

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

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
Свєгенія ГАЙОВИЧ: KEYC-СТАДІ: БЕЗПЕКА МЕСЕНДЖЕРІВ В ОСВІТІ.....	21
Роман КЕЛЕМЕН: КІБЕРБЕЗПЕКА , СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ 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 PROTSSENKO: 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 МЕЛЕГАНІЧ, 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 YEVPACK, 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
Габрієлла ЛОСКОРИХ, 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, KERÉKES 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 СЛАБКІХ МІСЦЬ	150
Артемій ЦІПІНЬО, Юліан МЕРЕНИЧ: ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В БОРОТБІ 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

Антон ДІВИНЕЦЬ
студент 4 курсу спеціальності «Інформаційні системи та технології»
Науковий керівник – Наталія ШУМИЛО
старший викладач кафедри інформатики та фізико-математичних дисциплін,
Ужгородський національний університет

ШТУЧНИЙ ІНТЕЛЕКТ ЯК ІНСТРУМЕНТ КІБЕРЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Штучний інтелект (ШІ) стає ключовим елементом сучасної кібербезпеки, особливо у контексті захисту критичної інфраструктури, такої як: енергетичні системи, транспортні мережі, водопостачання та фінансові структури. В умовах зростання складності та кількості кібератак, традиційні методи захисту виявляються недостатніми для своєчасного виявлення та реагування на нові загрози. Використання ШІ для кіберзахисту надає можливість автоматизувати процеси моніторингу та аналізу великих обсягів даних, які дозволяють оперативно виявляти аномалії, прогнозувати кіберзагрози і блокувати атаки на початкових етапах.

Одним із ключових напрямків використання ШІ у кіберзахисті є виявлення аномалій у системах критичної інфраструктури. Завдяки машинному навчанню, алгоритми можуть "вивчати" нормальну поведінку систем і виявляти відхилення, які можуть свідчити про потенційну кібератаку. Наприклад, компанія Darktrace, яка спеціалізується на кібербезпеці, використовує методи ШІ для аналізу трафіку в мережах своїх клієнтів.[1]

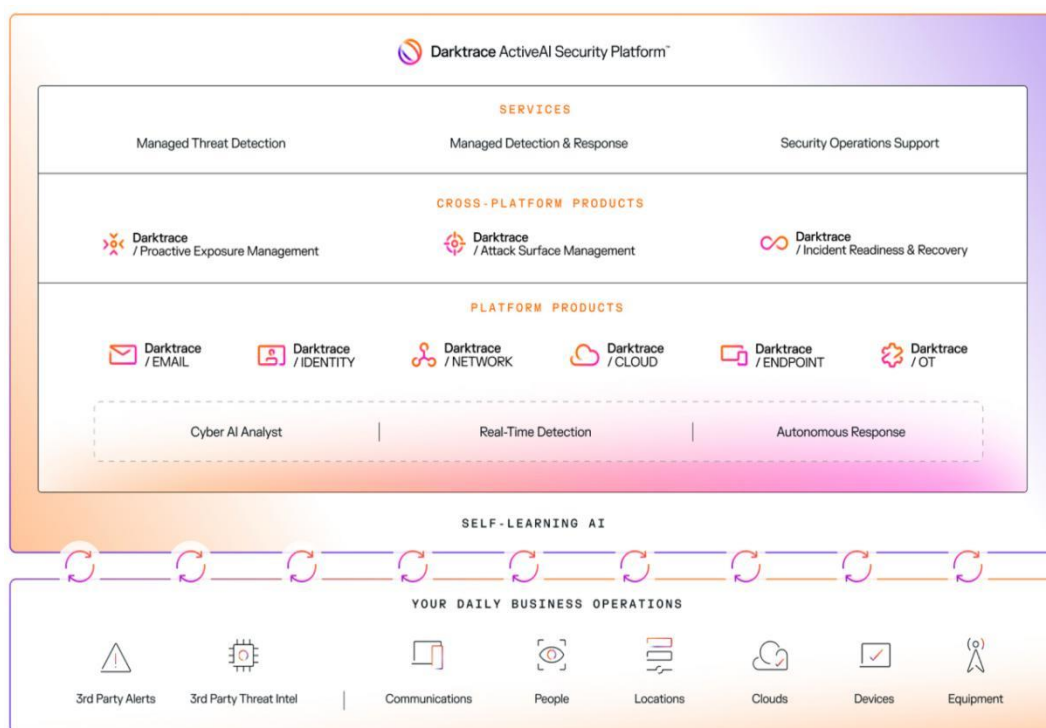


Рис. 1 Платформа захисту з використанням методи ШІ компанії Darktrace

Дана платформа здатна самостійно розпізнавати відхилення у поведінці мережі та блокувати підозрілі дії в режимі реального часу. Це дозволяє виявляти навіть ті атаки, які ще не мають відомих шаблонів або сигнатур, що є критично важливим для захисту від нових загроз, таких як “атаки нульового дня”. Також дана платформа здатна працювати автономно, а саме автоматично визначає підозрілу активність та вживати протоколи захисту для екосистеми структури.

Інший приклад застосування ШІ — це автоматизація процесів реагування на інциденти. Використання алгоритмів ШІ для управління кіберінцидентами значно зменшує час реакції на загрозу. Платформа, така як IBM QRadar, використовують машинне навчання для автоматизації процесів аналізу інцидентів та генерування рекомендацій для швидкого вирішення проблем. Це особливо важливо для захисту критичних систем, де навіть короточасний збій може мати катастрофічні наслідки, наприклад, у сфері енергопостачання чи водопостачання.[2]

Енергетичний сектор є одним із найвразливіших до кібератак, і приклади інцидентів у цій сфері демонструють, наскільки важливо інтегрувати ШІ в системи безпеки. Станом на 2021-2023 роки країна-агресор проводить дуже багато кібератак, що місяця кількість атак варіюється, проте можна чітко зазначити, що імплементування ШІ могло би зменшити їхню кількість та збільшити ефективність роботи системи захисту.

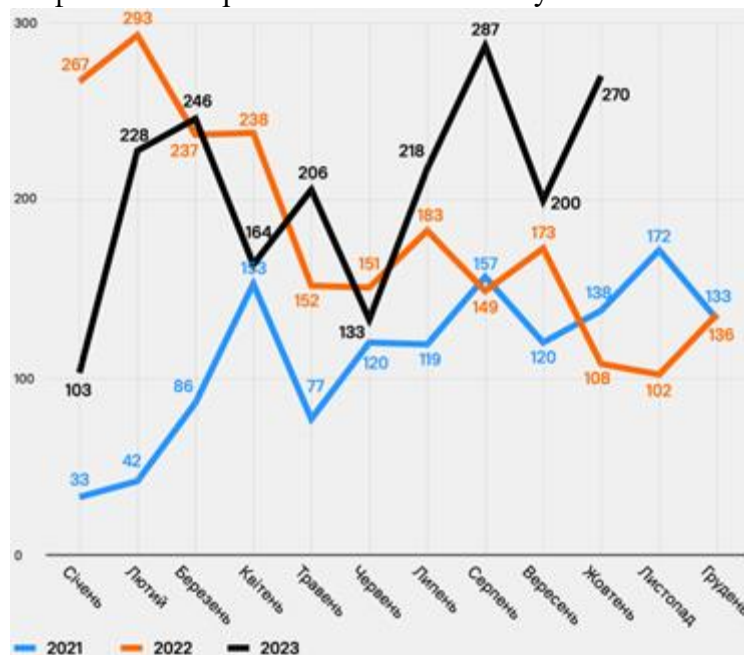


Рис. 2 Зображення графіку кібератак країни агресора у 2021-2023 роках [3]

Фінансові інституції також активно впроваджують ШІ для забезпечення кібербезпеки своїх систем. Наприклад, американська компанія JP Morgan використовує платформи на основі ШІ для виявлення шахрайських операцій та захисту від кібератак. Алгоритми аналізують мільйони транзакцій у реальному часі, виявляючи підозрілі патерни, які можуть свідчити про потенційну загрозу. Завдяки ШІ вдалося значно скоротити кількість шахрайств та знизити ризики для клієнтів.[4]

Однак разом із значними перевагами існують і виклики, пов'язані з використанням ШІ для кіберзахисту. Один з головних — це вразливість самих систем ШІ до атак. Зловмисники можуть використовувати методи "обману ШІ" (adversarial attacks), вводячи навмисні зміни у дані для дезорієнтації систем і змушуючи їх приймати неправильні рішення. Це створює новий рівень ризику для критичної інфраструктури, який вимагає постійного вдосконалення систем кіберзахисту. Даний метод використовується, коли система захисту, а саме база даних ШІ, нова та її потрібно протестувати. Після тестів систему оновлюють, що в свою чергу, призводить до покращення захисту та пришвидшення працездатності.

Ще одним викликом є питання етики та конфіденційності. Оскільки системи ШІ збирають і аналізують великі обсяги даних, існує ризик використання цих даних не за призначенням або порушення конфіденційності користувачів.

Таким чином, інтеграція ШІ у кіберзахист критичної інфраструктури є важливим і необхідним кроком для забезпечення надійності та стійкості цих систем. Проте ефективне використання ШІ потребує постійного розвитку технологій, впровадження нових рішень для

протидії атакам на самі системи ІІІ, а також забезпечення етичних стандартів та конфіденційності.

Список використаних джерел

1. Darktrace - [Електронний ресурс] – Режим доступу: <https://darktrace.com/platform>
2. IBM QRadar Suite - [Електронний ресурс] – Режим доступу: <https://www.ibm.com/qradar>
3. Російські хакери координують дії з військовими та посилюють атаки напередодні зими. Як Україна протистоїть кібератакам на енергосистему - [Електронний ресурс] – Режим доступу: <https://forbes.ua/company/rosiyski-khakeri-koordinuyut-dii-z-viyskovimi-ta-posilyuyut-ataki-naperedodni-zimi-yak-ukraina-protistoit-kiberatakam-na-energositemu-08112023-17242>
4. JP Morgan - [Електронний ресурс] – Режим доступу: <https://www.jpmorgan.com/global>

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 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.

