

# CYBER SECURITY IN CROSS-BORDER COOPERATION

BOOK OF CONFERENCE ABSTRACTS

---

International academic and practical conference

Berehove, 15–16 October 2024



КІБЕРБЕЗПЕКА  
В ТРАНСКОРДОННОМУ СПІВРОБІТНИЦТВІ

Міжнародна науково-практична конференція  
Берегове, 15–16 жовтня 2024 року

Збірник тез доповідей

CYBER SECURITY  
IN CROSS-BORDER COOPERATION

International academic and practical conference  
Berehove, 15–16 October 2024

Book of Conference Abstracts

KIBERBIZTONSÁG  
A HATÁROKON ÁTNYÚLÓ EGYÜTTMŰKÖDÉSBEN

Nemzetközi tudományos és szakmai konferencia  
Beregszász, 2024. október 15–16.

Absztraktkötet

**Міністерство освіти і науки України  
Закарпатський угорський інститут імені Ференца Ракоці II  
Ужгородський національний університет**

## **КІБЕРБЕЗПЕКА В ТРАНСКОРДОННОМУ СПІВРОБІТНИЦТВІ**

Міжнародна науково-практична конференція  
Берегове, 15–16 жовтня 2024 року

Збірник тез доповідей



**ЗУІ ім. ФЕРЕНЦА РАКОЦІ II**  
Берегове  
2024

Збірник містить тези доповідей міжнародної науково-практичної конференції «Кібербезпека в транскордонному співробітництві», яка відбулася 15–16 жовтня 2024 року в місті Берегове. Матеріали конференції охоплюють широке коло питань, пов'язаних із забезпеченням кібербезпеки в умовах посиленої глобальної взаємодії. Зокрема, тези доповідей конференції досліджують сучасні кіберзагрози, інтеграцію штучного інтелекту в системи безпеки, трансформації методів кіберзахисту та обмін закордонним досвідом. Учасниками конференції були обговорені підходи до вирішення актуальних питань інформаційної безпеки на міжнародному рівні та надання практичних знань студентам, фахівцям і дослідникам. Організатори конференції: Закарпатський угорський інститут імені Ференца Ракоці II та Ужгородський національний університет. Співорганізатори: Національний авіаційний університет, ІТ Степ Університет, Пряшівський університет у Пряшеві та Північний університетський центр у Бая-Маре Технічного університету Клуж-Напока.

Рекомендовано до видання у друкованій та електронній формі (PDF)  
рішенням Вченої ради Закарпатського угорського інституту імені Ференца Ракоці II  
(протокол №10 від «21» листопада 2024 року)

Підготовлено до видання кафедрами історії та суспільних дисциплін, обліку і аудиту, математики та інформатики Закарпатського угорського інституту імені Ференца Ракоці II і кафедрами програмного забезпечення систем, міжнародних студій та суспільних комунікацій Ужгородського національного університету спільно з Видавничим відділом ЗУІ ім. Ф. Ракоці II

За редакцією:

*Степан Черничко, Маріанна Марусинець, Єлизавета Молнар Д,  
Ганна Мелеганіч та Оксана Мулеса*

Технічне редагування: *Адам Доровці, Олександр Добош та Ігор Лях*

Коректура: *авторська*

Дизайн обкладинки: *Вівієн Товт*

УДК: *Бібліотека ім. Опаціої 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.

Публікації науково-педагогічних працівників і студентів Ужгородського національного університету виконано в рамках держбюджетної теми ДБ-921М «Захист інформаційної безпеки при управлінні проєктами міжнародного співробітництва на засадах гарантування національної безпеки України» за підтримки Міністерства освіти і науки України.



Проведення конференції та друк видання 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)

**Друк:** ТОВ «РІК-У» (адреса: вул. Карпатської України 36, м. Ужгород, 88006. Електронна пошта: print@rik.com.ua)

ISBN 978-617-8143-27-5 (м'яка обкладинка)

ISBN 978-617-8143-28-2 (PDF)

© Автори, 2024

© Редактори, 2024

© Закарпатський угорський інститут імені Ференца Ракоці II, 2024

**Ministry of Education and Science of Ukraine  
Ferenc Rakoczi II Transcarpathian Hungarian College  
of Higher Education  
Uzhhorod National University**

## **CYBER SECURITY IN CROSS-BORDER COOPERATION**

International academic and practical conference  
Berehove, 15–16 October 2024

Book of Conference Abstracts



Transcarpathian Hungarian College  
Berehove  
2024



**UDC 659.2.012.8:004.056(063)**

**C 89**

The book contains abstracts of presentations at the international academic and practical conference “Cybersecurity in Cross-Border Cooperation”, which took place on 15-16 October 2024 in Berehove. The conference materials cover a wide range of issues related to cybersecurity in the context of enhanced global interaction. In particular, the conference abstracts explore modern cyber threats, integration of artificial intelligence into security systems, transformation of cyber defence methods and exchange of foreign experience. The conference participants discussed approaches to addressing topical issues of information security at the international level and providing practical knowledge to students, professionals and researchers. Organisers of the conference: Ferenc Rakoczi II Transcarpathian Hungarian College of Higher Education and Uzhhorod National University. Co-organisers: National Aviation University, IT Step University, University of Presov and Northern University Center of Baia Mare at Technical University of Cluj-Napoca.

Recommended for publication in printed and electronic form (PDF file format)  
by the Academic Council of Ferenc Rakoczi II Transcarpathian Hungarian College of Higher Education  
(record No.10 of November 21, 2024)

This volume of conference materials has been prepared by the Department of History and Social Sciences, the Department of Accounting and Auditing, the Department of Mathematics and Informatics at the Ferenc Rakoczi II Transcarpathian Hungarian College of Higher Education, and the Department of Systems Software, the Department of International Studies and Public Communications at the Uzhhorod National University, and the Division of Publishing at the Transcarpathian Hungarian College.

Edited by:

*Stepan Chernychko, Marianna Marusynets, Yelyzaveta Molnar D.,  
Hanna Melehanych and Oksana Mulesa*

Technical editing: *Adam Dorovtsi, Sándor Dobos and Ihor Liakh*

Proof-reading: *the authors*

Cover design: *Vivien Tóth*

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 Ferenc Rakoczi II  
Transcarpathian Hungarian College of Higher Education)

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.

Publications of research and teaching staff and students at the Uzhhorod National University were implemented within the framework of the state budget theme DB-921M “Information Security Protection in the Management of International Cooperation Projects on the Basis of Ensuring the National Security of Ukraine” with the support of the Ministry of Education and Science of Ukraine.



The conference and the publication of the conference abstracts  
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)

**Printing:** “RIK-U” LLC (Address: Carpathian Ukraine Street 36, 88006 Uzhhorod, Ukraine. E-mail: print@rik.com.ua)

**ISBN 978-617-8143-27-5 (paperback)**

© Authors, 2024

**ISBN 978-617-8143-28-2 (PDF)**

© Editors, 2024

© Ferenc Rakoczi II Transcarpathian Hungarian College of Higher Education, 2024

**Ukrajna Oktatási és Tudományos Minisztériuma  
II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola  
Ungvári Nemzeti Egyetem**

## **KIBERBIZTONSÁG A HATÁROKON ÁTNYÚLÓ EGYÜTTMŰKÖDÉSBEN**

Nemzetközi tudományos és szakmai konferencia  
Beregszász, 2024. október 15–16.

Absztraktkötet



II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola  
Beregszász  
2024

A kiadvány 2024. október 15–16-án, Beregszászban *Kiberbiztonság a határokon átnyúló együttműködésben* címmel megrendezett nemzetközi tudományos és szakmai konferencián elhangzott előadások absztraktjait tartalmazza. Az előadások szerkesztett anyagai olyan kibervédelemi kérdéseket vizsgálnak a fokozódó globális együttműködés körülményeivel összefüggésben, mint a modern kibertámadások, a mesterséges intelligencia integrálása a biztonsági rendszerekbe, a kiberbiztonsági módszerek átalakulása és a nemzetközi kibervédelmi tapasztalatcsere. A konferencia résztvevői továbbá megvitatták az információbiztonság aktuális kérdéseinek lehetséges megoldásait nemzetközi szinten, valamint a tudás, ismeretanyag hallgatóknak, szakembereknek és kutatóknak történő átadásának módjait. A konferencia szervezői: a II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola és az Ungvári Nemzeti Egyetem. Társszervezők: Nemzeti Repülőmérnöki Egyetem, IT-STEP University, Eperjesi Egyetem, a Kolozsvári Műszaki Egyetem Nagybányai Északi Egyetemi Központja.

Nyomtatott és elektronikus formában (PDF-fájlformátumban) történő kiadásra javasolta  
a II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola Tudományos Tanácsa  
(2024. november 21., 10. számú jegyzőkönyv).

Kiadásra előkészítette a II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola Történelem- és Társadalomtudományi Tanszéke, Számvitel és Auditálás Tanszéke, Matematika és Informatika Tanszéke, Kiadói Részlege, valamint az Ungvári Nemzeti Egyetem Szoftverrendszerek Tanszéke, Nemzetközi Tanulmányok és Közszolgálati Kommunikáció Tanszéke együttműködve a II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola Kiadói Részlegével.

Szerkesztette:

*Csernicskó István, Maruszinec Marianna, Molnár D. Erzsébet,  
Melehánics Anna és Mulesza Okszana*

Műszaki szerkesztés: *Daróci Ádám, Dobos Sándor és Ljáh Ihor*

Korrektúra: *a szerzők*

Borítóterv: *Tóth Vivien*

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)

A monográfia tartalmáért és hitelességéért a szerzők viselik a felelősséget.

A szerzők álláspontja nem feltétlenül tükrözi a szerkesztők véleményét.

Az Ungvári Nemzeti Egyetem kutatói és oktatói munkatársainak és hallgatóinak publikációi Ukrajna Oktatási és Tudományos Minisztériumának támogatásával, a DB-921M „Az információbiztonság védelme a nemzetközi együttműködési projektek irányításában Ukrajna nemzetbiztonságának biztosítása alapján” című állami költségvetési projekt teljesítésének részeként készültek.



A konferenciát és a kiadvány 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)

**Nyomdai munkálatok:** „RIK-U” Kft. (cím: 88 006 Ungvár, Kárpáti Ukrajna u. 36. E-mail: print@rik.com.ua)

ISBN 978-617-8143-27-5 (puhatáblás)

ISBN 978-617-8143-28-2 (PDF)

© A szerzők, 2024

© A szerkesztők, 2024

© II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola, 2024



## ЗМІСТ / CONTENT / TARTALOM

|                                                                                                                                                                                  |           |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| <b>КІБЕРБЕЗПЕКА У СФЕРІ КУЛЬТУРИ КІБЕРСТІЙКОСТІ</b><br><b>CYBER SECURITY IN THE FIELD OF CYBER RESILIENCE CULTURE</b><br><b>KIBERBIZTONSÁG A KIBERREZILIENCIA TERÜLETÉN.....</b> | <b>13</b> |
| Віталій АНДРЕЙКО, Леонід ДЕРБАК: ОСОБЛИВОСТІ ДІЯЛЬНОСТІ США<br>У СФЕРІ КІБЕРБЕЗПЕКИ .....                                                                                        | 14        |
| Інна ЧЕРВІНСЬКА: КІБЕРБУЛІНГ В ОСВІТНЬОМУ СЕРЕДОВИЩІ:<br>МЕХАНІЗМИ РЕАГУВАННЯ ТА ПРОФІЛАКТИКИ.....                                                                               | 16        |
| Олександр БАТЮКОВ, Світлана ЛУЦЕНКО: ПСИХОЛОГО-ПРАВОВІ НАСЛІДКИ<br>КІБЕРБУЛІНГУ: ВПЛИВ ТА МЕХАНІЗМИ ЗАХИСТУ .....                                                                | 19        |
| Свєгенія ГАЙОВИЧ: KEYC-СТАДІ: БЕЗПЕКА МЕСЕНДЖЕРІВ В ОСВІТІ.....                                                                                                                  | 21        |
| Роман КЕЛЕМЕН: КІБЕРБЕЗПЕКА , СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ<br>ТА ЇХ ВПЛИВ НА МАЙБУТНІХ ФАХІВЦІВ ПРАВОЗНАВСТВА<br>У ПРОЦЕСІ НАВЧАННЯ В КОЛЕДЖІ .....                           | 23        |
| Андріана КЕЛЕМЕН: ШТУЧНИЙ ІНТЕЛЕКТ У ПРОФЕСІЙНІЙ ПІДГОТОВЦІ<br>МАЙБУТНІХ СОЦІАЛЬНИХ ПРАЦІВНИКІВ: ОЧІКУВАНІ ПЕРСПЕКТИВИ<br>ВІД ВПРОВАДЖЕННЯ .....                                 | 25        |
| Світлана РОМАНЮК: КІБЕРБЕЗПЕКА ДЛЯ МОЛОДШИХ ШКОЛЯРІВ:<br>ВИКЛИКИ ТА МОЖЛИВОСТІ .....                                                                                             | 27        |
| Марія ОЛІЯР: ПРОБЛЕМА КІБЕРБЕЗПЕКИ В ОСВІТНЬОМУ ПРОСТОРІ ЗВО.....                                                                                                                | 28        |
| Mykola PROTSSENKO: CYBERSECURITY: DEFENDING NETWORKS<br>FROM EVOLVING THREATS.....                                                                                               | 29        |
| Ігор ТОДОРОВ: КІБЕРБЕЗПЕКА В НОВІТНІХ БЕЗПЕКОВИХ УГОДАХ УКРАЇНИ.....                                                                                                             | 30        |
| <b>СУЧАСНІ ПРАКТИКИ У СФЕРІ КІБЕРБЕЗПЕКИ</b><br><b>MODERN PRACTICES IN THE FIELD OF CYBER SECURITY</b><br><b>MODERN GYAKORLATOK A KIBERBIZTONSÁG TERÜLETÉN.....</b>              | <b>31</b> |
| Anastasiya YEVTUSHENKO, Larysa TEREMINKO: CYBERSECURITY<br>IN THE CONTEXT OF CYBER RESILIENCE: UKRAINIAN EXPERIENCE .....                                                        | 32        |
| Валентина БІЛАН: КІБЕРЗАГРОЗИ ТА ЇХ ПРАВОВЕ РЕГУЛЮВАННЯ<br>В УМОВАХ МІЖНАРОДНИХ ЗБРОЙНИХ КОНФЛІКТІВ .....                                                                        | 33        |
| Марія МЕНДЖУЛ, Оксана МУЛЕСА: ПРОБЛЕМИ ГАРАНТУВАННЯ<br>КІБЕРБЕЗПЕКИ У ПРОЦЕСІ ТРАНСКОРДОННОГО СПІВРОБІТНИЦТВА<br>ПІД ЧАС ВОЄННОГО СТАНУ .....                                    | 35        |
| Валерія ЧОБАЛЬ, Ігор ЛЯХ: РОЛЬ ЛІНГВІСТИЧНОЇ ЕКСПЕРТИЗИ ТА<br>ШТУЧНОГО ІНТЕЛЕКТУ В ЗАБЕЗПЕЧЕННІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ .....                                                      | 37        |
| Марта ШЕЛЕМБА: ІНТЕГРАЦІЯ СУЧАСНИХ ЦИФРОВИХ ТЕХНОЛОГІЙ<br>У НАВЧАЛЬНИЙ ПРОЦЕС: ДОСВІД ДВНЗ «УЖГОРОДСЬКИЙ<br>НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ» .....                                      | 39        |
| Kira SHVED, Natalia BILOUS: MODELS AND TOOLS FOR EFFECTIVE RESPONSE<br>TO CYBER INCIDENTS IN THE CONTEXT OF CERT: CHALLENGES<br>AND PROSPECTS .....                              | 41        |
| Natalia TODOROVA: INTEGRATING CYBERSECURITY AND ARTIFICIAL<br>INTELLIGENCE INTO TERTIARY EDUCATION PEDAGOGY .....                                                                | 42        |

|                                                                                                                                                                                                                                                                                                                                                                                        |           |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| Ольга ГРИЩУК, Олександр КОРЧЕНКО: ВЕРИФІКАЦІЯ МАТЕМАТИЧНОЇ<br>МОДЕЛІ СИМТЕРИЧНОЇ КРИПТОГРАФІЧНОЇ СИСТЕМИ ЗАХИСТУ<br>МОВНОЇ ІНФОРМАЦІЇ НА ОСНОВІ ДИФЕРЕНЦІАЛЬНИХ ПЕРЕТВОРЕНЬ .....                                                                                                                                                                                                      | 43        |
| Юрій МАТЕЛЕШКО: ЦИФРОВА ДИПЛОМАТІЯ: ПЕРЕВАГИ ТА РИЗИКИ.....                                                                                                                                                                                                                                                                                                                            | 44        |
| Ганна МЕЛЕГАНІЧ, Каріна ТОВТИН: ОСОБЛИВОСТІ ФОРМУВАННЯ<br>КІБЕРДИПЛОМАТІЇ УКРАЇНИ .....                                                                                                                                                                                                                                                                                                | 45        |
| Оксана РЕЗВАН, Лідія ТКАЧЕНКО: ПСИХОЛОГІЯ БЕЗПЕЧНОГО ПРОСТОРУ<br>МЕШКАНЦІВ ПРИКОРДОННОГО ВОЄННОГО ХАРКОВА .....                                                                                                                                                                                                                                                                        | 46        |
| Лариса ТЕРЕМІНКО, Анастасія ЯРОШ, Анастасія ЄВТУШЕНКО:<br>СУЧАСНІ ПРАКТИКИ У СФЕРІ КІБЕРБЕЗПЕКИ .....                                                                                                                                                                                                                                                                                  | 48        |
| Михайло ШЕЛЕМБА: ЦИФРОВА ТРАНСФОРМАЦІЯ ОСВІТИ<br>У СФЕРІ МІЖНАРОДНИХ ВІДНОСИН: ВИКЛИКИ ТА ПЕРСПЕКТИВИ .....                                                                                                                                                                                                                                                                            | 49        |
| Diana BOBCHYNETS, Mariia IVANOVA, Ann DYSHLEVA: THE IMPACT<br>OF CROSS-BORDER CYBERCRIME ON GLOBAL SECURITY .....                                                                                                                                                                                                                                                                      | 50        |
| Ilia YEVPRAK, Natalia BILOUS: CYBER THREATS IN CROSS-BORDER<br>FINANCIAL TRANSACTIONS.....                                                                                                                                                                                                                                                                                             | 52        |
| Victoria KARPENKO, Evgenia LICHENKO, Ann DYSHLEVA: INTERNATIONAL<br>RESPONSE MECHANISMS TO CROSS-BORDER CYBER INCIDENTS .....                                                                                                                                                                                                                                                          | 53        |
| Olena KOVALCHUK, Maria MOGYLEVETS, Ann DYSHLEVA: CROSS-BORDER<br>COOPERATION IN CYBERSPACE: THE KEY TO SHAPING GLOBAL SECURITY<br>STANDARDS.....                                                                                                                                                                                                                                       | 55        |
| <b>ОСОБЛИВОСТІ ВИМОГ ДО КІБЕРЗАХИСТУ ІНФОРМАЦІЙНОЇ<br/>КОМУНІКАЦІЇ, ЕКОНОМІКИ ТА ІНШИХ СФЕР ДІЯЛЬНОСТІ ЛЮДИНИ<br/>REQUIREMENTS FOR CYBER PROTECTION OF INFORMATION<br/>COMMUNICATION, ECONOMY AND OTHER SPHERES<br/>OF HUMAN ACTIVITY<br/>INFORMÁCIÓS KOMMUNIKÁCIÓ, A GAZDASÁG ÉS AZ EMBERI<br/>TEVÉKENYSÉG EGYÉB TERÜLETEINEK KIBERBIZTONSÁGÁRA<br/>VONATKOZÓ KÖVETELMÉNYEK .....</b> | <b>57</b> |
| HIRES-LÁSZLÓ Kornélia, NAGY Mariann Zsuzsanna: A PISA-TESZTEK PÉNZÜGYI<br>MŰVELTSÉG KUTATÁSA ÉS A KIBERBIZTONSÁG.....                                                                                                                                                                                                                                                                  | 58        |
| LOSZKORIH Gabriella, BÁTORI Vivien: A KÉSZPÉNZ NÉLKÜLI ELSZÁMOLÁSOK<br>DIGITALIZÁLÁSA: A DIGITÁLIS KORSZAK ÚJ KIHÍVÁSAI.....                                                                                                                                                                                                                                                           | 63        |
| Габрієлла ЛОСКОРИХ, Оксана ПЕРЧІ: КІБЕРБЕЗПЕКА ЯК ВАЖЛИВИЙ ЕЛЕМЕНТ<br>ДЛЯ УСПІШНОГО ВПРОВАДЖЕННЯ ІНІЦІАТИВ BEPS .....                                                                                                                                                                                                                                                                  | 65        |
| Анастасія ОМЕЛЬЧЕНКО: РОЛЬ HR У ФОРМУВАННІ КОРПОРАТИВНОЇ<br>КІБЕРБЕЗПЕКИ: УПРАВЛІННЯ РИЗИКАМИ, ПОВ'ЯЗАНИМИ<br>З ЛЮДСЬКИМ ФАКТОРОМ .....                                                                                                                                                                                                                                                | 67        |
| Ростислав РОМАНЮК, Василь МОРОХОВИЧ: ОСОБЛИВОСТІ БЕЗПЕКИ<br>ТА КОНФІДЕНЦІЙНОСТІ ДАНИХ У МОБІЛЬНИХ ФІНАНСОВИХ ДОДАТКАХ.....                                                                                                                                                                                                                                                             | 68        |
| Victoriia KURDULIAN, Evheniy KUCHERIAVY, Nataliia DENISENKO:<br>INFORMATION SECURITY OF MODERN BUSINESS ORGANIZATIONS .....                                                                                                                                                                                                                                                            | 70        |
| Олена КОБУС, Степан БОНДАРЕНКО: КІБЕРЗАГРОЗИ ДЛЯ ВЕЛИКИХ ДАНИХ<br>(BIG DATA): СТРАТЕГІЇ ЗАХИСТУ І БЕЗПЕКИ .....                                                                                                                                                                                                                                                                        | 72        |
| Андрій МАЛЬЦЕВ, Л. ДАНЬКО -ТОВТИН: ТЕХНОЛОГІЯ «ZERO TRUST».....                                                                                                                                                                                                                                                                                                                        | 73        |

|                                                                                                                                                                |            |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| <b>КІБЕРБЕЗПЕКА: ЗАКОРДОННИЙ ДОСВІД</b>                                                                                                                        |            |
| <b>CYBER SECURITY: FOREIGN EXPERIENCE</b>                                                                                                                      |            |
| <b>KIBERBIZTONSÁG: KÜLFÖLDI TAPASZTALATOK.....</b>                                                                                                             | <b>75</b>  |
| DARÓCI Ádám, SZÁNTÓ Kevin: KIBERBIZTONSÁGI STRATÉGIÁK<br>AZ AMERIKAI EGYESÜLT ÁLLAMOKBAN .....                                                                 | 76         |
| MOLNÁR Ferenc, KERÉKES Ariána: GÖRÖGORSZÁG KIBERBIZTONSÁGA.....                                                                                                | 78         |
| Наталія ВАРОДІ, Сільвестер ІЖАК: СТАН КІБЕРБЕЗПЕКИ У СВІТІ<br>НА БАЗІ ДОСЛІДЖЕННЯ КОМПАНІЇ FLASHPOINT .....                                                    | 82         |
| Каріна ВАШКЕБА, Маріанна МАРУСИНЕЦЬ: КІБЕРБЕЗПЕКА: ДОСВІД ФРАНЦІЇ .....                                                                                        | 84         |
| Летісія СВЕДКУ, Маріанна МАРУСИНЕЦЬ: КІБЕРБЕЗПЕКА: ДОСВІД ОАЕ.....                                                                                             | 91         |
| Маріанна МАРУСИНЕЦЬ: ЗАХИСТ ОБ'ЄКТІВ КРИТИЧНОЇ НАЦІОНАЛЬНОЇ<br>ІНФРАСТРУКТУРИ ВІД КІБЕРАТАК: ДОСВІД ІРЛАНДІЇ.....                                              | 98         |
| MOLNÁR D. Erzsébet, ZSUKOVSKY Ágnes: DIGITÁLIS HATÁROK:<br>DÉL-KOREA ÉS MAGYARORSZÁG KIBERBIZTONSÁGI STRATÉGIÁINAK<br>ÖSSZEHASONLÍTÁSA .....                   | 102        |
| CSATÁRY György, VASS Jázmin: KIBERBIZTONSÁGI STRATÉGIÁK<br>AZ EGYESÜLT ÁLLAMOKBAN .....                                                                        | 105        |
| DARCSI Karolina, HUBER Alex: KIBERBIZTONSÁG NÉMETORSZÁGBAN.....                                                                                                | 108        |
| CSATÁRY György, SZENYKÓ Volodimir: KIBERBIZTONSÁG AZ EURÓPAI UNIÓ<br>ÉLETÉBEN .....                                                                            | 111        |
| Yelyzaveta MOLNAR D. Orsolya MÁTÉ: CANADA'S CYBERSECURITY.....                                                                                                 | 115        |
| Світлана КАЛАУР, Микола НАГОЛЮК: МОЖЛИВОСТІ ІНФОРМАЦІЙНИХ<br>ТЕХНОЛОГІЙ В СУЧАСНИХ УМОВАХ ОХОРОНИ ЗОВНІШНІХ КОРДОНІВ<br>ЄВРОПЕЙСЬКОГО СОЮЗУ .....              | 120        |
| Lubov PANTELLEIEVA, Natalia BILOUS: CYBERSECURITY:<br>A GLOBAL PRIORITY .....                                                                                  | 122        |
| <b>РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ</b>                                                                                                   |            |
| <b>THE ROLE OF ARTIFICIAL INTELLIGENCE IN INFORMATION SECURITY</b>                                                                                             |            |
| <b>A MESTERSÉGES INTELLIGENCIA SZEREPE AZ INFORMÁCIÓBIZTONSÁG</b>                                                                                              |            |
| <b>TERÜLETÉN.....</b>                                                                                                                                          | <b>123</b> |
| JAKAB Enikő, PAPP Gabriella: MESTERSÉGES INTELLIGENCIA ALAPÚ<br>OKTATÁSI ESZKÖZÖK BIZTONSÁGA: KIHÍVÁSOK ÉS MEGOLDÁSOK.....                                     | 124        |
| TEMETŐ Ádám, SZTOJKA Miroszláv: HOGYAN FORMÁLJA A MESTERSÉGES<br>INTELLIGENCIA AZ INFORMÁCIÓBIZTONSÁG JÖVŐJÉT? .....                                           | 126        |
| BOROS József, KUCSINKA Katalin: A MESTERSÉGES INTELLIGENCIA<br>ÉS A FŐISKOLÁS HALLGATÓK MATEMATIKAI KOMPETENCIATESZTEK<br>EREDMÉNYEINEK ÖSSZEHASONLÍTÁSA ..... | 130        |
| Юрій БІРКОВИЧ, Василь КУТ: ШТУЧНИЙ ІНТЕЛЕКТ ЯК ПЕРСПЕКТИВА<br>РОЗВИТКУ АНТИВІРУСНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ.....                                             | 131        |
| Maryna VASYLYK: PECULIARITIES OF USING ARTIFICIAL INTELLIGENCE<br>IN CYBERSECURITY.....                                                                        | 133        |
| Олександр ГУМЕННИЙ: КОНЦЕПТУАЛЬНА МОДЕЛЬ ІНТЕГРАЦІЇ<br>ШТУЧНОГО ІНТЕЛЕКТУ У СИСТЕМУ КІБЕРЗАХИСТУ НАВЧАЛЬНОЇ<br>ЦИФРОВОЇ ПЛАТФОРМИ .....                        | 134        |

|                                                                                                                                                                            |     |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| Олена ГУРСЬКА, Антон ЛУЧИЦЬКИЙ: ШТУЧНИЙ ІНТЕЛЕКТ<br>У ЗАБЕЗПЕЧЕННІ КІБЕРБЕЗПЕКИ: СУЧАСНІ ВИКЛИКИ ТА ПЕРСПЕКТИВИ .....                                                      | 135 |
| Олександр ДУБІВ: РЕАЛІЗАЦІЯ БАЗОВОЇ КІБЕРБЕЗПЕКИ У ГЕНОМНИХ ВЕБ-<br>ДОДАТКАХ: ШИФРУВАННЯ, БЕЗПЕКА ДАНИХ ТА ЗАХИСТ ВІД ВТРУЧАННЯ<br>НА ПРИКЛАДІ ІСНУЮЧОГО ВЕБ-ПРОЄКТУ ..... | 136 |
| Антон ДІВИНЕЦЬ, Наталія ШУМИЛО: ШТУЧНИЙ ІНТЕЛЕКТ<br>ЯК ІНСТРУМЕНТ КІБЕРЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ .....                                                              | 139 |
| Юрій КІШ, Ігор ЛЯХ: РИЗИКИ СУЧАСНИХ КІБЕРЗАГРОЗ<br>ДЛЯ МОБІЛЬНИХ ЗАСТОСУНКІВ .....                                                                                         | 142 |
| Деніел КЕЛАРЬ, Василь ВАКУЛЬЧАК: ВИКОРИСТАННЯ ШТУЧНОГО<br>ІНТЕЛЕКТУ В СФЕРІ ПРОМИСЛОВОЇ АВТОМАТИЗАЦІЇ .....                                                                | 144 |
| Кирил КОТУН: ПОЛІТИКА БЕЗПЕЧНОГО ЗАСТОСУВАННЯ ШТУЧНОГО<br>ІНТЕЛЕКТУ В УНІВЕРСИТЕТАХ СКАНДИНАВСЬКИХ КРАЇН .....                                                             | 146 |
| Володимир ОРЕЛ, Василь МОРОХОВИЧ: ВИКОРИСТАННЯ ШТУЧНОГО<br>ІНТЕЛЕКТУ ДЛЯ ЗАПОБІГАННЯ ЛЮДСЬКИМ ПОМИЛКАМ<br>У СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ .....                              | 148 |
| Антон СМОЛЕН, Михайло КЛЯП: ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ<br>ДЛЯ АНАЛІЗУ КРИПТОГРАФІЧНИХ ПРОТОКОЛІВ ТА ВИЯВЛЕННЯ ЇХ<br>СЛАБКІХ МІСЦЬ .....                               | 150 |
| Артемій ЦІПІНЬО, Юліан МЕРЕНИЧ: ВИКОРИСТАННЯ ШТУЧНОГО<br>ІНТЕЛЕКТУ В БОРОТБІ З ЗАГРОЗАМИ .....                                                                             | 152 |
| Олена ПЕТРУШЕВИЧ, Еніке ЯКОБ: ВПЛИВ ШТУЧНОГО ІНТЕЛЕКТУ<br>НА ІНФОРМАЦІЙНУ БЕЗПЕКУ У ВИКЛАДАННІ ІНФОРМАТИКИ .....                                                           | 154 |
| Artym ROSTYSLAV, Tetyana SHULHA: ARTIFICIAL INTELLIGENCE<br>AS AN INFORMATION SECURITY TOOL .....                                                                          | 155 |
| Polina TARAN, Viktoria SHVED, Nataliia DENISENKO: CAN ARTIFICIAL<br>INTELLIGENCE SURPASS HUMAN INTELLIGENCE: TECHNICAL<br>AND PHILOSOPHICAL PERSPECTIVES? .....            | 157 |
| Валерій КОЗЮРА: КЕРУВАННЯ КІБЕРБЕЗПЕКОЮ НА ОСНОВІ МОДЕЛЕЙ<br>ШТУЧНОГО ІНТЕЛЕКТУ .....                                                                                      | 158 |
| Богдан КОШТУРА, Марія МЕНДЖУЛ: ПРАВОВЕ РЕГУЛЮВАННЯ<br>ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ШТУЧНОГО ІНТЕЛЕКТУ .....                                                                       | 159 |
| Олександр РАДКЕВИЧ: ЦИФРОВА БЕЗПЕКА В ЕЛЕКТРОННИХ СИСТЕМАХ<br>ОЦІНЮВАННЯ ПРОФЕСІЙНОЇ ДІЯЛЬНОСТІ ПЕДАГОГІВ .....                                                            | 160 |
| Veronika KUKSA, Natalia BILOUS: AUTOMATION OF THREAT DETECTION<br>PROCESSES: IMPROVING THE QUALITY .....                                                                   | 161 |
| Olexandra ZADOROZHNA, Hanna SOROKUN: ARTIFICIAL INTELLIGENCE<br>AND CYBERSECURITY .....                                                                                    | 162 |
| Maksim BRODYAK, Natalia BILOUS: MODERN TRENDS AND CHALLENGES<br>OF CYBER SECURITY IN THE CONDITIONS OF DIGITAL TRANSFORMATION .....                                        | 163 |
| Антон ЛУЧИЦЬКИЙ, Олена ГУРСЬКА: ШТУЧНИЙ ІНТЕЛЕКТ<br>У ЗАБЕЗПЕЧЕННІ КІБЕРБЕЗПЕКИ: СУЧАСНІ ВИКЛИКИ ТА ПЕРСПЕКТИВИ .....                                                      | 164 |

**Євгенія ГАЙОВИЧ**  
*аспірант кафедри загальної педагогіки  
та педагогіки вищої школи,  
начальник відділу електронного навчання центру  
інформаційних технологій  
ДВНЗ «Ужгородський національний університет»*

### **КЕЙС-СТАДІ: БЕЗПЕКА МЕСЕНДЖЕРІВ В ОСВІТІ**

Ключові слова: освітній процес, освітні платформи, месенджери, IT-інструменти, кібербезпека.

Сучасний освітній процес дедалі більше характеризується використанням інформаційних технологій та систем, а освітньо-наукова комунікація здійснюється через різні месенджери і платформи. З огляду на питання онлайн-присутності в інформаційному, науковому, освітньому цифровому просторах виникає потреба дослідити безпеку каналів комунікації та ефективність у забезпеченні конфіденційності, захисту персональних даних і збереження інформації. Месенджери широко застосовуються для організації навчального процесу, але недостатня увага до питань кібербезпеки може створювати серйозні загрози для учасників освітнього середовища.

Наукова проблема полягає в дослідженні рівня безпеки найбільш популярних месенджерів, які використовуються в освітніх установах, на основі аналізу їхніх функціональних можливостей і систем захисту даних та окресленні основних кіберзагроз, пов'язаних з використанням месенджерів в освітньому процесі. Мета – оцінка безпеки популярних месенджерів в освітньому середовищі та надання рекомендацій щодо їх використання.

Станом на 2024 рік існує чимала кількість месенджерів. Німецька компанія зі збору та візуалізації даних Statista проаналізувала ринок використання месенджерів та визначила, що у 2024 році перші 5 сходинки рейтингу серед застосунків у світі посідають: WhatsApp (2 млрд користувачів), Facebook Messenger (1,3 млрд користувачів), WeChat (1,2 млрд користувачів), QQ (648 млн користувачів), Telegram (500 млн користувачів). Для порівняння, згідно з даними компанії InMind, в Україні у 2024 році найпопулярнішими месенджерами є Viber (73,6%), Facebook Messenger (42,7%), Telegram (31,6%), WhatsApp (25,3%), Skype (19,2%).

За аналізом вибірок можна зробити висновок, що ці месенджери спрямовані на особисте використання, де рівень безпеки має не менш важливе значення, ніж для установ, і зокрема освітніх. На жаль, часто месенджери особистого використання стають інструментами комунікації в робочому середовищі, у тому числі і в рамках освітнього процесу, що є не зовсім коректним. Українські дослідники та науковці, до прикладу С.Л. Лебедева та М.К. Лебедев [1], аналізують месенджери з точки зору зручності використання та функціоналу, але не з точки зору безпеки.

Найбільшу прихильність освітян отримали Viber та Telegram. У період карантину використання цих месенджерів серед освітян Закарпатської області складало понад 90%. Щодо безпеки, то ці застосунки не входять у топ найбезпечніших. За даними Cyber Division, Інститут дослідження кібервійни ICWR, Telegram не є безпечним месенджером і не рекомендується у використанні як для приватного спілкування, так і корпоративного, через наскрізне шифрування повідомлень не відбувається за замовчуванням, як у Signal, Threema чи WhatsApp. Це окрема функція у вигляді секретних чатів. До 99% спілкування в цьому месенджері відбувається поза «секретними» чатами. Весь контент, який продукується в Telegram за відсутності наскрізного шифрування за замовчуванням (метадані, чати, фото, відео, аудіо), зберігається на серверах назавжди, навіть якщо користувач видалить дані з телефону. Частина серверів Telegram знаходяться у росії, за даними OSINT, а також використовує для передачі мережевого трафіку лише російські компанії – RETN і LLC GLOBALNET. У цьому випадку так само адміністратори мережі можуть легко моніторити трафік, який є незашифрованим [2].



Платформи для комунікації в закладах освіти з акцентом на безпеку мають відповідати високим стандартам захисту даних та конфіденційності. Для цього потрібне комплексне рішення, а саме розгортання відповідних воркспейсів, які включатимуть додатки та застосунки для швидкої комунікації, зберігання даних та багаторівневе управління ними, а також забезпечуватимуть надійний рівень безпеки. Такі ресурси використовуються більше в закладах вищої освіти і менше в закладах загальної середньої та професійної.

Google Workspace – це пакет спеціалізованого хмарного програмного забезпечення й інструментів для спільної роботи від компанії Google. Продукти доступні широкому загалу безкоштовно, однак у версіях Google Workspace передбачені корпоративні функції – спеціальні адреси електронної пошти в домені компанії. Доменні облікові записи мають ряд переваг та надають ширший спектр можливостей. Google використовує наскрізне шифрування для всіх даних, що передаються між користувачами. Google Chat забезпечує шифрований прямий обмін повідомленнями, групові розмови та простори, які дозволяють користувачам створювати, призначати завдання та ділитися файлами в межах робочого середовища на додаток до спілкування в чаті. Платформа відповідає вимогам GDPR та стандартам захисту конфіденційності даних. До особливостей можна віднести адміністрування прав доступу, можливість контролю з боку IT-адміністраторів закладу.

Microsoft Teams – центр для командної роботи в Office 365 від Microsoft, який інтегрує користувачів, вміст і засоби, необхідні команді для ефективнішої роботи. Платформа забезпечує високий рівень захисту через наскрізне шифрування, двофакторну автентифікацію та інтеграцію з Microsoft 365, яка відповідає стандартам GDPR та інших регуляцій. Дані зберігаються в зашифрованому вигляді, що унеможливує несанкціонований доступ. Створення приватних каналів, захищений обмін файлами, адміністрування доступу до ресурсів – основні переваги ресурсу.

Slack – корпоративний месенджер, який пропонує розширені функції безпеки, такі як наскрізне шифрування даних під час передачі, а також управління доступом до робочих каналів. Платформа відповідає вимогам HIPAA, GDPR та інших стандартів. Відзначається контролем доступу через адміністрування, інтеграцією з системами безпеки, моніторингом активності.

Різноманіття ресурсів для комунікації буде і надалі збільшуватися через вимоги часу та глобалізаційні процеси. Тож вибір месенджерів повинен відбуватися з урахуванням безпекових критеріїв: наскрізне шифрування, двофакторна автентифікація, управління даними. Безсумнівно потрібне навчання учасників освітнього процесу основам кібербезпеки для роботи з платформами (створення надійних паролів, уникнення фішингових атак). І найголовнішим є розробка внутрішніх політик щодо використання месенджерів для навчальних цілей, правил комунікації з урахуванням відповідальності за дані.

Отже, месенджери є зручним та ефективним інструментом для навчальної комунікації, але потребують ретельної уваги та підходу до питань безпеки та вибору правильних платформ, а впровадження правил безпечного використання можуть суттєво знизити ризики для конфіденційності та захисту інформації в освіті.

#### **Список використаних джерел:**

1. Лебедева С. Л. Месенджер Telegram як основний і додатковий канал комунікації в освітньому процесі / С. Л. Лебедева, М. К. Лебедев // Інноваційна педагогіка. – 2022. – Вип. 54, Т. 2. – С. 193-196. DOI <https://doi.org/10.32782/2663-6085/2022/54.2.38>
2. Ризики telegram. Чи безпечно користуватися месенджером та чи пов'язаний він з ФСБ і ГРУ РФ? Розповідають фахівці Cyber Division та Інституту дослідження кібервійни ICWR. Електронний ресурс: <https://forbes.ua/innovations/riziki-telegram-chi-bezpechno-koristuvatisya-mesendzherom-ta-chi-povyazaniy-vin-z-fsb-ta-gru-rf-rozpovidayut-fakhivtsi-cyber-division-ta-institutu-doslidzhennya-kiberviyini-icwr-19022024-19311>

УДК 659.2.012.8:004.056(063)

К 38

**Кібербезпека в транскордонному співробітництві.** Наукове видання (Збірник тез доповідей) Закарпатського угорського інституту імені Ференца Ракоці II / Редактори: Степан Черничко, Маріанна Марусинець, Єлизавета Молнар Д, Ганна Мелеганич та Оксана Мулеса. Берегове: ЗУІ ім. Ференца Ракоці II, 2024. – 166 с. (українською, англійською та угорською мовами)

**ISBN 978-617-8143-27-5 (м'яка обкладинка)**

**ISBN 978-617-8143-28-2 (PDF)**

Збірник містить тези доповідей міжнародної науково-практичної конференції «Кібербезпека в транскордонному співробітництві», яка відбулася 15–16 жовтня 2024 року в місті Берегове. Матеріали конференції охоплюють широке коло питань, пов'язаних із забезпеченням кібербезпеки в умовах посиленої глобальної взаємодії. Зокрема, тези доповідей конференції досліджують сучасні кіберзагрози, інтеграцію штучного інтелекту в системи безпеки, трансформації методів кіберзахисту та обмін закордонним досвідом. Учасниками конференції були обговорені підходи до вирішення актуальних питань інформаційної безпеки на міжнародному рівні та надання практичних знань студентам, фахівцям і дослідникам. Організатори конференції: Закарпатський угорський інститут імені Ференца Ракоці II та Ужгородський національний університет. Співорганізатори: Національний авіаційний університет, ІТ Степ Університет, Пряшівський університет у Пряшеві та Північний університетський центр у Бая-Маре Технічного університету Клуж-Напока.

*Наукове видання*

# **КІБЕРБЕЗПЕКА В ТРАНСКОРДОННОМУ СПІВРОБІТНИЦТВІ**

Міжнародна науково-практична конференція  
Берегове, 15–16 жовтня 2024 року

Збірник тез доповідей

2024 р.

*Рекомендовано до видання у друкованій та електронній формі (PDF)  
рішенням Вченої ради Закарпатського угорського інституту імені Ференца Ракоці II  
(протокол №10 від «21» листопада 2024 року)*

Підготовлено до видання кафедрами історії та суспільних дисциплін, обліку і аудиту, математики та інформатики Закарпатського угорського інституту імені Ференца Ракоці II і кафедрами програмного забезпечення систем, міжнародних студій та суспільних комунікацій Ужгородського національного університету спільно з Видавничим відділом ЗУІ ім. Ф. Ракоці II

За редакцією:

*Степан Черничко, Маріанна Марусинець, Єлизавета Молнар Д,  
Ганна Мелеганіч та Оксана Мулеса*

Технічне редагування: *Адам Доровці, Олександр Добош та Ігор Лях*

Коректура: *авторська*

Дизайн обкладинки: *Вівієн Товт*

УДК: *Бібліотека ім. Опаціої 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.

Публікації науково-педагогічних працівників і студентів Ужгородського національного університету виконано в рамках держбюджетної теми ДБ-921М «Захист інформаційної безпеки при управлінні проектами міжнародного співробітництва на засадах гарантування національної безпеки України» за підтримки Міністерства освіти і науки України.

Проведення конференції та друк видання 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) *Свідоцтво про внесення суб'єкта видавничої справи до Державного реєстру видавців, виготовлювачів і розповсюджувачів видавничої продукції Серія ДК 7637 від 19 липня 2022 року*

**Друк:** ТОВ «РІК-У» (адреса: вул. Карпатської України 36, м. Ужгород, 88006. Електронна пошта: print@rik.com.ua) *Свідоцтво про внесення суб'єкта видавничої справи до Державного реєстру видавців, виготівників і розповсюджувачів видавничої продукції Серія ДК 5040 від 21 січня 2016 року*

Шрифт «Times New Roman».

Папір офсетний, щільністю 80 г/м<sup>2</sup>. Друк цифровий. Ум. друк. арк. 13,49.

Формат 70x100/16.

