatization

Given that we are working with Ukrainian and Russian languages, which have a vast number of word forms, and the unavailability of as sophisticated NLP libraries as for English, we implemented lemmatization independently using electronic dictionaries.

The construction of dictionaries mapping word forms to their lemmas is performed by extracting data from electronic Ukrainian and Russian language dictionaries. During extraction, dictionaries of correspondences for specific word forms to certain lemma are created (for some word forms, multiple lemmas may exist). An inverse dictionary, mapping lemma to word forms, is also generated. Subsequently, for word forms with multiple corresponding lemmas, we choose a single lemma (usually the most frequently occurring one, or in the case of equal occurrences, the first in the list). Word forms corresponding to all other lemmas are attributed to the chosen lemma. Although this approach may result in minor drawbacks when one word form belongs to different parts of speech (e.g., adjectives and nouns in our case), such situations are rare. This approach is preferred to a scenario in which some inflections are lemmatized into one lemma while others into a different one. After completing these steps, we establish a definitive dictionary of correspondences between noun cases and lemmas for use in preprocessing.

Additionally, during lemmatization, another correspondence dictionary mapping Russian lemmas to their Ukrainian counterparts is generated. To achieve this, we traverse the Russian-Ukrainian translation dictionary, searching for lemmas from the form-lemma dictionary described earlier for each pair of words. If lemmas are found for both words, and they are not identical, these lemmas are added to the lemma translation dictionary. Table 5 presents a systematic exposition of the sequential evolution of the initial text as it undergoes the procedures of text cleansing, preprocessing, and lemmatization.

Separation Of Common Prefixes In Compound Words

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

Prefixes such as "електро" (electro), "пневмо" (pneumo), "авто" (auto), and others, are separated from tokens to standardize different spellings (both combined and separate) of such words. This also enables the linkage of names containing suffixes of compound words written with and without such prefixes (e.g., "пневмонасос" (pneumopump) – which transforms to "пневмо насос" (pneumo pump) - and "насос" (pump) will be treated as similar tokens; otherwise, these two tokens would have been considered entirely different).

Deciphering Abbreviations

We created a file containing common word abbreviations / acronyms and their corresponding expansions. Abbreviations (including those with slashes and hyphens) were manually identified from a large dataset of job names. During preprocessing, tokens representing abbreviations are replaced with their expanded versions.

Synonyms

This is the specific aspect of the Ukrainian language – existence of “Surzhyk” (blending of Ukrainian and Russian words) and the abundance of synonyms.

We compiled a file containing synonyms for words and word combinations. Synonyms were identified during data processing (including during the creation of translation dictionaries from a list of all encountered translations). Some synonyms were also added based on logical considerations.

All synonym words are unified into a single form.

Vocabulary Size Reduction

As previously noted, the final token vocabulary size plays a pivotal role in determining the computational time and machine learning burden incurred in subsequent stages of the pipeline. Consequently, every step we undertake should exhibit a significant reduction in the volume of tokens.

Table 4 illustrates the outcomes of the algorithm when applied to a dataset comprising 10,288 initial sentences. When commencing with an initial count of 6,062 unique tokens, a sequence of preprocessing steps – including normalization, spell-checking, token disassembly, removal of stop-words, translation, lemmatization, and more – results in a reduction to 2,484 tokens, signifying a remarkable 59% decrease in the original vocabulary size. It is worth noting that since computational time exhibits exponential growth in relation to vocabulary size, this 59% reduction in vocabulary size translates to an impressive 84% reduction in both computational time and computational load.

Table 4

Step-by-step Vocabulary Size Reduction

STEP	STAGE	NR. OF TOKENS
1	Initial number of unique tokens	6 062
2	After normalization	4 847
3	Before lemmatization (after normalization, spell-checking, disassembling con-catenated tokens, stop-words, translation)	3 991
4	After lemmatization	2 484

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

4. Model selection

The three simplest yet most popular algorithms for text data classification are Naive Bayes, k-Nearest Neighbors (kNN), and Logistic Regression [21]. Each of these algorithms possesses a unique set of strengths and weaknesses, especially when applied to Natural Language Processing (NLP) tasks.

Naive Bayes

Naive Bayes is an algorithm based on Bayes' theorem with the assumption of independence among input features. The probability that a text with given features belongs to specific class is calculated using the Bayes' formula [29].

The algorithm advantages include simplicity, efficiency, and the ability to compute multiple classes simultaneously. It is straightforward to understand and implement, performs reliably even with small training datasets (if the independence assumption holds), and is suitable for large datasets. However, the independence assumption often fails in real-world NLP tasks where words are contextually dependent.

k-Nearest Neighbors (kNN)

The kNN is one of the simplest yet effective classification algorithms. Its essence lies in calculating the distance from a given object to all others, with the object being classified as belonging to the most frequent class among its k neighbors. This method advantages include that it requires no training, making kNN a lazy learning algorithm. It can handle nonlinear data and easily adapts to various types of NLP tasks. However, kNN fully exhibits the curse of dimensionality in high-dimensional spaces, where distances between points become less meaningful. Moreover, its speed drastically decreases as the dataset size grows, and the algorithm performs poorly with noisy data.

Logistic Regression

This classification algorithm is based on the logistic function [30]. The logistic or sigmoid function, which is S-shaped, transforms the linear combination of input parameters into a probability in the interval from 0 to 1.

Unlike classical regression, logistic regression is used not for prediction tasks but for classification and probability estimation. In addition to calculating probabilities that can be useful in estimating the classification results confidence, logistic regression advantages include easy scaling to large datasets and the possibility of regularization to avoid overfitting. On the other hand, logistic regression operates under the assumption of a linear relationship between input parameters, which mainly is far from true in NLP tasks. Moreover, it does not determine the importance of features as effectively as tree-based models. In the practical resolution of our task, the k-Nearest Neighbors (kNN) algorithm was selected for the works classification. Regrettably, none of the implemented algorithms demonstrated adequate accuracy in classifying parts. The highest recorded accuracy was 81.55%, achieved by the kNN algorithm. This outcome necessitated the development, training, and evaluation of a bespoke algorithm tailored to the tree-like architecture of the input data.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

5. Classification

Works Classification

Considering the fact that the works directory is relatively small, with each record consisting of 1-2 words (during preprocessing 180 initial rows / 358 initial tokens are transformed into 166 tokens), a slightly modified k-Nearest Neighbors (kNN) algorithm demonstrates good results. This algorithm does not have a training phase, so it belongs to lazy algorithms. Instead of training, works directory initialization is provided, which becomes a set of classes. Initialization includes two steps:

1. Synonyms are added to each class name based on input data processing (during review, markup, classification error analysis).
2. Key words are found for each name (initial and synonyms). Key words are those with minimal document frequency (DF) values in the corpus of all class names. In other words, these are words that occur least frequently among all others (usually only once).

The modified algorithm consists of the following steps:

- During classification, a list of preprocessed text strings of work names from the online GMS is input.
- All text strings are transformed by a vectorizer into binary vectors set (1 - token present in the string, 0 - token absent).
- The classifier finds the distances between the input names vectors and the nearest vectors of work class names using cosine similarity metric.
- For each of the nearest work classes, an additional check is made to see if there is a match by keyword; if not, the option is discarded.
- Among the classes with the minimum distance, the one whose token is closest to the beginning of the input name is selected.

Cosine similarity was chosen because it is a widely used similarity measure for real-valued vectors, which is especially important for parts classification. Additionally, cosine has the nice property that it is 1.0 for identical and 0.0 for orthogonal vectors [31]. The cosine similarity [32] between vectors A and B is calculated by the formula (4):

$$S_c(A, B) = \cos(\theta) = \frac{AB}{\|A\|\|B\|} = \frac{\sum_{i=1}^n A_i B_i}{\sqrt{\sum_{i=1}^n A_i^2} \sqrt{\sum_{i=1}^n B_i^2}} \quad (4)$$

At the algorithm end, tokens corresponding to the selected master-work class name are removed from the input name to leave only tokens corresponding to the spare part name. The method returns a list of pairs ID – work name corresponding to the input names list, as well as a list of cleaned input names for further parts classification.

Parts Classes And Training Sets Vectorization

The parts catalog is significantly more complex than the master-works directory and encompasses approximately 1,600 entries across all levels. Unlike in works,

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

where we did not engage with a tree-like directory structure, the tree plays a crucial role in the parts classification.

In preparation for training and classification, a class vectors tree is constructed. The foundation for this is the parts directory, wherein each tree vertex undergoes the following stages.

Child nodes initialization, "full names" construction

For each node, a set of names is constructed, which includes both the parent's and all the child names – the so-called "full name" (5):

$$full_name = [node's\ own\ name] + [own\ name + full_name\ of\ every\ child\ node] \quad (5)$$

Classes tree vectorization

The classes tree nodes vectorization occurs through the TF-IDF method use, widely employed in text classification. TF (Term Frequency) represents the ratio of the number of occurrences of a chosen word to the total word count of the document, indicating the word's importance within the document. IDF (Inverse Document Frequency) inversely quantifies the frequency with which a word appears across a collection of documents. Utilizing IDF diminishes the weight of commonly used words. The TF-IDF metric [17] is calculated using the formula (6-8):

$$TF - IDF = TF \times IDF \quad (6)$$

$$TF(t, d) = \frac{f_{t,d}}{\sum_{t' \in d} f_{t',d}}, \quad (7)$$

where: $f_{t,d}$ – raw count of a term t in document d

$\sum_{t' \in d} f_{t',d}$ – number of words in document d

$$IDF(t, D) = \log \frac{N}{|\{d \in D : t \in d\}|}, \quad (8)$$

where: N – total number of documents in the corpus, $N = |D|$

$|\{d \in D : t \in d\}|$ – number of documents, where term t appears, i.e. $TF(t, d) \neq 0$

For each node in the class tree, a unique matrix is constructed. The matrix rows represent the corresponding TF-IDF values of each token from the child nodes of the given node. Herein, the text for TF calculation is the full name of the parent node, while the corpus for IDF calculation consists of the child nodes full names set. Tokens are considered to be unigrams, direct and inverted bigrams – as the simplest options for the augmented dataset.

Selecting keywords and super keywords

Subsequent steps involve selecting keywords and super keywords. During the training, these receive additional weight, significantly aiding in classification accuracy.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

Keywords are identified based on the document frequency values of tokens in each of the child names. Keywords are those with a DF value of 1, meaning they occur in only one of the neighboring child classes.

If a node's name consists of only two words, it automatically becomes a super keyword, receiving even greater weight.

Training data vectorization

At this stage, for each input training string, a matrix is created using the same algorithm as for the class vectorizer.

The matrix rows are the corresponding TF-IDF values of the input string on the specific class node text corpus.

The augmented dataset set is created by tokenizing not only unigrams and bigrams but also bigram permutations. Such input string tokens bigram enrich the feature sets, as different word orders can have the same meaning but be found in different classes. For example, from "brake pads and discs," bigram permutations like "brake pads," "brake discs," "pads brake," "discs brake," "pads discs," "discs pads" are formed.

Now, everything is prepared for initiating the training process.

Parts classification algorithm

Prior to commencing the model training, let us examine the classification algorithm itself. If the model construction occurred in a bottom-up fashion, with each parent node encompassing information about all its children, the classification process unfolds in a top-down manner. Initially, an appropriate class at the tree first level is selected, followed by selection among child nodes at the second level, and so forth. The classification foundation rests on finding the node with the nearest vector. The vectors compared are the weighted rows of the class node matrix and the corresponding input string matrix row. It is reminded that the rows of the class node matrix correspond to the weighted TF-IDF values of tokens from child nodes. Hence, the nearest row in the matrix corresponds to a specific child node, which will determine the next step in the classification. Similar to the works classification, the distance between vectors is determined using cosine similarity. This metric's capability to work with real numbers becomes particularly useful here. Moreover, the value calculated through cosine similarity can be interpreted as the probability of classifying the input string into that specific class, enabling a confidence score computation. The confidence score is calculated as the ratio between the most likely class probability, chosen as the classification result, and that of the second most probable class. If the second class probability is 0, meaning no matches were found in any of the child classes and they are all zeros, or a match was found only in one class and all others are zeros, then a confidence is assigned an arbitrarily high value, for example, 1000.

6. Model training

Our prior chapter delineated the comprehensive process of hierarchical classification for automotive works and parts. However, constraints on space precluded detailed discussions of the training and evaluation processes, despite their

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

critical importance in the classification algorithm, which significantly enhanced the classification accuracy.

Additionally, the confidence scores computation and optimization were not thoroughly examined. Given that 99% of our data was unlabeled, the confidence issue was especially pivotal in our study.

This paper addresses these omissions by providing a detailed training and scoring processes exposition in the subsequent two chapters.

Following the tree construction and the initialization of the vectorizer and classifier for each node, a parameter tuning method for the tree is initiated, which in turn launches, in several threads, the parameter tuning method within each node, acting as potential sub-classifiers of our tree.

Prior to the parameter tuning iterations commencement, several preparatory steps are undertaken:

1. A training dataset is initialized, upon which each parameter values set will be evaluated at each iteration. This set includes input data – vectorized names from the sets comprising the full name of child nodes, as well as additional manually annotated names (which are given greater weight), and the output data – the corresponding child nodes and annotations classes.

2. An initial parameter values set at the node is evaluated. The evaluation function launches a one-step training data classification on the node classifier and checks the accuracy percentage of the resulting classes against the true class values.

The training occurs through the weights (parameters) optimization for the node's matrix tokens in the class tree, as well as weights (parameters) for the input (training) vector.

Initially, all class node matrix elements are assigned preliminary weights according to the following rules:

- Super keyword – 5.0, keyword – 2.5
- Direct child tokens – 2.0 (direct descendants tokens are given more attention than those of further descendants)
- Bigrams – 1.5,
- The first token in the name – 1.5
- Adjectives – 0.5
- Others – 1.0

The exact values for parameters during initialization are not critically important. What matters is that they are greater than 1 or less than 1, and subsequently, the iterative training algorithm will determine the optimal weights.

As with the matrices for class tree nodes, initial weights are determined for the input strings matrices. However, different rules apply here:

- Bigrams – 1.5
- The first token in the name – 1.5
- Tokens created from words in parentheses – 0.5
- Bigrams created from words on the edge of parentheses from both sides –

0.0

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

Parameter tuning iterative cycle then commences. If it does not conclude within 20 iterations, it halts at the last result. At each iteration, a parameter tuning step is performed:

1. For each parameter, its values are iterated from a possible values predefined set (for example, for most weights >1 , parameters from 1 to 10 are iterated in steps of $+0.5$, and for weights < 1 , parameters from 1 to 0 in steps of -0.05).

2. As we are changing parameter values, for each of the training rows, a re-initialization of the weighting parameters is pre-launched, as well as a re-vectorization of the input names (if the value of a parameter related to input vectorization was changed) or a re-initialization of the classifier (if parameters based on which the classifier vectors are built were changed).

3. These values are then evaluated on the training data – through classification and calculating Accuracy – the matches percentage between found and real classes.

4. The parameter and its value that achieve the maximum classification accuracy rating are selected.

5. A check for value update is performed.

- If a change in parameter value led to an increase in accuracy compared to the previous iteration, or accuracy remained the same but the parameter value became closer to 1 – update the node parameter values and proceed to the next iteration;

- If the parameter values iteration did not find a better value for any of the parameters – stop the cycle.

After completing the parameter tuning method on all nodes, the tree can be considered "trained" and used for further classification.

7. Unified confidence score for labeled and unlabeled data

Following classification, a pertinent question remains: how confident are we in its correctness? This is particularly relevant for unlabeled data, as well as for automated decision-making systems.

As noted, the classification result provides us with a classes set along with their probabilities, and confidence scores for each node of the tree. The challenge arises in how to accurately interpret multiple confidence scores. Simple dimensionality reduction methods, such as arithmetic mean or root mean square, which might intuitively be considered, lose crucial information from the tree structure.

In other words, is it better to have confidence closer to the tree's roots or its leaves? Which set provides greater overall confidence, (1000, 0.1, 0.1) or (0.1, 0.1, 1000)? If we were classifying city names, moving through the tree from country to state/region to city, then the set (1000, 0.1, 0.1) would imply high confidence in the country but not in the specific city, whereas (0.1, 0.1, 1000) indicates that we correctly identified Odesa, but it's unclear where exactly – in Ukraine or Texas.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

To address this issue, labeled data from the training set are used, on which traditional machine learning is conducted based on three confidence parameters using standard algorithms from the powerful Python library Scikit[33].

In our case, the machine learning process consisted of the following stages.

Parameters Engineering

In many machine learning algorithms, transforming input values is a necessary condition without which the algorithm won't converge to an optimal result due to excessively extreme input values or too significant difference between feature magnitudes. Moreover, most machine learning models train better and faster on as standardized data as possible.

- Clipping is performed (values less than a set minimum become the minimum, and those greater than a set maximum become the maximum) within a range from $\text{min}=0.000001$ to $\text{max}=1000$, to eliminate zero values and the most significant outliers over 1000.

- To capture not only linear dependencies between input parameters and the predicted value but also potential nonlinear input data behaviors, as well as to account for interactions between different input parameters, polynomial parameters up to degree 3 are generated. For example, from input parameters x_1, x_2, x_3 , polynomial parameters $x_1, x_1^2, x_1^3, x_1x_2, x_1x_3, x_1^2x_2, x_1^2x_3, x_1x_2x_3, x_2, x_2^2, x_2^2x_1$, etc., are formed.

- Logarithmic transformation of polynomial parameters is conducted to reduce the distribution positive skewness, where most values are relatively close to 0, but some highest values reach up to 109, thereby having a long "tail" to the right, and to bring them to values closer to each other and closer to 0.

- Values are standardized using a scaler. Typically, values are scaled relative to the mean and variance. In our case, RobustScaler from Scikit was chosen as the scaler, which is more resistant to outliers and uses the median and interquartile range instead of the usual mean and variance.

Training

GradientBoostingClassifier [34] was chosen as the classifier, which conducts classification based on boosted trees [35].

In practical applications, effectively deploying the GradientBoostingClassifier necessitates the careful adjustment of its hyperparameters, which play a critical role in shaping the model's accuracy and efficiency. This adjustment process typically involves empirical optimization, where methods such as grid search or random search are frequently employed to identify the most suitable hyperparameter settings.

The hyperparameters selected were:

- `n_estimators` – the simple models number (decision trees) that make up the ensemble
- `learning_rate` – the value that indicates how significant the contribution of each model in the ensemble is to the overall result
- `max_depth` – the maximum depth of the decision trees in the model
- `max_features` – the maximum number of features considered during the tree nodes splits

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

- `min_samples_split` – the minimum number of data points in a node (node samples) required to split a node
- `subsample` – the fraction of data (among all training data) taken for training each of the simple trees

Hyperparameter tuning was performed using GridSearch, i.e., trying all possible parameters combinations among given values sets with cross-validation.

The hyperparameters quality was assessed using BrierScoreLoss, which shows the average squared difference between the predicted class probability (value `pred_proba` of the model GradientBoostingClassifier, from 0 to 1, corresponding to how confident the model is that the outcome to which the obtained uncertainty scores correspond is correct) and the true accuracy (0 or 1, depending on the correctness of the classification on training data).

Classification

The GradientBoostingClassifier from the Scikit library is a robust classification algorithm for machine learning tasks, based on the boosting technique. Boosting is an ensemble method that constructs a series of models sequentially, with each subsequent model aiming to correct its predecessors' errors.

Initially, a decision tree model is created, typically a simple one. This model is imperfect, with accuracy slightly better than a random choice. The first step is not crucial; the iterative process is expected to significantly enhance it.

Next, a loss function is determined to evaluate the model's effectiveness. In this case, the function measures the discrepancy between predicted probabilities and actual class labels, specifically the deviation loss between them.

Gradient boosting methodically enhances the model. At each new step, new models are created to rectify the existing ensemble deficiencies:

- The loss function gradient based on the current model predictions is calculated. This gradient indicates the direction in which predictions should be altered to reduce loss.
- A new decision tree is trained to forecast these gradients for each item in the training set. This tree aims to predict the previous model errors.
- This new decision tree is added to the ensemble with a coefficient known as the learning rate. This coefficient controls the speed at which the model learns. The learning rate is a critically important hyperparameter in gradient boosting. It assesses and scales each tree contribution. If it is too high, the model may overfit; if too low, the model may require too many trees to converge to a satisfactory solution.
- The algorithm continues to add trees until the specified number of trees (`n_estimators`) is reached or until no further improvement can be made on the training set.

Boosted trees are prone to overfitting. Therefore, several regularization techniques are integrated into the GradientBoostingClassifier:

- Limiting the depth of trees with `max_depth`
- A fraction of the training data (`subsample`) is randomly selected to train each tree. This randomness enhances the model robustness.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

– Learning rate reduction – the `learning_rate` parameter scales the contribution of each tree, lowering the overfitting risk by diminishing the updates.

The data obtained after training allow for calculating a single confidence score for unlabeled data. The obtained confidence scores can be sorted from top to bottom. In doing so, homogenous names will have the same score and be located nearby, which is convenient for verifying the classification correctness. If the result is correct/incorrect for one name, it will be the same for all similar names. This allows for creating new classes or optimizing the algorithm immediately for a large number of input data. Table 5 shows the top and bottom five results of the parts classification, confidence scores by tree levels, and the final unified confidence.

Table 5

Top and bottom five parts classification results

TESTING DATA SAMPLE	LABEL ED	PREDIC T.	RES.	CONFIDENCE BY LEVELS			
				L-1	L-2	L-3	Unif.
заміна зовн. ручки і приводу замка чи двері	2011300	2011300	True	36	119	97	99.9%
зняття і установка консолі склоочисника	1200500	1200500	True	66	146	73	99.8%
замена сцепного шкворня	1050900	1050900	True	31	670	100	99.8%
установка обігрівального елемента сидіння	2030200	2030200	True	21	1,169	100	99.8%
зняття та встановлення маховика інерційн.	1080300	1080300	True	100	198	100	99.8%
...
заміна газонаповнених амортизат. капота	2010300	2011100	False	2	18	3	7.5%
ремонт клапана привода передній двері	2011300	1140400	False	6	5	15	5.5%
ремонт пжд	1160900	1120000	False	156	1	1	5.3%
замена клапана моторного тормоза	1031600	1140400	False	376	4	17	4.4%
перевірка клапана моторного тормоза	1031600	1140400	False	376	4	17	4.4%

8. Results achieved and conclusions

Based on proposed approach, a function library in Python was developed. The brief classification times – up to 125 ms for a single row and up to 56 seconds for eleven thousand rows – permit the use of the algorithm in an online mode for wide variety of problems. Accelerations by more than an order of magnitude are achieved

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

for data comprising thousands of rows, thanks to powerful Python algorithms optimized for working with large matrices. The library we developed is also optimized for rapid computation of large data arrays and utilizes all built-in Python optimization techniques. The classification accuracy varied across different datasets from 85% to 98% for works and from 87% to 96% for parts names. As shown in Table 6, the overall classification accuracy of the proposed algorithm nearly doubled after training, reaching 92.38%. The classification of works related to mechanical parts was most effective, while the classification of specialized tasks, such as transmission repair or truck repair works, was less accurate. The partial attribution of this variability to the incomplete directories for certain tasks points towards an potential enhancement area through the expansion and refinement of class directories. One of the significant ancillary benefits observed from our algorithm implementation is the missing terms identification that necessitate inclusion in the directories, thereby improving comprehensiveness and the classification system accuracy. This outcome also contributes valuable insights for domain-specific knowledge bases.

Table 5

Top and bottom five parts classification results

TESTING DATA SAMPLE	LABEL ED	PREDIC T.	RES.	CONFIDENCE BY LEVELS			
				L-1	L-2	L-3	Unif.
заміна зовн. ручки і приводу замка чи двері	2011300	2011300	True	36	119	97	99.9%
зняття і установка консолі склоочисника	1200500	1200500	True	66	146	73	99.8%
замена сцепного шкворня	1050900	1050900	True	31	670	100	99.8%
установка обігрівального елементу сидіння	2030200	2030200	True	21	1,16 9	100	99.8%
зняття та встановлення маховика інерційн.	1080300	1080300	True	100	198	100	99.8%
...
заміна газонаповнених амортизатор. капота	2010300	2011100	False	2	18	3	7.5%
ремонт клапана привода передньої двері	2011300	1140400	False	6	5	15	5.5%
ремонт пжд	1160900	1120000	False	156	1	1	5.3%
замена клапана моторного тормоза	1031600	1140400	False	376	4	17	4.4%
перевірка клапана моторного тормоза	1031600	1140400	False	376	4	17	4.4%

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

The research presented in this paper has successfully demonstrated the application of tree-based classification methodologies to the domain of Ukrainian technical text analysis, specifically focusing on the automotive industry.

Through the development of a Python function library, we have showcased our proposed approach capability to efficiently classify technical texts related to automotive repairs and parts, achieving classification times that support real-time application scenarios. This efficiency opens the algorithm up for a wide array of practical uses, from enhancing the call centers operational quality to the creation of automated chatbots and digital assistants for service advisors in automotive service stations.

In conclusion, the research underscores the profound potential of tree-based classification in navigating the complexities of technical text analysis within the automotive sector. By bridging the gap between structured data classification and the nuanced realm of natural language processing, we pave the way for advanced applications that could significantly impact various stakeholders, including insurance companies, automobile manufacturers, and vehicle owners as shown on Figure 3.



Figure 3. Practical implementation of automotive works and parts accurate classification

The ability to accurately predict maintenance costs and reliability of vehicle components from aggregated, labeled big data represents a substantial stride towards

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

demystifying the vehicle ownership total cost, thereby empowering consumers and industry players alike with valuable, actionable insights.

From the perspective of automotive manufacturers, this approach could substantially impact vehicle design, component reliability and safety, production processes, and warranty policies. Insurance companies may benefit from precise repair cost calculations and accurate assessments of residual vehicle value, leading to reduced expenses.

Automotive repair shops can enhance their services by implementing automated chatbots and digital assistants for service managers. Additionally, car owners will be able to determine not only the purchase price of a vehicle but also the total cost of ownership for specific model.

Table 6
Parts names classification results

MODEL TYPE	VECTORIZATION	ACCURACY, TRAINING DATA	ACCURACY, TEST DATA
custom model without weighting and training	count vectors TF-IDF vectors	— —	0.5174 0.6684
main model with weighted parameters after training	Count vectors TF-IDF vectors	0.9365 0.9552	0.9184 0.9238

Looking forward, we aim to extend our research to encompass more complex tasks, such as the extraction, identification, and classification of automotive-related works from extensive text bodies, including transcriptions of telephone calls.

9. References

- [1] Zhang, Z., Guo, K., Pan, G.: Improvement of phylogenetic method to analyze compositional heterogeneity. *BMC Syst Biol* 11 (Suppl 4), 79 (2017).
- [2] Albadri, N., Dekeyser, S.: A novel file system supporting rich file classification. *Computers and Electrical Engineering*, vol. 103 (2022)
- [3] Kim, SW., Gil, JM.: Research paper classification systems based on TF-IDF and LDA schemes. *Hum. Cent. Comput. Inf. Sci.* 9, 30 (2019)
- [4] Quinlan, J.R.: *C4.5: Programs for Machine Learning*. Morgan Kaufmann Publishers, Inc. (1993)
- [5] Breiman, L.: Random Forests. *Machine Learning* 45, pp. 5–32 (2001)
- [6] Friedman, J.H.: Greedy function approximation: A gradient boosting machine. *Ann. Statist.* 29 (5), pp. 1189 - 1232 (2001)
- [7] Aggarwal, C.C., Reddy, C.K.: *Data Clustering: Algorithms and Applications*. Chapman and Hall/CRC (2013)
- [8] Bauskar, S., Badole, V., Jain, P., Chawla, M.: Natural Language Processing based Hybrid Model for Detecting Fake News Using Content-Based Features and Social Features. *International Journal of Information Engineering and Electronic Business (IJIEEB)*, vol.11, No.4, pp. 1-10 (2019).

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

- [9] Gupta, A., Kaur, M., Bajaj, A., Khanna, A.: Entailment and Spectral Clustering based Single and Multiple Document Summarization. *International Journal of Intelligent Systems and Applications (IJISA)*, Vol.11, No.4, pp.39-51 (2019)
- [10] Parsafard, P., Veisi, H., Aflaki, N., Mirzaei, S.: Text Classification based on Discriminative-Semantic Features and Variance of Fuzzy Similarity. *International Journal of Intelligent Systems and Applications (IJISA)*, Vol.14, No.2, pp.26-39 (2022)
- [11] Trivedi, H., Panahiazar, M., Liang, A., Lituiev, D., Chang, P., Sohn, J., Chen, Y., Franc, B., Joe, B. & Hadley, D. “Large scale semi-automated labeling of routine free-text clinical records for deep learning”. *Journal of Digital Imaging*. 2018. [Scopus]. DOI: <https://doi.org/10.1007/s10278-018-0105-8>.
- [12] Nguyen, H. & Patrick, J. “Text mining in clinical domain: dealing with noise “KDD '16: Proceedings of the 22nd ACM SIGKDD.” *International Conference on Knowledge Discovery and Data Mining*. August 2016. p. 549–558. DOI: <https://doi.org/10.1145/2939672.2939720>.
- [13] Arenas, M., Botoeva, E., Kostylev, E. & Ryzhikov, V. “A note on computing certain answers to queries over incomplete databases”. In: *CEUR Workshop Proceedings. Proceedings of the 11th Alberto Mendelzon International Workshop on Foundations of Data Management and the Web*. Montevideo: Uruguay. 2017.
- [14] Li, Y., Currim, F. & Ram, S. “Data completeness and complex semantics in conceptual modeling”. *The Need for a Disaggregation Construct. Journal of Data and Information Quality*. 2022; 14 (4), Article No. 22: 1–21. [Scopus]. DOI: <https://doi.org/10.1145/3532784>.
- [15] Sebastian, M. P., & G, S. K. “Malayalam natural language processing: challenges in building a phrase-based statistical machine translation system”. *ACM Transactions on Asian and Low-Resource Language Information Processing*. 2022; 22 (4), Article No. 117: 1–51. [Scopus]. DOI: <https://doi.org/10.1145/3579163>.
- [16] Butnaru, A.-M. “Machine learning applied in natural language processing”. *ACM SIGIR Forum* . June 2020; 54 (1), Article No. 15: 1–3. DOI: <https://doi.org/10.1145/3451964.3451979>.
- [17] Vajjala, S., Majumder, B., Gupta, A. & Surana, H. “Practical natural language processing: A comprehensive guide to building real-world NLP systems”. Published by O'Reilly Media, Inc. 2020.
- [18] Mashtalir, S., Nikolenko, O., “Data preprocessing and tokenization techniques for technical Ukrainian texts”, *Applied Aspects of Information Technology*. Vol. 6 No. 3 (2023), 318-326. doi: 10.15276/aait.06.2023.22
- [19] Mashtalir, S., Nikolenko, O., “Advancing Automotive Technical Text Analysis: A Tree-Based Classification Approach for Ukrainian Texts”, *ICCSEEA2024* (2024), in press.
- [20] Mashtalir, S., Nikolenko, O., “Optimizing Hierarchical Classifiers with Parameter Tuning and Confidence Scoring”, *Applied Aspects of Information Technology*, in press.
- [21] Jurafsky, D. & Martin, J. “Speech and language processing”. Third Edition draft. 2018. – Available from: https://web.stanford.edu/~jurafsky/slp3/ed3book_jan72023.pdf.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

- [22] Cielen, D., Meysman, A., Ali, M.: *Introducing Data Science: Big Data, Machine Learning, and more, using Python tools*. Manning Publications (2016)
- [23] Mohammad, A. “Using Blockchain for Data Collection in the Automotive Industry Sector: A Literature Review”. *Journal of Cybersecurity and Privacy*. 2022. 2 (2). DOI: 10.3390/jcp2020014
- [24] Danielkiewicz, R. & Dzieńkowski, M. “Analysis of user experience during interaction with automotive repair workshop websites”. *Journal of Computer Sciences Institute*. 2024. Vol. 30: 39-46. DOI: 10.35784/jcsi.5416
- [25] Hemphill, T., Longstreet, P. & Banerjee, S. “Automotive repairs, data accessibility, and privacy and security challenges: A stakeholder analysis and proposed policy solutions”. *Technology in Society*. 2022. Vol. 71(3). DOI: 10.1016/j.techsoc.2022.102090
- [26] Winkler, W. E. “String Comparator Metrics and Enhanced Decision Rules in the Fellegi-Sunter Model of Record Linkage”. *Proceedings of the Section on Survey Research Methods*. American Statistical Association. 1990. p. 354–359. – Available from: <https://files.eric.ed.gov/fulltext/ED325505.pdf>.
- [27] Cohen, W. W., Ravikumar, P. & Fienberg, S. E. “A comparison of string distance metrics for name-matching tasks (PDF)”. *KDD Workshop on Data Cleaning and Object Consolidation*. 2003; 3: 73–78. – Available from: <https://www.cs.cmu.edu/afs/cs/Web/People/wcohen/postscript/kdd-2003-match-ws.pdf>.
- [28] Levenshtein, V. I. “Binary codes capable of correcting deletions, insertions, and reversals”. *Cybernetics and Control Theory*. 1966; 10 (8): 707–710.
- [29] Hand, D.J., Yu, K.: *Idiot's Bayes – not so stupid after all?*. *International Statistical Review*. Vol 69 part 3, pp. 385 - 399 (2001)
- [30] Hosmer, D. W., Lemeshow, S.: *Applied Logistic Regression*. 2nd edn. John Wiley & Sons, Inc. (2000)
- [31] Singhal, A.: *Modern Information Retrieval: A Brief Overview*. *Bulletin of the IEEE Computer Society Technical Committee on Data Engineering* 24 (4), pp. 35–43 (2001)
- [32] Tan, P.-N., Steinbach, M., Kumar, V.: *Introduction to Data Mining*. Addison-Wesley (2005)
- [33] Müller, A. & Guido, S. “*Introduction to Machine Learning with Python: A Guide for Data Scientists*”. 1st ed. Published by O'Reilly Media. 2016.
- [34] Géron, A. “*Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems*”. 3rd ed. Published by O'Reilly Media. 2022.
- [35] Bastos, J. “Predicting Credit Scores with Boosted Decision Trees”. *Forecasting*, 2022. Vol. 4(4): 925-935. DOI: 10.3390/forecast4040050

**ІЄРАРХІЧНА КЛАСИФІКАЦІЯ УКРАЇНСЬКИХ ТЕХНІЧНИХ
ТЕКСТІВ ЗА ДОПОМОГОЮ ДЕРЕВОВИДНИХ МОДЕЛЕЙ:
ЗАСТОСУВАННЯ В АВТОМОБІЛЬНІЙ ПРОМИСЛОВОСТІ**

С. Машталір ORCID: 0000-0002-0917-6622

Харківський національний університет радіоелектроніки

E-mail: sergii.mashtalir@nure.ua

О. Ніколенко ORCID: 0000-0002-6422-7824

Ужгородський національний університет

E-mail: oleksandr.nikolenko@uzhnu.edu.ua

Анотація. Ця стаття присвячена ієрархічній класифікації технічних українських текстів, зокрема класифікації ремонтних робіт і запасних частин, які використовуються для технічного обслуговування та обслуговування автомобілів. Ми вирішуємо проблеми, пов'язані з багатомовним введенням даних Розроблен новий алгоритм класифікації, який використовує векторизацію TF-IDF за допомогою уніграм і біграм, вибір ключових слів і косинусну подібність для класифікації. Описано метод навчання та оцінки моделі ієрархічної класифікації з використанням налаштування параметрів для кожного вузла в структурі дерева. Процес навчання передбачає ініціалізацію вагових коефіцієнтів для токенів у вузлах дерева класів і вхідних рядах з подальшим ітеративним налаштуванням параметрів для оптимізації точності класифікації. Початкові ваги призначаються на основі попередньо визначених правил, і ітераційний процес коригує ці ваги для досягнення оптимальної продуктивності. У документі також розглядається проблема інтерпретації кількох оцінок довіри з процесу класифікації, пропонуючи підхід машинного навчання для обчислення уніфікованої оцінки довіри. Ця оцінка допомагає оцінити надійність класифікації, особливо для немаркованих даних, шляхом перетворення вхідних значень, генерації поліноміальних параметрів і використання логарифмічних перетворень і масштабування. Класифікатор налаштовується за допомогою методів оптимізації гіперпараметрів, а остаточна модель забезпечує надійний показник достовірності для завдань класифікації, уможливаючи перевірку та оптимізацію результатів класифікації для великих наборів даних. Експериментальні результати демонструють покращення ефективності класифікації. Загальна точність класифікації зросла майже вдвічі після навчання, досягнувши 92,38%. Це дослідження надає практичні рішення для обробки великомасштабних немаркованих наборів даних в автомобільній промисловості. Розроблена методологія може покращити різні додатки, включаючи автоматизовані системи підтримки клієнтів, прогнозне обслуговування та процеси прийняття рішень для зацікавлених сторін, таких як страхові компанії та сервісні центри. Майбутня робота поширить цей підхід на більш складні завдання, такі як вилучення та класифікація інформації з обширних текстових джерел, таких як розшифровка телефонних розмов.

Ключові слова: NLP, деревовидна класифікація, машинне навчання, аналіз даних, прикладні інтелектуальні системи.

Section 3. Modeling and software engineering

UDC 519.711.7:519.816

**PROTECTION OF MULTILAYER NETWORK SYSTEMS FROM
SUCCESSIVE, GROUP AND SYSTEM-WIDE TARGETED
ATTACKS**

Dr.Sci. O. Polishchuk ORCID: 0000-0002-0054-7159

*Pidstryhach Institute for Applied Problems of Mechanics and Mathematics, National
Academy of Sciences of Ukraine, Ukraine*

E-mail: od_polishchuk@ukr.net

***Abstract.** Structural and flow approaches to the vulnerability analysis of multilayer network systems (MLNS) from targeted attacks and non-target lesions of various origins are considered. Local and global structural and flow characteristics of monoflow multilayer system elements are determined to build scenarios of targeted attacks on the structure and operation process of MLNS and evaluation their consequences. In order to simplify the construction and improve the efficiency of such scenarios, the concepts of structural and flow aggregate-networks of monoflow MLNS are introduced, and the relationship between the importance indicators of their elements and corresponding indicators of multilayer system nodes is shown. The advantages of flow-based approach over structural ones have been demonstrated, both in the sense of analyzing the vulnerability of real MLNS and evaluation the consequences of negative influences of different nature.*

***Keywords:** Complex network, network system, intersystem interactions, multilayer network system, flow model, aggregate-network, influence, betweenness, targeted attack, vulnerability.*

1. Introduction

Many internal and external negative influences can act on any real-world natural or man-made systems. Among such influences that can damage the system, we primarily highlight targeted attacks and its non-target lesions. A distinctive feature of targeted attacks is their intentionality and artificial nature (terrorist and hacker attacks, military aggression and financial and economic sanctions, etc.). In contrast to targeted attacks, non-target lesions can include various unintentional negative influences of natural or artificial origin (natural and man-made disasters, the spread of dangerous infectious diseases and so on). Such lesions can be local, group or system-wide and aimed at damaging both the structure and operation process of network systems (NS) and intersystem interactions. In paper [1], the typical scenarios of consecutive attacks on the structure and operation process of NS were considered and their connections with the development of countermeasures against the system non-target lesions were established. The usefulness of such scenarios lies in the fact that they, giving a picture of possible development of a certain type of

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

lesion, allow creating the most effective means of protection against it [2, 3]. In particular, the structural and flow NS models make it possible not only to build scenarios of the spread of negative influences of various origins, but also, compared to other system models, evaluate the level of local, group and system-wide losses resulting from the action of such influences during and after lesion [1]. The development of strategies for the protection of multilayer network systems, which describe the processes of intersystem interactions, is significantly complicated not only due to the increase of problem dimension, but also because the lesion of certain layer-system of such formation may not occur directly, for example, through a targeted attack on it, but consequentially as a result of attack on adjacent MLNS's layer [4, 5]. At the same time, lesions of various adjacent layers-systems can lead to different consequences (the influence of blocking the maritime and aviation layers of general transport system of Ukraine during Russian aggression on the railway and automobile layers is significantly different). Simultaneously, the quantity of local and global characteristics of MLNS elements, which describe the structural and functional features of not only internal, but also intersystem interactions, is increasing, and therefore, the amount of importance indicators of elements, which are used when building scenarios of targeted attacks on multilayer system, is increasing too [6]. The process of evaluation the consequences of MLNS lesions is also complicated, in particular, the negative influence of the directly damaged layers-systems on the adjacent ones [7, 8]. All these factors must be taken into account by the NS management systems, which are the part of man-made MLNS, for the effective organization of their protection and overcoming the consequences of various types of lesions. No large scale real-world complex system can protect or simultaneously restore all elements damaged by negative influences. Therefore, the calculation of objective importance indicators of nodes and edges of NS and MLNS plays a decisive role during the construction of effective scenarios of targeted attacks on them [9, 10]. Equally important is the value of these indicators for development the effective strategies for countering the spread of non-target lesions. The purpose of article is to determine on the basis of structural and flow models of intersystem interactions, the importance indicators of MLNS components and formation of effective scenarios of successive group and system-wide targeted attacks on multilayer network systems, as well as evaluation of consequences of separate system components lesions on different system layers and implementation of intersystem interactions in general.

2. A structural model of multilayer network system

The structural model of intersystem interactions is described by multilayer networks (MLNs) and displayed in the form [11]

$$G^M = \left(\bigcup_{m=1}^M G_m, \bigcup_{m,k=1, m \neq k}^M E_{mk} \right),$$

where $G_m = (V_m, E_m)$ determines the structure of m th network layer of MLN; V_m and E_m are the sets of nodes and edges of network G_m respectively; E_{mk} is the

**ADVANCES
IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES**

set of connections between the nodes of V_m and V_k , $m \neq k$, $m, k = \overline{1, M}$, and M is the number of MLN layers. The set $V^M = \bigcup_{m=1}^M V_m$ will be called the total set of MLN nodes, N^M – the number of elements of V^M .

Multilayer network G^M is fully described by an adjacency matrix

$$\mathbf{A}^M = \{\mathbf{A}^{km}\}_{m,k=1}^M, \tag{1}$$

in which the blocks \mathbf{A}^{mm} determine the structure of intralayer and blocks \mathbf{A}^{km} , $m \neq k$, – interlayer interactions. Values $a_{ij}^{km} = 1$ if the edge connected the nodes n_i^k and n_j^m exists, and $a_{ij}^{km} = 0$, $i, j = \overline{1, N^M}$, $m, k = \overline{1, M}$, if such edge don't exists. Blocks $\mathbf{A}^{km} = \{a_{ij}^{km}\}_{i,j=1}^{N^M}$, $m, k = \overline{1, M}$, of matrix AM are determined for the total set of MLN nodes, i.e. the problem of coordination of node numbers is removed in case of their independent numbering for each layer. In this paper, we consider partially overlapped MLN [12], in which connections are possible only between nodes with the same numbers from the total set of nodes V^M (Figure 1).

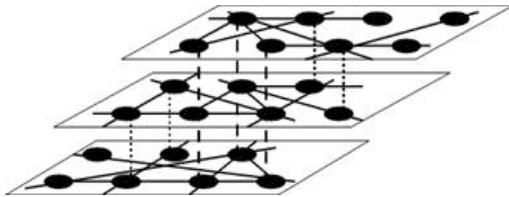


Figure 1. An example of structure of partially overlapped three-layer MLN

This means that each node can be an element of several systems and perform one function in them, but in different ways. Nodes through which interlayer interactions are carried out will be called MLNS transition points.

Multidimensional (multiflow) networks, which describe the structure of interactions between layers, each of which ensures the movement of specific type of flow different from other layers, are considered the most general case of MLN [13]. An example of two-dimensional network is a general transport system that ensures the movement of passenger and cargo flows [1]. A feature of such formations is the impossibility of flow transition from one layer to another (transformation of passengers into cargo and vice versa). Therefore, the characteristics of elements of multidimensional networks are usually described by vectors of these characteristics in each layer (degree, betweenness, closeness, eigenvector centralities and so on [14]). Scenarios of successive targeted attacks on the structure of such multilayer

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

networks are built using precisely these vectors of importance indicators of their elements [4, 6]. In the article [1] was proposed a method of decomposing multidimensional MLNS into monoflow multilayer systems, all layers of which ensure the movement of certain type of flow by different carriers or operator systems (movement of passengers or cargos through four-layer transport networks, which include railway, automobile, aviation and water system layers, respectively). The centrality of elements of monoflow MLNS can be determined not only for separate layers, but also for a multilayer network in general by constructing their aggregate-networks [15]. In addition to reducing the dimensionality of MLNS model by at least M times, the use of such structures makes it possible to solve a number of practically important problems of the theory of complex networks much more effectively [16].

2.1. A structural aggregate-network of multilayer system

The local characteristic \mathcal{E}_{ij} of the edge (n_i, n_j) in MLN, where n_i and n_j are the nodes from the total set of nodes V^M , which will be called its structural aggregate-weight, is the quantity of layers in which this edge is present. Structural aggregate-weight \mathcal{E}_{ii} of the MLN's node n_i is the quantity of layers of which it is a part, $i, j = \overline{1, N^M}$. For arbitrary multilayer network, the adjacency matrix $\mathbf{E} = \{\mathcal{E}_{ij}\}_{i, j=1}^{N^M}$ completely determines the weighted network (Figure 2), which will be called the structural aggregate-network of MLN. Since we are considering the case when interlayer connections are possible only between nodes with the same numbers of total set of MLNS nodes, the structure G_{ag}^M of this aggregate-network can be described in the form

$$G_{ag}^M = (V^M, E^M = \bigcup_{m=1}^M E_m) \quad (2)$$

in which the set E^M will be called the total set of MLN edges.

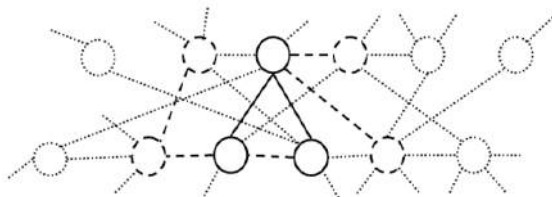


Figure 2. Aggregate-network of reflected in fig. 1 three-layer MLN (——— for $\mathcal{E}_{ij}=3$, - - - - for $\mathcal{E}_{ij}=2$, for $\mathcal{E}_{ij}=1$, $i, j = \overline{1, N^M}$)

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

The elements of matrix E define integral structural characteristics of multilayer network nodes and edges. For multiflow multidimensional networks, the aggregate-weights of edges of weighted aggregate-network determine the quantity of interactions of various types between the nodes of such structures. For monoflow MLNs, the aggregate-weight of each edge reflects the number of possible carriers or operator systems that can ensure the movement of corresponding type of flow. Therefore, the input (output) aggregate-degree of each node of weighted aggregate-network of monoflow MLNS is equal to the sum of input (output) degrees of this node in all its layers.

2.2. Targeted attacks on multilayer systems

We will build a scenario of targeted attack on monoflow multilayer network, using as importance indicator of its nodes the centrality of generalized degree d_i of node n_i in the total set of nodes VM of aggregate-network, i.e.

$$d_i = \sum_{j=1, j \neq i}^{N^M} (\varepsilon_{ij} + \varepsilon_{ji}) + \varepsilon_{ii}, \quad i = \overline{1, N^M} \quad (3)$$

This scenario consists of sequentially executing the following steps:

- 1) create the list of nodes of the set V^M in order of decreasing the values of their generalized degree centrality in aggregate-network;
- 2) delete the first node from created list;
- 3) if criterion of attack success is reached, then finish the execution of scenario, otherwise go to point 4;
- 4) since the structure of aggregate-network changes as a result of removal of node (and its connections), compile a new list of nodes of the set V^M that remained, in order of decreasing recalculated values of their generalized degree centrality, and proceed to point 2.

The criterion of attack success in this case can be division of MLN's aggregate-network into unconnected components, increase the average length of shortest path, etc. [9]. Likewise, similar scenarios can be developed for other types of structural centralities of aggregate-network nodes, including without recalculating the values of these centralities [17]. The last type scenarios are usually used when the system is unable to redistribute the functions of lesioned elements between those that remained undamaged. The main disadvantage of structural importance indicators of network system nodes is their ambiguity, because even D. Krackhardt, using example of fairly simple network, showed [18] that its node, which is important according to the value of one type centrality, may be unimportant according to the value of another type centrality. The most objective importance indicator of a node in MS's structure is its betweenness centrality [17], which is equal to the ratio of quantity of shortest paths passing through this node to the quantity of all shortest paths in the network [19]. However, the calculation of this indicator for networks that have billions of elements, is a rather difficult computational problem.

**ADVANCES
IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES**

2.3. Evaluation of the lesion consequences

In paper [1], it was shown that the structural model of MLNS makes it possible to determine the integral and partially local losses of multilayer network during and after targeted attack or its non-targeted lesion. The criterion of attack success can be not only the quantity of directly damaged (dd), but also quantity of consequentially injured (ci) by this attack MLN elements. The aggregate-network model allows us to identify such elements of multilayer network. Let us denote by $\Omega_{dd}^s = \{n_{i_1}, n_{i_2}, \dots, n_{i_k}\}$ the set of directly damaged (that is destroyed, completely blocked), as a result of attack, nodes of aggregate-network, and through $U(n_{i_l}) = \{n_{i_l}^1, n_{i_l}^2, \dots, n_{i_l}^{m_l}\}$ the set of nodes of this network adjacent to n_{i_l} , $l = \overline{1, k}$. Then the set $\Omega_{ci}^s = \bigcup_{l=1}^k U(n_{i_l})$ determines the group of consequentially injured by lesion of the set Ω_{dd}^s nodes of MLN's aggregate-network. It is obvious that the defeat of a certain group of nodes with the highest generalized degree, which is realized by the above scenario, will lead to maximization of the set of consequentially injured multilayer network nodes, which can serve as the main attack goal.

3. A flow model of multilayer network system

We will use the flow model proposed in the article [1] to determine the indicators of functional importance of monoflow MLNS's elements and build scenarios of successive targeted attacks on operation process of multilayer systems. This choice is explained by the fact that the majority of real-world systems are created precisely to ensure the movement of flows through the relevant networks (transport, financial, trade, energy, information, and so on) or the movement of flows directly ensures their vital activity (the movement of blood, lymph, neuroimpulses in a living organism, etc.). Stopping the movement of flows in such systems inevitably leads to the cessation of their existence. In general, by flow we mean a certain real positive function correlated to each edge of the network. Let us reflect the set of flows that pass through all edges of multilayer system in the form of flow adjacency matrix $VM(t)$, the elements of which are determined by the volumes of flows that passed through the edges of MLN (1) for the period $[t - T, t]$ up to the current moment of time $t \geq T$:

$$V^M(t) = \{V_{ij}^{km}(t)\}_{i,j=1}^N, \quad M, \quad k,m=1, \quad V_{ij}^{km}(t) = \frac{\tilde{V}_{ij}^{km}(t)}{\max_{s,g=1,M} \max_{l,p=1,N^M} \{\tilde{V}_{lp}^{sg}(t)\}}, \quad V_{ij}^{km}(t) \in [0, 1], \quad (4)$$

where $\tilde{V}_{ij}^{km}(t)$ is the volume of flows that passed through the edge (n_i^k, n_j^m) of multilayer network for the time period $[t - T, t]$, $i, j = \overline{1, N^M}$, $k, m = \overline{1, M}$,

**ADVANCES
IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES**

$t \geq T > 0$. It is obvious that structure of matrix $VM(t)$ completely coincides with the structure of matrix AM . The elements of MLNS flow adjacency matrix are determined on the basis of empirical data about movement of flows through MLNS edges. Currently, with the help of modern means of information extraction, such data can be easily obtained for many natural and the vast majority of man-made systems [20]. The matrix $VM(t)$ similarly to AM also has a block structure, in which the diagonal blocks $\mathbf{V}^{mm}(t)$ describe the volumes of intralayer flows in the m th layer, and the off-diagonal blocks $\mathbf{V}^{km}(t)$, $m \neq k$, describe the volumes of flows between the m th and k th layers of MLNS, $m, k = \overline{1, M}$, $t \geq T > 0$.

3.1. Flow aggregate-network of monoflow multilayer system

Let's define the concept of a flow aggregate-network of monoflow partially overlapped MLNS. Since we are considering the case when interlayer connections are possible only between nodes with the same numbers in total set of MLNS nodes, the structure of such aggregate-network can also be described in the form (2). Then the adjacency matrix $\mathbf{F}(t) = \{f_{ij}(t)\}_{i,j=1}^{N^M}$, the elements of which are calculated according to the formulas

$$f_{ij}(t) = \sum_{m=1}^M V_{ij}^{mm}(t), \quad i \neq j, \quad i, j = \overline{1, N^M}, \quad f_{ii}(t) = \sum_{m,k=1, m \neq k}^M V_{ii}^{mk}(t), \quad i = \overline{1, N^M},$$

completely defines a dynamic (in the sense of dependence on time) weighted network, which will be called the flow aggregate-network of this MLNS. The elements of matrix $F(t)$ determine the integral flow characteristics of the edges and transition points of multilayer system, namely, the off-diagonal elements of this matrix are equal to the total volumes of flows passing through the edge (n_i, n_j) , and the diagonal elements are equal to the total volumes of flows passing through the transition point n_i of MLNS during the time period $[t - T, t]$, $t \geq T > 0$, where (n_i, n_j) are the edges from the total set of edges EM , and n_i and n_j , $i, j = \overline{1, N^M}$, are the nodes from the total set of nodes VM .

3.2. Local flow characteristics of multilayer network systems elements

Let's determine the most important local flow characteristics of the MLNS elements. By local we mean a characteristic that describes the properties of element itself or one or another aspect of its interaction with directly connected (adjacent) elements of the system. The local flow characteristic of the edge (n_i^k, n_j^m) is equal to corresponding element of the flow model (4), i.e., the volume of flows that passed through this edge during the time period $[t - T, t]$, $t \geq T$. The local flow

**ADVANCES
IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES**

characteristic of edge (n_i, n_j) of the total set of edges EM is equal to the value of element $f_{ij}(t)$, $i \neq j$, and the transition points n_i – to the value of element $f_{ii}(t)$, of the flow adjacency matrix F(t), $t \geq T$. As mentioned above, during the study of monoflow MLNS properties, the flow characteristics can be determined for the set of interlayer interactions in general. Based on this, the parameters

$$\zeta_{ij}^{in}(t) = \sum_{m=1}^M V_{ji}^{mm}(t) = f_{ji}(t), \quad \zeta_{ij}^{out}(t) = \sum_{m=1}^M V_{ij}^{mm}(t) = f_{ij}(t), \quad i, j = \overline{1, N^M},$$

determine the input and output flow connection strength between nodes n_i and n_j of the total set of nodes VM, taking into account all ways of implementing this connection in different layers of MLNS. Then parameters

$$\zeta_i^{in}(t) = \sum_{j=1}^{N^M} \zeta_{ji}^{in}(t) = \sum_{j=1}^{N^M} \zeta_{ji}^{in}(t) = \sum_{j=1}^{N^M} f_{ji}(t), \quad \zeta_i^{out}(t) = \sum_{j=1}^{N^M} \zeta_{ij}^{out}(t) = \sum_{j=1}^{N^M} f_{ij}(t),$$

determine the input and output flow connection aggregate-strength of the node n_i , $i, j = \overline{1, N^M}$, with all adjacent nodes from the total set of MLNS nodes, respectively. Then the generalized flow aggregate-degree of node n_i in the process of intra- and intersystem interactions is determined by the formula

$$\psi_i(t) = \zeta_i^{in}(t) + \zeta_i^{out}(t) + \sum_{m=1}^M \sum_{k=1}^M V_{ii}^{mk}(t) = \sum_{j=1, j \neq i}^{N^M} (f_{ij}(t) + f_{ji}(t)) + f_{ii}(t), \quad t \geq T,$$

and is a functional analogue of the concept of centrality by generalized degree d_i , $i = \overline{1, N^M}$, which is calculated by formula (3).

Analogously to the above scenario of sequential targeted attack on MLNS structure (see section 1.2) using as importance indicators of elements the generalized structural degree d_i , a scenario of attack on MLNS operation process is being built using the generalized flow aggregate-degree $\psi_i(t)$, $t \geq T$, $i = \overline{1, N^M}$. A significant advantage of this scenario, compared to the structural one, is the consideration of not only aggregate-network nodes destroyed or completely blocked as a result of the attack, but also those whose operation process was limited as a result of the corresponding negative influence. Thus, the flow approach makes it possible, even at the level of using local importance indicators of the elements, to more accurately determine both the results of targeted attack (the level of lesion of directly attacked nodes) and the consequences of this attack for consequentially injured adjacent nodes of MLNS. Moreover, structural and functional scenarios can be combined. In particular, if the first several nodes in the list of the most important in terms of generalized flow aggregate-degree have the same value of this indicator, then they can be additionally ordered according to the decreasing values of generalized structural degree of these nodes. However, as in the case of structural, the functional scenarios, which use as importance indicators the local characteristics of MLNS elements, among the consequentially injured only adjacent to directly

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

damaged nodes are taken into account. This situation is quite acceptable for assortative networks [21], in which connections between elements are generally limited to adjacent nodes, but not for disassortative ones, the structure of which has the majority of man-made NCs, the connections between elements of which are usually implemented by paths.

Another advantage of the flow-based approach compared to the structural ones is the possibility of prioritizing the recovery of damaged but not completely destroyed system elements. The list of recovery priorities in general may not coincide with the list of the most important MLNS nodes according to a certain centrality. In particular, the importance of object restoration can be determined by the formula

$$\gamma = \alpha(1 - \beta_{after}/\beta_{before})/\alpha_{max}$$

in which α is the value of selected centrality for the damaged node, α_{max} is the maximum value of this centrality for all system nodes, β_{after} is the average volume of flows in the node after damage, β_{before} is the average volume of flows in the node before the lesion. According to this formula, a more damaged node among less important ones may require priority restoration.

3.3. Global flow characteristics of multilayer network system elements

Let's determine the most important global flow characteristics of the MLNS elements. By global we mean the characteristics of system element which describe one or another aspect of its interaction with all other elements or the system at a whole [16].

3.3.1. Influence parameters of system node

Denote by $V^{out}(t, n_i^m, n_j^l)$ the total volume of flows generated in the node n_i^m and directed for final acceptance at MLNS node n_j^l for the period $[t - T, t]$, $t \geq T$.

Parameter $V^{out}(t, n_i^m, n_j^l)$ determines the real strength of influence of node n_i^m on node n_j^l of multilayer system for the duration period T , $i, j = \overline{1, N^M}$, $m, l = \overline{1, M}$.

Denote by $R_i^{m,l,out}(t) = \{j_i^l, \dots, j_{i_{l^{ml}(t)}}^l\}$ the set of numbers of all nodes of the l th

MLNS layer, which are the final receivers of flows generated in the node n_i^m , $L_i^{ml}(t)$ is the quantity of elements of the set $R_i^{m,l,out}(t)$, which can also change during the period $[t - T, t]$, $t \geq T$. Parameter

$$\xi_i^{m,l,out}(t) = \sum_{j \in R_i^{m,l,out}(t)} V^{out}(t, n_i^m, n_j^l) / s(\mathbf{V}^M(t)), \quad \xi_i^{m,l,out}(t) \in [0, 1], \quad (5)$$

**ADVANCES
IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES**

determines the strength of influence of node n_i^m , as a flow generator, on the l th layer-system in general, $t \geq T$, $i = \overline{1, N^M}$, $m, l = \overline{1, M}$. In formula (5), the value

$$s(\mathbf{V}^M(t)) = \sum_{m,k=1}^M \sum_{i,j=1}^{N^M} V_{ij}^{mk}(t),$$

as the sum of all elements of matrix $\mathbf{V}^M(t)$ is the global flow characteristic of MLNS, which is equal to the total volumes of flows that passed through the multilayer system during the period $[t-T, t], t \geq T$.

The power of influence of node n_i^m on the l th layer-system is determined by means of parameter

$$p_i^{m,l,out}(t) = L_i^{ml}(t) / N^M, p_i^{m,l,out} \in [0, 1],$$

and the set $R_i^{m,l,out}(t)$ will be called the influence domain of node n_i^m on the l th MLNS layer-system. Parameters $\xi_i^{m,l,out}(t)$, $p_i^{m,l,out}(t)$, and $R_i^{m,l,out}(t)$ will be called the output influence parameters of the node n_i^m as generators of flows on the l th MLNS layer-system, $i = \overline{1, N^M}$, $m, l = \overline{1, M}$. Analogously to the output ones are determined parameters of the strength $\xi_i^{l,m,in}(t)$, power $p_i^{l,m,in}(t)$, and domain $R_i^{l,m,in}(t)$ of input influence, which will be called the input influence parameters of the l th MLNS layer-system on the node n_i^m , as final receiver of flows generated in the nodes of the l th layer. The values of input and output influence parameters of the node n_i^m on l th layer make it possible to quantitatively determine how the lesion of this node will influence on functioning of the l th MLNS layer, namely, how many, which elements of the l th layer and in which measure will be consequentially injured, $i = \overline{1, N^M}$, $m, l = \overline{1, M}$, $[t-T, t], t \geq T$.

The output strength of influence of the node n_i^m as generator of flows on MLNS at a whole during the time period $[t-T, t], t \geq T$, is calculated according to the formula

$$\xi_i^{m,out}(t) = \sum_{l=1}^M \xi_i^{m,l,out}(t) / M, \xi_i^{m,out}(t) \in [0, 1], \quad (6)$$

in which the value $\xi_i^{m,l,out}(t)$ is determined by the formula (5). Domain of output influence $R_i^{m,out}(t)$ of the node n_i^m on MLNS is defined by the ratio

$$R_i^{m,out}(t) = \bigcup_{l=1}^M R_i^{m,l,out}(t).$$

**ADVANCES
IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES**

Then the power $p_i^{m,out}(t)$ of output influence of the node n_i^m on MLNS is equal to the ratio of quantity of elements of the set $R_i^{m,out}(t)$ to the value NM. Similarly to output ones, the strength $\zeta_i^{m,in}(t)$, domain $\overline{R_i^{m,in}(t)}$ and power $p_i^{m,in}(t)$ of the MLNS input influence on the node n_i^m , $i = \overline{1, N^M}$, $m = \overline{1, M}$, as the final receiver of flows, during the time period $[t - T, t]$, $t \geq T$ are determined. Lesion of the node-generator of flows means the need to find a new source of supply for the final receivers, and the receiver node – to search for new markets for producers, which will lead to at least temporary difficulties in their functioning. The influence parameters of separate node of MLNS allow us to determine what quantitative losses this will lead to and how many elements and which elements of intra- and intersystem interactions will spread.

3.3.2. Betweenness parameters of system node

The next type of global flow characteristics of MLNS elements are their betweenness parameters [16], which determine the importance of a node or an edge of multilayer network system in ensuring the movement of transit flows during intra- and intersystem interactions. In order to shorten the presentation, we will focus on the determination of betweenness parameters of MLNS transition points, as the most important elements that ensure intersystem interactions in monoflow partially overlapped multilayer systems. Denote by $V_i^{ml}(t)$ the total volume of flows that passed through the transition point n_i^{ml} during period $[t - T, t]$, $t \geq T$, $i = \overline{1, N^M}$, $m, l = \overline{1, M}$.

The value

$$\Phi_i^{ml}(t) = V_i^{ml}(t) / s(\mathbf{V}^M(t)), \quad \Phi_i^{ml}(t) \in [0, 1], \quad (7)$$

which determines the specific weight in the system the flows passing through the transition point n_i^{ml} during time period $[t - T, t]$, $t \geq T$, will be called the measure of betweenness of this transition point in the process of interaction of the l th and m th MLNS layers. The set M_i^{ml} of all nodes of l th and m th MLNS layers, which are generators and final receivers of flows transiting through the node n_i^{ml} , will be called the betweenness domain, and the ratio η_i^{ml} of the quantity of nodes in the set M_i^{ml} to the value NM is the betweenness power of transition point n_i^{ml} , $i = \overline{1, N^M}$, $m, l = \overline{1, M}$.

**ADVANCES
IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES**

The betweenness parameters of transition point n_i^m in the process of intersystem interactions within the entire MLNS will be determined as follows. The measure of betweenness $\Phi_i^m(t)$ of transition point n_i^m in the entire multilayer system can be calculated using the formula

$$\Phi_i^m(t) = \sum_{l=1, l \neq m}^M \Phi_i^{ml}(t) / (M - 1), \quad \Phi_i^m(t) \in [0, 1], \quad (8)$$

in which the value $\Phi_i^{ml}(t)$ is calculated according to (7). The betweenness domain of transition point n_i^m in the entire MLNS is determined by the ratio

$$M_i^m(t) = \bigcup_{l=1, l \neq m}^M M_i^{ml}(t).$$

Then the power $N_i^m(t)$ of betweenness of transition point n_i^m in the MLNS at a whole is equal to the ratio of quantity of elements of the set $M_i^m(t)$ to the value NM. Note, that for nodes that are not transition points of MLNS, the parameters of measure, domain and power of betweenness are determined according to the same principles. Similarly, it is possible to determine the parameters of measure $\Phi_{ij}^m(t)$, domain $M_{ij}^m(t)$, and power $N_{ij}^m(t)$ of betweenness for the edge (n_i^m, n_j^m) of MLNS m th layer, $i, j = \overline{1, N^M}$, $m = \overline{1, M}$, $[t - T, t]$, $t \geq T$. The values of betweenness parameters of MLNS node n_i^m , $i = \overline{1, N^M}$, $m = \overline{1, M}$, allow us by means of quantitative measurement to determine how the lesion of this node will affect the provision of transit flows through the multilayer system and to what extent, how many and which elements will be consequentially injured.

3.3.3. Specific scenarios of targeted attacks

The importance of node n_i of the total set of MLNS nodes as generator, final receiver or flow transitor is calculated using formulas

$$\xi_i^{out}(t) = \sum_{m=1}^M \xi_i^{m,out}(t) / M, \quad (9)$$

$$\xi_i^{in}(t) = \sum_{m=1}^M \xi_i^{m,in}(t) / M, \quad \xi_i^{out}, \xi_i^{in}(t) \in [0, 1], \quad (10)$$

$$\Phi_i(t) = \sum_{m=1}^M \Phi_i^m(t) / M, \quad \Phi_i(t) \in [0, 1], \quad i = \overline{1, N^M}, \quad [t - T, t], \quad t \geq T, \quad (11)$$

respectively. Domains of input $R_i^{in}(t)$, output $R_i^{out}(t)$ influence, and betweenness $M_i(t)$ of the node n_i in MLNS will determine by formulas

$$R_i^{in}(t) = \bigcup_{m=1}^M R_i^{m,in}(t), \quad R_i^{out}(t) = \bigcup_{m=1}^M R_i^{m,out}(t), \quad M_i(t) = \bigcup_{m=1}^M M_i^m(t),$$

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

and the powers of input $p_i^{in}(t)$, output $p_i^{out}(t)$ influence, and betweenness $N_i(t)$ of the node n_i on MLNS at a whole as the ratio of quantity of elements of the sets $R_i^{in}(t)$, $R_i^{out}(t)$, and $M_i(t)$, $i = \overline{1, N^M}$, to the value NM respectively.

Depending on the purpose of attack, the targets of lesion can be nodes-generators, nodes – final receivers, nodes-transitors of flows or only transition points of MLNS. For each of these types of multilayer system elements, it is possible to build specific scenarios of targeted attacks, using as importance indicators of nodes the parameters of influence or betweenness, determined above by formulas (5), (6), (9), (10) or (7), (8), (11) respectively. For example, an embargo on energy carriers means blocking generator nodes (countries that extract and supply such carriers), a ban on the supply of high-tech products (microcircuits, modern computers or equipment) – blocking the final receivers of flows (countries or companies that use such products), blocking of transit nodes (prohibition of international air flights over the territory of Russia or crossing of the Bosphorus Strait by its military ships) – redirection of the flow traffic by other routes. Before carrying out an attack on generator (final receivers) or transit nodes, it is possible to identify domains of output (input) influence or domains of betweenness, which allow us to identify nodes that may be consequentially injured by the attack, as well as to quantify the possible level of their losses. It makes sense to carry out such actions before imposing sanctions against the aggressor country. Quantifying the losses of sanctioning party compared to the damage done to attacked system allows us to determine the feasibility of attack.

3.3.4. Aggregate-network and lesion consequences

It is obvious that the influence and betweenness parameters of MLNS nodes and edges are related to the influence and betweenness parameters of nodes and edges of its flow aggregate-network. Thus, the output strength of influence of node n_i of the general set VM in the aggregate-network is equal to the value $\xi_i^{out}(t)$ calculated by formula (9), the domain of output influence of this node is the projection of domain $R_i^{out}(t)$ onto the aggregate-network (2), and the power of output influence is equal to the ratio of quantity of elements of this projection to the value NM. The input strength of aggregate-network influence on a node n_i is equal to the value $\xi_i^{in}(t)$, which is calculated by formula (10), the domain of input influence of this node is the projection of domain $R_i^{in}(t)$ onto the aggregate-network (2), and the power of the input influence is equal to the ratio of quantity of elements of this projection to the value NM. The measure of betweenness of node n_i in the

**ADVANCES
IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES**

aggregate-network is equal to the value $\Phi_i(t)$, which is calculated by formula (11), the domain of betweenness of this node is the projection of domain $M_i(t)$ onto the aggregate-network (2), and the power of betweenness is equal to the ratio of quantity of elements of this projection to the value NM.

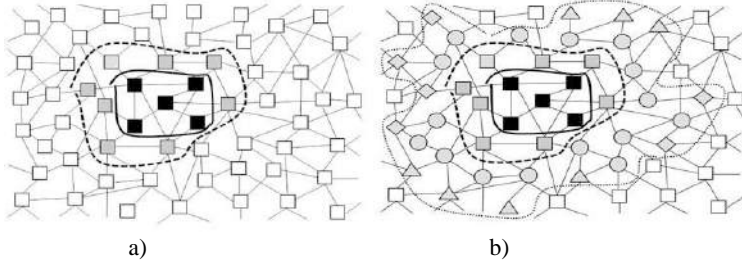


Figure 3. Consequences of targeted attack, obtained on the basis of analysis of structural aggregate-network (a) and parameters of influence and betweenness of flow aggregate-network nodes (b)

Figure 3 contains an example of lesions received by MLNS aggregate-network as a result of targeted attack. Here the black squares bounded by continuous curve indicate the directly damaged nodes, and dark gray squares bounded by a dashed curve indicate the consequentially injured nodes adjacent to the directly damaged ones obtained on the basis of structural approach, white squares indicate undamaged nodes (Figure 3 a). In Figure 3 b, the gray rhombuses, triangles, and circles bounded by a dotted curve indicate consequentially injured generator, final receivers, and transistor nodes obtained on the basis of flow approach, respectively. As follows from these figures, the domain of consequentially injured elements determined on the basis of flow approach can be much larger and more accurate in the sense of displaying the node type than the domain of adjacent to directly damaged nodes of the network system determined on the basis of the structural approach.

3.3.5. Parameters of interaction and comprehensive targeted attack scenario

Based on the input and output influence as well as betweenness parameters of the node n_i , we can determine the global indicators of interaction of this node with the MLNS at a whole, namely, the parameter $\Xi_i(t)$ of interaction strength of the node n_i with multilayer system, which is calculated according to the formula

$$\Xi_i(t) = (\xi_i^{out}(t) + \xi_i^{in}(t) + \Phi_i(t)) / 3, \quad t \geq T, \quad (12)$$

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

determines its overall role in multilayer system as generator, final receiver and flow transitor; the domain $\Omega_i(t)$ of interaction of the node n_i with MLNS is determined by the formula

$$\Theta_i(t) = R_i^{in}(t) \cup R_i^{out}(t) \cup M_i(t),$$

and the power of interaction of the node n_i with MLNS is equal to the ratio of quantity of elements of domain $\Omega_i(t)$, $t \geq T$, to the value NM. It is obvious that interaction parameters of MLNS nodes are related to the interaction parameters of its flow aggregate-network nodes. Thus, the strength of interaction of node n_i of the general set of nodes VM with the MLNS flow aggregate-network is equal to the value $\Xi_i(t)$, which is calculated according to formula (12), the domain of interaction of this node is the projection of domain $\Omega_i(t)$ onto the aggregate-network (2), and the power of interaction is equal to the ratio of quantity of elements of this projection to the value NM.

Let's build a scenario of consistent targeted attack on multilayer system, choosing as an importance indicator of node the strength of its interaction with MLNS flow aggregate-network. Such scenario, which achieves the comprehensiveness of attack on the functionally most important system nodes, will look like this:

- 1) compile a list of nodes of the set V^M in order of decreasing values of their strength of interaction with the flow aggregate-network;
- 2) delete the first node from the created list;
- 3) if the criterion of attack success is reached, then finish the execution of scenario, otherwise go to point 4;
- 4) since the operation process of flow aggregate-network changes as a result of removing a node (and its connections), compile a new list of nodes of the set V^M that remained in the order of decreasing recalculated values of their interaction strength with flow aggregate-network and proceed to point 2.

In this case, it is advisable to choose a reduction in the volume of flows $s(V^M(t)), t \geq T > 0$, in MLNS by a certain predetermined value as the criterion for the attack success.

4. Simultaneous group attacks on the multilayer network systems

It is obvious that simultaneous group attacks or non-target system lesions are much more difficult than successive attacks on the most important MLNS elements, both from the point of view of its protection and overcoming the consequences [22]. In this section, for the sake of brevity, we will limit ourselves to the consideration of targeted attacks on the MLNS aggregate-network.

4.1. Classification of targetet group attacks

We divide simultaneous group negative influences into one-time (the attack on Pearl Harbor on December 7, 1941), repeated (the permanent bombing of London during the Second World War) and successive (attacks on transformer stations of the Ukrainian power system in 2022-2024). Repeated group attacks are carried out regularly at certain time intervals on the same system objects. Consecutive group attacks differ from repeated ones by changing the targets. A particular danger is that successful sequential group attacks can lead to system-wide MLNS lesions, for example, a prolonged blackout in the country. In the case of targeted attacks, this separation is often determined by the attacker's ability to launch subsequent massive attacks and the ability of attacked system to effectively defend and counter them. It is clear that each of above types of attack requires the development of specific type of scenarios for its most likely implementation. The simplest scenario of one-time group attack is obviously implemented by attempt to simultaneously defeat a group of the most important MLNS elements according to determined centrality. The repeated attack scenario is realized by attempt to damage a preselected and previously attacked, but not destroyed, group of multilayer system elements. A sequential group attack scenario involves the consecutive execution of following steps:

- 1) compile a list of groups of MLNS aggregate-network's nodes in order of decreasing indicators of their importance in the system, selected according to a certain feature;
- 2) delete the first group from the created list;
- 3) if the criterion of attack success is reached, then complete the execution of scenario, otherwise go to point 4;
- 4) since the system structure changes as a result of removal of certain group of nodes (and their connections), compile a new list of groups in order of decreasing recalculated indicators of their importance in the MLNS aggregate-network and proceed to point 2.

If, during implementation of last scenario, a certain group of nodes contains too many elements that the attacker is unable to damage simultaneously, then such group is divided into the minimum quantity of connected subgroups available for such attacks. In addition, the execution of scenario may terminate when the attacking party has exhausted the resources to continue the attack. It follows from the above scenarios that the main way to increase their effectiveness is to choose the importance indicators of group in multilayer network system, the lesion of which will cause it the greatest damage. The most obvious way of such choice is to form a list of MLNS aggregate-network's nodes in order of decreasing the values of their centrality of selected type and form a group from the first nodes of this list, the quantity of which is determined by the ability of attacker to carry out a simultaneous attack on them. The second method is based on the principle of nested hierarchy of the network system [23]. The method proposed by us consists in applying the concept of k-core of aggregate-network, as the largest subnet of source network, the centrality of which, according to the generalized structural degree of nodes, is at

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

least $k > 1$ [24]. This method is based on the use of the most structurally important components of aggregate-network and obviously fits into the above scenario of successive group attacks. In particular, groups are initially selected for the maximum value k for a given aggregate-network, which is then sequentially reduced until the attack success criterion is met.

During the development of scenarios of simultaneous group attacks on MLNS operation process, as a functionally most important component of the flow aggregate-network, the concept of its flow λ -core [25] can be used, as the largest subsystem of source system, elements of flow adjacency matrix $F(t)$ of which have values not less than $\lambda \in [0, 1]$. It is obvious that the larger the value λ , the more important from a functional point of view aggregate-network's components are reflected by its λ -core. They can become one of the primary targets of simultaneous group attack. Similarly, as for aggregate-network elements, we can determine the parameters of influence and betweenness of its λ -core, which significantly deepens the analysis of network system lesions.

4.2. Optimization of targeted group attack scenarios

One of the ways to protect the system is to counterattack the intruder. It is clear that the organizers of such counterattacks also suffer considerable losses. That is, the problem of optimizing attack scenarios arises, namely, how to destroy or block the operation of minimum quantity of nodes of attacked party, to cause it the greatest possible lesion. A similar situation is observed during the development of scenarios for combating the spread of non-target lesions, for example, epidemics of dangerous infectious disease. In particular, how to minimize the volume of passenger flows through the transportation network by blocking the smallest possible quantity of nodes that ensure the movement of these flows. Obviously that it is advisable to take into account not only the magnitude of direct negative influence, but also the scale of mediated lesion consequences. Let's illustrate this on the example of railway layer of the country's general transport system. Above, for the construction of simultaneous group attacks scenarios, it was proposed to use the concepts of structural k - and flow λ -core of network system. We will show that the use of flow λ -cores compared to structural k -cores of MLNS aggregate-networks is significantly more effective when building scenarios of group targeted attacks, both from the point of view of possible lesion of the most functionally important aggregate-network's components, and for the purpose of optimizing these scenarios in terms of the quantity of attack targets. Let's consider the railway transport system (RTS) of the western region of Ukraine. In fig. 4a shows the structure of this system, and in fig. 4b – the same structure, but in the form of weighted network, which schematically reflects the volumes of cargo flows that passed through its edges during 2021 (the thickness of lines is proportional to the volumes of flows). Note that this real-world network contains 354 nodes in total, but in fig. 4a-b, only 29 nodes and 62 edges are displayed (transit nodes with structural degree 2 are not shown, and an edge is considered to be a line

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

that connects two nodes with degree greater than 2). In fig. 4c contains the structural 4-core of RTS, which includes 12 nodes and 35 edges, and in fig. 4d is its flow 0.8-core, which contains 4 nodes and 12 edges. One of the main disadvantages of k-cores compared to flow cores is the possibility of excluding functionally important components of the network system (path A-B in fig. 4d).

From fig. 4 also follows that the flow 0.8-core reflects a functionally more important subsystem of RTS and the target of group attack on it is a much smaller quantity of nodes than 4-core of corresponding structure.

Easy to see that in both cases, a successful attack on NS nodes selected with the help of k- and λ -cores will lead to actual termination of its operation process, as it divides RTS into unconnected components (fig. 4e), but in the second case, the goal of attack is achieved with significantly less efforts (three times in terms of quantity of nodes and edges). Thus, the flow-based approach allows us to build scenarios that are much more optimal from the point of view of attacking side's efforts than the structural one.

By analyzing the parameters of influence and betweenness of 0.8-core of given RTS fragment, it was established that all elements of this fragment will be consequentially injured by a successful targeted attack on it.

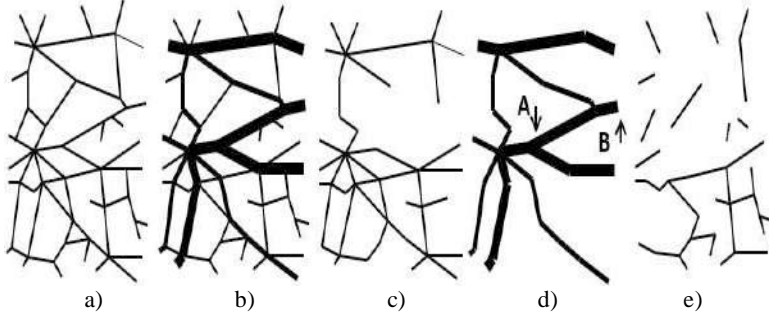


Figure 4. Examples of structure (a), operation process (b), structural 4-core (c), flow 0.8-core (d), and the addition to flow 0.8-core in the source structure (e) of railway transport system of the Western region of Ukraine

5. Simultaneous system-wide attacks on the multilayer network systems

Typical scenarios of successive and simultaneous targeted attacks on layers-systems of MLNS are built according to the same principles as corresponding scenarios of such attacks on elements and subsystems of multilayer systems [1] with the difference that the objects of attack are the layers of MLNS. At the same time, the main way to improve the effectiveness of such attacks is the selection of structural and/or functional importance indicators of MLNS layer, the lesion of which will cause the greatest damage to it.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

5.1. Structural and functional importance indicators of MLNS system-layers

The global structural characteristics of multilayer network, which is generated by monoflow partially overlapped MLNS, can be considered the quantity of layers-networks that are part of it, as well as the dimension, density, diameter, average length of the shortest path, the total quantity of transition points [11], etc. Let us define some general and most important for the vulnerability analysis of structure of intersystem interactions characteristics of the layers of partially overlapped MLNS, the values of which should be taken into account during construction the scenarios of system-wide targeted attacks:

- 1) the specific weight of the set of nodes of the m^{th} layer in the total set of nodes of partially overlapped MLN;
- 2) the specific weight of the set of edges of the m^{th} layer in the total set of edges of partially overlapped MLN;
- 3) input degree of the m^{th} layer, which is equal to quantity of transition point into this layer from all other layers of MLN or total quantity its input interlayer connections;
- 4) output degree of the m^{th} layer, which is equal to quantity of transition point from this layer into all other layers of MLN or total quantity its output interlayer connections;
- 5) the specific weight of transition points of the m^{th} layer in the set of all transition points of partially overlapped MLN, which is determined availability of interlayer interactions for this layer, $m = \overline{1, M}$.

Let us determine the most important flow characteristics of system-layers in monoflow partially overlapped multilayer network system, values of which should be taken into account during construction scenarios of system-wide targeted attacks:

- 1) the specific volumes of intralayers flows in the m^{th} MLNS layer;
- 2) the specific volumes of output flows of the m^{th} layer in MLNS, which reflect its role as a flow generator in multilayer system;
- 3) the specific volumes of input flows of the m^{th} layer in MLNS, which reflect its role as a final receiver of flows in multilayer system;
- 4) the specific volumes of transit flows that pass through the m^{th} MLNS layer, $m = \overline{1, M}$.

It should be noted that the layers with the highest values of structural and functional importance indicators listed above can become the primary targets of system-wide attacks on MLNS and be used during construction the scenarios for such attacks.

5.2. Influence and betweenness parameters of MLNS system-layers

Such global flow characteristics of nodes and subsystems of MLNS were determined in the monograph [16], as parameters of their output and input influence and betweenness.

**ADVANCES
IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES**

These parameters make it possible to calculate the importance of separate components of multilayer system as generators, final receivers and transitors of flows and allow us to build effective scenarios of successive and simultaneous group targeted attacks on the process of intersystem interactions. However, for the formation of effective scenarios of successive system-wide attacks, it is advisable to determine the influence and betweenness parameters of separate MLNS system-layers.

5.2.1. Influence parameters of system-layers

Output strength of influence of the m^{th} layer as generator of flows on the l^{th} MLNS layer as final receiver of these flows during the time period $[t-T, t], t \geq T > 0$, is calculated by the formula

$$\xi^{m,l,out}(t) = \sum_{i=1}^{N^M} \xi_i^{m,l,out}(t) / N^M, \quad \xi^{m,l,out}(t) \in [0,1], \quad (13)$$

in which the parameter $\xi_i^{m,l,out}(t)$ is calculated by formula (5). Domain $R^{m,l,out}(t)$ of output influence of the m^{th} layer on the l^{th} MLNS layer are determined as union of influence domains of nodes-generators of flows of the m^{th} layer on the nodes – final receivers these flows in l^{th} MLNS layer, and the power of this influence $p^{m,l,out}(t)$

is equal to the ratio of quantity of elements of the domain $R^{m,l,out}(t)$ to value N^M .

Similarly, the input strength $\xi^{m,l,in}(t)$, domain $R^{m,l,in}(t)$ and power $p^{m,l,in}(t)$ of influence of the m^{th} layer as final receiver of flows on the l^{th} MLNS layer as generator of these flows are determined during the time period $[t-T, t], t \geq T > 0$, $m \neq l, m, l = \overline{1, M}$.

The output strength of influence of the m^{th} layer as generator of flows on the MLNS at a whole is calculated by formula

$$\xi^{m,out}(t) = \sum_{l=1, l \neq m}^M \xi^{m,l,out}(t) / (M - 1), \quad \xi^{m,out}(t) \in [0,1],$$

in which the value $\xi^{m,l,out}(t)$ is calculated according to (13) and domain of this influence is determined by the ratio

$$R^{m,out}(t) = \bigcup_{l=1, l \neq m}^M R^{m,l,out}(t).$$

The power of output influence of the m^{th} layer on the MLNS at a whole is equal to the ratio of quantity of element of domain $R^{m,out}(t)$ to the value N^M . Similarly, the input strength $\xi^{m,in}(t)$, domain $R^{m,in}(t)$ and power $p^{m,in}(t)$ of influence of

**ADVANCES
IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES**

MLNS on the m^{th} layer as final receiver of flows are determined during the time period $[t-T, t], t \geq T > 0$. The values of parameters of input and output influence of the m^{th} layer on the l^{th} layer or MLNS at a whole make it possible to quantitatively determine how the lesion of this layer will impact on the operation process of the l^{th} layer and the multilayer network system in general, and how many components of intersystem interactions and to what extent will be affected, $m, l = \overline{1, M}$.

5.2.2. Betweenness parameters of system-layers

The next type of global flow characteristics of each MLNS layer is its betweenness parameters, which determine the importance of layer of the multilayer network system in ensuring the movement of transit flows during intersystem interactions [16]. The measure of betweenness of the m^{th} layer within the entire MLNS during period $[t-T, t], t \geq T > 0$, as transitor of flows is calculated using the formula

$$\Phi^m(t) = \sum_{i=1}^{N^M} \Phi_i^m(t) / N^M, \Phi^m(t) \in [0,1],$$

in which the value $\Phi_i^m(t)$ is calculated by formula (8). Betweenness domain of the m^{th} layer in MLNS at a whole is determined from the ratio

$$M^m(t) = \bigcup_{i=1}^{N^M} M_i^m(t),$$

in which $M_i^m(t)$ denotes the betweenness domain of i^{th} transition point of the m^{th} layer within the entire MLNS, and the betweenness power of the m^{th} layer $N^m(t)$ is equal to the ratio of quantity of elements of domain $M^m(t)$, $[t-T, t], t \geq T > 0$, to the value N^M . The values of betweenness parameters of the m^{th} layer in MLNS make it possible to quantitatively determine how the lesion of this layer will impact on the process of intersystem interactions in general and how many, which components of the multilayer system and to what extent will be affected, $m = \overline{1, M}$.

5.2.3. Interaction parameters of system-layers

Based on the parameters of input and output influence, as well as betweenness parameters of the m^{th} layer, we can form a global indicator of interaction of this layer with MLNS in general, namely, parameter $\Xi^m(t)$ of the strength of interaction of the m^{th} layer with multilayer system, which is calculated according to the formula

$$\Xi^m(t) = (\xi^{m,out}(t) + \xi^{m,in}(t) + \Phi^m(t)) / 3,$$

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

and defines its overall role in multilayer system as generator, final receiver and transitor of flows; domain $\Omega^m(t)$ of interaction of the m^{th} layer with MLNS is determined by the ratio

$$\Omega^m(t) = R^{m,out}(t) \cup R^{m,in}(t) \cup M^m(t),$$

and the power of interaction of the m^{th} layer with MLNS is equal to the ratio of quantity of elements of the domain $\Omega^m(t)$, $m = \overline{1, M}$, $t \geq T > 0$, to the value N^M . It is clear that interaction parameters of a layer with multilayer network system define the importance of this layer in the process of intersystem interactions and make it possible to quantitatively determine how the lesion of this layer will impact on the MLNS operation process and how many, exactly which of its components will be influenced and to what extent.

5.2.4. A comprehensive system-wide attack scenario

Let us build a scenario of successive targeted system-wide attack, choosing the parameter of strength of layer interaction with multilayer system as its importance indicator. Such scenario, which achieves the comprehensiveness of attack on the most functionally important MLNS layers, will look like this:

- 1) compile the list of MLNS layers in order of decreasing values of the parameters of strength of their interaction with multilayer system;
- 2) remove the first layer from the created list;
- 3) if the criterion of attack success is reached, then complete the execution of scenario, otherwise go to point 4;
- 4) since the structure and operation process of multilayer system changes due to removal of certain layer (and its interlayer connections), compile a new list of layers in the order of decreasing values of the parameters of strength of their interaction with MLNS and proceed to point 2.

In this case, it is advisable to choose the reduction of volumes of flows $s(\mathbf{V}^M(t))$, $t \geq T > 0$, in the multilayer system by a certain predetermined value as the attack success criterion. The next most difficult to ensure protection and overcome the consequences are simultaneous attacks on several or all MLNS layers, which include hybrid wars, sanctions against countries that pose a threat to world security, etc. The scenarios of such attacks are built according to the same principles as those of simultaneous group attacks, with the difference that the attack targets are not the most important by certain characteristics the groups of nodes, but the MLNS layers.

5.3. Targeted attacks and the scale of system lesions

The concept of system protection is closely related to determining the scale of targeted attack and its consequences. In particular, it is advisable to distinguish:

- 1) the scale of planned and executed attack, which is determined by the quantity of targets expected to be hit and the quantity of means used for this purpose, for example, 50 energy infrastructure facilities and 100 cruise and ballistic missiles aimed at them for destruction;

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

2) the scale of direct lesion, that is, the quantity of targets critically damaged or completely destroyed by the attack, for example, out of 100 launched missiles, 85 were shot down by anti-missile and anti-aircraft defenses, and the remaining 15 missiles hit 10 targets; in this case, the scale of direct damage is equal to the percentage of destroyed objects from the quantity of planned ones;

3) the scale of consequentially injured system elements, i.e. the quantity of objects that suffered certain damage as a result of the attack in addition to those directly damaged, for example, introduction of blackout schedules caused by consecutive and simultaneous attacks on the energy infrastructure of Ukraine.

The scale of direct damage is related to the quantitative indicator of system's protection, which is equal to the percentage of destroyed means of damage from all involved. The scale of mediated lesion, as well as the level of protection against it, is much more difficult to calculate, because it must take into account the disruption of structure and destabilization of the work of all system elements and even the moral and psychological damage caused as a result of the attack.

The concept of system sensitivity to the consequences of negative influence can be associated with the scale of indirect lesion, as the ratio of quantity of directly damaged to the quantity of consequentially injured elements. It is obvious that the closer the value of this indicator is to zero, the more sensitive the system is to negative influences, since a small quantity of directly damaged generates a large quantity of consequentially injured MLNS elements.

Therefore, it makes sense to believe that the nature of attack should be determined not only by the quantity of directly damaged MLNS elements, but also by the scale of indirect losses caused to the system, although it is much more difficult to ensure its protection against such lesion.

6. Conclusions

In 2019-2024, humanity faced two global challenges, the first of which (Covid-19 pandemic) is a vivid example of real-world system-wide non-target lesion, and the second is a targeted attack (attack of the Russian Federation on Ukraine) and the resulting threat of a global food, energy, and financial crisis and reverse comprehensive sanctions against the aggressor, the negative consequences of which affected almost all countries of the world.

Humanity proved to be unprepared for such challenges, but no less dangerous threats remain. Over the past half century, 67% of biological species known to man have disappeared, and over the past 20 years, the costs of combating climate disasters have increased 8 times. Currently, scientists know more than 20 viruses of dangerous infectious diseases, the mutations of which can lead to the spread of pandemics, much more catastrophic than Covid-19, the threat of global military and even intercivilizational conflicts is increasing, etc.

This confirms the relevance of studying the features of successive, group and system-wide lesions of complex network and multilayer network systems and developing methods of effective protection against them.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

The concepts of structural and flow aggregate-networks of monoflow multilayer network system are introduced in the article in order to reduce the dimensionality of MLNS models and simplify the analysis of their vulnerability to heterogeneous negative influences.

The main local and global structural and flow characteristics of multilayer system and its aggregate-network elements are determined and the relationship between them is established.

These characteristics are chosen as importance indicators of MLNS nodes, with the help of which effective structural and functional scenarios of successive, group and system-wide targeted attacks on multilayer network systems are built. It is shown how, on the basis of various models of intersystem interactions, the domains of directly damaged and consequentially injured by the negative influence the system elements are determined. To optimize the scenarios of simultaneous group attacks, as a means of active protection against the source of negative influence, the application of flow cores of the MLNS's aggregate-network is proposed. The advantages of such scenarios over structural ones based on the concept of k-core of aggregate-network are shown on the example of real-world network system.

The advantages of flow-based approach for studying the vulnerability of intersystem interactions process and quantifying the level of losses caused to this process as a result of various negative influences are established. An objective evaluation of the scale of real or potential lesions allows us to develop strategies to protect not only separate MLNS elements, but also the system as a whole, and to prevent the consequences of local targeted attacks and non-target lesions from growing into group and system-wide ones.

The next steps of our research are the study of MLNS vulnerability damage not nodes, but connections of complex network and multilayer network systems, which are much easier to implement in practice and can lead to granulation of intra- and intersystem interactions.

7. References

- [1] O. Polishchuk, M. Yadzhak, On the Vulnerability and Protection Strategies of Complex Network Systems and Intersystem Interactions, *CEUR-WS* 3538 (2023) 267-281.
- [2] M. Bellingerio, D. Cassi, S. Vincenzi, Efficiency of attack strategies on complex model and real-world networks, *Physica A: Statistical Mechanics and its Applications* 414 (2014) 174-180. doi: 10.1016/j.physa.2014.06.079.
- [3] Q. Nguyen et al, Conditional attack strategy for real-world complex networks, *Physica A: Statistical Mechanics and its Applications* 530 (2019) 12156. doi: 10.1016/j.physa.2019. 121561.
- [4] M. Alonso et al, Cyber-physical vulnerability assessment in smart grids based on multilayer complex networks, *Sensors* 21 17 (2021) 5826.
- [5] F. Zhou et al, Influence of interlink topology on multilayer network robustness, *Sustainability* 12(3) (2020) 1202. doi: 10.3390/su12031202.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

- [6] B. Fan et al, Critical nodes identification for vulnerability analysis of power communication networks, *IET Communications* 14 4 (2020) 703-713. doi: 10.1049/iet-com.2019.0179.
- [7] J. Bluszcz, M. Valente, The Economic Costs of Hybrid Wars: The Case of Ukraine, *Defence and Peace Economics* 33 1 (2022) 1-25. doi: 10.1080/10242694.2020.1791616.
- [8] N. Vindegaard, M.E. Benros, COVID-19 pandemic and mental health consequences: Systematic review of the current evidence, *Brain, Behavior, and Immunity* 89 (2020) 531-542. doi: 10.1016/j.bbi.2020.05.048.
- [9] J. Mariyam, D.S. Lekha, Need for a realistic measure of attack severity in centrality based node attack strategies, in *Complex Networks and Their Applications XI*, R.M. Benito et al, Eds. Springer: Cham (2022) 857-866.
- [10] L. Glenn, Understanding the influence of all nodes in a network, *Science Reports* 5 (2015) 8665. doi: 10.1038/srep08665.
- [11] S. Boccaletti et al, The structure and dynamics of multilayer networks, *Physics Reports* 544 1 (2014) 1-122. doi: 10.1016/j.physrep.2014.07.001.
- [12] L.G. Alvarez-Zuzek et al, Dynamic vaccination in partially overlapped multiplex network, *Physical Review E* 99 (2019) 012302. doi: 10.1103/PhysRevE.99.012302.
- [13] M. Berlingerio et al, Multidimensional networks: foundations of structural analysis, *World Wide Web* 16 (2013) 567–593. doi: 10.1007/s11280-012-0190-4.
- [14] A. Saxena, S. Iyengar, Centrality measures in complex networks: A survey, arXiv: 2011. 07190, 2020.
- [15] O. Polishchuk, Structural Cores and Problems of Vulnerability of Partially Overlapped Multilayer Networks, in *Complex Networks and Their Applications XI*, H. Cherifi et al, Eds. Springer: Cham (2023) 613-624. doi: 10.1007/978-3-031-21127-0_50.
- [16] O.D. Polishchuk, M.S. Yadzhak, Models and methods of comprehensive research of complex network systems and intersystem interactions. Pidstryhach Institute for Applied Problems of Mechanics and Mathematics, National Academy of Sciences of Ukraine: Lviv, 2023.
- [17] Yu. Holovach et al, Complex networks, *Journal of physical studies* 10 4 (2006) 247–289. doi: 10.30970/jps.10.247.
- [18] D. Krackhardt, Assessing the political landscape: Structure, cognition, and power in organizations, *Administrative Science Quarterly* 35 2 (1990) 342–369. doi: 10.2307/2393394.
- [19] A. Barrett, M. Barthelemy, A. Vespignani, The architecture of complex weighted networks: Measurements and models, in *Large Scale Structure and Dynamics of Complex Networks*, G. Caldarelli, Eds. World Scientific: Singapore (2007) 67-92. doi: 10.1142/9789812771681_0005.
- [20] A.-L. Barabasi, The architecture of complexity, *IEEE Control Systems Magazine* 27 4 (2007) 33-42. doi: 10.1109/MCS.2007.384127.
- [21] R. Noldus, P. Van Mieghem, Assortativity in complex networks, *Journal of Complex Networks* 3 4 (2015) 507-542. doi: 10.1093/comnet/cnv005.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

- [22] O. Polishchuk, Protection of Complex Network Systems From Targeted Attacks and Non-Target Lesions, Qeios (2024) RH65Y6. doi: 10.32388/RH65Y6.
- [23] O. Polishchuk, M. Yadzhak, Network structures and systems: III. Hierarchies and networks, System research and informational technologies 4 (2018) 82-95. doi: 0.20535/SRIT. 2308-8893.2018.4.07.
- [24] S.N. Dorogovtsev, A.V. Goltsev, J.F.F. Mendes, K-core organization of complex networks. Physical review letters 96(4) (2006) 040601. doi: 10.1103/PhysRevLett.96.040601.
- [25] O. Polishchuk, M. Yadzhak, Network structures and systems: II. Cores of networks and multiplexes. System research and informational technologies 3 (2018) 38-51. doi: 10.20535/SRIT.2308-8893.2018.3.04.

ЗАХИСТ БАГАТОРІВНЕВИХ МЕРЕЖЕВИХ СИСТЕМ ВІД ПОСЛІДОВНИХ, ГРУПОВИХ І ЗАГАЛЬНОСИСТЕМНИХ ЦІЛЕСПРЯМОВАНИХ АТАК

Dr.Sci. О. Поліщук

*Інститут прикладних проблем механіки і математики ім. Підстригача НАН
України, Україна
E-mail: od_polishchuk@ukr.net*

Анотація. Розглянуто структурний і потоковий підходи до аналізу вразливості багаторівневих мережевих систем (MLNS) від цілеспрямованих атак і нецільових уражень різного походження. Визначено локальні та глобальні структурні та потокові характеристики елементів монопотоккової багатошарової системи для побудови сценаріїв цілеспрямованих атак на структуру та процес функціонування MLNS та оцінки їх наслідків. Для спрощення побудови та підвищення ефективності таких сценаріїв введено поняття структурних і потокових агрегатів-мереж монопотоккових МЛНС та показано зв'язок між показниками важливості їх елементів та відповідними показниками вузлів багатошарової системи. Продемонстровано переваги потокового підходу перед структурним, як у сенсі аналізу вразливості реальних MLNS, так і оцінки наслідків негативних впливів різного характеру.

Ключові слова: складна мережа, мережева система, міжсистемні взаємодії, багаторівнева мережева система, модель потоку, агрегатна мережа, вплив, міжсистемність, цілеспрямована атака, вразливість.

**NEW STATISTICAL CRITERIA FOR CHECKING
INDEPENDENCE OF BIT RANDOM VARIABLES AND
SEQUENCES**

Dr.Sci. L. Kovalchuk ORCID: 0000-0003-2874-7950

*G.E. Pukhov Institute for Modelling in Energy Engineering, Ukraine
E-mail: lusi.kovalchuk@gmail.com*

Dr.Sci. A. Davydenko ORCID: 0000-0001-6466-1690

*G.E. Pukhov Institute for Modelling in Energy Engineering, Ukraine
E-mail: davidenkoan@gmail.com*

O. Bespalov 0000-0001-7126-6752

*G.E. Pukhov Institute for Modelling in Energy Engineering, Ukraine
E-mail: alexb5dh@gmail.com*

***Abstract.** The paper proposes strictly justified two statistical criteria for checking the pairwise independence of bit sequences, which can be considered as realization of random variables from a certain set. The corresponding algorithms that implement the independence check according to these criteria are also developed and clearly step-by-step formulated. The resulting tools are very relevant for statistical verification of the cryptographic qualities of various cryptographic primitives, the functioning of which relates to the generation of random/pseudo-random sequences. Such crypto-primitives include not only random/pseudorandom sequence generators, but also stream ciphers, combined encryption algorithms (i.e., block algorithms in stream modes), etc. Using the proposed criteria allows checking the independence of the different parts of output sequences, or the independence of the output sequences from the sequences of internal states and input data. It should be noted that such independence is a necessary condition for the output sequence to be considered unpredictable. The article also considered comparative analysis of two given criteria and results of their applications to sequences of different types.*

***Keywords:** statistical criterion, random variables, independence of random variables, random number generation, statistical checking of independence*

1. Introduction

When creating new cryptographic algorithms, in particular pseudorandom/random number generators (RNG/PRNG), or stream ciphers, the following requirements must be met [1, 2]: analytical justification of the algorithm's resistance to main known attacks; statistical investigations of the cryptographic properties of the algorithm's output gamma (often the properties of intermediate gammas of the algorithm are also investigated, such as the sequence of its internal states, or so).

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

At the same time, we can often see the lack of attention paid to an equally important issue concerning statistical investigations of the mutual independence of parts of the output sequence, as well as the independence of input data, intermediate gammas, sequences of internal states, and output sequences. Indeed, if, for example, the output sequence depends on the input sequence or on the intermediate gamma, the algorithm may be vulnerable to certain types of statistical attacks, or its output sequence may not have the property of unpredictability.

In this paper we propose two new criteria for checking independence of sequences, obtained from RNG/PRNG.

They are based on two different methods, though both of them use calculating the determinant of the correlation matrix. We also give detailed step-by-step description of two corresponding algorithms for independence checking. The first criterion is based on several statements, formulated and proved in this work below. It has such main advantages as significantly lower computational complexity and intuitive clarity of corresponding algorithm. The other advantage is that it needs no tables with probabilistic distributions, such as χ^2 or normal. Its disadvantage is some requirements to the length of the sequences to be analyzed, and the larger the number of sequences we check, the larger their length should be. The second criterion is based on the existing method, explained below. The algorithm, corresponding to the second criterion, is much more complicated and uses tables of χ -square distribution for large number of degrees of freedom. But its undeniable advantage is high accuracy, which testifies to a small value of second type error.

The paper is organized in the follow way. In the Introduction, we formulated the main task of our work and explained its importance for practical applications in cryptology. In the Section 1 we briefly described the state of the art in the considered topic and show the gap in existing results. In the Section 2 we formulate the problem and give main designations, which are necessary for further investigations. In the Section 3 we prove necessary statements to justify the first criterion. Then in the Section 4 we construct the first criterion of sequence independence, and describe corresponding Algorithm 1. The Section 5 gives the results of experiments with Algorithm 1 application. The Section 6 contains theoretical information, necessary for creation of the second criterion. Then in the Section 7 we construct the corresponding Algorithm 2 and describe the results of its applications. In the Section 8 we give conclusion and discussion of the obtained results.

2. Related work

A lot of statistical tools, like commonly used sets of statistical tests, exist for statistical investigations of the cryptographic properties of the output gamma of RNG/PRNG or stream ciphers [1, 2, 3]. But there is currently no standardized or at least generally accepted methodology for checking the statistical independence of sequences, which may be interpreted as independence of random variables with corresponding realizations. The relevance of creating a tool for checking the independence of input-output sequences is substantiated, for example, in [4],

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

although the number of scientific papers on this topic is much smaller than works on the development of new encryption algorithms or gamma generators [4, 5, 6, 7, 8], or work on estimation of the cryptographic qualities of generators and sequences [9, 10]. Paper [4] is quite close to this work, but its results are only experimental and were obtained for a different problem statement. In this paper, the author performs an experimental study of the independence of the statistical tests themselves rather than the independence of the sequences. Also, a similar problem concerning the dependencies between the bits of input/output sequences in stream ciphers is claimed in [11]. But the purpose of this work is almost the opposite of ours: it investigates how to define whether a stream cipher has sufficient diffusion property, i.e., whether each bit of the output sequence depends on many bits of the input sequence. An appropriate example of investigation of the independence of sequences of internal states for stream cipher was performed, for example, in [12]. For this purpose, the method proposed in [13] was used, which builds corresponding correlation matrix and calculates its determinant. This method is quite workable, but it has certain disadvantages. It is cumbersome and intuitively unclear, requires a large number of calculations, and requires the usage of tables of several distributions, which makes it not very convenient for practice. In addition, when performing statistical research, it is desirable to use several criteria rather than one – for example, the number of separate tests in the NIST STS [3] is 16 (15 in the updated one), and with all "subtests" it is more than 150.

3. Statement of the problem

In this section we introduce the main designations, which will be used below, and then conclude with formal description of the problem.

Let $m, n \in \mathbf{N}$, and
$$X = \{X^{(i)}, i \in \overline{1, n}\} \tag{1}$$

be a set of sequences of independent equally distributed random variables,
 $X^{(i)} = (x_1^{(i)}, \dots, x_m^{(i)})$ with $x_k^{(i)} \in \{0, 1\}$, and define $a^{(i)} = Ex_k^{(i)} = P(x_k^{(i)} = 1)$,

$$\left(\sigma^{(i)}\right)^2 = Var(x_k^{(i)}) \tag{2}$$

In what follows, we consider the sequence $(x_1^{(i)}, \dots, x_m^{(i)})$ as a realization of a random variable $X^{(i)}$. Let's formulate a hypothesis H_0 as "the sequences in set (1) are pairwise independent". Alternative hypothesis H_1 is complex and is formulated as a "hypothesis H_0 is not true."

The purpose of this work is to build and justify a statistical criterion that will recognize the hypothesis H_0 with a given significance level α .

**ADVANCES
IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES**

4. Designations and auxiliary statements needed for the first criterion and Algorithm 1

In this section, we will formulate and prove several statements necessary for solving the problem formulated in section 0.

Consider random variables

$$r_k^{(i,j)} = \frac{(x_k^{(i)} - a^{(i)}) \cdot (x_k^{(j)} - a^{(j)})}{\sigma^{(i)} \cdot \sigma^{(j)}}, \quad i, j \in \overline{1, n}, \quad k \in \overline{1, m}. \quad (3)$$

Proposition 1

Let the sequences $X^{(i)}$ and $X^{(j)}$ are independent. Then:

$$E(r_k^{(i,j)}) = 0, \quad Var(r_k^{(i,j)}) = 1, \quad i, j \in \overline{1, n}, \quad k \in \overline{1, m}$$

if $a^{(i)} = \frac{1}{2}, i \in \overline{1, n}$, then $(r_k^{(i,i)})^2 = 1$.

Proof:

1. If the sequences $X^{(i)}$ and $X^{(j)}$ are independent, then the random variables $x_k^{(i)}$ and $x_k^{(j)}$ are also independent, $k \in \overline{1, m}$. Therefore

$$E(r_k^{(i,j)}) = \frac{E(x_k^{(i)} - a^{(i)}) \cdot E(x_k^{(j)} - a^{(j)})}{\sigma^{(i)} \cdot \sigma^{(j)}} = 0$$

Next,

$$\begin{aligned} Var(r_k^{(i,j)}) &= E(r_k^{(i,j)} - E(r_k^{(i,j)}))^2 = E(r_k^{(i,j)})^2 = \\ &= E \frac{(x_k^{(i)} - a^{(i)})^2 \cdot (x_k^{(j)} - a^{(j)})^2}{(\sigma^{(i)})^2 \cdot (\sigma^{(j)})^2} = \frac{1}{(\sigma^{(i)})^2 \cdot (\sigma^{(j)})^2} \cdot E(x_k^{(i)} - a^{(i)})^2 \cdot E(x_k^{(j)} - a^{(j)})^2 = \\ &= \frac{1}{(\sigma^{(i)})^2 \cdot (\sigma^{(j)})^2} \cdot Var(x_k^{(i)}) \cdot Var(x_k^{(j)}) = 1 \end{aligned}$$

2. If $a^{(i)} = \frac{1}{2}$, then $(r_k^{(i,i)})^2 = \frac{(x_k^{(i)} - \frac{1}{2})^2}{(\sigma^{(i)})^2}$. Next, since $x_k^{(i)} \in \{0, 1\}$, then $x_k^{(i)} - \frac{1}{2} \in \{\pm \frac{1}{2}\}$, and $(x_k^{(i)} - \frac{1}{2})^2 = \frac{1}{4}$.

In addition, $(x_k^{(i)})^2 = x_k^{(i)}$, so

**ADVANCES
IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES**

$$\text{Var}(x_k^{(i)}) = E(x_k^{(i)})^2 - (E(x_k^{(i)}))^2 = E(x_k^{(i)})(1 - E(x_k^{(i)})) = \frac{1}{4},$$

whence $(r_k^{(i,i)})^2 = 1$.

The proposition is proved.

For arbitrary $n \in N$, define S_n the group of all permutations of length n , and also define $S_n^{(l)} \subset S_n$ as a subset of permutations that have exactly l fixed points.

Proposition 2

Let $n \in N$ and q be positive integer. Let matrix $A = (a_{ij})_{i,j=1}^n$ be a square matrix such that:

1. $a_{ii} = 1, i \in \{1, \dots, n\}$;
2. $\forall i, j \in \{1, \dots, n\}, i \neq j: a_{ij} = a_{ji}$ and $|a_{ij}| \leq q, \forall i, j \in \{1, \dots, n\}, i \neq j$.

Then the following inequality holds:

$$\left| \det A - 1 + \sum_{1 \leq i < j \leq n} a_{ij}^2 \right| \leq e^{n^2 q} - 1 - n^2 q - \frac{n^3(n-1)}{2} \cdot q^2. \tag{4}$$

Proof:

By the definition of the matrix determinant, and considering the notation introduced at the beginning of the section, we get

$$\det A = \sum_{\sigma \in S_n} \left\{ (-1)^{\text{sign} \sigma} \prod_{i=1}^n a_{i, \sigma(i)} \right\} = \sum_{l=0}^n \sum_{\sigma \in S_n^{(l)}} \left\{ (-1)^{\text{sign} \sigma} \prod_{i=1}^n a_{i, \sigma(i)} \right\}. \tag{5}$$

Next, we note that

$$\left| S_n^{(n)} \right| = 1, \text{ that is, the set } S_n^{(n)} \text{ consists of a single identical permutation}$$

$\left| S_n^{(n-1)} \right| = 0$ since there are no permutations of the length n with $n-1$ fixed points

$\left| S_n^{(n-2)} \right| = C_n^2$, i.e., the number of elements of this set is equal to the number of ways in which the fixed points can be chosen, and the two remaining points are rearranged

in addition, note that this set coincides with the set of all possible permutations that are inversions of two elements; and $\left| S_n^{(l)} \right| \leq C_n^l \cdot (n-l)!$, in the general case.

To prove the last inequality, it is enough to choose fixed points in C_n^l ways, and all the other points can be rearranged in $(n-l)!$ ways; note that we get inequality

**ADVANCES
IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES**

rather than equality, since the permutation of $n-l$ points may give us additional fixed points. That is, the value $|S_n^{(l)}| \leq C_n^l \cdot (n-l)!$ determines the number of such permutations which have *not less than* $n-l$ fixed points.

Now consider separately each term on the right-hand side of (5) for $l \in \{0, \dots, n\}$:

if $l = n$ the corresponding term will be equal to 1

if $l = n-1$ the corresponding term will be equal to 0

if $l = n-2$ the corresponding term will be equal to $-\sum_{1 \leq i < j \leq n} a_{ij}^2$, since the

inversion is an odd substitution, and taking into account the condition $a_{ij} = a_{ji}$.

Therefore, equality (5) can be rewritten as

$$\det A - 1 + \sum_{1 \leq i < j \leq n} a_{ij}^2 = \sum_{l=0}^{n-3} \sum_{\sigma \in S_n^{(l)}} \left\{ (-1)^{\text{sign } \sigma} \prod_{i=1}^n a_{i, \sigma(i)} \right\},$$

whence

$$\left| \det A - 1 + \sum_{1 \leq i < j \leq n} a_{ij}^2 \right| \leq \sum_{l=0}^{n-3} \sum_{\sigma \in S_n^{(l)}} \prod_{i=1}^n |a_{i, \sigma(i)}|. \tag{6}$$

Next, it is easy to see that for $\sigma \in S_n^{(l)}$ there are exactly l units in the product $\prod_{i=1}^n |a_{i, \sigma(i)}|$ (the number of fixed points of the permutation is equal to the number of diagonal matrix elements in the product), then, according to the condition 2) of the

Proposition 2, $\prod_{i=1}^n |a_{i, \sigma(i)}| \leq q^{n-l}$.

Therefore, inequality (6) can be rewritten as

$$\begin{aligned} \left| \det A - 1 + \sum_{1 \leq i < j \leq n} a_{ij}^2 \right| &\leq \sum_{l=0}^{n-3} C_n^l \cdot (n-l)! \cdot q^{n-l} \leq \\ &\leq \sum_{l=3}^n C_n^l \cdot l! \cdot q^l \leq \sum_{l=3}^n C_n^l \cdot l! \cdot q^l \leq \sum_{l=3}^n C_n^l \cdot (n \cdot q)^l = \\ &= \sum_{l=3}^n C_n^l \cdot (n \cdot q)^l = \sum_{l=0}^n C_n^l \cdot (n \cdot q)^l - 1 - n^2 \cdot q - \frac{n \cdot (n-1)}{2} \cdot (n \cdot q)^2 = \\ &= (1 + n \cdot q)^n - 1 - n^2 \cdot q - \frac{n \cdot (n-1)}{2} \cdot (n \cdot q)^2 = \end{aligned}$$

$$\begin{aligned}
 &= \left(1 + \frac{n^2 \cdot q}{n}\right)^n - 1 - n^2 \cdot q - \frac{n \cdot (n-1)}{2} \cdot (n \cdot q)^2 \leq \\
 &\leq e^{n^2 \cdot q} - 1 - n^2 \cdot q - \frac{n^3 \cdot (n-1)}{2} \cdot q^2,
 \end{aligned}$$

which proves equality (4).

Corollary 1

If, in the terms of Statement 2, set $q = \frac{\delta}{n^2}$, for some $\delta \in (0, 1)$, then from inequality (4) we obtain the inequality:

$$\left| \det A - 1 + \sum_{1 \leq i < j \leq n} a_{ij}^2 \right| \leq e^\delta - 1 - \delta - \frac{\delta^2 (n-1)}{2n},$$

that for sufficiently large n can be rewritten as

$$\left| \det A - 1 + \sum_{1 \leq i < j \leq n} a_{ij}^2 \right| \leq e^\delta - 1 - \delta - \frac{\delta^2}{2}.$$

In particular, when $\delta = 1$ we have:

$$\left| \det A - 1 + \sum_{1 \leq i < j \leq n} a_{ij}^2 \right| \leq e - 2.5 \tag{7}$$

Define $R^{(i,j)}$ as

$$R^{(i,j)} = \frac{1}{m} \sum_{k=1}^m r_k^{(i,j)} \tag{8}$$

Because $R^{(i,j)}$ is the average of independent random variables with zero expectation and unit variance, it is easy to see that

$$E\left(R^{(i,j)}\right) = 0 \quad \text{Var}\left(R^{(i,j)}\right) = \frac{1}{m} \tag{9}$$

Below we prove two statements that allow us to construct the first statistical criterion. The first statement is based on Chebyshev inequality [14], the second one is based on Chernoff inequality [15]. Either of them can be used to construct the criterion, although, as it will be shown later, the probability estimate in the second one is always more accurate.

Proposition 3

Let $q > 0$ and $\varepsilon \in (0, 1)$. Then, if the sequences $X^{(i)}$ and $X^{(j)}$, defined in (1), are

independent, and $m > \frac{1}{\varepsilon \cdot q^2}$, then the next inequality holds:

**ADVANCES
IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES**

$$P\left(\left|R^{(ij)}\right| > q\right) \leq \varepsilon \tag{10}$$

The proof follows from Chebyshev inequality and the formulas (9).

Proposition 4

Let $q > 0$ and $\varepsilon \in (0,1)$. Then, if the sequences $X^{(i)}$ and $X^{(j)}$, defined in (1), are

independent, and $m > \frac{\ln \frac{2}{\varepsilon}}{q^2}$, then the next inequality holds:

$$P\left(\left|R^{(ij)}\right| > q\right) \leq \varepsilon \tag{11}$$

Proof:

According to Chernoff's inequality, $\forall a > 0$ the next inequality is true:

$$P\left(\left|\sum_{k=1}^m r_k^{(i,j)}\right| > a\right) \leq 2e^{-\frac{a^2}{2 \cdot m}}$$

whence

$$P\left(\frac{\left|\sum_{k=1}^m r_k^{(i,j)}\right|}{m} > \frac{a}{m}\right) = P\left(R^{(ij)} > \frac{a}{m}\right) \leq 2e^{-\frac{a^2}{2 \cdot m}}$$

Set $q = \frac{a}{m}$; then the last inequality can be rewritten as

$$P\left(R^{(ij)} > q\right) \leq 2e^{-q^2 \cdot m} \tag{12}$$

and for $m > \frac{\ln \frac{2}{\varepsilon}}{q^2}$ we get $2e^{-q^2 \cdot m} < \varepsilon$.

The Proposition is proved.

Note that from inequality $m > \frac{1}{\varepsilon \cdot q^2}$ we have $m > \frac{\ln \frac{2}{\varepsilon}}{q^2}$, so Proposition 4 gives a more accurate lower bound for the value of m .

5. Construction of a statistical criterion and algorithm for testing the hypothesis about sequence independence.

In this section we construct a new statistical criterion for checking the independence of sequences and develop the corresponding algorithm.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

The basic idea behind the criterion can be described informally as follows. Let's set a certain level of significance α (probability of the 1st type error). If the sequences (1) are pairwise independent, then for sufficiently large m (chosen according to Propositions 3 or 4), we can construct correlation matrix $A = \left(R^{(ij)} \right)_{i,j=1}^n$, which elements (except diagonal elements) will be less than a certain value q with a probability not less than $1 - \alpha$. The value q should be chosen in a such way that the right-hand side of (4) is sufficiently small – for example, $q = \frac{1}{n^2}$. Then calculate the elements of a matrix A and its determinant and check the inequality (4). Then, according to the choice of the sequence length, for pairwise independent sequences, the probability that inequality (4) does not hold does not exceed α .

Let us have access to sources of sequence generation (1) and can obtain sequences of sufficient length from them (the required length depends on the number of n sequences and the desired level of significance).

It should be noted that the algorithm below is focused on checking the independence of the sources that generate the corresponding sequences. This is the task that is most relevant for practical applications. But, with certain modifications, it can also be used to check the independence of given sequences.

Algorithm 1:

Input: level of significance α ; number n of sequences to be tested.

1. Compute

$$q = \frac{1}{n^2} \quad \text{and} \quad m = \left\lceil \frac{\ln \frac{2}{\alpha}}{q^2} \right\rceil. \quad (13)$$

2. Generate (from corresponding sources or one source, depending on the set task) n sequences $X^{(i)}$, $i \in \overline{1, n}$, of the lengths at least t . Note that there is no need to generate sequences if the task is to check the independence of sequences from a given set, but we need to be sure that their lengths are at least m .

$$A = \left(R^{(ij)} \right)_{i,j=1}^n$$

3. Calculate the elements of a matrix using formulas (3) and (8).

4. Compute $d = \det A$.

5. Compute

$$t = \left| \det A - 1 + \sum_{1 \leq i < j \leq n} a_{ij}^2 \right|.$$

6. If $t \leq e - 2.5 \approx 0.218$, then hypothesis H_0 accepted, otherwise rejected.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

As we can see from the formula (13), the lower bound of the value m increases when the value α decreases, and increases when the value n increases. Note that if the level of significance α is not less than 0.001, and the number of sequences is not larger than 100, the lengths of sequences $m = 10^8$ is sufficient for testing.

To simplify the application of this algorithm, we propose the Table 1 with reference values of the lower bound of the sequences length m for different frequently used values of two other parameters, the level of significance α and the number of sequences n .

Table 1

The lower bound of parameter m

n α	10	20	30	40	50
0.05	36 889	590 221	2 987 993	9 443 532	23 055 497
0.01	52 984	847 731	4 291 638	13 563 693	33 114 484
0.005	59 915	958 635	4 853 087	15 338 150	37 446 654
0.001	76 010	1 216 145	6 156 731	19 458 311	47 505 641

6. Experimental results of the Algorithm 1 application

Practical applications of the proposed criteria give the next results:

- 1) for sequences obtained from the certified generator (described in Appendix A in [16]), in 10 experimental sets of 100 sequences, hypothesis H_0 was accepted;
- 2) for sequences obtained using counter, in 10 experimental sets of 100 sequences, hypothesis H_0 was rejected 9 times and accepted 1 time;
- 3) for sequences obtained from file with extension avi, in 10 experimental sets of 100 sequences, hypothesis H_0 was rejected 10 times;
- 4) for set of 100 sequences, where 50 of them were generated from the certified generator, and other 50 were obtained from them, using some transformations, hypothesis H_0 was rejected 10 times out of 10.

We also applied this test to sets of sequences, which were created to be dependent. To describe these results, we introduce the term “experiment”. Under one experiment we will understand the following procedure:

- to generate definite number of sequences (for example, 20 sequences) of sufficient lengths (for example, 10^6 or larger), using some certified generator;
- to introduce dependences in chosen sequences (if necessary);
- to create correlation matrix and to evaluate the value f .

Below we describe the results obtained in such experiments.

- 1) **50% of sequences are dependent in half of the characters.** For 100 experiments, each with 20 sequences, we firstly got 20 sequences from certified PRNG, then chose 10 of them, and then each second element of these chosen sequences was changed in such a way, that introduce dependency on correspondent

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

elements of the first 10 sequences. For these 100 experiments, we got the next range of the value t : $t \in [1.55233507592079; 1.56300829290009]$. It means that in all experiments the value lays deeply in critical region, so the criterion strongly recognized dependent sequences.

2) **50% of sequences are dependent in 33% of the characters.** For 100 experiments, each with 20 sequences, we firstly got 20 sequences from certified PRNG, then chose 10 of them, and then each third element of these chosen sequences was changed in such a way, that introduces dependency on correspondent elements of the first 10 sequences. For these 100 experiments, we got the next range of the value t : $t \in [0.416068024780703; 0.422475116952477]$. It is still essentially larger than the edge of critical region (which is 0.218), but much closer to this edge than in previous experiments. These results show that the larger dependency between sequences, the deeply in critical region the statistics t takes values.

3) **25% of sequences are dependent in half of the characters.** For 100 experiments, each with 20 sequences, we firstly got 20 sequences from certified PRNG, then chose 5 of them, and then each second element of these chosen sequences was changed in such a way, that introduce dependency on correspondent elements of the first 5 sequences. For these 100 experiments, we got the next range of the value t : $t \in [0.484858277736367; 0.489774359187274]$. This range is closer to the edge of critical region, than in the first series of experiments, but further than in the second series of experiments. So the criterion can recognized dependency even in case when 75% of sequences are independent.

4) **Archive files.** For all 1000 experiments, $t \in [0.0000134436852349293; 124.401400670346]$, and in less than 1% cases the value of t is less than 0.218, or outside critical region.

7. Designations and auxiliary statements needed for the second criterion and Algorithm 2

Let us have a set τ_i of m bit sequences of the length l :

$$X^{(i)} = (x_1^{(i)}, \dots, x_l^{(i)}), \quad i \in \overline{1, m}, \quad x_k^{(i)} \in \{0, 1\}. \quad (14)$$

$$a^{(i)} = \frac{1}{l} \sum_{k=1}^l x_k^{(i)}$$

Define the sample average of these sequences. Usually, the sequences under investigations are obtained from RNG/PRNG; in such cases we may assume that $a^{(i)} = 0.5$. But the proposed criterion is still true for more general cases.

The criterion proposed below is based on the results, described in [13], and uses sample correlation matrix.

For sequences (14), define values

**ADVANCES
IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES**

$$D_{ij} = \frac{1}{l-1} \sum_{k=1}^l (x_k^{(i)} - a^{(i)})(x_k^{(j)} - a^{(j)}),$$

which are sample pairwise correlations, and build sample correlation matrix

$$\mathbf{R} = (R_{ij})_{i,j=1}^m, \text{ где } R_{ij} = \frac{D_{ij}}{\sqrt{D_{ii}}\sqrt{D_{jj}}}, \quad i, j \in \overline{1, m}.$$

Note that for pairwise independent random variables $X^{(i)}, i \in \overline{1, m}$, the matrix \mathbf{R} is identity matrix I , so its determinant is equal to 1. But in our case this matrix was built as empirical, according to the results of statistical experiments. Then for creating the criterion for checking hypothesis H_0 , that «sequences are pairwise independent» with given significance level α (for example, $\alpha = 10^{-3}$) we use the determinant $d = \det \mathbf{R}$ of the matrix \mathbf{R} .

The distribution law of the determinant d is rather complicated, but for large enough values of l we can use its asymptotical form: if sequences are pairwise independent, then

$$\mathbf{P}\{-n \cdot \ln d \leq v\} = \mathbf{P}\{\chi_f^2 \leq v\} + \frac{\gamma}{n^2} (\mathbf{P}\{\chi_{f+4}^2 \leq v\} - \mathbf{P}\{\chi_f^2 \leq v\}) + O(n^{-3}), \quad (15)$$

where

$$f = \frac{m(m-1)}{2}, \quad n = l - \frac{2m+11}{6}, \quad \gamma = \frac{m(m-1)(2m^2 - 2m - 13)}{288},$$

and χ_f^2 is a random variable with χ -square distribution with f degrees of freedom.

Note that for $l \geq 10^5, m \geq 100$ one can use approximation

$$\mathbf{P}\{-n \cdot \ln d \leq v\} \approx \mathbf{P}\{\chi_f^2 \leq v\}.$$

As we can see, in case of approximation of (15) we delete the positive values in its right part, so the obtained critical region corresponds to the large significance level then was set.

For hypothesis H_0 , under given significance level $\alpha = 1 - P(-n \cdot \ln d \leq v)$, the critical region is $-n \cdot \ln d > v$, or $d \in \left(0; e^{-\frac{v}{n}}\right)$.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

After performing calculations according (15) or its approximation, we get critical region for parameter $d = \det \mathbf{R}$, which corresponds to given significance level α (for example, if $l = 10^6$, $m = 100$, then critical region for parameter d under given $\alpha = 10^{-3}$ is the region $d \in (0; 0.994754314)$; under given $\alpha = 10^{-2}$ the critical region is $d \in (0; 0.994830549)$). The critical regions for these or other levels may be found using tables for χ^2 -square distribution with f degree of freedoms (if $f \leq 30$) or using normal approximation (if $f \geq 30$). Thus, for $f \rightarrow \infty$, χ^2 -square distribution tends to normal distribution with parameters $N(f, \sqrt{2f})$. It means that if $f \geq 30$ then one may use approximation

$$\mathbf{P}\{\chi_f^2 \leq v\} = \mathbf{P}\left\{\frac{\chi_f^2 - f}{\sqrt{2f}} \leq \frac{v - f}{\sqrt{2f}}\right\} \approx F\left(\frac{v - f}{\sqrt{2f}}\right),$$

where $F(x)$ is cumulative distribution function of normal distribution.

Table 2

Values of determinant of correlation matrix for 20 series of 100 sequences, each of the length of 10^6 bits, generated using certified PRNG

Series numbers	Values of determinant	Series numbers	Values of determinant
1	0.995169	11	0.995223
2	0.995150	12	0.995219
3	0.995164	13	0.995193
4	0.995178	14	0.995174
5	0.995172	15	0.995205
6	0.995182	16	0.995188
7	0.995163	17	0.995219
8	0.995168	18	0.995247
9	0.995166	19	0.995227
10	0.995201	20	0.995205
Sample average			0.99519065

In other words, for given significance level α , to calculate limit statistics v_α one needs, at first, to find corresponding limit statistics z_α , using tables of normal distribution, and after this to calculate limit statistics for χ_f^2 as $v_\alpha = z_\alpha \cdot \sqrt{2f} + f$.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

As example, in Table 2 the values of d are given, calculated for 20 series of 100 sequences, each of the length of 10^6 bits.

8. Description of Algorithm 2 and results of its application

Based on results described in Section 8, we can derive the next Algorithm 2.

Algorithm 2:

Input: level of significance α ;
set of sequences (14).

$$a^{(i)} = \frac{1}{l} \sum_{k=1}^l x_k^{(i)}$$

1. For given sequences, calculate the values
2. For given sequences, calculate the values

$$D_{ij} = \frac{1}{l-1} \sum_{k=1}^l (x_k^{(i)} - a^{(i)})(x_k^{(j)} - a^{(j)})$$

3. Calculate the values $R_{ij} = \frac{D_{ij}}{\sqrt{D_{ii}} \sqrt{D_{jj}}}$, $i, j \in \overline{1, m}$.

4. Build correlation matrix $\mathbf{R} = (R_{ij})_{i,j=1}^m$.

5. Calculate $d = \det \mathbf{R}$.

6. Calculate the next values:

$$f = \frac{m(m-1)}{2}, \quad n = l - \frac{2m+11}{6}, \quad \gamma = \frac{m(m-1)(2m^2 - 2m - 13)}{288}$$

7. If $f < 30$, then for given significance level α , using tables for χ_f^2 -distribution, find such value v_α , that $\mathbf{P}\{\chi_f^2 \geq v_\alpha\} = \alpha$.

Else, if $f \geq 30$, then do the next steps.

- 7.1. For given significance level α , using tables for normal distribution, find such value z_α , that $\Phi(z_\alpha) = 1 - \alpha$ (if tables consists of values of cumulative distribution function for normal distribution $\Phi(x)$), or such z_α , that

$$\Phi_0(z_\alpha) = \frac{1}{2} - \alpha \quad (\text{if tables consists of values of function } \Phi_0(x) = \Phi(x) - \frac{1}{2}).$$

Example: using tables of values of function $\Phi_0(x)$ in reference book of Bernshtain and Semendyaev, for $\alpha = 0.01$ we get $z_\alpha = 2.33$; for $\alpha = 0.001$ we get $z_\alpha = 3.1$.

**ADVANCES
IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES**

7.2. Calculate the value v_α as

$$v_\alpha = z_\alpha \cdot \sqrt{2f} + f$$

8. If inequality $d \geq e^{-\frac{v_\alpha}{n}}$ holds, then hypothesis H_0 about pairwise independence is accepted, in the opposite case H_0 is rejected.

On the Figure 1 below we give the comparative results of application of Algorithm 2 to the sequences, obtained from the PRNG (black lines) and limit values of the value d , calculated according Algorithm 2 (red dotted lines), for different values of the sequences length l (from 200000 to 1000000 bits) and different numbers of sequences m (from 10 to 100). As we can see, the values of parameter d , calculated for given sequences, are very close to the edge of critical region. It means that this criterion is very accurate and has very small error of the second type (probability to accept H_0 in case when it is wrong).

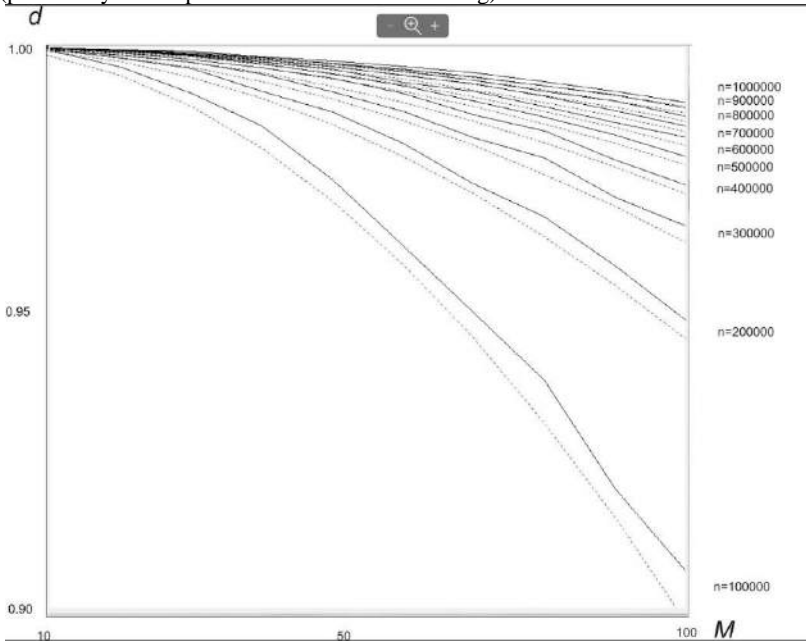


Figure 1. Comparison of results of PRNG testing according Algorithm 2 and limit statistics for determinant of correlation matrix

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

For these experiments, the stream cipher Krip [12] was used as PRNG. Note that this cipher was investigated using a lot of statistical tests, in particular NIST test suite [3], hence it may be considered as PRNG of high quality.

During investigations of statistical properties of RNG/PRNG, or stream ciphers, one may need to check the independence of different sequences, obtained on different steps of working of this generator. For example, it is necessary to check the independence of output gamma, internal state sequences, and input data, etc. And we need to be sure that all the parts of these sequences are pairwise independent.

In this case one may use Algorithms 1 or 2 for total set of the sequences, which consists of all sequences, obtained on different steps of generator's work. For example, we may take half of the sequences from inner states and half from output gamma.

If we cryptographic quality of stream cipher, then the set of sequences for checking should contain sequences created using different (randomly chosen) keys and initialization vectors. The number of sequences should be not less than 100, and their lengths should be not less than 10^6 .

9. Conclusion and discussion

The proposed criteria for checking pairwise independence of random values/sequences are rather simple and convenient in practice. Their practical applications show that they work "in both directions": accept hypothesis H_0 for sets of independent sequences and reject H_0 in opposite case.

The experimental results show that the both proposed criteria reject hypothesis about independence in case when the number of sequences, which may be considered as independent, is up to 75%.

They may be used, along with other statistical tests, for checking statistical qualities of stream or combined ciphers and for random/pseudorandom number generators before adoption.

One of the tasks for the further investigations is more detailed comparative analysis of behavior of these two criteria for different types of sequences, obtained from sources with different nature, including stream cipher Krip [12]. It should be noted, that the first proposed criterion gives more rough estimation of the edges of critical region, if compare with the second one.

This leads to situation when the sequences with a slight dependency may be defined as independent. But in case when dependency is strong enough, it works well, as was shown in our experiments in Section 7. At the same time, the first criterion is much more easily to apply, it needs a small amount of calculations, and needs no tables of distribution functions for widely used distributions, like normal or hi-square distribution. From this point of view, we suggest to use the first criterion for primary analysis of RNG, or PRNG, or stream cipher.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

If this criterion decides that sequences obtained from the source are independent, then we may continue to analyze the source more deeply, applying the second criterion and other tests. But in opposite case, when the source fails the first criterion, it means that this source can't be used in cryptographic applications and needs at least significant improvements.

The other interesting question is to find such modification of these criteria, which may be used not only for checking independence of sequences or corresponding random variables, but also for checking independence of statistical tests from the different test suits, like NIST or Diehard.

This problem is also of great importance, because excluding "redundant" tests from the suit allows to reduce significantly the time of application of the test suite. In the current form, the proposed criteria can't be used for this purpose, and it's a great challenge to invent suitable modification and to prove its relevance.

10. Funding and support

The research was conducted within the framework of project 2023.04/0020, "Development of Methods and Layout of the "DEMETRA" ARM for Regular and Periodic Control of the Functioning of Cryptographic Applications Using Statistical Methods," funded by the National Research Foundation of Ukraine (NRFU).

11. References

- [1] Christof Paar, Jan Pelzl, "Stream Ciphers", Chapter 2 of "Understanding Cryptography, A Textbook for Students and Practitioners". Springer, 2009. URL: https://dosen.itats.ac.id/sitiagustini/wp-content/uploads/sites/78/2017/05/Understanding_Cryptography_Chptr_2-Stream_Ciphers.pdf.
- [2] Matt J. B. Robshaw, Stream Ciphers Technical Report TR-701, version 2.0, RSA Laboratories, 1995 <https://www.networkdls.com/Articles/tr-701.pdf>.
- [3] A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST Special Publication 800-22, 1999. Rev. 1. – 131 p.
- [4] Almaraz Luengo, E.; Román Villaizán, J. Cryptographically Secured Pseudo-Random Number Generators: Analysis and Testing with NIST Statistical Test Suite. *Mathematics* 2023, 11, 4812. URL: <https://doi.org/10.3390/math11234812> (1 in the list).
- [5] Suwais, K.; Almanasra, S. Strike: Stream Cipher Based on Stochastic Lightning Strike Behaviour. *Appl. Sci.* 2023, 13, 4669. URL: <https://doi.org/10.3390/app13084669>, <https://www.mdpi.com/2076-3417/13/8/4669>.
- [6] Wu, S.-T. A Key-Based Multi-Mode Clock-Controlled Stream Cipher for Real-Time Secure Communications of IoT. *Electronics* 2023, 12, 1076. URL: <https://doi.org/10.3390/electronics12051076>.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

- [7] Melosik, M.; Galan, M.; Naumowicz, M.; Tylczyński, P.; Koziol, S. Cryptographically Secure PseudoRandom Bit Generator for Wearable Technology. *Entropy* 2023, 25, 976. URL: <https://doi.org/10.3390/e25070976>.
- [8] Bikos, A.; Nastou, P.E.; Petroudis, G.; Stamatiou, Y.C. Random Number Generators: Principles and Applications. *Cryptography* 2023, 7, 54. URL: <https://doi.org/10.3390/cryptography7040054>.
- [9] Piątkowski, J.; Szymoniak, S. Methodology of Testing the Security of Cryptographic Protocols Using the CMMTree Framework. *Appl. Sci.* 2023, 13, 12668. URL: <https://doi.org/10.3390/app132312668>.
- [10] Crocetti, L.; Nannipieri, P.; Di Matteo, S.; Fanucci, L.; Saponara, S. Review of Methodologies and Metrics for Assessing the Quality of Random Number Generators. *Electronics* 2023, 12, 723. URL: <https://doi.org/10.3390/electronics12030723>.
- [11] Madarro-Capó, E.J.; Ramos Piñón, E.C.; Sosa-Gómez, G.; Rojas, O. Practical Improvement in the Implementation of Two Avalanche Tests to Measure Statistical Independence in Stream Ciphers. *Computation* 2024, 12, 60. URL: <https://doi.org/10.3390/computation12030060>, <https://www.mdpi.com/2079-3197/12/3/60>.
- [12] Kovalchuk L.V., Koriakov I.V., Alekseychuk A.N. Krip: high-speed hardware-oriented stream cipher based on a non-autonomous nonlinear shift register. 2023. *Cybernetics and System Analysis* Vol.59, P. 16–26. URL: <https://doi.org/10.1007/s10559-023-00538-6> (date of access: 27.04.2024).
- [13] Anderson, T.W. *An Introduction to Multivariate Statistical Analysis*. John Wiley & Sons, New York. 1958. 500 p.
- [14] Feller, W. (1968) *An Introduction to Probability Theory and Its Applications*, Vol. 1. 3rd Edition, John Wiley & Sons, New York.
- [15] Michel Goemans. Chernoff bounds, and some applications. Lecture notes. 2015. URL: <https://math.mit.edu/~goemans/18310S15/chernoff-notes.pdf>.
- [16] DSTU 9041:2020 Information technologies. Cryptographic protection of information. Short message encryption algorithm based on twisted elliptic Edwards curves.

**НОВІ СТАТИСТИЧНІ КРИТЕРІЇ ДЛЯ ПЕРЕВІРКИ
НЕЗАЛЕЖНОСТІ БІТНИХ ВИПАДКОВИХ ЗМІННИХ ТА
ПОСЛІДОВНОСТЕЙ**

Dr.Sci. Л. Ковальчук ORCID: 0000-0003-2874-7950

*Г.Є. Пуховський інститут моделювання в енергетиці, Україна
E-mail: lusi.kovalchuk@gmail.com*

Dr.Sci. А. Давиденко ORCID: 0000-0001-6466-1690

*Г.Є. Пуховський інститут моделювання в енергетиці, Україна
E-mail: davidenkoan@gmail.com*

О. Беспалов 0000-0001-7126-6752

*Г.Є. Пуховський інститут моделювання в енергетиці, Україна
E-mail: alexb5dh@gmail.com*

Анотація. У статті запропоновано строго обґрунтовані два статистичні критерії для перевірки попарної незалежності бітових послідовностей, які можна розглядати як реалізацію випадкових величин із певної множини. Також розроблено та чітко покроково сформульовано відповідні алгоритми, які реалізують перевірку незалежності за цими критеріями. Отримані інструменти дуже актуальні для статистичної перевірки криптографічних якостей різних криптографічних примітивів, функціонування яких пов'язане з генерацією випадкових/псевдовипадкових послідовностей. Такі крипто-примітиви включають не лише генератори випадкових/псевдовипадкових послідовностей, але й потокові шифри, комбіновані алгоритми шифрування (тобто блокові алгоритми в потокових режимах) тощо. Використання запропонованих критеріїв дозволяє перевіряти незалежність різних частин вихідних послідовностей, або незалежність вихідних послідовностей від послідовностей внутрішніх станів і вхідних даних. Слід зазначити, що така незалежність є необхідною умовою для того, щоб вихідна послідовність вважалася непередбачуваною. У статті також розглянуто порівняльний аналіз двох наведених критеріїв та результати їх застосування до послідовностей різних типів.

Ключові слова: статистичний критерій, випадкові величини, незалежність випадкових величин, генерація випадкових чисел, статистична перевірка незалежності

Section 4. Mathematical and simulation modeling

УДК 004.412:519.25

**ЧОТИРЬОХФАКТОРНА НЕЛІНІЙНА РЕГРЕСІЙНА МОДЕЛЬ
ДЛЯ ОЦІНЮВАННЯ РОЗМІРУ JAVA-ЗАСТОСУНКІВ НА
РАННІХ СТАДІЯХ РОЗРОБКИ**

О. Орєхов ORCID: 0000-0002-0001-0140

*Національний університет кораблебудування імені адмірала Макарова,
Україна*

E-mail: oleksandr.oriekhov@nuos.edu.ua

***Анотація.** У роботі розглядається побудова чотирьохфакторної нелінійної регресійної моделі для оцінки кількості рядків коду KLOC JAVA-застосунків. Оцінювання розміру JAVA-застосунку є актуальною науково-практичною задачею, яка невід'ємно пов'язана з життєвим циклом розробки програмного забезпечення (ПЗ). Метою роботи є підвищення достовірності оцінювання кількості рядків коду JAVA-застосунків на ранніх стадіях розробки ПЗ за метриками діаграми класів шляхом побудови чотирьохфакторної нелінійної регресійної моделі. Об'єктом дослідження є процес оцінювання розміру JAVA-застосунків з відкритим кодом. Предметом дослідження є математичні моделі для оцінювання розміру JAVA-застосунків. Для досягнення поставленої мети було зібрано навчальну та тестові вибірки інформації з метрик JAVA-застосунків із відкритим програмним кодом, проведено аналіз та порівняння існуючих математичних моделей і рівнянь для оцінювання розміру JAVA-застосунків. На базі навчальної вибірки, побудовано чотирьохфакторну нелінійну регресійну модель та її інтервали прогнозування для оцінювання розміру JAVA-застосунків на основі нормалізуючого перетворення Бокса-Кокса за метриками кількості класів, загальною кількістю унікальних викликів методів в класах, середнім значенням кількості зв'язків між класами та середнім значенням кількості видимих методів на клас. Отримана чотирьохфакторна нелінійна регресійна модель має меншу середню величину відносної похибки, вище значення відсотка передбачення для рівня відносної похибки 0,25 та вище значення коефіцієнту детермінації у порівнянні з існуючими моделями, що дозволяє підвищити достовірність оцінювання кількості рядків коду JAVA-застосунків.*

***Ключові слова:** оцінювання кількості рядків коду, JAVA-застосунок, негаусівські дані, нормалізуюче перетворення Бокса-Кокса, нелінійна регресійна модель.*

1. Вступ

Оцінка трудомісткості розробки програмного забезпечення є одним з ключових показників для бізнесу при формуванні бюджету та плануванні часу

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

розробки. Ця задача є важливою для ІТ-компаній, оскільки дозволяє отримати прогноз кількісних показників ресурсів, які необхідні для створення програмного проєкту, допоможе враховувати ризики і ресурси та дозволить підвищити ефективність процесу розробки. Критерії достовірної оцінки ґрунтуються на здатності її підтримувати успішну реалізацію програмного проєкту. Заниження або завищення оцінки трудомісткості може призвести до певних проблем. Достовірна оцінка є джерелом інформації для формування реальних витрат по ресурсам проєкту, що дозволяє менеджерам проєкту прийняти найбільш ефективні рішення для досягнення поставлених цілей [1].

Статистика успішності програмних проєктів, яка представлена компанією The Standish Group за період 25 років [2], має помірну позитивну динаміку в бік збільшення частки успішно реалізованих проєктів. Так, в 1994 частка успішно реалізованих проєктів складала 16%, а в 2020 році відсоток таких проєктів (виконані вчасно, в межах бюджету, реалізовано 100% вимог) вже становив 35%. Статистика провальних проєктів зменшилась з 31% до 19% за період з 1994 по 2020 рік. А частка проєктів, які зазнали проблеми (не вклалися в терміни, або вийшли за рамки бюджету, або функціонал не був повністю реалізований у відповідності до вимог), має незначну тенденцію до зменшення, біля 4% , рис. 1.

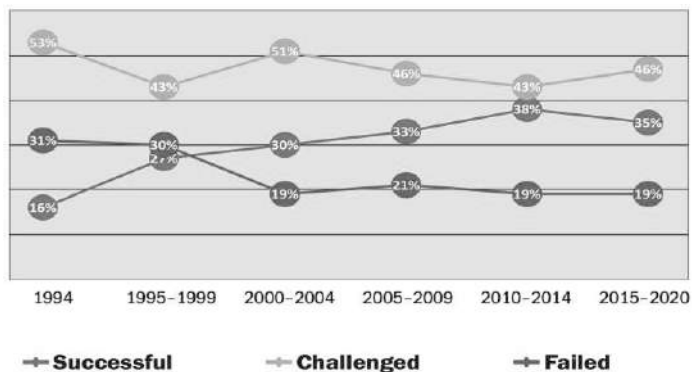


Рисунок 1. Дослідження успішності реалізації ІТ проєктів за даними The Standish Group за період з 1994 року по 2020 рік [2].

Де **successful** – успішні проєкти, **challenged** – проєкти з певними проблемами при реалізації, **failed** – проєкти, які провалились

Крім того дослідження The Standish group [3] доводить, що чим більший і складніший проєкт, тим вище імовірність появи труднощів при реалізації програмного проєкту відповідно до вимог, бюджету та часових рамок (рис. 2.), що були встановлені на початкових етапах планування.

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

	SUCCESSFUL	CHALLENGED	FAILED	TOTAL
Grand	6%	51%	43%	100%
Large	11%	59%	30%	100%
Medium	12%	62%	26%	100%
Moderate	24%	64%	12%	100%
Small	61%	32%	7%	100%

Рисунок 2. Статистика успішності розробки ПЗ в залежності від його розміру [3]

Мова програмування JAVA є однією з найбільш поширених мов програмування на сучасному ринку розробки ПЗ. JAVA - це високорівнева мова програмування, створена компанією Sun Microsystems (зараз Oracle) у 1995 році. Вона широко використовується в багатьох сферах, таких як розробка веб-застосунків, наукові обчислення, розробка штучного інтелекту, розробка мобільних застосунків та ігор [4]. Згідно з результатами досліджень та індексами популярності мов програмування, такими як IEEE, TIOBE, JAVA постійно утримується на передових позиціях [5, 6].

Але, не дивлячись на стрімкий розвиток галузі інформаційних технологій, дослідження успішності завершення проектів ПЗ показали, що існують проблеми із достовірністю оцінювання трудомісткості та вартості розробки ПЗ. Аналіз останніх досліджень і публікацій показав, що збільшення достовірності оцінювання розміру ПЗ можливо досягти враховуючи такі особливості, як фактори середовища при оцінці трудомісткості розробки ПЗ за допомогою таких параметричних моделей як СОСОМО II та інших [7].

Тому оцінка розміру програмного забезпечення на ранніх етапах розробки програмного проекту, яка використовується в параметричних моделях оцінок трудомісткості та вартості є важливою науково-практичною задачею. Для досягнення достовірного рівня оцінювання розміру ПЗ потрібні відповідні математичні моделі, які враховують особливості мови програмування, такої як JAVA [7].

Метою і завданнями дослідження є підвищення достовірності оцінювання розміру JAVA-застосунків на ранніх стадіях розробки на основі наборів даних інформації з метрик коду проектів з відкритим кодом за метриками діаграми класів із застосування чотирьохфакторної нелінійної регресійної моделі.

Для досягнення поставленої мети необхідно вирішити наступні завдання:

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

1. Провести аналіз існуючих моделей оцінювання розміру JAVA-застосунків. Дослідити їх переваги та недоліки. Порівняти існуючі моделі за критеріями якості регресійних моделей.

2. Удосконалити чотирьохфакторну нелінійну регресійну модель для оцінювання розміру програмних JAVA-застосунків на ранніх стадіях розробки за метриками діаграми класів із застосування багатовимірних нормалізуючих перетворень та визначити довірчий інтервал та інтервал прогнозування.

3. Побудувати довірчий інтервал і інтервал прогнозування нелінійної регресійної моделі оцінювання розміру JAVA-застосунків.

Об'єктом дослідження є процес оцінювання розміру кількості рядків коду JAVA-застосунків.

Предметом дослідження є нелінійні регресійні моделі для оцінювання розміру програмних JAVA-застосунків.

2. Аналіз існуючих математичних моделей для оцінки розміру JAVA-застосунків

Для оцінювання розміру JAVA-застосунків з відкритим кодом побудовано як лінійні [8, 9] так і нелінійні [10,11,12,13] регресійні рівняння та моделі в залежності від різної кількості та варіації метрик з концептуальної моделі даних у вигляді UML діаграм, зокрема діаграм класів. Так в [8, 9] запропоновані трьохфакторні лінійні регресійні рівняння для оцінювання JAVA-застосунків з відкритим кодом та інформаційних систем. Але, як відомо, при побудові лінійних регресійних моделей необхідно виконання певних умов, зокрема похибки повинні бути розподілені за нормальним законом, що можливо лише в поодиноких випадках для інформації з метрик програмних застосунків. Роботи [10,11,12,13] пропонують нелінійні регресійні моделі з різною кількістю факторів та наборів даних, які були використані для побудови цих моделей. Так [10] пропонує трьохфакторну нелінійну регресійну модель для оцінки розміру інформаційних систем на базі набору даних з робіт [8, 9], робота [11] пропонує однофакторну нелінійну регресійна модель для оцінювання JAVA веб-застосунків, ці регресійні моделі не беруть до уваги особливості оцінювання JAVA-застосунків які не є інформаційними системами або веб-застосунками. Робота [12] пропонує чотирьох факторну нелінійну регресійну модель на основі перетворення Джонсона з сім'ї SB, але вона, як і [10], має певні обмеження границь допустимих значень, що накладене нормалізуючим перетворенням. Крім того, робота [12] доводить, що зі збільшенням факторів нелінійних регресійних моделей, зменшується ширина інтервалу прогнозування та довірчого інтервалу, це, в свою чергу, дозволяє врахувати оптимістичний та песимістичний сценарії. У [13, 14, 15] доведено що застосування вибірки більшого розміру та методів перехресного затвердження (Cross-Validation) дозволяє досягти більшої стійкості та надійності регресійних моделей у порівнянні з регресійними моделями, які

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

побудовані на вибірках з відносно невеликим розміром та без застосування методу перехресного затвердження.

Для порівнянні математичних моделей за критеріями якості, були зібрані дані за метриками програмного коду 571 JAVA-застосунків, розташованих на платформі GitHub (<https://github.com>). За допомогою інструменту СК (<https://github.com/mauricioaniche/ck>) отримані наступні метрики: кількість рядків коду (KLOC), загальна кількість класів (CLASS), загальна кількість унікальних викликів методу в класі (RFC), загальна кількість значень згуртованості методів класу (LCOM), загальна кількість статичних методів (SMQ), загальна кількість видимих методів (VMQ), загальна кількість атрибутів класів (TFQ), зв'язність між класами (CBO). Ці метрики можна отримати на ранній стадії проєктування з концептуальної моделі застосунку. Отриманий набір даних був розділений випадковим чином на навчальну і тестову вибірки з розмірами в 286 та 285 рядків даних відповідно. Розподіл метрик відносно KLOC наведені на рис. 3.

Для оцінки достовірності прогнозування регресійних моделей та рівнянь використовуються такі критерії якості, як коефіцієнт детермінації R^2 , значення середньої величини відносної похибки $MMRE$ [14] та значення відсотка передбачення для рівня відносної похибки 0,25 - $PRED(0,25)$ [14].

Коефіцієнт детермінації R^2 визначається як

$$R^2 = 1 - \frac{SSE}{SST}, \quad (1)$$

де SSE - сума квадратів залишків (the residual sum of squares) або сума квадратів помилок (the error sum of squares), $SSE = \sum_{i=1}^N (y_i - \hat{y}_i)^2$; SST - загальна сума квадратів (the total sum of squares), $SST = \sum_{i=1}^N (y_i - \bar{y})^2$.

Критерій $MMRE$ визначається як

$$MMRE = \frac{1}{N} \sum_{i=1}^N MRE_i \quad (2)$$

де MRE_i - значення величини відносної похибки для i -го рядку даних випадкової величини

$$MRE_i = \left| \frac{(y_i - \hat{y}_i)}{y_i} \right| \quad (3)$$

Значення відсотка передбачення для рівня відносної похибки 0,25 $PRED$,

$$PRED(0,25) = \frac{1}{N} \sum_{i=1}^N \begin{cases} 1, & \text{if } MRE_i \leq 0,25 \\ 0, & \text{otherwise} \end{cases} \quad (4)$$

Достовірність оцінювання регресійними моделями вважається прийнятною, якщо значення $MMRE \leq 0,25$, значення $PRED(0,25) \geq 0,75$. Значення R^2 вважається прийнятним, якщо воно більше за 0,75 [17].

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

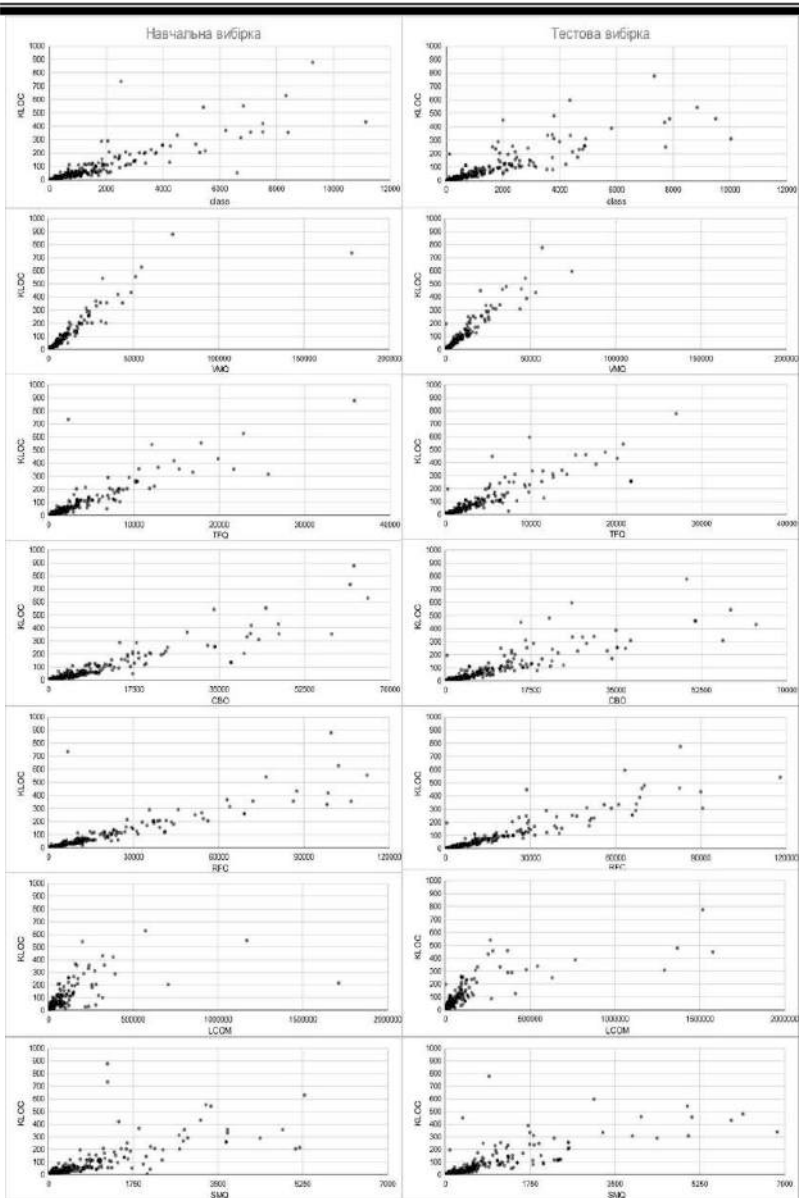


Рисунок 3. Розподіл даних навчальної та тестової вибірок

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

У роботі [13] існуючі регресійні моделі і рівняння оцінювання розміру рядків коду JAVA-застосунків [8, 9, 10, 11, 12] були перевірені за множинним коефіцієнтом детермінації R^2 (1), середньою величиною відносної помилки $MMRE$ (2) і відсотком прогнозованих результатів, для яких величини відносної помилки MRE (3) менші за 0,25, $PRED(0,25)$ (4). Результат перевірки показав їх незадовільний рівень достовірності як для навчальної так і для тестової вибірок.

Так оцінки R^2 , $MMRE$ та $PRED(0,25)$ для лінійних регресійних рівнянь [8, 9] вийшли за межі допустимих значень, що свідчить про відсутність достовірних оцінок кількості рядків коду для JAVA-застосунків. Трьохфакторна нелінійна регресійна модель [10] не може бути застосована, оскільки через обмеження нормалізуючих перетворень значення оцінки кількості рядків коду не існують для 242 точок значень навчальної вибірки та для 236 точок значень тестової вибірки через обмеження нормалізуючого перетворення. В свою чергу чотирьохфакторна нелінійна регресійна модель [12] не може бути застосована для 22 точок значень навчальної вибірки та для 25 точок значень тестової вибірки через обмеження нормалізуючого перетворень. Незадовільні значення критеріїв можуть бути викликані різними причинами, зокрема, нормалізуючі перетворення існуючих моделей можуть мати певні обмеження, змінами в мові програмування JAVA та підходах розробки ПЗ, що впливають на структури та синтаксис програмних проєктів, недостатній рівень об'єктивності представлення генеральної сукупності вибірками, на основі яких були побудовані математичні моделі, тощо.

В роботі [13] було побудовано однофакторні нелінійні регресійні моделі для оцінювання кількості рядків коду (Y) в залежності від кількості класів (X) на базі нормалізуючих перетворень десяткового логарифму, Бокса-Кокса і Джонсона сім'ї SB та двофакторну нелінійну регресійну модель на базі нормалізуючого перетворення Джонсона сім'ї SB із застосуванням вище наведених навчальної і тестової вибірок (за метриками кількості класів X_1 та X_2 – загальною кількістю видимих методів класів). Результати порівнянн отриманих нелінійних регресійних моделей за критеріями якості R^2 , $MMRE$ та $PRED(0,25)$ наведені в Таблиці 1.

Слід зазначити що значення R^2 , $MMRE$ та $PRED(0,25)$ суттєво не відрізняються для однофакторних нелінійних регресійних моделей між собою для обох вибірок. Побудована двофакторна нелінійна регресійна модель із застосування перетворення десяткового логарифма має найкращі показники у порівнянні з побудованими в роботі [13] нелінійними регресійними моделями не дивлячись на застосування складних нормалізуючих перетворень. Це пояснюється тим, що введення додаткової незалежного фактору регресії підвищує достовірність оцінювання залежної змінної. Модель (23) має високі

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

значення критеріїв якості R^2 та $MMRE$ та задовільне значення критерію якості $PRED(0,25)$.

Таблиця 1

Критерії якості однофакторних та двофакторних нелінійних регресійних моделей

Математична модель	Навчальна вибірка			Тестова вибірка		
	R^2	MMRE	PRED(0,25)	R^2	MMRE	PRED(0,25)
Однофакторна нелінійна регресійна модель на базі перетворення десяткового логарифму	0,7266	0,3522	0,4720	0,7170	0,3350	0,4632
Однофакторна нелінійна регресійна модель на базі перетворення Бокса-Кокса	0,7291	0,3514	0,4790	0,7159	0,3354	0,4780
Однофакторна нелінійна регресійна модель на базі перетворення Джонсона сімейства SB	0,6825	0,3593	0,4790	0,6616	0,3417	0,4702
Двофакторна нелінійна регресійна модель на базі перетворення десяткового логарифму	0,8002	0,2332	0,6853	0,8981	0,1964	0,7158

Отже, існуючі регресійні моделі і рівняння [8, 9, 10, 11, 12, 13] були перевірені за множинним коефіцієнтом детермінації R^2 , середньою величиною відносної помилки $MMRE$ (2) і відсотком прогнозованих результатів, для яких величини відносної помилки MRE (4) менші за 0,25, $PRED(0,25)$ (4). Результат перевірки показав їх незадовільний рівень достовірності для навчальної і тестової вибірок. Таким чином виникає необхідність вдосконалення існуючих моделей для оцінювання кількості рядків коду (KLOC) JAVA-застосунків.

3. Метод побудови нелінійної регресійної моделі

Зазвичай дані за метриками програмного коду не розподілені за нормальним законом, що робить обмежену можливість використання лінійних регресійних моделей для оцінювання розміру рядків коду ПЗ. Теоретичною умовою застосування лінійних регресійних моделей є нормальний розподіл багатовимірних даних або нормальний розподіл залишків регресії ϵ . Тому у випадку оцінювання розміру JAVA-застосунків переходять до застосування

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

нелінійних регресійних моделей. Для побудови нелінійних регресійних моделей для оцінювання кількості рядків коду JAVA-застосунків було обрано методи, застосовані у роботах [16, 17], які ґрунтуються на застосуванні взаємозворотних нормалізуючих перетворень з ітеративним видаленням викидів. У випадку виявлення викиду, метод повертається до першого кроку, використовуючи модифіковану вибірку без виявленого викиду з попередньої ітерації. Застосування нормалізуючих перетворень дозволяє перейти до побудови лінійних регресійних моделей на основі нормалізованих даних із подальшим їх перетворенням в нелінійні регресійні моделі.

Нелінійна регресійна модель має такий загальний вигляд

$$Y = F(X_1, X_2, \dots, X_k, \epsilon), \quad (5)$$

де ϵ – випадкова величина (ВВ) розподілена за нормальним законом, $\epsilon = \mathcal{N}(0, \sigma_\epsilon^2)$, яка визначає залишки, F – нелінійна регресійна модель на основі k - факторів, Y - залежна змінна KLOC.

На першому кроці проводиться нормалізація негаусівських багатовимірних даних.

Нехай взаємозворотне багатовимірне нормалізуюче перетворення негаусівського випадкового вектора $P = \{Y, X_1, X_2, \dots, X_k\}^T$ у гаусівський випадковий вектор $T = \{Z_Y, Z_1, Z_2, \dots, Z_k\}^T$ задано як

$$T = \psi(P) \quad (6)$$

Обернене перетворення до (6) має вигляд

$$P = \psi^{-1}(T) \quad (7)$$

де ψ - вектор взаємозворотніх функцій нормалізуючого перетворення, $\psi = \{\psi_Y, \psi_1, \psi_2, \dots, \psi_k\}^T$.

Для нормалізації багатовимірних негаусівських даних навчальної вибірки було обрано взаємозворотне нормалізуюче перетворення Бокса-Кокса [18], яке задається як

$$Z = \begin{cases} (X^\lambda - 1)/\lambda, & \text{if } \lambda \neq 0 \\ \ln(X), & \text{if } \lambda = 0 \end{cases} \quad (8)$$

де λ – параметри перетворення Бокса-Кокса.

Для оцінки параметрів нормалізуючого перетворення (6) було обрано метод метод максимальної правдоподібності

$$\hat{\theta} = \underset{\theta}{\arg \max} l(\theta), \quad (9)$$

де $l(\theta)$ - логарифмічна функція правдоподібності, θ - вектор параметрів перетворення $\theta = \{\lambda_1, \lambda_2, \dots, \lambda_k\}$, k - розмірність багатовимірних даних. Для перетворення Бокса-Кокса логарифмічна функція правдоподібності [19] для багатовимірних даних задано як

$$l(X, \theta) = \sum_{j=1}^k (\lambda_j - 1) \sum_{i=1}^N \ln(X_{ij}) - \frac{N}{2} \ln[\det(S_N)] \quad (10)$$

**ADVANCES
IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES**

де N - розмір вибірки, S_N - вибіркова коваріаційна матриця

$$S_N = \frac{1}{N} \sum_{i=1}^N (Z_i - \bar{Z})(Z_i - \bar{Z})^T \quad (11)$$

де Z_i - гаусівський випадковий вектор, $Z_i = (Z_{i1}, Z_{i2}, \dots, Z_{ik})^T$; \bar{Z} - вектор вибіркових середніх, $\bar{Z} = (\bar{Z}_1, \bar{Z}_2, \dots, \bar{Z}_k)^T$.

На другому кроці виконується перевірка нормального розподілу багатовимірних даних за допомогою критерію Мардія [21], який ґрунтується на відповідності нормальному закону розподілу параметрів багатовимірної асиметрії ($\beta_{1,k}$) та ексцесу ($\beta_{2,k}$)

$$\beta_{1,k} = \frac{1}{N^2} \sum_{i=1}^N \sum_{j=1}^N [(X_i - \bar{X})^T S_N^{-1} (X_j - \bar{X})]^3, \quad (12)$$

$$\beta_{2,k} = \frac{1}{N} \sum_{i=1}^N [(X_i - \bar{X})^T S_N^{-1} (X_i - \bar{X})]^2, \quad (13)$$

де X - k -розмірний вектор випадкової величини, $X = (X_1, X_2, \dots, X_k)$, а S_N — зміщена вибіркова коваріаційна матриця багатовимірної ВВ X , визначена як

$$S_N = \frac{1}{N} \sum_{i=1}^N (X_i - \bar{X})(X_i - \bar{X})^T, \quad (14)$$

де \bar{X} - це вектор вибіркових середніх, $\bar{X} = (\bar{X}_1, \bar{X}_2, \dots, \bar{X}_k)^T$.

За тестом Мардія очікувана асиметрія багатовимірних даних дорівнює 0, очікуваний ексцес становить $k(k+2)$ для багатовимірного нормального закону розподілу.

Для $\beta_{1,k}$ застосовується тестова статистика

$$\frac{N}{6} \beta_{1,k} \leq \chi^2, \quad (15)$$

яка має наближений розподіл χ^2 з $k(k+1)(k+2)/6$ ступенями свободи та рівнем значущості α .

Для $\beta_{2,k}$ у якості тестової статистики використовується $1 - \alpha$ квантиль \mathcal{N} нормального закону розподілу з математичним сподіванням $\mu = k(k+2)$ та дисперсією $\sigma^2 = 8k(k+2)/N$

$$\beta_{2,k} \leq \mathcal{N}_{1-\alpha}(\mu, \sigma^2). \quad (16)$$

На цьому кроці багатовимірні викиди із багатовимірних нормалізованих даних знаходяться за методом квадрату відстані Махаланобіса [22]. Визначається чи є одна багатовимірна точка із набору даних викидом, якщо в багатовимірному негаусівському наборі даних є багатовимірний викид, то таку точку відкидають і відбувається перехід до першого етапу, інакше до наступного етапу. Значення квадрату відстані Махаланобіса це елементи головної діагоналі матриці d^2 , розміром $N \times N$.

$$d^2 = (Z_i - \bar{Z})^T S_N^{-1} (Z_i - \bar{Z}), \quad (17)$$

**ADVANCES
IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES**

де S_N — зміщена вибіркова коваріаційна матриця (14), Z - ВВ з нормальним розподілом. Суть цього методу полягає в тому, що значення $d_{i^2}, i = 1, 2, \dots, N$, які перевищують значення квантилю розподілу χ^2 для рівня значущості α вважаються викидами і виключаються із вибірки. Зазвичай використовується значення $\alpha = 0,005$ для цього методу.

На третьому кроці відбувається побудова лінійної регресійної моделі на основі нормалізованої багатовимірної вибірки, яка має вигляд

$$Z_y = \hat{Z}_y + \varepsilon = \hat{b}_0 + \hat{b}_1 Z_1 + \hat{b}_2 Z_2 + \dots + \hat{b}_k Z_k + \varepsilon, \quad (18)$$

де $\hat{b}_0, \hat{b}_1, \hat{b}_2, \dots, \hat{b}_k$ - оцінки параметрів лінійної регресійної моделі, які знаходяться за методом найменших квадратів.

На четвертому кроці необхідно перевірити розподіл залишків регресії ε побудованої лінійної регресійної моделі на відповідність нормальному закону розподілу. Якщо розподіл залишків лінійної регресійної моделі для нормалізованих даних не є нормальним, тоді необхідно відкинути точку даних, для якої модуль залишку є максимальним і повернутись до першого кроку.

На п'ятому кроці, після побудови моделі лінійної регресії (18) для нормалізованих даних, застосувавши зворотнє нормалізуюче перетворення (7), нелінійна регресійна модель буде мати наступний вигляд

$$Y = \psi_Y^{-1}(\hat{Z}_y + \varepsilon) = \psi_Y^{-1}(\hat{b}_0 + \hat{b}_1 Z_1 + \hat{b}_2 Z_2 + \dots + \hat{b}_k Z_k + \varepsilon), \quad (19)$$

де ψ_Y^{-1} - функція зворотнього нормалізуючого перетворення перетворення оцінки лінійної регресії.

На шостому кроці побудови нелінійної регресійної моделі, будується верхня та нижня границі інтервалу прогнозування та проводиться пошук точок значень які знаходяться поза інтервалами прогнозування, якщо такі точки знайдені, то вони вважаються викидами і вилучаються із вибірки. Границі інтервалів прогнозування нелінійної регресії визначаються за наступною формулою

$$\hat{Y}_{PI} = \psi_Y^{-1} \left(\hat{Z}_y \pm t_{\alpha/2, v} S_{Z_y} \left\{ 1 + \frac{1}{N} + (Z_X^+)^T S_Z^{-1} (Z_X^+) \right\}^{1/2} \right), \quad (20)$$

де $t_{\alpha/2, v}$ - квантиль t-розподілу Стьюдента з $v = N - k - 1$ ступенями

свободи та $\alpha/2$ - рівнем значущості; $S_{Z_y}^2 = \frac{1}{v} \sum_{i=1}^N (Z_{y_i} - \hat{Z}_{y_i})^2$; Z_X^+ - вектор центральних факторів(регресорів), який містить значення $\{Z_{1_i} - \bar{Z}_1, Z_{2_i} - \bar{Z}_2, \dots, Z_{k_i} - \bar{Z}_k\}$; S_Z - $k \times k$ матриця

$$S_Z = \begin{bmatrix} S_{Z_q} & S_{Z_r} \end{bmatrix}, \quad (21)$$

де $S_{Z_q} S_{Z_r} = \sum_{i=1}^N (Z_{q_i} - \bar{Z}_q)(Z_{r_i} - \bar{Z}_r)$, $q, r = 1, 2, \dots, k$

4. Побудова чотирьохфакторної нелінійної регресійної моделі для оцінки розміру JAVA-застосунків

Для досягнення мети підвищення достовірності оцінювання розміру KLOC (Y) JAVA-застосунків, побудуємо чотирьохфакторну нелінійну регресійну модель на основі навчальної вибіркою даних (рис. 3) за параметрами кількості класів (CLASS) X_1 , загальною кількістю унікальних викликів методів в класах (RFC) X_2 , середнім значенням кількості зв'язків між класами (aCBO) X_3 та середнім значенням кількості public та protected методів на клас (aVMQ) X_4 . Вибір наведених факторів регресійної моделі зроблений з урахуванням мультиколінеарності, оскільки високий рівень кореляції факторів регресії між собою підвищує чутливість моделі до випадкових змін у даних, знижує стабільність моделі та робить оцінку ваг параметрів моделі менш точною. Відсутність мультиколінеарності визначено за за коефіцієнтом впливу дисперсії (VIFs) для факторів регресії. Для багатфакторної регресійної моделі з k -факторами X_i , $i=1, 2, \dots, k$, коефіцієнти VIFs представлені діагональними елементами оберненої кореляційної $k \times k$ матриці. Якщо значення коефіцієнту VIF перевищує 10, то це свідчить про наявність проблем із мультиколінеарністю [20]. Для факторів X_1 , X_2 , X_3 та X_4 значення коефіцієнтів VIFs дорівнюють 6,3, 6,5, 1,3, та 1,2 відповідно, що свідчить про відсутність мультиколінеарності між факторами регресійної моделі. Багатовимірні дані були перевірені за критерієм Мардіа на відповідність нормальному закону розподілу для рівня значущості $\alpha = 0,005$. Результати перевірки показали, що розподіл п'ятивимірних даних X_1 (CLASS), X_2 (RFC), X_3 (aCBO), X_4 (aVMQ) та Y (KLOC) є негаусівським, оскільки тестова статистика для багатовимірної асиметрії ($N \cdot \beta_1/6 = 12707,58$) цих даних перевищує значення 60,27 квантилю розподілу χ^2 , для 35 ступенів свободи, та значення багатовимірного ексцесу $\beta_2 = 399,58$, що є більшим за значення квантилю розподілу Гауса, яке становить 37,55, де $m = 35$ та $\sigma = 0,99$. Отже перехід до побудови нелінійної регресійної моделі є виправданим. Негаусівські дані навчальної вибірки були перетворені в гаусівські дані із застосування нормалізуючого перетворення Бокса-Кокса. Оцінки параметрів багатовимірного нормалізуючого перетворення (8) залежного фактора Y та незалежних факторів X_1 , X_2 , X_3 та X_4 мають наступні значення $\hat{\lambda}_Y = -0,050162$, $\hat{\lambda}_{X_1} = 0,014653$, $\hat{\lambda}_{X_2} = -0,028591$, $\hat{\lambda}_{X_3} = 0,650591$ та $\hat{\lambda}_{X_4} = -0,02$ відповідно для останньої ітерації. Оцінку параметрів перетворення було отримано за методом максимальної правдоподібності для багатовимірних даних [19] шляхом максимізації логарифмічної функції правдоподібності (9). На другому кроці було визначено і виключено із вибірки 25 багатовимірних викидів із нормалізованої вибірки. На останній ітерації багатовимірні нормалізовані дані були перевірені за критерієм Мардіа на відповідність

**ADVANCES
IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES**

нормальному закону розподілу для рівня значущості $\alpha=0,005$. Результати перевірки показали, що розподіл п'ятивимірних даних Z_1, Z_2, Z_3, Z_4 та Z_Y є нормальним, оскільки тестова статистика для багатовимірної асиметрії $N \cdot \beta_1/6 = 56,36$ цих даних не перевищує значення 60,27 квантилю розподілу χ^2 , для 35 ступенів свободи, та значення багатовимірного ексцесу $\beta_2 = 35,29$ менше за значення квантиля розподілу Гауса, яке становить 37,70, де $m = 35$ та $\sigma = 1,05$. Далі для нормалізованих даних побудовано лінійну регресійну модель

$$Z_Y = \hat{Z}_Y + \varepsilon = \hat{b}_0 + \hat{b}_1 Z_1 + \hat{b}_2 Z_2 + \hat{b}_3 Z_3 + \hat{b}_4 Z_4 + \varepsilon. \quad (22)$$

Оцінки параметрів чотирьохфакторної лінійної регресійної моделі на основі нормалізованих даних, отримані за методом найменших квадратів, становлять $\hat{b}_0 = -4,726846$, $\hat{b}_1 = 0,238926$, $\hat{b}_2 = 0,756442$, $\hat{b}_3 = -0,089933$ та $\hat{b}_4 = 0,415064$.

Шляхом застосування зворотнього нормалізуючого перетворення (7) до лінійної регресії (22), чотирьохфакторна нелінійна регресійна модель має наступний вигляд

$$Y = \psi_Y^{-1}(\hat{Z}_Y + \varepsilon) = \psi_Y^{-1}(\hat{b}_0 + \hat{b}_1 Z_1 + \hat{b}_2 Z_2 + \hat{b}_3 Z_3 + \hat{b}_4 Z_4 + \varepsilon). \quad (23)$$

На шостому кроці, для моделі (23) побудовано інтервал прогнозування та виявлено 6 викидів, які були ітеративно вилучені із нормалізованої навчальної вибірки. Для останньої ітерації значення нормалізованих вибіркового середніх $\bar{Z}_1, \bar{Z}_2, \bar{Z}_3$ та \bar{Z}_4 становлять 6,741137, 7,747876, 3,375148 та 1,530621 відповідно. Квантиль t -розподілу Стьюдента $t_{\alpha/2, \nu} = 2,594580$ для рівня значущості $\alpha = 0,01$ та 250 ступенів свободи; $S_{Z_Y} = 0,137762$. Обернена матриця (14) має вигляд

$$S_{\bar{Z}}^{-1} = \begin{bmatrix} 0,0758, & -0,1071, & 0,0195, & 0,0430 \\ -0,1071, & 0,1556, & -0,0285, & -0,0645 \\ 0,0195, & -0,0285, & 0,0121, & 0,0058, \\ 0,0430, & -0,0645, & 0,0058, & 0,0706 \end{bmatrix}$$

Чотирьохфакторна нелінійна регресійна модель побудована за 32 ітерації, з багатовимірних нормалізованих даних було вилучено 31 багатовимірну точку як викид.

Для чотирьохфакторної нелінійної регресійної моделі знайдено довірчий інтервал, який має наступний вигляд

$$\hat{Y}_{PI} = \psi_Y^{-1} \left(\hat{Z}_Y \pm t_{\alpha/2, \nu} S_{Z_Y} \left\{ \frac{1}{N} + (Z_X^*)^T S_{\bar{Z}}^{-1} (Z_X^*) \right\}^{1/2} \right). \quad (24)$$

5. Результати

Отриману чотирьохфакторну нелінійну регресійну модель (23) для оцінювання кількості рядків коду JAVA-застосунків перевірено за допомогою

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

критеріїв якості регресійних моделей R^2 , $MMRE$ та $PRED(0,25)$, які мають значення 0,8242, 0,1621 та 0,8042 відповідно для навчальної вибірки та 0,8981, 0,1536 та 0,8211 відповідно для тестової вибірки, що свідчить про прийнятний рівень достовірності оцінки розміру JAVA-застосунків за допомогою отриманої нелінійної регресійної моделі у порівнянні з існуючими лінійними регресійними рівняннями та нелінійними регресійними моделями з роботи [13] (табл. 1).

Для порівняння достовірності прогнозування та якості отриманої регресійної моделі (23) побудовано інтервал прогнозування за навчальною вибіркою для однофакторної нелінійної регресійної моделі оцінки KLOC від параметру кількості класів (CLASS) X на основі нормалізуючого перетворення Бокса-Кокса з роботи [13].

Подібно до отриманої чотирьохфакторної нелінійної регресійної моделі (23), однофакторна нелінійна модель побудовано за тими ж методами [16, 17], що базуються на статистичному аналізі багатовимірних даних та багатовимірних взаємозворотних нормалізуючих перетвореннях.

Оцінки параметрів перетворення Бокса-Кокса однофакторної моделі мають наступні значення $\hat{\lambda}_Y = 0,002738$, $\hat{\lambda}_X = 0,030707$ а оцінки лінійної регресії мають вигляд $\hat{b}_0 = -2,697047$, $\hat{b}_1 = 0,857236$. Для отриманого інтервалу прогнозування значення нормованих вибіркових середніх $\bar{Z}_X = 7,045051$. Квантиль t -розподілу Стюдента має значення $t_{\alpha/2, \nu} = 2,594025$ для рівня значущості $\alpha = 0,01$ та 272 ступенів свободи; $S_{Z_Y} = 0,358707$.

Обернена матриця (14) складається з одного елемента $S_{Z^{-1}} = 1,529482 \cdot 10^{-3}$.

З навчальної вибірки випадковим чином було обрано 30 з 286 рядків даних для порівняння фактичних значень рядків коду (Y) та їх оцінок KLOC (\hat{Y}) за регресійними моделями, а також їх нижньої (LB) та верхньої межі (UB) інтервалів прогнозування Таблиця 2.

Порівняння ширини інтервалу прогнозування однофакторної та чотирьохфакторної нелінійних регресійних моделей оцінено за формулою

$$DIFF = \left(1 - \frac{\sum_{i=1}^N |UB_{4X_i} - LB_{4X_i}|}{\sum_{i=1}^N |UB_{1X_i} - LB_{1X_i}|} \right) \cdot 100\% \quad (25)$$

де UB_{4X_i}, LB_{4X_i} - i -тий інтервал прогнозування чотирьохфакторної нелінійної регресійної моделі (25) та UB_{1X_i}, LB_{1X_i} - i -тий інтервал прогнозування однофакторної нелінійної регресійної моделі на базі перетворення Бокса-Кокса [13].

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

Таблиця 2.

Порівняння оцінок KLOC та інтервалів прогнозування нелінійних регресійних моделей

#	Однофакторна нелінійна регресійна модель на основі Johnson SB				Чотирьохфакторна нелінійна регресійна модель на основі Johnson SB		
	<u>Y</u>	<u>Ŷ</u>	<u>LB</u>	<u>UB</u>	<u>Ŷ</u>	<u>LB</u>	<u>UB</u>
1	1.649	1.687	0.520	5.453	1.643	0.926	2.965
2	1.769	1.733	0.534	5.600	1.891	1.065	3.415
3	1.806	3.108	0.963	9.992	1.944	1.088	3.535
4	1.848	1.641	0.506	5.306	1.596	0.902	2.870
5	2.013	1.641	0.506	5.306	1.658	0.937	2.986
...
6	7.522	9.564	2.987	30.509	8.293	4.484	15.641
7	7.609	11.621	3.634	37.030	8.314	4.492	15.691
8	7.628	8.727	2.724	27.853	6.407	3.492	11.983
9	8.056	9.285	2.900	29.623	9.562	5.155	18.093
10	8,056	9,285	2,900	29,623	9,562	5,155	18,093
...
11	16.056	14.210	4.448	45.236	18.360	9.700	35.489
12	16.098	9.704	3.031	30.952	10.948	5.867	20.846
13	16.202	10.311	3.222	32.876	14.232	7.566	27.331
14	16.398	10.124	3.163	32.284	15.359	8.148	29.559
15	16.583	14.683	4.596	46.735	7.354	3.982	13.850
...
16	28.724	32.742	10.280	103.900	30.421	15.835	59.751
17	29.139	45.379	14.259	143.888	35.407	18.323	69.977
18	29.296	23.981	7.522	76.173	25.235	13.211	49.264
19	29.575	8.448	2.637	26.968	34.412	17.487	69.350
20	29.591	11.903	3.722	37.923	21.758	11.412	42.389
...
21	64.504	60.178	18.919	190.722	47.373	24.287	94.568
22	65.525	45.884	14.418	145.486	65.229	33.014	132.023
23	66.253	100.858	31.721	319.514	50.521	25.726	101.586
24	66.455	44.723	14.053	141.812	59.534	30.028	120.939
25	66.695	37.155	11.670	117.866	55.095	28.057	110.778
...
26	205.51	289.349	90.906	917.617	235.629	113.912	500.996
27	208.68	137.768	43.327	436.468	178.114	87.140	373.880
28	208.96	106.094	33.368	336.100	150.519	73.989	314.346
29	216.61	300.958	94.545	954.518	220.525	106.233	470.675
30	222.65	188.859	59.379	598.493	248.491	120.069	528.630
N

Отримана оцінка вказує, що інтервал прогнозування чотирьохфакторної нелінійної регресійної моделі на **42,62%** вужчий за інтервал прогнозування

однофакторної нелінійної регресійної моделі на базі перетворення Бокса-Кокса [13].

6. Обговорення отриманих результатів

Отримано чотирьохфакторну нелінійну регресійну модель для ранньої оцінки KLOC JAVA-застосунків, використовуючи методи побудови нелінійних регресійних моделей на основі багатовимірного нормалізуючого перетворення Бокса-Кокса. Вибір методу зумовлений негаусівським розподілом п'ятивимірних даних інформації з метрик коду за критерієм Мардіа та залишків регресії за критерієм χ^2 Пірсона.

В порівнянні з існуючими моделями отримана чотирьохфакторна нелінійна регресійна модель (23) має кращі показники якості для оцінювання кількості рядків коду Java-застосунків за критеріями якості R^2 , $MMRE$ та $PRED(0,25)$. Значення оцінок критеріїв якості знаходяться в допустимих межах $R^2 \geq 0,75$, $MMRE \leq 0,25$ та $PRED(0,25) \geq 0,75$ як для навчальної, так і для тестової вибірок, що свідчить про прийнятну точність отриманої моделі та мають наступні значення $R^2 = 0,8242$, $MMRE = 0,1621$, $PRED(0,25) = 0,8042$ для навчальної вибірки та $R^2 = 0,8981$, $MMRE = 0,1536$, $PRED(0,25) = 0,8211$ для тестової вибірки. Застосування методу перехресного затвердження підвищує впевненість в стійкості та надійності отриманої моделі. Крім того, ширина інтервалу прогнозування (20) моделі (23) на **42,62%** менша (Таблиця 2), ніж інтервал прогнозування однофакторної нелінійної регресійної моделі, що дозволяє підвищити точність оцінки параметру розміру, з урахуванням оптимістичного та песимістичного сценаріїв при плануванні розробки ПЗ.

До переваг запропонованої моделі (23) можна віднести можливість оцінки KLOC на ранніх етапах проєктування JAVA-застосунків з використанням чотирьох метрик коду, таких як загальна кількість класів (CLASS), загальна кількість унікальних викликів методів у класах (RFC), середнім значенням кількості зв'язків між класами (aCBO) та середнім значенням видимих методів на клас (aVMQ), які можна отримати на ранніх етапах планування проєкту з діаграм класів UML. До недоліків запропонованої моделі (23) можна віднести наступні обмеження інтервалів значень незалежних змінних, де $CLASS \in [25 ; 11147]$, $RFC \in [45 ; 117847]$, $aCBO \in [0,12 ; 24,57]$ та $aVMQ \in [1,59 ; 85,92]$.

Незважаючи на використання великої вибірки метрик коду, запропонована модель побудована лише на основі проєктів з відкритим кодом JAVA-застосунків з платформи GitHub. Хоча модель досягла прийнятного рівня достовірності відповідно до критеріїв якості регресійних моделей [14], напрямки подальших досліджень можуть бути спрямовані у бік вдосконалення

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

моделі, шляхом розширення кількості та розділення незалежних факторів моделі, наприклад з урахуванням успадкування, або використання параметру кількості інтерфейсів окремо від кількості класів.

7. Висновки

Отримана чотирьохфакторна нелінійна регресійна модель вирішує важливу проблему оцінки розміру JAVA-застосунків на ранніх стадіях планування програмного проєкту з використанням метрик діаграми класів UML: загальної кількості класів (CLASS), загальної кількості унікальних викликів методів у класах (RFC), середнє значення кількості зв'язків між класами (aCBO) та середнього значення кількості public та protected методів на клас (aVMQ).

Наукова новизна отриманих результатів полягає в тому, що чотирьохфакторну нелінійну регресійну модель удосконалено у порівнянні з існуючими моделями та рівнянням для ранньої оцінки KLOC JAVA-застосунків із використанням багатовимірного нормалізуючого перетворення Бокса-Кокса; вперше побудовано чотирьохфакторну нелінійну регресійну модель з використанням вибірки, розміром більше 250 точок даних; достовірність, стійкість та надійність моделі перевірено на тестовій вибірці аналогічного розміру.

Отримана модель, у порівнянні з іншими нелінійними регресійними моделями, має вище значення коефіцієнта детермінації R^2 , менше значення середньої відносної похибки *MMRE* та більше значення відсотка передбачення рівня відносної похибки *PRED(0,25)* як для навчальної, так і для тестової вибірок, а інтервал передбачення є меншим у порівнянні з однофакторною нелінійною регресійною моделлю на основі однакового нормалізуючого перетворення.

Оцінки критеріїв якості отриманої регресійної моделі для навчально та тестової вибірок суттєво не відрізняються, а отже це свідчить, що вибірки мають високий рівень репрезентативності генеральної сукупності.

Практичне значення отриманих результатів дозволяє рекомендувати побудовану модель для використання на практиці. Запропонована модель реалізована у вигляді програмного продукту, який може бути використаний менеджерами проєктів для оцінки трудомісткості розробки програмного забезпечення на мові JAVA на ранніх стадіях планування проєкту з метою зниження ризиків та оптимізації витрат.

Перспективи подальших досліджень можуть включати розширення та розділення набору незалежних факторів, використання інших багатовимірних нормалізуючих перетворень та збільшення розміру вибірки даних для побудови нелінійної регресійної моделі.

8. Література

- [1] S. McConnel, *Software Estimation: Demystifying the Black Art*, Microsoft Press, Redmond, Washington, USA, 2006, 352 p.
- [2] J. Johnson, H. Mulder, *Endless Modernization: How Infinite Flow Keeps Software Fresh*, The Standish Group, Hans Mulder's Lab, 2021. https://www.researchgate.net/publication/348849361_Endless_Modernization_How_Infinite_Flow_Keeps_Software_Fresh
- [3] The Standish Group, *Chaos report 2015*, 2015. https://standishgroup.com/sample_research_files/CHAOSReport2015-Final.pdf
- [4] Oracle, Java, 2024, URL: <https://www.oracle.com/my/java/>
- [5] IEEE, “Top Programming Languages 2022”, url: <https://spectrum.ieee.org/top-programming-languages-2022>
- [6] TIOBE. “TIOBE Index of programming languages”, url: <https://www.tiobe.com/tiobe-index/>
- [7] Фаріонова Т. А., Орехов О. С., Аналіз сучасного стану методів оцінювання трудомісткості розробки програмного забезпечення, Збірник наукових праць НУК ім. адм. Макарова, No. 1 (494), Миколаїв, Україна, 2024, С. 102-111. doi: [https://doi.org/10.15589/znп2024.1\(494\).15](https://doi.org/10.15589/znп2024.1(494).15)
- [8] H. B. K. Tan, Y. Zhao, H. Zhang, Estimating LOC for information systems from their conceptual data models, *Proceedings - International Conference on Software Engineering*, 2006, pp. 321-330. doi: 10.1145/1134285.1134331.
- [9] H. B. K. Tan, Y. Zhao, H. Zhang, Conceptual Data Model-Based Software Size Estimation for Information Systems, *ACM Transactions of Software Engineering and Methodology*, No. 19, 2009. doi: 10.1145/1571629.1571630.
- [10] Приходько Н. В., Приходько С. Б., Нелінійна регресійна модель для оцінювання розміру програмного забезпечення промислових інформаційних систем на Java, *Моделювання та інформаційні технології*, том 85, 2018, С. 81–88. url: http://nbuv.gov.ua/UJRN/Mtit_2018_85_14
- [11] Макарова Л. М., Приходько Н. В., Кудін О. О, Побудова нелінійної регресійної моделі для оцінювання розміру веб-додатків, реалізованих мовою Java, *Вісник Херсонського національного технічного університету*, № 2 (69), 2019, С. 145–153. url: <http://eir.nuos.edu.ua/handle/123456789/4443>
- [12] Приходько С. Б., Приходько Н. В., Смикодуб Т. Г., Чотирихфакторна нелінійна регресійна модель для оцінювання розміру JAVA-застосунків з відкритим кодом, *Вчені записки ТНУ імені В. І. Вернадського, Серія: технічні науки*, том 31 (70) № 2 ч.1, 2020, С. 157–162. doi:10.32838/2663-5941/2020.2-1/25
- [13] Орехов О. С., Фаріонова Т. А., Математичні моделі для оцінювання розміру JAVA-застосунків, *Вісник Херсонського національного технічного університету*, № 2 (89), Херсон, 2024, С. 196-203. doi: <https://doi.org/10.35546/kntu2078-4481.2024.2.28>
- [14] D. Port, M. Korte, Comparative studies of the model evaluation criterions MMRE and PRED in software cost estimation research, *Proceedings of the 2nd*

ADVANCES IN INFORMATION-CONTROL SYSTEMS AND TECHNOLOGIES

ACM-IEEE International Symposium on Empirical Software Engineering and Measurement, New York, 2008, pp. 51–60. doi:10.1145/1414004.1414015

[15] J. Jia , W. Qiu, Research on an Ensemble Classification Algorithm Based on Differential Privacy, IEEE Access, 2020, P. 99. doi:10.1109/ACCESS.2020.2995058

[16] S. Prykhodko, N. Prykhodko, Mathematical Modeling of Non-Gaussian Dependent Random Variables by Nonlinear Regression Models Based on the Multivariate Normalizing Transformations, volume 1265 of Mathematical Modeling and Simulation of Systems (MODS'2020), Advances in Intelligent Systems and Computing, 2021, pp. 166-174. doi:10.1007/978-3-030-58124-4_16

[17] S. Prykhodko, N. Prykhodko, L. Makarova, A. Pukhalevych, Outlier Detection in Non-Linear Regression Analysis Based on the Normalizing Transformations, 2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), Lviv-Slavske, Ukraine, 2020, pp. 407–410. doi:10.1109/TCSET49122.2020.235464.

[18] G. E. P. Box, An analysis of transformations, Journal of the Royal Statistical Society (B), No.2 (26), 1964, pp. 211-252.

[19] R. A. Johnson, D.W. Wichern, Applied Multivariate Statistical Analysis, Pearson Prentice Hall, 2007, p. 800.

[20] I. Olkin, A. R. Sampson, Multivariate Analysis: Overview, in N. J. Smelser, P. B. Baltes, International encyclopedia of social & behavioral sciences (eds.) 1st edn., Elsevier, Pergamon, 2001, pp. 10240–10247.

[21] K. V. Mardia, Measures of multivariate skewness and kurtosis with applications, volume 57 of Biometrika, 1970, pp. 519–530, doi:10.1093/biomet/57.3.519.

[22] S. Chatterjee, B. Price, Regression analysis by example, New York: John Wiley & Son, 1977, 228 p.

**THE FOUR-FACTOR NONLINEAR REGRESSION MODEL FOR
EARLY JAVA-APPLICATIONS SIZE ESTIMATION**

O. Oriekhov. ORCID: 0000-0002-0001-0140

Makarov National University of Shipbuilding, Ukraine.

E-mail: oleksandr.oriekhov@nuos.edu.ua

***Abstract.** The paper is devoted to a four-factor nonlinear regression model building for early software lines of code (KLOC) estimation of JAVA applications. JAVA-application size estimation is an important scientific and practical task that is inextricably linked to the software development life cycle. The aim of the study is to increase the reliability and accuracy of JAVA-applications code lines estimation at the early stages of software development by building a four-factor nonlinear regression model using UML class diagram metrics. The object of the study is the process of size estimation for open-source Java-software. The subject of the study is the nonlinear regression models to estimate the software size. To achieve this goal, we collected training and test samples of JAVA-software code metrics information, analyzed and compared existing mathematical models and equations for JAVA-application size estimation. Using the training sample, the four-factor nonlinear regression model and its prediction intervals are built to estimate JAVA applications software size on a basis of the Box-Cox normalization transformation by the metrics of the total quantity of classes, the total quantity of unique method invocations in classes, the average value of classes relationships, and the average value of visible methods per class. The obtained four-factor nonlinear regression model has a lower estimate of mean magnitude of relative error, a higher estimate of percentage of prediction for magnitude of relative error of 0.25, and a higher estimate of determination coefficient in comparison to existing models, which confirm the reliability and accuracy increasing of early KLOC estimation of JAVA applications.*

***Keywords:** number of lines of code, JAVA application, non-Gaussian data, Box-Cox normalizing transformation, nonlinear regression model.*

Наукове видання

**РОЗВИТКИ
ІНФОРМАЦІЙНО-
КЕРУЮЧИХ СИСТЕМ ТА
ТЕХНОЛОГІЙ**

Монографія

Під наук. ред. проф. В. Вичужаніна

Укр. та англ. мовами

Підписано до друку 27.09.2024. Формат 60×84/16.
Папір офсетний. Гарнітура Times New Roman. Цифровий друк.
Умовно-друк. арк. 22,2. Тираж 300. Замовлення № 1024-73.
Ціна договірна. Віддруковано з готового оригінал-макета.

Українсько-польське наукове видавництво «Liha-Pres»

79000, м. Львів, вул. Технічна, 1
87-100, м. Торунь, вул. Лубіцка, 44
Телефон: +38 (050) 658 08 23

E-mail: editor@liha-pres.eu

Свідоцтво суб'єкта видавничої справи

ДК № 6423 від 04.10.2018 р.