

ЗБІРНИК ТЕЗ / ABSZTRAKTKÖTET / ABSTRACTS



Berehove, 27-28 March 2025



ІННОВАЦІЙНІ ЦИФРОВІ МЕТОДИ В ГАЛУЗІ ОСВІТИ ТА ДОСЛІДЖЕНЬ

Міжнародна науково-практична конференція



INNOVATÍV DIGITÁLIS MÓDSZEREK AZ OKTATÁS ÉS KUTATÁS TERÜLETÉN

Nemzetközi tudományos-gyakorlati konferencia



INNOVATIVE DIGITAL METHODS IN EDUCATION AND RESEARCH

International scientific and practical conference

ІННОВАЦІЙНІ ЦИФРОВІ МЕТОДИ
В ГАЛУЗІ ОСВІТИ ТА ДОСЛІДЖЕНЬ

Міжнародна науково-практична конференція
Берегове, 27–28 березня 2025 року

Збірник тез доповідей

INNOVATÍV DIGITÁLIS MÓDSZEREK
AZ OKTATÁS ÉS KUTATÁS TERÜLETÉN

Nemzetközi tudományos-gyakorlati konferencia
Beregszász, 2025. március 27–28.

Absztraktkötet

INNOVATIVE DIGITAL METHODS
IN EDUCATION AND RESEARCH

International scientific and practical conference
Berehove, 27–28 March 2025

Book of Conference Abstracts

Закарпатський угорський інститут імені Ференца Ракоці II

ІННОВАЦІЙНІ ЦИФРОВІ МЕТОДИ В ГАЛУЗІ ОСВІТИ ТА ДОСЛІДЖЕНЬ

Міжнародна науково-практична конференція
Берегове, 27–28 березня 2025 року

Збірник тез доповідей



ЗУІ ім. ФЕРЕНЦА РАКОЦІ ІІ
Берегове
2025

Збірник містить тези доповідей міжнародної науково-практичної конференції *Інноваційні цифрові методи в галузі освіти та досліджень*, яка відбулася 27–28 березня 2025 року в місті Берегове. Матеріали конференції охоплюють широке коло питань, пов'язаних із виявленням найновіших тенденцій у застосуванні інноваційних цифрових методів і засобів в освіті та науці. Конференція зосередилась на викликах та можливостях інтеграції цифрових технологій у навчальний процес, а також на розвитку дослідницьких методів. Зокрема, тези доповідей конференції досліджують впровадження цифрових технологій у шкільну та вищу освіту, використання штучного інтелекту, методичні інновації, алгебраїчні структури, теорію ймовірностей і моделювання, а також застосування цифрових інструментів у наукових дослідженнях. Учасники конференції обговорили підходи до вирішення актуальних питань, пов'язаних із застосуванням інноваційних методів у навчанні, використанням штучного інтелекту у викладанні математики, інтеграції цифрових технологій у освітній процес, а також удосконаленням методики викладання дисциплін у закладах вищої освіти. Особлива увага була приділена сучасним тенденціям у педагогічних дослідженнях та можливостям адаптації освітніх програм до потреб сучасного студентства. Організаторами конференції були кафедра математики та інформатики спільно з Науковим товариством студентів і молодих вчених Закарпатського угорського інституту імені Ференца Ракоці II.

Рекомендовано до видання в електронній формі (PDF)
рішенням Вченої ради Закарпатського угорського інституту імені Ференца Ракоці II
(протокол №2 від «24» березня 2025 року)

Підготовлено до видання кафедрою математики та інформатики спільно з Видавничим відділом Закарпатського угорського інституту імені Ференца Ракоці II

За редакцією:

*Каталін Кучінка, Олександр Тилишак, Мирослав Стойка, Еніке Якоб,
Габрієлла Пап та Адам Доровці*

Технічне редагування: *Олександр Тилишак, Олександра Полінські та Олександр Добош*

Коректура: *Ільдико Гріца-Варцаба та авторська*

Дизайн обкладинки: *Іштван Балог*

УДК: *Бібліотека ім. Опаці Чері Яноша при ЗУІ ім. Ф.Ракоці II*

Відповідальний за випуск:

Олександр Добош (начальник Видавничого відділу ЗУІ ім. Ф.Ракоці II)

Відповідальність за зміст і достовірність публікацій покладається на авторів тез доповідей.

Точки зору авторів публікацій можуть не співпадати з точкою зору редакторів.

Проведення конференції та видання збірника тез доповідей в електронній формі (PDF)
здійснено за підтримки уряду Угорщини.



Видавництво: Закарпатський угорський інститут імені Ференца Ракоці II (адреса: пл. Кошута 6, м. Берегове, 90202. Електронна пошта: foiskola@kmf.uz.ua; kiado@kmf.uz.ua)

ISBN 978-617-8143-36-7 (PDF)

© Автори, 2025

© Редактори, 2025

© Закарпатський угорський інститут імені Ференца Ракоці II, 2025

II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola

INNOVATÍV DIGITÁLIS MÓDSZEREK AZ OKTATÁS ÉS KUTATÁS TERÜLETÉN

Nemzetközi tudományos-gyakorlati konferencia
Beregszász, 2025. március 27–28.

Absztraktkötet



II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola
Beregszász
2025

A kiadvány a 2025. március 27–28-án Beregszászban *Innovatív digitális módszerek az oktatás és kutatás területén* címmel megrendezett nemzetközi tudományos-gyakorlati konferencián elhangzott előadások absztraktjait tartalmazza. A konferencia anyagai széles körű kérdéseket ölelnek fel, amelyek az innovatív digitális módszerek és eszközök alkalmazásával, legújabb trendjeinek használatával kapcsolatosak az oktatásban és a tudományban. Középpontjában a digitális technológiák tanulási folyamatba való integrálásának kihívásai és lehetőségei, valamint a kutatási módszerek fejlesztése álltak. A konferencia előadásainak összefoglalói különösen az iskolai és felsőoktatásban alkalmazott digitális technológiák bevezetését, a mesterséges intelligencia használatát, a módszertani innovációkat, az algebrai struktúrákat, a valószínűség-számítást és modellezést, valamint a digitális eszközök tudományos kutatásban való alkalmazását vizsgálják. A résztvevők megvitatták az innovatív oktatási módszerek alkalmazásával, a mesterséges intelligencia matematikaoktatásban való felhasználásával, a digitális technológiák oktatási folyamatba való integrációjával, valamint a felsőoktatási tantárgyak oktatási módszereinek fejlesztésével kapcsolatos aktuális kérdések megoldási megközelítéseit. Különös figyelmet fordítottak a pedagógiai kutatások modern tendenciáira és az oktatási programok korszerű hallgatói igényekhez való igazításának lehetőségeire. A konferenciát a II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola Matematika és Informatika Tanszéke, valamint a Hallgatók és Fiatal Kutatók Tudományos Egyesülete szervezte.

Elektronikus formában (PDF-fájlformátumban) történő kiadásra javasolta
a II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola Tudományos Tanácsa
(2025. március 24., 2. számú jegyzőkönyv).

Kiadásra előkészítette a II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola
Matematika és Informatika Tanszéke, valamint a Kiadói Részlege.

Szerkesztette:

*Kucsinka Katalin, Tiliscsák Olekszandr, Sztójka Mirosláv, Jakab Enikő,
Papp Gabriella és Daróci Ádám*

Műszaki szerkesztés: *Tiliscsák Olekszandr, Palinszky Alexandra és Dobos Sándor*

Korrektúra: *Gricza-Varcaba Ildikó és a szerzők*

Borítóterv: *Balog István*

ETO-besorolás: a II. RF KMF Apáczai Csere János Könyvtára

A kiadásért felel:

Dobos Sándor (a II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola Kiadói Részlegének vezetője)

Az absztraktok tartalmáért és hitelességéért a szerzők viselik a felelősséget.

A szerzők álláspontja nem feltétlenül tükrözi a szerkesztők véleményét.

A konferenciát és a kiadvány elektronikus formában (PDF-fájlformátumban) történő
megjelentetését Magyarország Kormánya támogatta.



Kiadó: II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola (cím: 90 202 Beregszász, Kossuth tér 6. E-mail: foiskola@kmf.uz.ua; kiado@kmf.uz.ua)

ISBN 978-617-8143-36-7 (PDF)

© A szerzők, 2025

© A szerkesztők, 2025

© II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola, 2025

**Ferenc Rakoczi II Transcarpathian Hungarian College
of Higher Education**

**INNOVATIVE DIGITAL METHODS
IN EDUCATION AND RESEARCH**

International scientific and practical conference
Berehove, 27–28 March 2025

Book of Conference Abstracts



Transcarpathian Hungarian College
Berehove
2025

The book contains abstracts of presentations at the international scientific and practical conference *Innovative Digital Methods in Education and Research*, which took place on March 27–28, 2025, in the city of Berehove. The conference materials cover a wide range of issues related to identifying the latest trends in the application of innovative digital methods and tools in education and science. The conference focused on the challenges and opportunities of integrating digital technologies into the learning process, as well as on the development of research methods. In particular, the abstracts explore the implementation of digital technologies in school and higher education, the use of artificial intelligence, methodological innovations, algebraic structures, probability theory and modeling, and the application of digital tools in scientific research. The participants discussed approaches to addressing current issues related to the use of innovative teaching methods, the application of artificial intelligence in mathematics education, the integration of digital technologies into the educational process, and the improvement of teaching methodologies in higher education institutions. Special attention was given to contemporary trends in pedagogical research and the possibilities of adapting educational programs to the needs of modern students. The conference were organized by the Department of Mathematics and Informatics and by the Scientific Association of Students and Young Researchers at the Ferenc Rakoczi II Transcarpathian Hungarian College of Higher Education.

Recommended for publication in electronic form (PDF file format)
by the Academic Council of Ferenc Rakoczi II Transcarpathian Hungarian College
of Higher Education (record No.2 of March 24, 2025)

This volume of conference materials has been prepared by the Department of Mathematics and Informatics at the Ferenc Rakoczi II Transcarpathian Hungarian College of Higher Education and the Division of Publishing at the Transcarpathian Hungarian College.

Edited by:

*Katalin Kuchinka, Oleksandr Tylyshchak, Myroslav Stoika, Enikő Jakab,
Gabriella Papp and Adam Daroci*

Technical editing: *Oleksandr Tylyshchak, Alexandra Palinszky and Sándor Dobos*

Proof-reading: *Ildikó Gricza-Varcaba and the authors*

Cover design: *István Balog*

Universal Decimal Classification (UDC): *Apáczai Csere János Library of Ferenc Rakoczi II
Transcarpathian Hungarian College of Higher Education*

Responsible for publishing:

Sándor Dobos (head of the Division of Publishing of Transcarpathian Hungarian College)

Responsibility for the content and accuracy of publications rests with the authors of the conference abstracts. The views of the authors of publications may not coincide with the views of the editors.

The conference and the publication of the conference abstracts in electronic form (PDF file format) sponsored by the government of Hungary.



Publishing: Ferenc Rakoczi II Transcarpathian Hungarian College of Higher Education (Address: Kossuth square 6, 90202 Berehove, Ukraine. E-mail: foiskola@kmf.uz.ua; kiado@kmf.uz.ua)

ISBN 978-617-8143-36-7 (PDF)

© Authors, 2025

© Editors, 2025

© Ferenc Rakoczi II Transcarpathian Hungarian College of Higher Education, 2025

ЗМІСТ / TARTALOMJEGYZÉK / CONTENTS

Пленарні доповіді / Plenáris előadások / Plenary reports	17
1. <i>Gergely Pintér.</i> Interaktív és gamifikált taneszközök, tanulászervező szolgáltatások a Nemzeti Köznevelési Portálon	18
2. <i>Igor Orlovskiy, Olena Tymoshenko.</i> Beyond Traditional Testing: Enhancing Mathematical E-learning with STACK and Step-by-Step Assessment	19
Секція 1: Сучасні цифрові технології в шкільній освіті / 1. szekció: Iskolai oktatás modern digitális eszközökkel / Section 1: Modern Digital Technologies in School Education	23
3. <i>József Boros, Katalin Kucsinka.</i> A II. RF KMF alapképzésben részt vevő hallgatói matematikai kompetenciamérésének eredményei a 2024–2025-ös tanévben	24
4. <i>Alexandra Bodnár, Katalin Pally.</i> Matematikai kompetenciamérés Beregszász alsó tagozatos diákjainak körében	26
5. <i>Інна Червінська, Андрій Червінський.</i> Використання ресурсів цифрової педагогіки в освітньому процесі: реалії та виклики	28
6. <i>Enikő Balogh, Enikő Jakab.</i> Digitális eszközök az algebra tanításában: kifejezések és egyenletek új megközelítésben	33
7. <i>Ілдіко Гребя.</i> Інформаційно-комунікаційні технології у підготовці майбутніх учителів початкової школи до роботи в умовах інклюзивного навчання учнів	35
8. <i>Ádám Daróci, Ádám Végh.</i> Programozható robotok szerepe az oktatásban	39
9. <i>Eleonóra Jakab, Gabriella Takács, Kamilla Kutasi.</i> Korszerű digitális technológiák a biológia oktatása során: innovatív módszerek és tantárgy-pedagógiai alkalmazások lehetőségei	42
10. <i>Enikő Jakab.</i> Metakognitív stratégiák és digitális eszközök szerepe a matematikaoktatásban	45
11. <i>Martina Jánki, Livia Mészáros.</i> Digitális eszközök és az online oktatás integrálása a korszerű iskolai tanításba	47
12. <i>Erik Komárnicki, Katalin Kucsinka.</i> Az algoritmikus gondolkodás fejlesztési lehetőségei	50
13. <i>Gyöngyi Kovács.</i> Innovatív digitális módszerek alkalmazása a művészeti oktatásban	51

14. <i>Наталія Круглова, Ольга Пелехата, Олександр Диховичний.</i> Застосування Wolfram language і R при створенні олімпіадних завдань з математики	54
15. <i>Yuriy Mlavets, Kateryna Moskvychova, Olena Tymoshenko.</i> From Group-Based Learning to Individual Educational Trajectories in Online Platforms	57
16. <i>Алла Іванівна Смоліна.</i> Використання GeoGebra при розв'язанні шкільних планіметричних задач.	60
17. <i>Юлія Петечук.</i> Формування інформаційно-цифрової компетентності здобувачів освіти при викладанні математики	63
18. <i>Krisztofer Petrecki, Ádám Daróci.</i> Webes felület kidolgozása a kárpátaljai magyar iskolák kompetenciaméréséhez	67
19. <i>Олена Петрушевич, Еніке Якоб.</i> Як штучний інтелект формує майбутнє ІТ-освіти	69
20. <i>Світлана Романюк.</i> Цифрова компетентність як пріоритет сучасної освіти	71
21. <i>Ádám Temető, Mirosláv Sztojka.</i> A tanulók informatikaórákon mutatott érdeklődésének összehasonlító elemzése az Új ukrán iskola rendszerében	74
22. <i>Катерина Шовш, Тетяна Кучай, Олена Біда.</i> Теоретичні основи використання сучасних освітніх технологій при підготовці вчителів початкових класів	77
23. <i>Ольга Синявська, Антоніна Тегза.</i> Парний і множинний коефіцієнт Кендалла при перевірці узгодженості світових рейтингів університетів за різними показниками	80
24. <i>Marianna Székely.</i> Térképolvasási stratégiák vizsgálata szemmozgáskövető eszköz segítségével kárpátaljai iskolások körében	83
25. <i>Сергій Вапнічний, Микола Дронь, Каталін Кучінка, Олександр Міца.</i> Табори з програмування: як вони формують майбутнє покоління ІТ-спеціалістів	85
26. <i>Krisztián Váradi, Kornélia Hires-László.</i> A Kárpát-medencei magyarság oktatásterminológiai adatbázisa	88
Секція 2: Методичні інновації у вищій освіті / 2. szekció: Módszertani újítások a felsőoktatásban / Section 2: Methodological Innovations in Higher Education	93
27. <i>Tímea Krisztina Ardelean, Edit Veres.</i> Digitális jövő az oktatásban – A mesterséges intelligencia megítélése egyetemi hallgatók körében	94

28. <i>István Csernicskó, Béla Rácz.</i> A digitális oktatásszervezés kezdetei a Rákóczi-főiskolán: az IRIS és a VIR	98
29. <i>Олександр Диховичний, Наталія Круглова, Катерина Москвичова, Ольга Пелехата.</i> Дослідження математичних моделей педагогічних тестів з вищої математики	101
30. <i>Вікторія Дзямко, Віталій Дзямко.</i> Складові інноваційних методик сучасного вищого навчального закладу	103
31. <i>Ferenc Héjja, Tamás Bartók, Gergely Kocsis.</i> The effect of using Generative AI in Education	106
32. <i>Zsuzsa Gonda, Zsolt Hollóy.</i> The Process of Developing and Applying the RED Measurement Tool	109
33. <i>Áron Hives.</i> Advancing Education with EduBase: AI-Enhanced Assessment and Personalized Learning	112
34. <i>Ágota Figula, Emese Kása.</i> The investigation of the teaching of calculus among electrical engineering and physics students	113
35. <i>Надія Матвійшина, Олена Пшенична, Галина Шило.</i> Інтеграція інноваційних методів в електронний курс, створений на базі Moodle	115
36. <i>Krisztina Molnár, Béla Nagy, Erzsébet Kohut.</i> Mesterséges intelligencia mint a genetikaoktatás katalizátora	118
37. <i>Gabriella Papp, Judit Kulin.</i> Comparison of the reliability of e-tests in higher education of mathematics	121
38. <i>Rudolf Polgár, Anna Horváth, Boglárka Eszter Bálint.</i> Matematikatanár szakos hallgatók oktatásmódszertani képzése kombinált mikrotanítási környezetben	123
39. <i>Ганна Сливка-Тилищак, Мирослава Герич.</i> Практичне застосування перевірки статистичних гіпотез у педагогічних дослідженнях	129
40. <i>Éva Sütő, Ibolya Revákné Markóczi.</i> Innovative teaching method—LEGO Duplo in STEM education	131
41. <i>Márta Turcsányi-Szabó.</i> Changing workforce requirements need paradigm shift in education	133
42. <i>Gábor Ujhelyi.</i> LLM-ek alkalmazhatósága beadott feladatok kiértékelésében	135
43. <i>Ibolya Veress-Bágyi.</i> Az összeállított kérdéssorunk többszörözése a kérdésbankhoz a generatív mesterséges intelligencia segítségével	137

Секція 3: Алгебраїчні структури та їх застосування /	
3. szekció: Algebrai struktúrák és alkalmazásaik / Section 3:	
Algebraic Structures and Their Applications	139
44. <i>Bilal Ahmad Rather</i> . Extremal topological indices and their applications in drug design	140
45. <i>Ágota Figula</i> . Malcev-like binary Lie algebras	141
46. <i>Andriy Gatalevych</i> . Bezout duo ring R is an elementary divisor ring iff R is a ring of neat range 1	143
47. <i>Ágnes Kápolnai</i> . Group rings with metabelian unit groups in characteristic 2	144
48. <i>Volodymyr Prokip</i> . On symmetric solutions of the matrix equation $AX = B$ over a Bezout domain	146
49. <i>Patrik Pista, Viktor Traski</i> . A prímszámokkal kapcsolatos megfigyelések. A Mersenne-prímekkel kapcsolatos új észrevételek	149
50. <i>Liudmila Sabinina</i> . On 2-nilpotent loops of 2 generators of exponent 2	152
51. <i>Volodymyr Shchedryk</i> . General linear group and idempotent matrices over a field	153
52. <i>Myroslav Stoika</i> . Projective matrix representations of finite groups	154
53. <i>Олександр Тилищак</i> . Застосування групових кілець скінченних груп у побудові розширених бінарних кодів Голея	155
Секція 4: Застосування цифрових інструментів у дослідженні: виклики та можливості / 4. szekció: Digitális eszközök alkalmazása a kutatásban: kihívások és lehetőségek / Section 4: The Application of Digital Tools in Research: Challenges and Opportunities	
	157
54. <i>Йосеф Головач, Іван Дудаш</i> . Угорсько-український (українсько-угорський) математичний тлумачний онлайн-словник	158
55. <i>Attila Fazekas</i> . Replikációs krízis jelensége a mesterséges intelligencia területén használt osztályozók esetében	161
56. <i>Olha Hopkalo, Lyudmyla Sakhno</i> . On sample paths properties of sub-Gaussian type random fields and applications to stochastic heat equations	165
57. <i>Hajnalka Izsák</i> . Experiences from an online interview-based study conducted in a juvenile correctional institution	167
58. <i>Олег І. Клесов</i> . Розподіл Санкт-Петербурзької гри	169

59. Оксана Лагода, Володимир Лагода, Артем Мусік. Аналіз геометричних властивостей дерматоскопічних зображень як метод ранньої діагностики меланом	171
60. Marta Litynska, Olha Pelekhata. The use of artificial intelligence for the selection of methods for the analysis of sea water samples	174
61. Іван Половко, Микола Маляр. Оцінка стану водних ресурсів у регіоні	177
62. Іван Маргітич, Людвіг Горей. Задача Коші для гіперболічного рівняння з випадковою правою частиною	180
63. Олександр Міца, Андрій Шапочка, Ігор Шапочка, Віктор Дуло. Визначення максимальної кліки при накладанні обмежень на кількість ребер	182
64. Михайло Михасюк. Задача Коші для рівняння коливання струни на площині з випадковими факторами з простору Орліча	184
65. Юлія Мисло, Михайло Пагіря. Атака на шифр RSA на базі правильних ланцюгових дробів	187
66. Alexandra Palinszky, Attila Fazekas. Jupyter Notebook – interaktív vizualizációs eszköz az oktatásban és a kutatásban	190
67. Iryna Rozora, Yurii Mlavets, Olga Vasylyk. Some properties of stochastic processes from the space $\mathbf{F}_{\psi}(\Omega)$	194
68. Ганна Іванівна Сливка-Тилищак, Марія Олександрівна Тилищак. Побудова вибірок множин міри нуль	198
69. Kevin Szántó, István Kolozsvári, József Holovács, Erzsébet Kohut. A Fodor István Természettudományi Kutatóközpont állattani múzeumának online elérése	200
70. Ferenc Szilágyi. A digitalizáció hatása a történeti földrajzi kutatásokban – bihar közigazgatási térképsorozata	203
71. Krisztián Váradí. Iskolai nyelvitájkép-kutatások határon innen és túl	205
72. Ольга Василик, Тетяна Маловічко, Ростислав Ямненко. φ -Субгауссові процеси дробового ефекту	209
Секція 5 (онлайн): Цифрові інструменти в науці та освіті / 5. szekció (online szekció): Digitális eszközök a kutatásban és iskolai oktatásban / Section 5 (online): Digital tools in research and education	213
73. Степан Бабич, Юрій Жигуц. Контактні задачі про взаємодію нескінченного стрингера і двох однакових попередньо напружених смуг	214

74. <i>Edith Debreñti</i> . Using the Poly-Universe toolkit in elementary classes	218
75. <i>János Dudás, József Holovács, Béla Rácz</i> . IRIS – digitális oktatásszervezés a II. Rákóczi Ferenc Kárpátaljai Magyar Főiskolán	220
76. <i>Мирослава Глебена, Марія Ломага</i> . Хмарні технології як альтернатива програмному забезпеченню у шкільному курсі інформатики	224
77. <i>Олександра Качмар</i> . Цифрові трансформації культури: можливості та виклики дослідження суспільних змін	226
78. <i>István Kolozsvári, István Hadnagy, Anita Szikura, Enikő Nagy-Kolozsvári, Erzsébet Kohut</i> . A Kárpátaljai élőlény-monitorozó alkalmazás aktuális lehetőségei az oktatásban és környezetkutatásokban	229
79. <i>Наталія Кондрук, Інна Герода</i> . Застосування штучного інтелекту у кібербезпеці	232
80. <i>Dmytro Malyskyi, Oleksandra Astashkina, Vasyl Ignatyshyn</i> . Seismicity of Mars	237
81. <i>Marianna Marusynets</i> . Challenges and opportunities for the application of artificial intelligence in the republic of Ireland	242
82. <i>Krisztina Megyeri, Brigitta Szilágyi</i> . Innovatív digitális módszerek hátrányos helyzetű tanulók felzárkóztatásában	247
83. <i>Anastasiia Melnyk, Iryna Rozora</i> . Statistical Estimation and Hypothesis Testing on Impulse Response Function	249
84. <i>Lilla Pető</i> . Is Culture Measurable? An Analysis of the Effectiveness of Public Cultural Institutions from the Perspective of Cultural Learning	251
85. <i>Ібоя Самборовскі-Нодь</i> . Використання цифрових баз даних в історичних дослідженнях	252
86. <i>Віктор Шаботько</i> . Штучний інтелект в шкільному курсі інформатики	253
87. <i>Brigitta Szilágyi</i> . Innovatív digitális módszerek a bemeneti mérések lebonyolításában	256
88. <i>Lajos Toldi</i> . A jövő iskolája: innovatív digitális technológiák integrációja a tanításban	257
89. <i>Johanna Tripo, Edith Debreñti</i> . Tanító- és tanárképzésben részt vevő hallgatók külső és belső motivációinak vizsgálata korrespondenciaelemzés alkalmazásával	261

90. *Олексій Веретюнкін*. Ключові завдання веб-додатків у фокусі документації: порівняння React, Angular і Vue

АТАКА НА ШИФР RSA НА БАЗІ ПРАВИЛЬНИХ ЛАНЦЮГОВИХ ДРОБІВ

ЮЛІЯ МИСЛО, МИХАЙЛО ПАГІРЯ

Кафедра твердотільної електроніки та інформаційної безпеки
Ужгородський національний університет, Ужгород, Україна
julia.pah@gmail.com

Кафедра твердотільної електроніки та інформаційної безпеки
Ужгородський національний університет, Ужгород, Україна
pahirya@gmail.com

Людство завжди прагнуло зберегти свої секрети — особисті, ділові, військові політичні тощо. Важлива інформація передавалася і передається у зашифрованому вигляді. Методи шифрування/дешифрування даних вивчаються, досліджуються та удосконалюються в рамках криптології, яка складається з двох взаємопов'язаних частин — криптографії та криптоаналізу. На практиці використовуються шифри із симетричними та асиметричними ключами.

Якщо M — відкритий текст, а C — криптограма, зашифроване повідомлення, то рівняння шифрування та дешифрування запишуться наступним чином [1]:

$$C = E_{k_1}(M), \quad M = D_{k_2}(C), \quad \text{де } k_1, k_2 \text{ — ключі.}$$

За час t_g противник може здійснити "грубу силу", "брутальну атаку" на шифр реалізувавши повний перебір значень ключа. Це може ефективно спрацювати, коли простір ключів K має не велику потужність. З іншого боку, всяка інформація, в незалежності від її важливості, має свій термін актуальності, час t_a . Якщо $t_g \gg t_a$, то проводити перебір ключів є недоречно, а вибрані ключі шифру вважають практично стійкими.

Широке використання шифрів з асиметричними ключами пояснюється тим, що а) ключі та алгоритм шифрування можна передавати по відкритим каналам зв'язку; б) ключ дешифрування відомий лише отримувачу повідомлень; в) зламування ключа дешифрування належить до важко розв'язуваних математичних задач.

Для реалізації шифрування за RSA алгоритмом потрібно: А) вибрати два великих простих числа p та q , що мають однаковий порядок, і

обчислити їх добуток $n = pq$; В). вибрати два цілих числа e та d , що задовольняють умову $ed \equiv 1 \pmod{\varphi(n)}$, де $\varphi(n) = (p-1)(q-1)$.

Функція Ойлера $\varphi(n)$ визначає порядок мультиплікативної групи $\mathbb{Z}_n^*$, тобто множину оборотних за модулем $\varphi(n)$ елементів. Пара чисел $\langle n, e \rangle$ визначає відкритий ключ шифрування, який публікується відкрито, тріада $\langle p, q, d \rangle$ утворює секретний або приватний ключ алгоритму, що відомий лише отримувачу зашифрованих повідомлень.

Відкрите повідомлення оцифровують і розбивають на блоки довжини $M < n$. Рівняння шифрування в алгоритмі RSA визначається співвідношенням

$$C = E(M) = M^e \pmod{n}.$$

Рівняння дешифрування записується наступним чином

$$M = D(C) = C^d \pmod{n}.$$

Здійснити атаку на RSA алгоритм можна двома шляхами: А) визначити для числа n його співмножники p та q , тобто розв'язати задачу факторизації числа n ; В) знайти значення функції Ойлера $\varphi(n)$ і через відоме значення e обчислити обернений елемент d . Ці задачі еквівалентні за складністю.

Відомі алгоритми факторизації — метод Ферма, метод пробного ділення, ρ -метод Полларда та інші [6] успішно працюють, коли множники середнього класу. За допомогою цих методів досягається результат за досить тривалий час виконання. Деякі із методів мають високі вимоги до оперативної пам'яті або важко реалізуються на практиці.

Реалізація алгоритму RSA вимагає тривалого часу для шифруванні та дешифруванні. Щоб підвищити ефективність процесу передачі інформації можна зменшити кількість бітів при виборі відкритого ключа e або секретного ключа d . Необхідність вибирати один із ключів шифрування e чи дешифрування d малим виникають у випадку, коли шифрування або дешифрування здійснюються на комп'ютерах різної потужності, або коли існує потреба швидкого виконання дешифрування повідомлень із-за їх великої кількості чи важливості інформації. В одно час, вибір одного із ключів малим несе загрозу безпеці крипто-системи.

Вінер [8] запропонував алгоритм, який при виконанні певних додаткових умов із відомих значень відкритого ключа $\langle e, n \rangle$ дозволяє знайти секретний ключ d . Цей алгоритм базується на використанні правильних ланцюгових дробів [7, 2].

Нехай виконується нерівність $q < p < 2q$ і робиться припущення, що секретний ключ d задовольняє співвідношення

$$d < \frac{\sqrt[4]{n}}{3}. \quad (1)$$

Пошук секретного ключа здійснюється наступним чином: відношення складових відкритого ключа e/n подається правильним ланцюговим дробом

$$e/n = [a_0; a_1, a_2, \dots, a_k, \dots], \quad a_i \in \mathbb{N}$$

і послідовно знаходяться знаменники Q_k підхідних дробів

$$P_k/Q_k = [a_0; a_1, a_2, \dots, a_k]$$

за формулою Волліса $Q_k = a_k Q_{k-1} + Q_{k-2}$, де $Q_{-1} = 0$, $Q_0 = 1$. Вибирається деяке число M . Секретним ключем d буде те значення знаменника Q_k , для якого виконується еквівалентність

$$(M^e)^{Q_k} \equiv M \pmod{n}.$$

Оцінка (1) допустимих значень секретного ключа d , для яких атака Вінера успішна, покращена [4]

$$d < n^{0.292}. \quad (2)$$

В [5] доведено, що коли елемент відкритого ключа $e \approx n^t$, то секретна частина ключа відновлюється, якщо

$$d < 2\sqrt{2}n^{\frac{3}{4}-\frac{t}{2}}. \quad (3)$$

Коли $t = 1$, тоді

$$d < 2\sqrt{2}n^{1/4},$$

і отримана оцінка у більш як 8 разів перевищує оцінку Вінера.

Для жодної із оцінок (1)–(3) не доведено, що вона є абсолютною і не може бути покращена. Числові експерименти показують, що метод правильних ланцюгових дробів дозволяє знайти таємний ключ d в деяких випадках, коли оцінки не виконуються.

1. О.Г. Корченко, and В.П. Сіденко, and Ю.О. Дрейс *Прикладна криптологія: системи шифрування*, Державний університет телекомунікацій, 2014.
2. М. Пагірйа, *Наближення функцій ланцюговими дробами*, Гражда, Ужгород, 2016.
3. S. Abubakar, and M. Ariffin, and M. Asbullah, *A New Improved Bound for Short Decryption Exponent on RSA Modulus $n = pq$ using Wiener's Method*, Malaysian Journal of Mathematical Sciences(2019), **13**, 89–99.
4. D. Boneh, and G. Durfee, *Cryptanalysis of RSA with private key d less than $N^{0.292}$* , IEEE transactions on Information Theory(2000), **46**, no. 4, 1339–1349.
5. M. Bunder, and J. Tonien *A New Attack on the RSA Cryptosystem Based on Continued Fractions.*, Malaysian Journal of Mathematical Sciences(2017), **11**, 45–57.
6. Al. Menezes, and P. C. Van Oorschot, and S. A. Vanstone, *Handbook of applied cryptography*, CRC press, 2018.
7. O. Perron, *Die Lehre von den Kettenbrüchen*, Stuttgart: Teubner, 1954.
8. M. J. Wiener, *Cryptanalysis of short RSA secret exponents*, IEEE Transactions on Information theory, **36**(1990), no. 3, 553–558.

Інноваційні цифрові методи в галузі освіти та досліджень. Наукове видання (Збірник тез доповідей) Закарпатського угорського інституту імені Ференца Ракоці II / Редактори: Каталін Кучінка, Олександр Тилищак, Мирослав Стойка, Еніке Якоб, Габрієлла Пап та Адам Доровці. Берегове: ЗУІ ім. Ференца Ракоці II, 2025. – 266 с. (українською, угорською та англійською мовами)

ISBN 978-617-8143-36-7 (PDF)

Збірник містить тези доповідей міжнародної науково-практичної конференції *Інноваційні цифрові методи в галузі освіти та досліджень*, яка відбулася 27–28 березня 2025 року в місті Берегове. Матеріали конференції охоплюють широке коло питань, пов'язаних із виявленням найновіших тенденцій у застосуванні інноваційних цифрових методів і засобів в освіті та науці. Конференція зосередилась на викликах та можливостях інтеграції цифрових технологій у навчальний процес, а також на розвитку дослідницьких методів. Зокрема, тези доповідей конференції досліджують впровадження цифрових технологій у шкільну та вищу освіту, використання штучного інтелекту, методичні інновації, алгебраїчні структури, теорію ймовірностей і моделювання, а також застосування цифрових інструментів у наукових дослідженнях. Учасники конференції обговорили підходи до вирішення актуальних питань, пов'язаних із застосуванням інноваційних методів у навчанні, використанням штучного інтелекту у викладанні математики, інтеграцією цифрових технологій у освітній процес, а також удосконаленням методики викладання дисциплін у закладах вищої освіти. Особлива увага була приділена сучасним тенденціям у педагогічних дослідженнях та можливостям адаптації освітніх програм до потреб сучасного студентства. Організаторами конференції були кафедра математики та інформатики спільно з Науковим товариством студентів і молодих вчених Закарпатського угорського інституту імені Ференца Ракоці II.

Наукове видання

ІННОВАЦІЙНІ ЦИФРОВІ МЕТОДИ В ГАЛУЗІ ОСВІТИ ТА ДОСЛІДЖЕНЬ

Міжнародна науково-практична конференція
Берегове, 27–28 березня 2025 року

Збірник тез доповідей

2025 р.

*Рекомендовано до видання в електронній формі (PDF)
рішенням Вченої ради Закарпатського угорського інституту імені Ференца Ракоці II
(протокол №2 від «24» березня 2025 року)*

Підготовлено до видання кафедрою математики та інформатики
спільно з Видавничим відділом Закарпатського угорського інституту
імені Ференца Ракоці II

За редакцією:

*Каталін Кучінка, Олександр Тилищак, Мирослав Стойка, Еніке Якоб,
Габрієлла Пап та Адам Доровці*

Технічне редагування: *Олександр Тилищак, Олександра Полінські та Олександр Добош*

Коректура: *Ільдико Гріца-Варцаба та авторська*

Дизайн обкладинки: *Іштван Балог*

УДК: *Бібліотека ім. Опацої Черє Яноша при ЗУІ ім. Ф.Ракоці II*

Відповідальний за випуск:

Олександр Добош (начальник Видавничого відділу ЗУІ ім. Ф.Ракоці II)

Відповідальність за зміст і достовірність публікацій покладається на авторів
тез доповідей. Точки зору авторів публікацій можуть не співпадати
з точкою зору редакторів.

Проведення конференції та видання збірника тез доповідей
в електронній формі (PDF) здійснено за підтримки уряду Угорщини.

Видавництво: Закарпатський угорський інститут імені Ференца Ракоці II
(адреса: пл. Кошута 6, м. Берегове, 90202. Електронна пошта: foiskola@kmf.uz.ua;
kiado@kmf.uz.ua) *Свідомство про внесення суб'єкта видавничої справи до
Державного реєстру видавців, виготовлювачів і розповсюджувачів видавничої
продукції Серія ДК 7637 від 19 липня 2022 року*

Шрифт «LaTeX (Roman)». Розмір сторінок: A5 (148x210мм).
Обсяг в авторських аркушах 12,55 (501 842 знаків із пробілами)

