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

УДК 659.2.012.8:004.056(063)
К 38

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, IT 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 Мелеганич та Оксана Мулеса

Технічне редагування: *Адам Доровці, Олександр Добош та Ігор Лях*
Коректура: *авторська*
Дизайн обкладинки: *Вівієн Товт*
УДК: *Бібліотека ім. Опацої Чере Яноша при ЗУІ ім. Ф.Ракоці II*

Відповідальний за випуск:
Олександр Добош (начальник Видавничого відділу ЗУІ ім. Ф.Ракоці II)

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)

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)

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

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

ETO 659.2.012.8:004.056(063)
K 38

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 együttműköve
a II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola Kiadói Részlegével.

Szerkesztette:
Csernicskó István, Maruszinec Marianna, Molnár D. Erzsébet,
Melehánics Anna és Mulesza Okszána

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)

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)

ЗМІСТ / CONTENT / TARTALOM

КІБЕРБЕЗПЕКА У СФЕРІ КУЛЬТУРИ КІБЕРСТІЙКОСТІ
CYBER SECURITY IN THE FIELD OF CYBER RESILIENCE CULTURE
KIBERBIZTONSÁG A KIBERREZILIENCIA TERÜLETÉN 13

Віталій АНДРЕЙКО, Леонід ДЕРБАК: ОСОБЛИВОСТІ ДІЯЛЬНОСТІ США У СФЕРІ КІБЕРБЕЗПЕКИ 14

Інна ЧЕРВІНСЬКА: КІБЕРБУЛІНГ В ОСВІТНЬОМУ СЕРЕДОВИЩІ: МЕХАНІЗМИ РЕАГУВАННЯ ТА ПРОФІЛАКТИКИ 16

Олександр БАТЮКОВ, Світлана ЛУЦЕНКО: ПСИХОЛОГО-ПРАВОВІ НАСЛІДКИ КІБЕРБУЛІНГУ: ВПЛИВ ТА МЕХАНІЗМИ ЗАХИСТУ 19

Євгенія ГАЙОВИЧ: КЕЙС-СТАДІ: БЕЗПЕКА МЕСЕНДЖЕРІВ В ОСВІТІ 21

Роман КЕЛЕМЕН: КІБЕРБЕЗПЕКА , СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХОЛОГІЇ ТА ЇХ ВПЛИВ НА МАЙБУТНІХ ФАХІВЦІВ ПРАВОЗНАВСТВА У ПРОЦЕСІ НАВЧАННЯ В КОЛЕДЖІ 23

Андріана КЕЛЕМЕН: ШТУЧНИЙ ІНТЕЛЕКТ У ПРОФЕСІЙНІЙ ПІДГОТОВЦІ МАЙБУТНІХ СОЦІАЛЬНИХ ПРАЦІВНИКІВ: ОЧІКУВАНІ ПЕРСПЕКТИВИ ВІД ВПРОВАДЖЕННЯ 25

Світлана РОМАНЮК: КІБЕРБЕЗПЕКА ДЛЯ МОЛОДШИХ ШКОЛЯРІВ: ВИКЛИКИ ТА МОЖЛИВОСТІ 27

Марія ОЛІЯР: ПРОБЛЕМА КІБЕРБЕЗПЕКИ В ОСВІТНЬОМУ ПРОСТОРІ ЗВО 28

Mykola PROTSENKO: CYBERSECURITY: DEFENDING NETWORKS FROM EVOLVING THREATS 29

Ігор ТОДОРОВ: КІБЕРБЕЗПЕКА В НОВІТНІХ БЕЗПЕКОВИХ УГОДАХ УКРАЇНИ 30

СУЧАСНІ ПРАКТИКИ У СФЕРІ КІБЕРБЕЗПЕКИ
MODERN PRACTICES IN THE FIELD OF CYBER SECURITY
MODERN GYAKORLATOK A KIBERBIZTONSÁG TERÜLETÉN 31

Anastasiya YEVTUSHENKO, Larysa TEREMINKO: CYBERSECURITY IN THE CONTEXT OF CYBER RESILIENCE: UKRAINIAN EXPERIENCE 32

Валентина БІЛАН: КІБЕРЗАГРОЗИ ТА ЇХ ПРАВОВЕ РЕГУЛЮВАННЯ В УМОВАХ МІЖНАРОДНИХ ЗБРОЙНИХ КОНФЛІКТІВ 33

Марія МЕНДЖУЛ, Оксана МУЛЕСА: ПРОБЛЕМИ ГАРАНТУВАННЯ КІБЕРБЕЗПЕКИ У ПРОЦЕСІ ТРАНСКОРДОННОГО СПІВРОБІТНИЦТВА ПІД ЧАС ВОЄННОГО СТАНУ 35

Валерія ЧОБАЛЬ, Ігор ЛЯХ: РОЛЬ ЛІНГВІСТИЧНОЇ ЕКСПЕРТИЗИ ТА ШТУЧНОГО ІНТЕЛЕКТУ В ЗАБЕЗПЕЧЕННІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ 37

Марта ШЕЛЕМБА: ІНТЕГРАЦІЯ СУЧАСНИХ ЦИФРОВИХ ТЕХНОЛОГІЙ У НАВЧАЛЬНИЙ ПРОЦЕС: ДОСВІД ДВНЗ «УЖГОРОДСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ» 39

Kira SHVED, Natalia BILOUS: MODELS AND TOOLS FOR EFFECTIVE RESPONSE TO CYBER INCIDENTS IN THE CONTEXT OF CERT: CHALLENGES AND PROSPECTS 41

Natalia TODOROVA: INTEGRATING CYBERSECURITY AND ARTIFICIAL INTELLIGENCE INTO TERTIARY EDUCATION PEDAGOGY 42

Ольга ГРИЩУК, Олександр КОРЧЕНКО: ВЕРИФІКАЦІЯ МАТЕМАТИЧНОЇ МОДЕЛІ СИМТЕРИЧНОЇ КРИПТОГРАФІЧНОЇ СИСТЕМИ ЗАХИСТУ МОВНОЇ ІНФОРМАЦІЇ НА ОСНОВІ ДИФЕРЕНЦІАЛЬНИХ ПЕРЕТВОРЕНЬ 43

Юрій МАТЕЛЕШКО: ЦИФРОВА ДИПЛОМАТІЯ: ПЕРЕВАГИ ТА РИЗИКИ..... 44

Ганна МЕЛЕГАНИЧ, Каріна ТОВТИН: ОСОБЛИВОСТІ ФОРМУВАННЯ КІБЕРДИПЛОМАТІЇ УКРАЇНИ 45

Оксана РЕЗВАН, Лідія ТКАЧЕНКО: ПСИХОЛОГІЯ БЕЗПЕЧНОГО ПРОСТОРУ МЕШКАНЦІВ ПРИКОРДОННОГО ВОЄННОГО ХАРКОВА 46

Лариса ТЕРЕМІНКО, Анастасія ЯРОШ, Анастасія ЄВТУШЕНКО: СУЧАСНІ ПРАКТИКИ У СФЕРІ КІБЕРБЕЗПЕКИ 48

Михайло ШЕЛЕМБА: ЦИФРОВА ТРАНСФОРМАЦІЯ ОСВІТИ У СФЕРІ МІЖНАРОДНИХ ВІДНОСИН: ВИКЛИКИ ТА ПЕРСПЕКТИВИ 49

Diana BOBCHYNETS, Mariia IVANOVA, Ann DYSHLEVA: THE IMPACT OF CROSS-BORDER CYBERCRIME ON GLOBAL SECURITY 50

Illia YEVPAK, Natalia BILOUS: CYBER THREATS IN CROSS-BORDER FINANCIAL TRANSACTIONS..... 52

Victoria KARPENKO, Evgenia LICHENKO, Ann DYSHLEVA: INTERNATIONAL RESPONSE MECHANISMS TO CROSS-BORDER CYBER INCIDENTS 53

Olena KOVALCHUK, Maria MOGYLEVETS, Ann DYSHLEVA: CROSS-BORDER COOPERATION IN CYBERSPACE: THE KEY TO SHAPING GLOBAL SECURITY STANDARDS..... 55

ОСОБЛИВОСТІ ВИМОГ ДО КІБЕРЗАХИСТУ ІНФОРМАЦІЙНОЇ КОМУНІКАЦІЇ, ЕКОНОМІКИ ТА ІНШИХ СФЕР ДІЯЛЬНОСТІ ЛЮДИНИ
REQUIREMENTS FOR CYBER PROTECTION OF INFORMATION COMMUNICATION, ECONOMY AND OTHER SPHERES OF HUMAN ACTIVITY
INFORMÁCIÓS KOMMUNIKÁCIÓ, A GAZDASÁG ÉS AZ EMBERI TEVÉKENYSÉG EGYÉB TERÜLETEINEK KIBERBIZTONSÁGÁRA VONATKOZÓ KÖVETELMÉNYEK 57

HIRES-LÁSZLÓ Kornélia, NAGY Mariann Zsuzsanna: A PISA-TESZTEK PÉNZÜGYI MŰVELTSÉG KUTATÁSA ÉS A KIBERBIZTONSÁG..... 58

LOSZKORIH Gabriella, BÁTORI Vivien: A KÉSZPÉNZ NÉLKÜLI ELSZÁMOLÁSOK DIGITALIZÁLÁSA: A DIGITÁLIS KORSZAK ÚJ KIHÍVÁSAI..... 63

Габріелла ЛОСКОРІХ, Оксана ПЕРЧІ: КІБЕРБЕЗПЕКА ЯК ВАЖЛИВИЙ ЕЛЕМЕНТ ДЛЯ УСПІШНОГО ВПРОВАДЖЕННЯ ІНІЦІАТИВ BEPS 65

Анастасія ОМЕЛЬЧЕНКО: РОЛЬ HR У ФОРМУВАННІ КОРПОРАТИВНОЇ КІБЕРБЕЗПЕКИ: УПРАВЛІННЯ РИЗИКАМИ, ПОВ'ЯЗАНИМИ З ЛЮДСЬКИМ ФАКТОРОМ 67

Ростислав РОМАНЮК, Василь МОРОХОВИЧ: ОСОБЛИВОСТІ БЕЗПЕКИ ТА КОНФІДЕНЦІЙНОСТІ ДАНИХ У МОБІЛЬНИХ ФІНАНСОВИХ ДОДАТКАХ..... 68

Victoriia KURDULIAN, Evheniy KUCHERIAVY, Nataliia DENISENKO: INFORMATION SECURITY OF MODERN BUSINESS ORGANIZATIONS 70

Олена КОБУС, Степан БОНДАРЕНКО: КІБЕРЗАГРОЗИ ДЛЯ ВЕЛИКИХ ДАНИХ (BIG DATA): СТРАТЕГІЇ ЗАХИСТУ І БЕЗПЕКИ 72

Андрій МАЛЬЦЕВ, Л. ДАНЬКО -ТОВТИН: ТЕХНОЛОГІЯ «ZERO TRUST»..... 73

КІБЕРБЕЗПЕКА: ЗАКОРДОННИЙ ДОСВІД
CYBER SECURITY: FOREIGN EXPERIENCE
KIBERBIZTONSÁG: KÜLFÖLDI TAPASZTALATOK 75

DARÓCI Ádám, SZÁNTÓ Kevin: KIBERBIZTONSÁGI STRATÉGIÁK AZ AMERIKAI EGYESÜLT ÁLLAMOKBAN 76

MOLNÁR Ferenc, KEREKES Ariána: GÖRÖGORSZÁG KIBERBIZTONSÁGA 78

Наталія ВАРОДІ, Сільвестер ІЖАК: СТАН КІБЕРБЕЗПЕКИ У СВІТІ 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 ІНФРАСТРУКТУРИ ВІД КІБЕРАТАК: ДОСВІД ІРЛАНДІЇ 98

MOLNÁR D. Erzsébet, ZSUKOVSZKY Ágnes: DIGITÁLIS HATÁROK: DÉL-KOREA ÉS MAGYARORSZÁG KIBERBIZTONSÁGI STRATÉGIÁINAK ÖSSZEHASONLÍTÁSA 102

CSATÁRY György, VASS Jázmin: KIBERBIZTONSÁGI STRATÉGIÁK AZ EGYESÜLT ÁLLAMOKBAN 105

DARCSI Karolina, HUBER Alex: KIBERBIZTONSÁG NÉMETORSZÁGBAN 108

CSATÁRY György, SZENYKÓ Volodimir: KIBERBIZTONSÁG AZ EURÓPAI UNIÓ ÉLETÉBEN 111

Yelyzaveta MOLNAR D. Orsolya MÁTÉ: CANADA'S CYBERSECURITY 115

Світлана КАЛАУР, Микола НАГОЛЮК: МОЖЛИВОСТІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В СУЧАСНИХ УМОВАХ ОХОРОНИ ЗОВНІШНІХ КОРДОНІВ ЄВРОПЕЙСЬКОГО СОЮЗУ 120

Lubov PANTELLEIEVA, Natalia BILOUS: CYBERSECURITY: A GLOBAL PRIORITY 122

РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ
THE ROLE OF ARTIFICIAL INTELLIGENCE IN INFORMATION SECURITY
A MESTERSÉGES INTELLIGENCIA SZEREPE AZ INFORMÁCIÓBIZTONSÁG TERÜLETÉN 123

JAKAB Enikő, PAPP Gabriella: MESTERSÉGES INTELLIGENCIA ALAPÚ OKTATÁSI ESZKÖZÖK BIZTONSÁGA: KIHÍVÁSOK ÉS MEGOLDÁSOK 124

TEMETŐ Ádám, SZTOJKA Miroszláv: HOGYAN FORMÁLJA A MESTERSÉGES INTELLIGENCIA AZ INFORMÁCIÓBIZTONSÁG JÖVŐJÉT? 126

BOROS József, KUCSINKA Katalin: A MESTERSÉGES INTELLIGENCIA ÉS A FŐISKOLÁS HALLGATÓK MATEMATIKAI KOMPETENCIATESZTEK EREDMÉNYEINEK ÖSSZEHASONLÍTÁSA 130

Юрій БІРКОВИЧ, Василь КУТ: ШТУЧНИЙ ІНТЕЛЕКТ ЯК ПЕРСПЕКТИВА РОЗВИТКУ АНТИВІРУСНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ 131

Maryna VASYLYK: PECULIARITIES OF USING ARTIFICIAL INTELLIGENCE IN CYBERSECURITY 133

Олександр ГУМЕННИЙ: КОНЦЕПТУАЛЬНА МОДЕЛЬ ІНТЕГРАЦІЇ ШТУЧНОГО ІНТЕЛЕКТУ У СИСТЕМУ КІБЕРЗАХИСТУ НАВЧАЛЬНОЇ ЦИФРОВОЇ ПЛАТФОРМИ 134

Олена ГУРСЬКА, Антон ЛУЧИЦЬКИЙ: ШТУЧНИЙ ІНТЕЛЕКТ
У ЗАБЕЗПЕЧЕННІ КІБЕРБЕЗПЕКИ: СУЧАСНІ ВИКЛИКИ ТА ПЕРСПЕКТИВИ 135

Олександр ДУБІВ: РЕАЛІЗАЦІЯ БАЗОВОЇ КІБЕРБЕЗПЕКИ У ГЕНОМНИХ ВЕБ-ДОДАТКАХ: ШИФРУВАННЯ, БЕЗПЕКА ДАНИХ ТА ЗАХИСТ ВІД ВТРУЧАННЯ НА ПРИКЛАДІ ІСНУЮЧОГО ВЕБ-ПРОЄКТУ 136

Антон ДІВИНЕЦЬ, Наталія ШУМИЛО: ШТУЧНИЙ ІНТЕЛЕКТ
ЯК ІНСТРУМЕНТ КІБЕРЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ 139

Юрій КІШ, Ігор ЛЯХ: РИЗИКИ СУЧАСНИХ КІБЕРЗАГРОЗ
ДЛЯ МОБІЛЬНИХ ЗАСТОСУНКІВ 142

Деніел КЕЛАРЬ, Василь ВАКУЛЬЧАК: ВИКОРИСТАННЯ ШТУЧНОГО
ІНТЕЛЕКТУ В СФЕРІ ПРОМИСЛОВОЇ АВТОМАТИЗАЦІЇ 144

Кирил КОТУН: ПОЛІТИКА БЕЗПЕЧНОГО ЗАСТОСУВАННЯ ШТУЧНОГО
ІНТЕЛЕКТУ В УНІВЕРСИТЕТАХ СКАНДИНАВСЬКИХ КРАЇН 146

Володимир ОРЕЛ, Василь МОРОХОВИЧ: ВИКОРИСТАННЯ ШТУЧНОГО
ІНТЕЛЕКТУ ДЛЯ ЗАПОБІГАННЯ ЛЮДСЬКИМ ПОМИЛКАМ
У СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ 148

Антон СМОЛЕН, Михайло КЛЯП: ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ
ДЛЯ АНАЛІЗУ КРИПТОГРАФІЧНИХ ПРОТОКОЛІВ ТА ВИЯВЛЕННЯ ЇХ
СЛАБКИХ МІСЦЬ 150

Артемій ЦІПІНЬО, Юліан МЕРЕНИЧ: ВИКОРИСТАННЯ ШТУЧНОГО
ІНТЕЛЕКТУ В БОРОТЬБІ З ЗАГРОЗАМИ 152

Олена ПЕТРУШЕВИЧ, Еніке ЯКОБ: ВПЛИВ ШТУЧНОГО ІНТЕЛЕКТУ
НА ІНФОРМАЦІЙНУ БЕЗПЕКУ У ВИКЛАДАННІ ІНФОРМАТИКИ 154

Artym ROSTYSLAV, Tetyana SHULHA: ARTIFICIAL INTELLIGENCE
AS AN INFORMATION SECURITY TOOL 155

Polina TARAN, Viktoria SHVED, Nataliia DENISENKO: CAN ARTIFICIAL
INTELLIGENCE SURPASS HUMAN INTELLIGENCE: TECHNICAL
AND PHILOSOPHICAL PERSPECTIVES? 157

Валерій КОЗЮРА: КЕРУВАННЯ КІБЕРБЕЗПЕКОЮ НА ОСНОВІ МОДЕЛЕЙ
ШТУЧНОГО ІНТЕЛЕКТУ 158

Богдан КОШТУРА, Марія МЕНДЖУЛ: ПРАВОВЕ РЕГУЛЮВАННЯ
ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ШТУЧНОГО ІНТЕЛЕКТУ 159

Олександр РАДКЕВИЧ: ЦИФРОВА БЕЗПЕКА В ЕЛЕКТРОННИХ СИСТЕМАХ
ОЦІНЮВАННЯ ПРОФЕСІЙНОЇ ДІЯЛЬНОСТІ ПЕДАГОГІВ 160

Veronika KUKSA, Natalia BILOUS: AUTOMATION OF THREAT DETECTION
PROCESSES: IMPROVING THE QUALITY 161

Olexandra ZADOROZHNA, Hanna SOROKUN: ARTIFICIAL INTELLIGENCE
AND CYBERSECURITY 162

Maksim BRODYAK, Natalia BILOUS: MODERN TRENDS AND CHALLENGES
OF CYBER SECURITY IN THE CONDITIONS OF DIGITAL TRANSFORMATION 163

Антон ЛУЧИЦЬКИЙ, Олена ГУРСЬКА: ШТУЧНИЙ ІНТЕЛЕКТ
У ЗАБЕЗПЕЧЕННІ КІБЕРБЕЗПЕКИ: СУЧАСНІ ВИКЛИКИ ТА ПЕРСПЕКТИВИ 164

Yelyzaveta MOLNAR D.
PhD (History)
Associate Professor at the Department of History and Social Sciences
director of the Tivadar Lehoczky Social Sciences Research Centre
Ferenc Rákóczi II Transcarpathian Hungarian College of Higher Education
Orsolya MÁTÉ
2nd year student
Department of History and Social Sciences, major of international relations, public communications and regional studies at the Ferenc Rákóczi II Transcarpathian Hungarian College of Higher Education

CANADA'S CYBERSECURITY

Key words: *cybersecurity, technology, COVID-19, threat.*

In today's interconnected world, cybersecurity has become a pivotal concern for nations, and Canada is no exception. As technology advances, so too do the threats that jeopardize the security of individuals, organizations, and the country's critical infrastructure. With increasing reliance on digital systems, the potential for cyberattacks grows, impacting everything from personal data to national security. The rise of the internet and digital technologies has transformed how businesses operate and how individuals communicate, but it has also opened the door to malicious actors seeking to exploit vulnerabilities. Cybersecurity threats can range from ransomware attacks that lock users out of their systems to data breaches that compromise sensitive personal information. These threats are not just technical issues; they can have significant economic and social implications, affecting public trust and national security.

Canada's cybersecurity environment is characterized by a diverse array of threats. These range from cybercrime perpetrated by individuals and organized groups to state-sponsored attacks targeting critical infrastructure. Recent years have seen a surge in incidents of ransomware, phishing, and data breaches, significantly impacting both private enterprises and public institutions. According to the Canadian Centre for Cyber Security (CCCS), sectors such as healthcare, finance, and energy are particularly vulnerable, often serving as attractive targets for cybercriminals looking to exploit weaknesses. In 2021, the Canadian Centre for Cyber Security (CCCS) reported a staggering increase in ransomware incidents, with a 151% rise compared to the previous year. This trend is echoed globally; according to Cybersecurity Ventures, ransomware attacks are projected to occur every 11 seconds by 2021, up from every 40 seconds in 2016. This alarming statistic underscores the urgency for effective cybersecurity measures (CCCS, 2022).

The COVID-19 pandemic further exacerbated the cybersecurity landscape, as many organizations rapidly transitioned to remote work, inadvertently expanding their attack surfaces in unprecedented ways. With employees accessing corporate networks from home, often on personal devices and unsecured Wi-Fi connections, potential vulnerabilities multiplied significantly. According to a report by the Cybersecurity and Infrastructure Security Agency (CISA), this shift led to a noticeable increase in cyber incidents, emphasizing how the rapid adoption of remote work arrangements created new opportunities for cybercriminals (CISA, 2020).

Cybercriminals quickly adapted to this new normal, launching targeted phishing campaigns that exploited the heightened fears and uncertainties surrounding the pandemic. For example, studies from cybersecurity firms indicated that the volume of phishing emails surged, with some organizations reporting increases of up to 600% during the early months of the pandemic (Mimecast, 2020). These attacks were often crafted to appear as communications from trusted entities, such as health organizations or government agencies, containing urgent information about COVID-19 protocols, vaccine availability, or financial assistance. Such messages lured individuals into clicking on malicious links or downloading harmful attachments, which compromised both personal and organizational data.

Moreover, many employees lacked adequate cybersecurity training and awareness. As companies rushed to implement remote work policies, training sessions were often abbreviated or overlooked altogether. A study by IBM found that 95% of cybersecurity breaches are due to human error,

highlighting the critical role that employee awareness plays in maintaining security (IBM, 2021). The abrupt transition meant that many workers were unprepared for the increased risks associated with remote work, leaving significant gaps in knowledge about safe online practices. As a result, employees became more susceptible to social engineering tactics, creating an environment ripe for exploitation.

In addition to phishing attacks, cybercriminals exploited security gaps in home networks. Many employees relied on personal routers and devices that were not configured with the same level of security as those found in corporate environments. A report from the Federal Bureau of Investigation (FBI) indicated that unpatched software vulnerabilities and weak home network security were frequently targeted by cybercriminals, allowing unauthorized access to sensitive corporate information (FBI, 2020). Without robust firewalls and intrusion detection systems, home networks became easy targets for attackers seeking unauthorized access to organizational systems.

This evolving landscape underscores the urgent need for effective cybersecurity measures tailored to remote work environments. Organizations must not only reinforce their existing cybersecurity frameworks but also adopt new strategies to address the unique challenges posed by remote work. This includes implementing multifactor authentication, conducting regular security assessments, and providing comprehensive cybersecurity training to employees, ensuring they are equipped to recognize and respond to potential threats (Chaffey, 2021).

The pandemic has fundamentally altered the way we work, and as a result, the need for a proactive approach to cybersecurity has never been more critical. Organizations must recognize that the shift to remote work is likely to persist in some capacity, necessitating a long-term commitment to cybersecurity investment and innovation. According to the World Economic Forum, the ongoing hybrid work model may become a standard practice, which means that businesses must adapt their cybersecurity strategies accordingly (World Economic Forum, 2021). By adopting a forward-thinking mindset and prioritizing the security of remote work environments, organizations can better protect themselves against the evolving tactics of cybercriminals, ultimately safeguarding their operations and sensitive data.

Moreover, the rapid adoption of new technologies, including cloud computing and the Internet of Things (IoT), has expanded the attack surface available to malicious actors. Each connected device and online service presents potential vulnerabilities that can be exploited. The literature indicates that as the digital landscape evolves, so too must the strategies employed to mitigate these threats (Dunn Cavelty, 2013). The challenge lies in ensuring that security protocols keep pace with technological advancements.

In response to these challenges, the Canadian government has implemented several initiatives aimed at strengthening the nation's cybersecurity posture. Recognizing the increasing complexity of cyber threats, the 2018 National Cyber Security Strategy emphasizes a multi-faceted approach that encourages collaboration among government agencies, private sector stakeholders, and civil society. This strategy underscores the need for resilience by focusing on prevention, response, and recovery from cyber incidents (Public Safety Canada, 2018).

A central tenet of the strategy is the promotion of partnerships across various sectors. The government acknowledges that cybersecurity is a shared responsibility and that effective defense requires the engagement of all stakeholders. Research highlights the importance of public-private partnerships in enhancing cybersecurity resilience, as these collaborations facilitate information sharing, threat intelligence, and best practices (NIST, 2020). For instance, the Canadian Cyber Security Strategy fosters cooperation between the Canadian Centre for Cyber Security (CCCS) and private sector entities, enabling organizations to access timely threat assessments and resources.

Furthermore, the strategy highlights the importance of building a robust cybersecurity workforce. The Canadian government has recognized that a skilled workforce is essential for developing and maintaining effective cybersecurity measures. The 2018 strategy outlines plans to enhance education and training in cybersecurity fields, promoting initiatives that engage educational institutions and industry players. Literature indicates that organizations with a strong emphasis on training and

development are better equipped to handle cyber threats, as employees become more adept at recognizing and responding to potential risks (Cybersecurity Workforce Framework, 2017).

In addition to workforce development, the National Cyber Security Strategy places a strong emphasis on public awareness and education. Recognizing that human error is a significant factor in many cyber incidents, the strategy aims to equip Canadians with the knowledge and skills needed to navigate the digital landscape safely. Programs aimed at raising awareness about cybersecurity best practices are crucial, as studies show that informed users are less likely to fall victim to cyber attacks (Holt et al., 2020). Campaigns targeting schools, businesses, and community organizations help instill a culture of cybersecurity, ultimately leading to greater resilience at the societal level.

Another key aspect of the strategy is the commitment to enhancing the security of critical infrastructure. The Canadian government has identified critical sectors—such as energy, healthcare, and finance—that are essential for national security and economic stability. By establishing sector-specific frameworks, the government seeks to ensure that these sectors have the necessary protocols and resources to withstand and recover from cyber incidents. Research underscores the importance of protecting critical infrastructure, as disruptions in these sectors can have cascading effects on the broader economy and public safety (Heidt et al., 2018).

Lastly, the strategy emphasizes the need for continuous adaptation and improvement in cybersecurity practices. As cyber threats evolve, so too must the measures employed to combat them. This includes investing in research and development of new technologies and strategies to enhance threat detection and response capabilities. The literature suggests that an agile and adaptive approach to cybersecurity is essential for organizations to stay ahead of potential threats (Dunn Cavelty, 2013). By fostering an environment of innovation and collaboration, Canada can better position itself to face the challenges of an ever-changing cyber landscape.

In conclusion, the 2018 National Cyber Security Strategy represents a comprehensive approach to enhancing Canada's cybersecurity posture. By emphasizing collaboration, workforce development, public awareness, protection of critical infrastructure, and continuous improvement, the government aims to build a resilient and secure digital environment. As Canada moves forward, the ongoing commitment to these principles will be crucial in addressing the multifaceted nature of cyber threats and safeguarding the nation's digital future.

The establishment of the CCCS as a central authority for cybersecurity in Canada has been a significant development. The CCCS provides critical resources, threat intelligence, and guidance to both the public and private sectors. Its role is to foster a culture of cybersecurity awareness and preparedness across the nation. In 2021, the CCCS issued over 100 threat advisories, informing organizations about emerging threats and vulnerabilities (CCCS, 2022).

One notable initiative is the Cybersecurity Strategy for the Federal Government, which aims to improve the security of government networks and systems while also setting an example for the private sector. This strategy includes measures for enhancing incident response capabilities and protecting sensitive information. It also promotes information sharing between government and industry to create a more unified defense against cyber threats.

While government efforts are crucial, the private sector plays an equally important role in Canada's cybersecurity landscape. Many businesses, particularly small and medium-sized enterprises (SMEs), are often ill-prepared for cyber threats. The Canadian Internet Registration Authority (CIRA) notes that a significant number of SMEs lack basic cybersecurity measures, making them susceptible to attacks (CIRA, 2021). Initiatives like CyberSecure Canada aim to address this gap by providing resources and certification to help businesses bolster their cybersecurity practices.

Public awareness is also a critical factor. Educational campaigns focused on promoting cyber hygiene and best practices are essential in equipping citizens and organizations with the knowledge needed to defend against cyber threats. Research indicates that informed users are less likely to fall victim to cybercrime, making education a key component of prevention strategies (Holt et al., 2020). Programs in schools, community organizations, and workplaces play a vital role in raising awareness about potential risks and teaching people how to protect themselves online.

Furthermore, partnerships between government and the private sector have proven effective in addressing cybersecurity challenges. Information sharing initiatives, such as the Cyber Security Information Sharing Partnership (CSISP), facilitate the exchange of threat intelligence, allowing organizations to stay ahead of emerging threat.

Despite significant progress, Canada's cybersecurity landscape faces several ongoing challenges. The rapid pace of technological advancement often outstrips existing regulatory frameworks, creating gaps in security and oversight. Emerging technologies like artificial intelligence and machine learning introduce new vulnerabilities that must be addressed proactively (Kshetri, 2021). Additionally, the growing sophistication of cyber threats necessitates continuous adaptation and investment in cybersecurity measures.

The issue of cybersecurity skills shortages also poses a challenge. The demand for cybersecurity professionals far exceeds the available talent pool, leading to gaps in expertise that can hinder an organization's ability to defend against attacks. Educational institutions are beginning to respond by offering more cybersecurity programs, but it will take time to develop a workforce equipped to meet the increasing demands of the industry.

Another significant challenge is the evolving nature of cyber threats. Cybercriminals are becoming increasingly sophisticated, employing advanced tactics and techniques to breach defenses. State-sponsored attacks add another layer of complexity, as nation-state actors often have substantial resources at their disposal, enabling them to conduct prolonged and targeted campaigns against critical infrastructure.

Looking to the future, Canada must prioritize research and development in cybersecurity technologies while fostering a culture of innovation. Collaborative efforts between academic institutions, government, and the private sector can drive advancements in threat detection and response capabilities. Additionally, the literature emphasizes the need for a more robust legal framework to address the complexities of cybercrime, ensuring that laws keep pace with technological evolution (Brenner, 2010).

Furthermore, establishing a national cybersecurity training and certification program could help bridge the skills gap and prepare more professionals for careers in cybersecurity. Encouraging diversity in the cybersecurity workforce can also enhance innovation and problem-solving capabilities. Engaging underrepresented groups and promoting STEM education among youth will be crucial in building a more resilient workforce.

Canada's cybersecurity landscape is a complex interplay of challenges and opportunities. As cyber threats become increasingly sophisticated, the nation must continue to adapt its strategies to safeguard critical infrastructure, businesses, and citizens. By investing in education, fostering collaboration, and embracing innovation, Canada can enhance its resilience against an ever-evolving array of cyber threats. The ongoing commitment to a comprehensive approach will be essential in securing Canada's digital future.

References

5. Brenner, S. W. (2010). *Cybercrime: Criminal threats in the information age*. Santa Clara Computer and High Technology Law Journal.
6. Canadian Centre for Cyber Security (CCCS). (2022). *Cyber Threat Assessment 2022*. Government of Canada.
7. Chaffey, D. (2021). *Cybersecurity in a Post-Pandemic World: Strategies for Remote Work*. Smart Insights.
8. Federal Bureau of Investigation (FBI). (2020). *Cyber Crime: A Report on Cyber Incidents During the COVID-19 Pandemic*.
9. Canadian Internet Registration Authority (CIRA). (2021). *Cybersecurity for SMEs: A national snapshot*.
10. Dunn Cavelty, M. (2013). *Cybersecurity: An international perspective*. Routledge.
11. Holt, T. J., et al. (2020). *Cybersecurity awareness and education: The importance of public awareness campaigns*. Journal of Information Systems Security.

12. Kshetri, N. (2021). *Cybersecurity and the role of emerging technologies*. International Journal of Information Management.
13. Public Safety Canada. (2018). *National Cyber Security Strategy*.

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 Мелеганич та Оксана Мулеса

Технічне редагування: *Адам Доровці, Олександр Добош та Ігор Лях*
Коректура: *авторська*
Дизайн обкладинки: *Вівієн Товт*
УДК: *Бібліотека ім. Опацої Чере Яноша при ЗУІ ім. Ф.Ракоці II*

Відповідальний за випуск:
Олександр Добош (начальник Видавничого відділу ЗУІ ім. Ф.Ракоці II)

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) *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/м². Друк цифровий. Ум. друк. арк. 13,49.
Формат 70x100/16.

ISBN 978-617-8143-27-5