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

DARCSI Karolina
adjunktus,
Történelem- és Társadalomtudományi Tanszék,
Lehoczky Tivadar Társadalomtudományi Kutatóközpont kutatója,
II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola
HUBER Alex
II. évfolyamos
nemzetközi kapcsolatok, társadalmi kommunikáció
és regionális tanulmányok szakos hallgató,
II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola

KIBERBIZTONSÁG NÉMETORSZÁGBAN

Németország nemcsak gazdasági mutatói és lakosságszáma alapján Európa vezető állama, hanem a digitális és kiberbiztonság terén is kiemelkedő eredményeket tud felmutatni. Az ország a digitális piacot érintően igen kiterjedt és fejlett szabályozással rendelkezik, és sikeresen integrálódott a nemzetközi folyamatokba is.

A tanulmány Németország digitális és kiberbiztonsági helyzetét vázolja fel, ismertetve a főbb vonatkozó dokumentumokat és a szervezeti hátteret. Bár impozánsak az elért eredmények, a következő években további fejlesztésekre van szükség valamennyi területen ahhoz, hogy Németország a lehető legteljesebb mértékben képes legyen állami intézményeit és állampolgárait a kibertámadásoktól megvédeni.

Kulcsszavak: kiberbiztonság, Németország, digitális biztonság [1].

Németországban igen korán, már 1980 években bevezették az internetet. Ekkoriban még a Deutsche Telekom volt az egyetlen szolgáltató, amely a BXT (Bildschirmtext) hálózatot használta.

A Deutsche Telekom egészen 1995-ig őrizte monopol helyzetét Németországban, csak ezt követően nyitották meg a piacot a magánvállalkozások előtt. S bár a privatizáció lezajlott, a német állam és a szövetségi kormányok még mindig magukénak tudhatják a Deutsche Telekom részvényeinek egyharmadát, és jelenleg is ez az „állami vállalat” az ország legnagyobb internetszolgáltatója [2].

A Digitális Agenda 2014–2017 elnevezésű stratégiai dokumentumot a német szövetségi kormány 2014 augusztusában adta ki. A digitális teret illetően ez a dokumentum szerepel a stratégiai hierarchia csúcsán, mivel ezt maga a szövetségi kormány jegyzi meg. Az agenda a német lakosságot a középpontba helyezve három alapvető stratégiai célt rögzített: az elterjedését és a foglalkoztatottság szintjének növelését, a digitális lehetőségekhez való hozzáférése és a részvétel biztosítására, valamint a bizalom és a biztonság megteremtése. Az e célok megvalósításához szükséges alapot az alkotmányban rögzített értékek biztosítják, amelyek érvényesülését nemcsak a valós, hanem a virtuális világban is biztosítani kell [3].

A digitális infrastruktúra vonatkozásában az egyik fontos lépése a 2016. január 27-i gyors internethálózatok kiépítését megkönnyítő szabályozást tartalmazó törvény elfogadása volt.

A fiatalok ösztönzésképpen külön kormányzati segítséget kapnak a digitális gazdasági vállalkozások és munkahelyek megteremtéséhez, az IT-vállalatok és startupok működtetéséhez. Ezzel kapcsolatban összességében elmondható, hogy Németország már jelenleg is igen jó mutatókkal rendelkezik.

A német kiberbiztonsági szervezetrendszer

A német stratégiafejlődés mozgatórugója a szövetségi belügyminisztérium, amely szorosan együttműködik a Külügyminisztériummal, a Védelmi Minisztériummal, a Gazdasági és Energetikai Minisztériummal és az Igazságügyi Minisztériummal.

2011-ben a kormány felállította a Nemzeti Incidenskezelő Központot (Nationales Cyber-Abwehrzentrum – NCAZ), melynek feladata a kormányzati szervek közötti műveleti szintű kooperáció és IT-incidensek esetén a válaszlépések összehangolása.

A NCAZ az incidensekre való gyors reagálás érdekében nemzeti irányítási-vezetési és elemzőközponti funkciókat lát el. Emellett tájékoztatja a társadalmat a kibertámadásokról, sérülékenységekről és az elkövetőkről.

A Belügyminisztérium irányítása alá tartozó Szövetségi Információbiztonsági Hivatal (Bundesamt für Sicherheit in der Informationstechnik – BSI) felel az incidenskezelő központ feladatainak végrehajtásáért. Más hatóságok, mint a Szövetségi Alkotmányvédelmi Hivatal (Bundesamt für Verfassungsschutz – BfV), a Civil Védelem és Katasztrófavédelmi Szövetségi Hivatal (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe – BBK), a Szövetségi Bűnügyi Hivatal (Bundeskriminalamt – BKA), a Szövetségi Rendőrség (Bundespolizei – BPOL), a Bűnügyi Vámhivatal (Zollkriminalamt – ZKA), a Szövetségi Hírszerzési Hivatal (Bundesnachrichtendienst – BND), a német hadsereg (Bundeswehr) és a kritikusinfrastruktúra-üzemeltetőket felügyelő hivatalok is együttműködnek egymással az incidenskezelő központon belül a konkrét eseteknek megfelelően. A központ incidens esetén a Szövetségi Belügyminisztériumot közvetlenül tájékoztatja [4].

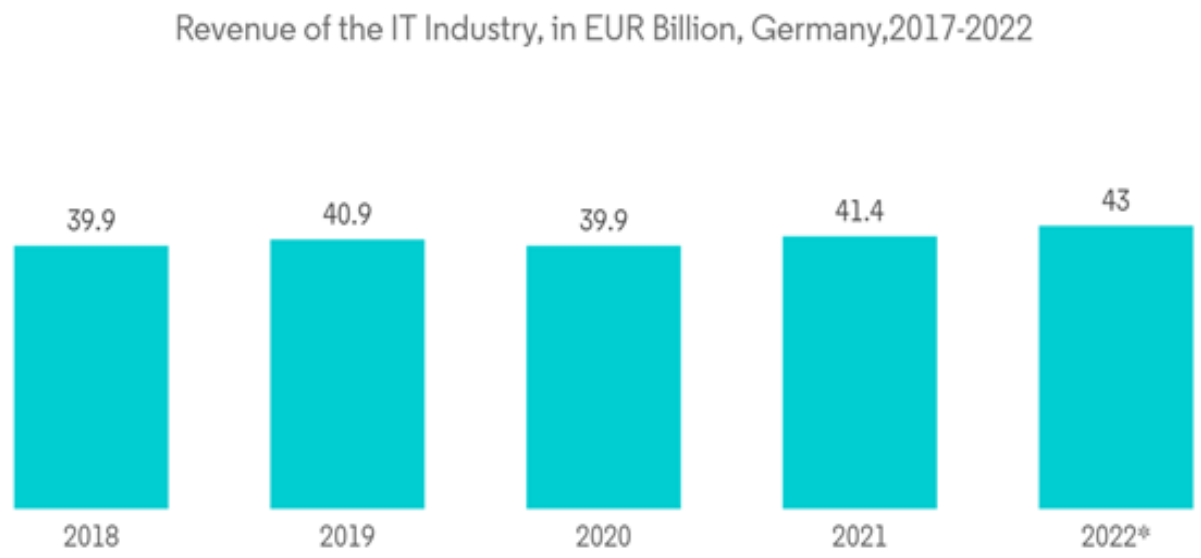
A Szövetségi Bűnügyi Hivatal (Bundeskriminalamt – BKA) szintén a Belügyminisztérium irányítása alá tartozik, és magasan szervezett, kiemelt jelentőségű bűnügyek kapcsán a kibertérben is tevékeny. Külön kiberbűnözési részleggel is rendelkezik, ahol az ilyen bűncselekményekkel kapcsolatos kompetenciák és információk összefutnak [5].

Németország kiberbiztonsági piaci részesedése

A német kiberbiztonsági piac méretét 2024-ben 12,60 milliárd USD-ra becsülik, 2029-re pedig várhatóan eléri a 21,47 milliárd USD-t, ami 11,25%-os CAGR-növekedést jelent a 2024–2029 közötti előrejelzési időszakban [8].

A kereskedelmi platformok megjelenésével járó kibertámadások száma növekedni kezdett. Az okoseszközök terjedése és a felhőmegoldások elterjedése csak néhány tényező a piac növekedésében. A kiberfenyegetések az intelligens és IoT-technológiával rendelkező eszközök használatának növekedésével várhatóan tovább fognak fejlődni. Ennek megfelelően a cégek haladó kiberbiztonsági megoldásokat fogadnak el és alkalmaznak a kibertámadások észlelésére, minimalizálására és kockázatának mérséklésére, ezáltal elősegítve a piac növekedését.

A német kiberbiztonsági piac félig konszolidált olyan jelentős szereplők jelenlétével, mint a Cisco Systems, az IBM, a Dell Technologies, a Fortinet és az Intel Security. A piac szereplői olyan stratégiákat alkalmaznak, mint például a partnerségek vagy a felvásárlások, hogy bővítsék termékkínálatukat, s fenntartható versenyelőnyre tegyenek szert.



Németország diverzifikált kiberbiztonsági ökoszisztémával rendelkezik, ahol a kiberbiztonsággal foglalkozó induló vállalkozások, kutatószervezetek és egyetemek széles spektruma található. Az ország kormányzati politikája különösen támogató, olyan erőfeszítéseket tesz, mint a Nemzeti Kiberbiztonsági Stratégia és a Kiberbiztonsági Törvény [6].

A kibertámadások számának növekedése a régióban várhatóan növeli a kiberbiztonsági megoldásokat. A német Szövetségi Információbiztonsági Hivatal (BSI) 2022-ben például azt állította, hogy a fogyasztók általános aggodalma a közelmúltban enyhén emelkedett az elmúlt három évhez képest. A válaszadók körülbelül 29%-a azt nyilatkozta, hogy volt már internetes bűncselekmény áldozata.

A korábbi években ez az arány 25% volt. A válaszadók negyede tapasztalt csalást és lopást az internetes vásárlás során.

A kiberbiztonsági piacon kulcsfontosságú az olyan kockázatok kezelése, mint a harmadik felek szállítóinak kockázatai, a felügyelt biztonsági szolgáltatók, mint a (MSSP-k) változásai, valamint a felhőalapú stratégia felé való elmozdulás. Mivel a vállalkozások egyre inkább külső beszállítókra számítanak különféle szolgáltatók és technológiák tekintetében, a kapcsolódó kockázatok is növekednek.

Az elmúlt néhány évben a biztonsági rendszerek megnehezítették a támadók számára a kritikus adatok elérését. Ennek eredményeként a hétköznapi felhasználók egyre inkább óvakodnak az internet biztonságától. Azok a megoldások, amelyek néhány évvel ezelőtt működtek, most irrelevánsak. A kibertámadások azonosításához és helyreállításához a szervezeteknek több erőforrásra van szüksége, és magasabb felkészültségre. Sok esetben előfordulhat, hogy a szervezetnek napokra teljesen le kell állítani a tevékenységét, hogy felépüljön egy incidens vagy támadás után. Rossz tervezés és nem megfelelő infrastruktúra esetén az incidens utáni felépülési idő jelentősen hosszú lehet.

A kiberbűnözők a kibertámadások lehetőségeit látták a COVID–19-világjárványban. Az otthonról dolgozó alkalmazottak sebezhetővé váltak.

A világjárvány után megnőtt a kiberbiztonság iránti igény, mivel a hónapokig tartó üzletmenet-folytonossági tervek (BCP) végrehajtását tervező vállalkozások – beleértve az információbiztonsági megfigyelést és a karanténkörülmények között történő reagálást – a kiberbiztonság fokozására összpontosítottak. Így a digitalizáció és a méretezhető IT-infrastruktúra iránti növekvő kereslet mellett a vizsgált piac gyorsan növekszik.

Az információs technológia (IT) és a távközlés létfontosságú a vállalkozások, a kormányzati szervek és a szervezetek számára. A robusztus kiberbiztonsági intézkedések iránti igény döntő jelentőségűvé vált az összekapcsolt hálózatok, a felhőalapú számítástechnika és a digitális kommunikáció növekvő függőség miatt. Az informatikai és telekommunikációs végfelhasználók a globális kiberbiztonsági piac jelentős részét alkotják, mivel meg akarják védeni érzékeny adataikat, hálózataikat és kommunikációjukat a fejlődő kiberfenyegetésekkel szemben [7].

Bár az EU-n belül sokat költenek a kiberbiztonságra, és jóval fejlettebb technológiával bírnak, mint az egykori posztszovjet térség országai, mégis, még maga Németország sincs kellően felkészülve egy esetleges nagyszabású kibertámadásra, mivel nem rendelkezik működő válságkezelő rendszerrel – figyelmeztetett a Szövetségi Információbiztonsági Hivatal (BSI) vezetője 2024 nyarán. A német kiberbiztonsági hatóság, a BSI (Bundesamt für Sicherheit in der Informationstechnik) vezetőjének nyilatkozata szerint a német kibervédelem szervezetrendszere nem alkalmas egy összehangolt kibertámadás kezelésére, ezért folyamatosan szükséges azt fejleszteni és bővíteni.

Felhasznált források:

1. https://folyoirat.ludovika.hu/index.php/neb/article/view/3615/2898
2. https://folyoirat.ludovika.hu/index.php/neb/article/view/3615/2898
3. https://folyoirat.ludovika.hu/index.php/neb/article/view/3615/2898
4. https://folyoirat.ludovika.hu/index.php/neb/article/view/3615/2898
5. https://hhk.uni-nke.hu/document/hhk-uni-nke-hu/2_2021_MIC_RP.pdf
6. https://www.globenewswire.com/news-release/2024/09/16/2946526/0/en/Germany-Cybersecurity-Market-Share-Analysis-Industry-Trends-Growth-Forecasts-2024-2029.html
7. https://www.globenewswire.com/news-release/2024/09/16/2946526/0/en/Germany-Cybersecurity-Market-Share-Analysis-Industry-Trends-Growth-Forecasts-2024-2029.html
8. Dublin, 2024. szeptember 16. (GLOBE NEWSWIRE) – Németország kiberbiztonsága – Piaci részesedés elemzése, iparági trendek és statisztikák, növekedési előrejelzések (2024–2029).

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