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

Каріна ВАШКЕБА
студентка 2 курсу
спеціальності Міжнародні відносини, суспільні комунікації та регіональні студії
кафедри історії та суспільних дисциплін
Закарпатського угорського інституту імені Ференца Ракоці II
***Науковий керівник* – Маріанна МАРУСИНЕЦЬ**
кандидат філологічних наук, доцент,
доцент кафедри історії та суспільних дисциплін,
старший дослідник Науково-дослідного центру імені Тіводора Легоцькі
Закарпатського угорського інституту імені Ференца Ракоці II

КІБЕРБЕЗПЕКА: ДОСВІД ФРАНЦІЇ

Анотація. *Дослідження присвячене аналізу кібербезпеки у Франції, зокрема її національних стратегій та правових механізмів у контексті сучасних глобальних викликів. Окрему увагу приділено вивченню нормативних актів, таких як Закон LOPMI та Національна кіберстратегія, а також діяльності основних державних інституцій, таких як ANSSI та CNIL, що займаються захистом інформаційних систем і персональних даних. Робота досліджує досвід Франції у впровадженні кіберзахисту на рівні держави та приватного сектору, а також роль міжнародної співпраці у сфері кібербезпеки. Висвітлено ключові загрози, серед яких дезінформація, кіберзлочинність та шпіонаж, і проаналізовано ефективність заходів, спрямованих на їх нейтралізацію. Дослідження акцентує на важливості розвитку кіберграмотності серед населення та інтеграції кібербезпеки у всі сфери суспільного життя.*

Ключові слова: *кібербезпека, Франція, кіберзагрози, дезінформація, кіберзлочинність, ANSSI, CNIL, Національна кіберстратегія, інформаційні системи.*

В умовах стрімкої глобалізації та широкого розповсюдження інформаційних технологій, питання кібербезпеки стає надзвичайно важливим для кожної країни, незалежно від її економічного розвитку або геополітичної позиції. Кіберзагрози, що виникають у цифровому середовищі, зачіпають як державні структури, так і приватний сектор, створюючи ризики для національної безпеки, економічної стабільності та суспільного спокою. Сучасний світ все частіше стає свідком складних і витончених кібероперацій, які можуть порушувати функціонування критичної інфраструктури, викликати хаос у фінансових системах, ставити під загрозу персональні дані громадян та підривати довіру до державних інституцій.

Особливу загрозу становлять деструктивні інформаційні кампанії, спрямовані на дестабілізацію політичної та соціальної ситуації всередині країн. Такі операції впливу можуть викликати масову дезінформацію, спотворювати суспільну думку та розколювати єдиний інформаційний простір держави. Країни, які прагнуть послабити своїх конкурентів або отримати стратегічні переваги, часто використовують кіберзагрози як інструмент для досягнення своїх геополітичних цілей. У цьому контексті кібербезпека стає одним з основних напрямків забезпечення національної стійкості, адже вона включає не лише технічний захист від атак, а й формування стратегії інформаційної стійкості, здатної запобігти дезінформаційним кампаніям та зміцнити довіру громадян до національних інститутів.

Постановка проблеми. Франція, як одна з провідних європейських держав, несе особливу відповідальність за забезпечення безпеки як на національному, так і на міжнародному рівні, особливо після виходу Великої Британії з Європейського Союзу. З огляду на те, що Франція є єдиною державою ЄС з ядерною зброєю та постійним членством у Раді Безпеки ООН, її роль у захисті як європейської, так і глобальної безпеки значно зростає. У цьому контексті важливо розглянути, як кіберзагрози, що дедалі частіше стають інструментом геополітичного впливу та дестабілізації, впливають на національну безпеку Франції.

Кібербезпека стає невід'ємною частиною зовнішньої та внутрішньої безпекової політики Франції. З одного боку, відкриті кордони в межах Шенгенської зони та активні міграційні

процеси з Африки та Азії підвищують уразливість держави перед можливими кібератаками. З іншого боку, активна зовнішня політика Франції в Європі, Середземномор'ї, Африці та на Близькому Сході також створює додаткові виклики для захисту її інформаційного простору. В умовах сучасного цифрового світу кібероперації можуть використовуватися як для безпосереднього впливу на політичні та соціальні процеси в державі, так і для підриву її стратегічної позиції на міжнародній арені.

Проблема дослідження полягає в тому, щоб проаналізувати, які ключові виклики кібербезпеки стоять перед Францією сьогодні, та якими ресурсами й засобами вона володіє для їх подолання. Також важливо дослідити, яким чином кіберзагрози інтегруються в систему загроз національної безпеки Франції, а також як ця держава будує свою стратегію кіберстійкості, співпрацюючи з міжнародними партнерами для протидії кіберзлочинності та дезінформаційним кампаніям.

Аналіз останніх досліджень і публікацій з теми кібербезпеки Франції вказує на високу актуальність проблеми як в контексті національної безпеки, так і в рамках європейської політики у сфері безпеки та оборони. Серед наукових праць, присвячених цій тематиці, можна виділити роботи європейських та українських дослідників, які висвітлюють різні аспекти кіберзахисту та безпеки. У своїх дослідженнях науковці підкреслюють важливість кібербезпеки як стратегічного напрямку зовнішньої політики Франції, зокрема в умовах зростання міжнародних конфліктів та загроз з боку кіберзлочинності.

Роботи авторів, як Ж. Брісет та М. Арзаканян, зосереджуються на аналізі політики Франції в рамках загальноєвропейської стратегії кібербезпеки, яка є важливим компонентом загальної безпекової архітектури ЄС. Вони досліджують інтеграцію кіберзахисту у національну безпекову політику Франції, зокрема її роль як одного з ключових гравців у Європі після виходу Великої Британії з ЄС. Водночас автори, такі як О. Барабанов та В. Барановський, акцентують увагу на інституційних аспектах формування європейської кібербезпеки, аналізуючи участь Франції у міжнародних структурах, таких як НАТО та Європейське оборонне агентство.

Інші дослідники, зокрема І. Бусигіна та М. Стрежньова, фокусуються на викликах, пов’язаних із захистом національних інформаційних систем від іноземних кіберзагроз та дезінформаційних кампаній, які є особливо актуальними в умовах сучасної гібридної війни. Їхні праці аналізують роль Франції у глобальних процесах боротьби з кіберзагрозами, розглядаючи кібербезпеку як один із ключових елементів забезпечення національної стійкості.

Проте більшість наукових робіт зосереджені на зовнішніх аспектах кібербезпеки, залишаючи недостатньо дослідженими питання внутрішньої кіберстійкості Франції, зокрема розвиток її інституційної спроможності протистояти кіберзлочинності та захищати критичну інфраструктуру. Важливим залишається подальше дослідження питань, пов’язаних з координацією зусиль між різними відомствами та агенціями, а також співпрацею з приватним сектором у боротьбі з кіберзлочинністю.

Отже, аналіз наукових праць показує, що хоча кібербезпека є предметом численних досліджень, питання забезпечення національної кіберстійкості Франції вимагає подальшого розгляду, зокрема у контексті її внутрішньої політики та практичної реалізації заходів кіберзахисту.

Метою статті є аналіз сучасних викликів кібербезпеки Франції та оцінка її національної стратегії кіберзахисту в умовах глобалізації та зростання кіберзагроз. Дослідження спрямоване на вивчення заходів, які Франція вживає для забезпечення національної кіберстійкості, захисту критичної інфраструктури, протидії кіберзлочинності та дезінформаційним кампаніям, а також на оцінку її ролі в рамках європейської та глобальної систем безпеки.

2. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ. Основні положення військової доктрини Франції викладені в «Білій книзі», перше видання якої вийшло у 1972 році, ґрунтуючись на ідеях Шарля де Голля про незалежність і велич республіки. Доктрина передбачала захист національних територій, участь у безпеці Європи та захист віддалених регіонів, де Франція

має стратегічні інтереси. Попри зміни у зовнішній політиці, подальші видання «Білої книги» продовжували дотримуватися принципів «голлізму», адаптуючи доктрину до нових глобальних викликів, включаючи розвиток кіберзагроз. У «Білій книзі» 2013 року відзначено переорієнтацію країни на співпрацю з НАТО, ініційовану ще Ніколя Саркозі та продовжену Еммануелем Макроном [3]. Документ «Стратегічний огляд» 2017 року підтвердив зміцнення трансатлантичних зв'язків і розвиток незалежної європейської оборони, що стало основою для створення «Програми розвитку збройних сил на 2019-2025 роки», яка передбачає модернізацію армії та підвищення її спроможностей [10].

Усі зазначені вище документи формують цілісну систему військово-політичних, військово-стратегічних та військово-економічних засад, які складають основу сучасної військової доктрини Франції. Вони відображають поточні пріоритети країни у сфері оборони та безпеки, адаптуючи стратегії до нових викликів, з якими стикається світ. Важливим аспектом цих доктринальних документів є акцент на різноманітних загрозах сучасного світу, зокрема таких, як кібератаки, які стають усе частішим інструментом міжнародних конфліктів і підривають національні інфраструктури.

Сучасна військова доктрина Франції враховує не лише традиційні загрози, але й новітні виклики, що виникають у зв'язку з розвитком інформаційних технологій. Окремо варто зазначити, що в умовах цифровізації та глобальної комунікації особливої актуальності набуває проблема дезінформації, яка стала потужним інструментом впливу на суспільство та міжнародні відносини. Французькі законодавці вже давно визнали дезінформацію серйозною загрозою для національної безпеки, оскільки вона здатна підірвати довіру до державних інститутів, вплинути на політичні процеси та дестабілізувати громадський порядок. Це, в свою чергу, підкреслює важливість кібербезпеки як невід'ємної складової захисту держави в умовах сучасних глобальних загроз.

Регулювання дезінформації у Франції здійснюється, зокрема, на основі Закону про свободу преси, який був ухвалений ще в 1881 році. У статті 27 цього закону детально визначено, що розуміється під терміном «фальшиві новини» та встановлено відповідальність за їх поширення. Так, публікація, відтворення або поширення будь-якими засобами недостовірної інформації, сфабрикованих матеріалів або тих, що були поширені з недобросовісною метою і можуть порушити громадський порядок або сприяти його порушенню, карається штрафом у розмірі 45 000 євро. Якщо ж такі дії ставлять під загрозу дисципліну або мораль у збройних силах чи можуть зашкодити військовим зусиллям країни, штраф може сягати 135 000 євро. Однак, як зазначають експерти, через складність доведення факту того, що певна інформація дійсно порушує громадський порядок або має дестабілізуючий вплив, ці положення закону на практиці застосовуються досить рідко [5].

Ще одним важливим законодавчим актом, спрямованим на регулювання інформаційного простору, є Закон про довіру в цифровій економіці (LCEN, Loi pour la confiance dans l'économie numérique), який було ухвалено 21 червня 2004 року. Цей закон встановлює правову основу для боротьби з контентом в Інтернеті, який сприяє розпалюванню ненависті, дискримінації або порушенню громадського порядку. Закон передбачає механізми, за допомогою яких суд може вимагати видалення з мережі будь-якого контенту, що порушує законодавство в цій сфері. Ці заходи дозволяють оперативно реагувати на випадки поширення незаконного контенту, забезпечуючи баланс між свободою слова та необхідністю дотримання правових норм у цифровому середовищі [7]. Таким чином, закон LCEN слугує важливим інструментом для підтримання безпеки та захисту прав громадян в умовах швидкого розвитку цифрових технологій.

У 2015 році Франція ухвалила Національну кіберстратегію (Stratégie nationale pour la sécurité du numérique), яка звертає увагу на те, що всі цифрові платформи, включаючи соціальні мережі, можуть формувати думку таким чином, який може не відповідати реальним цінностям країни. Часто такі платформи використовуються для поширення дезінформації та пропаганди, що призводить до негативного впливу на суспільну думку. У випадках, коли ці платформи сприяють поширенню цінностей, які суперечать основоположним інтересам

Франції, такі дії підпадають під регулювання законодавства, яке стосується національної безпеки та оборони [11]. Таким чином, кіберстратегія Франції наголошує на необхідності контролю та регулювання цифрового простору з метою захисту країни від інформаційних загроз, що можуть підривати її національні інтереси та безпеку.

Французька стратегія кібербезпеки спрямована на досягнення п'яти основних цілей, які мають на меті створення «цифрової республіки», забезпечуючи при цьому як безпеку, так і стійкість інформаційно-комунікаційних технологій (ІКТ). До цих стратегічних пріоритетів належать:

1) Захист ключових національних інтересів у кіберпросторі, що включає охорону державних інформаційних систем та критично важливих елементів інфраструктури.

2) Забезпечення довіри між учасниками цифрового простору, а також захист конфіденційності та персональних даних користувачів. Це досягається через розробку спеціалізованих кіберзахисних продуктів і надання технічної та юридичної підтримки.

3) Підвищення рівня обізнаності про кібербезпеку та розвиток відповідних можливостей на національному рівні. Це включає в себе освітні ініціативи та підготовку фахівців у цій сфері.

4) Створення сприятливих умов для розвитку підприємництва, залучення інвестицій в ІКТ-сектор та підтримку інноваційного бізнесу, що стимулює економічне зростання в цифровій сфері.

5) Розробка стратегії або «дорожньої карти» для досягнення європейської цифрової автономії, що сприяє зниженню залежності від зовнішніх технологій і зміцненню власного потенціалу у сфері кібербезпеки [11].

Ці пріоритети відображають амбіції Франції у створенні безпечної та інноваційної цифрової інфраструктури, здатної захищати національні інтереси в умовах зростання глобальних кіберзагроз.

У листопаді 2016 року Національна Асамблея Франції ухвалила закон, який має на меті зміцнення незалежності, свободи та плюралізму засобів масової інформації (Loi visant à renforcer la liberté, l'indépendance et le pluralisme des médias). Цей закон зобов'язує медіаорганізації впровадити кодекс етики, який регулює їхню діяльність, а також створити спеціальний комітет з етичних питань. Завданням цього комітету є допомога у вирішенні внутрішніх конфліктів, що можуть виникати всередині редакцій, а також у суперечках між власниками медіа та журналістськими колективами. Такий підхід спрямований на забезпечення більшої прозорості та підвищення довіри до засобів масової інформації, що є важливим аспектом підтримки свободи слова та забезпечення плюралізму думок у суспільстві [8].

У травні 2020 року парламент Франції ухвалив новий закон, який зобов'язує онлайн-платформи видаляти контент, що пропагує педофілію або тероризм, протягом однієї години з моменту його виявлення. Якщо платформи не виконають цю вимогу, їм загрожують штрафні санкції у розмірі до 4% від загального обсягу їхнього доходу. Закон також регулює видалення інших видів «шкідливого» контенту, встановлюючи термін у 24 години для їхнього усунення. Крім цього, впроваджується нова посада – цифровий прокурор, а також створюється спеціальний урядовий орган, який буде відповідати за нагляд і забезпечення дотримання закону, гарантуючи своєчасне видалення незаконного контенту з платформ [2].

У жовтні 2020 року депутати від партії «Вперед, республіка!» внесли на розгляд законопроєкт «Про глобальну безпеку», який охоплював широкий спектр питань, що стосуються діяльності правоохоронних органів. Однак найбільший резонанс у суспільстві викликала стаття 24 цього законопроєкту. Вона передбачала покарання за публікацію фотографій, відеозаписів або будь-яких інших матеріалів, які дозволяють ідентифікувати співробітників поліції або жандармерії. Якщо такі матеріали були поширені з метою завдання фізичної або психологічної шкоди правоохоронцям, правопорушник міг отримати покарання у вигляді одного року ув’язнення або штрафу [4]. Однак через масові акції протесту, під час яких громадськість висловила занепокоєння щодо можливого порушення свободи слова, французький парламент вирішив відкликати цю статтю. Протестувальники вважали, що це

положення могло суттєво обмежити їхнє право на вільне висловлювання та контроль за діями правоохоронців.

Закон LOPMI, ухвалений у січні 2023 року, позиціонував Францію серед лідерів країн, які займають жорсткішу позицію щодо вебсайтів, що використовуються для здійснення злочинної діяльності [9]. Хоча цей закон є новаторським кроком у боротьбі з кіберзлочинністю, його практичне застосування залишається на ранніх стадіях. Через новизну закону прокурорам поки що не вдалося отримати жодних вироків за його використання, але очікується, що найближчим часом він стане ефективним інструментом у протидії незаконній діяльності в мережі.

Також слід наголосити, що у Франції створено низку державних і неурядових інституцій, які займаються питаннями запобігання кіберзлочинності. Однією з найвідоміших серед них є Національна комісія з обчислювальної техніки та свобод (CNIL). Основна мета діяльності CNIL полягає в захисті персональних даних громадян. У сучасному цифровому світі CNIL виконує функцію регулятора у сфері захисту персональних даних, надає підтримку фахівцям у галузі кібербезпеки, а також допомагає громадянам контролювати свої особисті дані та реалізовувати свої права. Починаючи з 2004 року, CNIL отримала право накладати санкції на компанії, які порушують Закон про інформатику, картотеки та свободи, ухвалений у 1978 році [6].

Окрему роль у боротьбі з кіберзлочинністю у Франції відіграє Верховний орган з питань поширення творів та захисту прав в Інтернеті (HADOPI). Ця структура займається регулюванням діяльності, пов’язаної з нелегальним завантаженням інформації, зокрема визначає поняття незаконного скачування та розробляє нормативні акти для протидії такій діяльності. Одним із ключових кроків стало ухвалення Закону про триступеневу заборону доступу до Інтернету, який пройшов схвалення у Вищому конституційному суді Франції у другій редакції. Закон передбачає поступове обмеження доступу до мережі для тих користувачів, які неодноразово порушують авторські права шляхом нелегального завантаження захищеного контенту [6].

У системі правоохоронних органів Франції також діють спеціалізовані підрозділи, спрямовані на боротьбу зі злочинами в сфері інформаційних технологій. Починаючи з 1998 року, Національна жандармерія визначила вирішення проблем, пов'язаних з інноваційними технологіями, як один зі своїх пріоритетів. З цією метою були створені спеціалізовані структури та навчальні заклади. Серед них можна виділити:

1. Відділ кіберзлочинів технічного обслуговування судових досліджень та документації (STRJD), який займається моніторингом Інтернет-мереж з метою виявлення злочинів, пов'язаних із нелегальним обігом даних. Цей підрозділ здійснює перевірку сайтів, Інтернет-ресурсів, груп новин, мереж обміну файлами та соціальних мереж на наявність порушень, таких як злочини проти людей і майна.

2. Комп'ютерний і електронний відділ Інституту кримінального розслідування Національної жандармерії (IRCGN), який розробляє новітні методи та програмне забезпечення для автоматизованого виявлення педофілів та інших кіберзлочинців.

3. Відомчі бригади інформації та судових розслідувань (BDRIJ), що також займаються питаннями боротьби з кіберзлочинністю на рівні департаментів, зокрема розслідуванням порушень у сфері інформаційних технологій.

Ці підрозділи відіграють ключову роль у забезпеченні кібербезпеки та протидії злочинам, що здійснюються через Інтернет.

Одним із ключових суб'єктів боротьби з кіберзлочинністю у Франції є Національне агентство безпеки інформаційних систем (ANSSI), яке відповідає за кібербезпеку країни та тісно співпрацює з державними спецслужбами. Діяльність ANSSI спрямована на впровадження Французької національної стратегії цифрової безпеки, яка була оголошена 16 жовтня 2015 року. Ця стратегія є результатом скоординованих зусиль різних урядових структур і націлена на вирішення проблем, що виникають у цифрову епоху. Водночас наголошено, що цифрова трансформація сприяє не лише інноваціям та економічному

розвитку, але й приносить нові загрози для держави, бізнесу та громадян. Серед цих загроз: кіберзлочинність, шпигунство, пропаганда, саботаж та зловживання персональними даними, що підриває довіру та безпеку в цифровій сфері

ANSSI визначила кілька ключових напрямків у своїй діяльності: забезпечення захисту державних інформаційних систем та критично важливої інфраструктури, підтримка безпеки для важливих економічних і соціальних операторів, а також забезпечення цифрової довіри, конфіденційності та захисту персональних даних. Окрім цього, агентство приділяє велику увагу підвищенню обізнаності суспільства, навчанню та розвитку кібернавичок, як на початкових етапах, так і в рамках безперервної освіти. Також серед пріоритетів ANSSI – підтримка бізнес-середовища у сфері цифрових технологій, розробка промислової політики, стимулювання експорту та глобалізації [1, с. 158]. Важливим елементом залишається забезпечення цифрової стратегічної автономії Франції та підвищення стійкості її кіберпростору.

На основі аналізу досвіду Франції у сфері кібербезпеки можна зробити кілька важливих висновків. По-перше, кібербезпека у Франції є невід'ємною складовою національної безпеки, що підтверджується значною кількістю стратегій, законів та нормативних актів, спрямованих на захист критичної інфраструктури, державних і приватних інформаційних систем. Франція активно розвиває як національні, так і міжнародні механізми захисту від кіберзагроз, співпрацюючи з іншими державами в рамках НАТО та Європейського Союзу. Важливою частиною стратегії є захист персональних даних, розвиток інформаційної грамотності та регулювання цифрового простору для запобігання дезінформації та пропаганди.

Серед перспектив подальших досліджень можна виділити кілька напрямків. Перш за все, необхідно глибше дослідити ефективність впроваджених законів та стратегій, зокрема таких, як LOPMI 2023 року, щодо боротьби з кіберзлочинністю. Важливим є також вивчення питання взаємодії державних інституцій із приватним сектором у сфері кібербезпеки, оскільки ці відносини можуть сприяти створенню більш ефективної та стійкої цифрової інфраструктури. Крім того, особливу увагу слід приділити питанням міжнародної співпраці та обміну досвідом у протидії глобальним кіберзагрозам, що стають дедалі складнішими.

Список використаних джерел:

1. Таволжанський О. В. Особливості забезпечення кібербезпеки у сучасному світі: огляд суб’єктів запобігання кіберзлочинності. *Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького*. *Серія : Право*. 2018. № 6. С. 154-163.
2. France to force web giants to delete some content within the hour. *REUTERS*. 2020. URL: https://www.reuters.com/article/us-france-tech-regulation/france-to-force-web-giants-to-delete-some-content-within-the-hour-idUSKBN22P2JU. (дата звернення: 20.09.2024).
3. Livre blanc sur la défense et la sécurité nationale. 2013. URL: http://www.livreblanc defenseetsecurite.gouv.fr/index.html (дата звернення: 20.09.2024).
4. Loi «Sécurité globale» : la majorité va proposer «une nouvelle écriture complète de l'article 24». 2020. URL: https://www.lefigaro.fr/politique/loi-securite-globalela-majorite-va-proposer-une-nouvelle-ecriture-complete-de-l-article-24-20201130. (дата звернення: 20.09.2024).
5. Loi du 29 juillet 1881 sur la liberté de la presse. URL: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006070722. (дата звернення: 20.09.2024).
6. Loi favorisant la diffusion et la protection de la création sur Internet URL : http://www.senat.fr/dossier-legislatif/pjl07-405.html (дата звернення: 20.09.2024).
7. Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique . URL: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte= JORFTEXT000000801164 (дата звернення: 20.09.2024).

8. LOI n° 2016-1524 du 14 novembre 2016 visant à renforcer la liberté, l'indépendance et le pluralisme des médias. URL: https://www.legifrance.gouv.fr/eli/loi/2016/11/14/MCCX1603797L/jo (дата звернення: 20.09.2024).
9. LOI n° 2023-22 du 24 janvier 2023 d'orientation et de programmation du ministère de l'intérieur https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047046768 (дата звернення: 20.09.2024).
10. Revue stratégique 2017 . URL: https://www.defense.gouv.fr/dgris/politique-de-defense/revue-strategique/revue-strategique. (дата звернення: 20.09.2024).
11. Stratégie nationale pour la sécurité du numérique. URL: https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_fr.pdf. (дата звернення: 20.09.2024).

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