THE ROLE OF SECURITY IN CROSS-BORDER AND INTERNATIONAL COOPERATION

Book of Conference Abstracts

The international scientific and practical conference

Berehove, 8–9 October 2025

РОЛЬ БЕЗПЕКИ В ТРАНСКОРДОННОМУ ТА МІЖНАРОДНОМУ СПІВРОБІТНИЦТВІ

Міжнародна науково-практична конференція
Берегове, 8–9 жовтня 2025 року

Збірник тез доповідей

THE ROLE OF SECURITY IN CROSS-BORDER AND INTERNATIONAL COOPERATION

International scientific and practical conference
Berehove, 8–9 October 2025

Book of Conference Abstracts

A BIZTONSÁG SZEREPE A HATÁRON ÁTNYÚLÓ ÉS NEMZETKÖZI EGYÜTTMŰKÖDÉSBEN

Nemzetközi tudományos és szakmai konferencia
Beregszász, 2025. október 8–9.

Absztraktkötet

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

РОЛЬ БЕЗПЕКИ В ТРАНСКОРДОННОМУ ТА МІЖНАРОДНОМУ СПІВРОБІТНИЦТВІ

Міжнародна науково-практична конференція
Берегове, 8–9 жовтня 2025 року

Збірник тез доповідей

Університет Ракоці
Берегове
2025

УДК 004.056(063)(048.4)
Р 68

Збірник містить тези доповідей (українською, англійською та угорською мовами) міжнародної науково-практичної конференції «Роль безпеки в транскордонному та міжнародному співробітництві», яка відбулася 8–9 жовтня 2025 року в місті Берегове. Матеріали конференції висвітлюють широкий спектр проблем, пов'язаних із забезпеченням безпеки в умовах сучасних транскордонних та міжнародних викликів. Збірник тез доповідей охоплює питання політичних, соціальних, правових і технологічних аспектів безпеки, а також інтеграцію штучного інтелекту та цифрових технологій у систему захисту інформації. Організатори конференції: Закарпатський угорський університет імені Ференца Ракоці II та Ужгородський національний університет. Співорганізатори: Кафедра ЮНЕСКО «Неперервна професійна освіта XXI століття» НАПН України, Південноукраїнський національний педагогічний університет імені К. Д. Ушинського, Черкаський національний університет імені Богдана Хмельницького, Державний університет «Київський авіаційний інститут», Університет Григорія Сковороди в Переяславі, Міжнародний гуманітарний університет, Херсонський державний університет, Берегівський навчальний центр Матіасу Корвінусу Колегіуму, Пряшівський університет у Пряшеві, Жешувський університет, Ускюдарський університет, Північний університетський центр у Бая-Маре Технічного університету Клуж-Напока.

Рекомендовано до видання у друкованій та електронній формі (PDF)
рішенням Вченої ради Закарпатського угорського університету імені Ференца Ракоці II
(протокол №12 від «17» грудня 2025 року)

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

За редакцією:
Степан Черничко, Маріанна Марусинець, Єлизавета Молнар Д, Оксана Мулеса та Ганна Мелеганич

Технічне редагування: *Адам Доровці, Олександр Добош та Анастасія Сенько*
Підготовка до видання у друкованій та електронній формі (PDF): *Анастасія Сенько*
Коректура: *авторська*
Дизайн обкладинки: *Вівієн Товт*
УДК: *Бібліотека ім. Опацої Чере Яноша Університету Ракоці*

Відповідальний за випуск:
Олександр Добош (начальник Видавничого відділу Університету Ракоці)

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 університет імені Ференца Ракоці II (адреса: пл. Кошута 6, м. Берегове, 90202. Електронна пошта: egyetem@kme.org.ua; office@kme.org.ua)
Друк: ТОВ «РІК-У» (адреса: вул. Карпатської України 36, м. Ужгород, 88006. Електронна пошта: print@rik.com.ua)

ISBN 978-617-8143-50-3 (м'яка обкладинка)
ISBN 978-617-8143-51-0 (PDF)

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

THE ROLE OF SECURITY IN CROSS-BORDER AND INTERNATIONAL COOPERATION

International scientific and practical conference
Berehove, 8–9 October 2025

Book of Conference Abstracts

University of Rakoczi
Berehove
2025

UDC 004.056(063)(048.4)
R 79

The book contains abstracts of presentations (in Ukrainian, English, and Hungarian) at the international scientific and practical conference “The Role of Security in Cross-Border and International Cooperation”, which took place on 8-9 October 2025 in Berehove. The conference materials highlight a wide range of issues related to ensuring security in the context of modern cross-border and international challenges. The book of conference abstracts covers political, social, legal, and technological aspects of security, as well as the integration of artificial intelligence and digital technologies into information protection systems. Organisers of the conference: Ferenc Rakoczi II Transcarpathian Hungarian University and Uzhhorod National University. Co-organisers: UNESCO Department "Continuous Professional Education of the 21st Century" of the National Academy of Sciences of Ukraine, K. D. Ushynsky South Ukrainian National Pedagogical University, Bohdan Khmelnytsky National University of Cherkasy, State University "Kyiv Aviation Institute", Hryhorii Skovoroda University in Pereiaslav, International Humanitarian University, Kherson State University, Berehove Training Center of Mathias Corvinus Collegium, University of Prešov, University of Rzeszów, Üsküdar University, 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 University
(record No.12 of December 17, 2025)

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 University, 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 University of Rakoczi.

Edited by:
Stepan Chernychko, Marianna Marusynets, Yelyzaveta Molnar D., Oksana Mulesa and Hanna Melehanych

Technical editing: *Adam Dorovtsi, Sándor Dobos and Anasztázia Szenykó*
Prepared for publication in printed and electronic form (PDF file format): *Anasztázia Szenykó*
Proof-reading: *the authors*
Cover design: *Vivien Tóth*
Universal Decimal Classification (UDC): *Apáczai Csere János Library of University of Rakoczi*

Responsible for publishing:
Sándor Dobos (head of the Division of Publishing of Ferenc Rakoczi II Transcarpathian Hungarian University)

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 University (Address: Kossuth square 6, 90202 Berehove, Ukraine. E-mail: egyetem@kme.org.ua; office@kme.org.ua)
Printing: “RIK-U” LLC (Address: Carpathian Ukraine Street 36, 88006 Uzhhorod, Ukraine. E-mail: print@rik.com.ua)

ISBN 978-617-8143-50-3 (paperback)
ISBN 978-617-8143-51-0 (PDF)

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

A BIZTONSÁG SZEREPE A HATÁRON ÁTNYÚLÓ ÉS NEMZETKÖZI EGYÜTTMŰKÖDÉSBEN

Nemzetközi tudományos és szakmai konferencia
Beregszász, 2025. október 8–9.

Absztraktkötet

Rákóczi Egyetem
Beregszász
2025

ETO 004.056(063)(048.4)
B 68

A tudományos kiadvány 2025. október 8–9-én, Beregszászban *A biztonság szerepe a határon átnyúló és nemzetközi együttműködésben* címmel megrendezett nemzetközi tudományos és szakmai konferencián elhangzott előadások absztraktjait tartalmazza ukrán, angol és magyar nyelven. Az előadások szerkesztett anyagai a biztonság biztosításával kapcsolatos széleskörű kérdéseket tárgyalják a mai határon átnyúló és nemzetközi kihívások összefüggésében. Az absztraktkötet a biztonság politikai, társadalmi, jogi és technológiai aspektusait, valamint a mesterséges intelligencia és a digitális technológiák integrációját is vizsgálja az információvédelem rendszerébe. A konferencia szervezői: a II. Rákóczi Ferenc Kárpátaljai Magyar Egyetem és az Ungvári Nemzeti Egyetem. Társszervezők: az Ukrán Nemzeti Pedagógiai Akadémia UNESCO „XXI. századi folyamatos szakképzés" Tanszéke, K.D. Usinszkij Dél-ukrajnai Nemzeti Pedagógiai Egyetem, Cserkaszi Bohdan Hmelnickij Nemzeti Egyetem, Kijevi Állami Repülőmérnöki Egyetem, Perejaszlavi Hrihorij Szkovoroda Egyetem, Nemzetközi Humántudományi Egyetem, Herszoni Állami Egyetem, a Mathias Corvinus Collegium Beregszászi Képzési Központja, Eperjesi Egyetem, Rzeszówi Egyetem, Üsküdari Egyetem és a Kolozsvári Műszaki Egyetem Nagybányai Északi Egyetemi Központja.

Nyomtatott és elektronikus formában (PDF-fájlformátumban) történő kiadásra javasolta
a II. Rákóczi Ferenc Kárpátaljai Magyar Egyetem Tudományos Tanácsa
(2025. december 17., 12. számú jegyzőkönyv).

Kiadásra előkészítette a II. Rákóczi Ferenc Kárpátaljai Magyar Egyetem 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.

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

Műszaki szerkesztés: *Daróci Ádám, Dobos Sándor és Szenykó Anasztázia*
Előkészítés nyomtatott és elektronikus formában (PDF-fájlformátumban) történő kiadásra: *Szenykó Anasztázia*
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 Egyetem Kiadói Részlegének vezetője)

Az absztraktok 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 Egyetem (cím: 90 202, Beregszász, Kossuth tér 6. E-mail: egyetem@kme.org.ua; office@kme.org.ua)
Nyomdai munkálatok: „RIK-U" Kft. (cím: 88 006 Ungvár, Kárpáti Ukrajna u. 36. E-mail: print@rik.com.ua)

ISBN 978-617-8143-50-3 (puhatáblás)
ISBN 978-617-8143-51-0 (PDF)

ЗМІСТ / CONTENT / TARTALOM

Olha P. KOTOVSKA
PhD, associate professor
Lviv Polytechnic National University
Bandera Str., 12, Lviv, Ukraine 79013
0000-0002-8479-915X

Myron D. PACAI
CEO
Institute of Cybersecurity and Analytics
Shevchenka Str., 72, 3a, Lviv, 79039
0009-0002-2575-4549

Taras V. TCHAIKOVSKY
PhD, associate professor
Lviv Polytechnic National University
Bandera Str., 12, Lviv, Ukraine 79013
0000-0002-1166-8749

CYBER THREATS AND DIGITAL GOVERNANCE IN UKRAINE AND THE EU IN 2022–2024 IN THE CONTEXT OF ENSURING CYBER RESILIENCE

Abstract The work is devoted to identifying key trends in cyber threats, analyzing types of vulnerabilities, as well as determining responsible groups and sectors that suffer the greatest losses. Data from open sources, including international and Ukrainian agencies and organizations on information security, as well as indices and reports of leading organizations in the field of cybersecurity and digitalization, are processed. The negative impact of the full-scale invasion of the Russian Federation into Ukraine on the global level of cybercrime is shown and it is proposed to increase the level of cyber resilience through the development of digital services and overcoming digital gaps (disruptions).

Keywords: cybersecurity, cyber incidents, global risks, economic sectors, digital services **.**

Introduction

This year's 20th World Economic Forum report identifies state-sponsored armed conflict as the top global risk in 2025 (World Economic Forum, 2025), which, given the Ukrainian realities, is obvious. In the two-year perspective, geopolitical tensions will increase due to disinformation (first place) and cyber espionage and war (fifth place). For Ukraine, this negative trend is already part of hybrid warfare: cyberattacks paralyze the activities of critical infrastructure facilities, the banking system, the public sector, energy, healthcare, and digital services. At the same time, Ukraine continues to increase the level of digitalization and cyber defense in these extremely difficult conditions. Despite the long-term war, Ukraine demonstrates significant progress in digital development, the government has successfully transferred data and services to international cloud platforms, which guarantees their security, accessibility, and sustainability, and ensures uninterrupted access to the Internet. This strategic approach not only protects the country’s digital assets, but also helps maintain economic activity and public services, strengthening Ukraine’s position as a resilient and forward-looking leader in digital technologies (UN Department, 2024).

Cybersecurity is becoming one of the key areas that determine the resilience of modern society to global challenges. Starting from 2022, in the conditions of a full-scale Russian-Ukrainian war and destabilization of the situation in the Middle East; the USA, Ukraine, Great Britain and EU countries suffer the most from cyberattacks. The number of cyberattacks related to geopolitical events has especially increased with the beginning of the full-scale invasion of the Russian Federation into Ukraine. This is confirmed by reports from government incident response teams (Computer Emergency Response Team of Ukraine (CERT-UA), the European Union Agency for Network and Information Security (ENISA), the German Federal Office for Information Security (BSI), the British

National Technical Authority for Cyber Threats and Information Assurance (NCSC), the French Cybersecurity Agency (ANSSI) and others), as well as the US Cybersecurity and Infrastructure Protection Agency (CISA) and the Israeli National Cybersecurity Directorate (INCD), which record and analyze such threats.

The goal of this work is to identify key trends in cyber threats, analyze types of vulnerabilities and economic consequences of attacks, and develop proposals for implementing effective policies through digitalization and measures to counter cyber attacks.

Materials and Methods

In 2000-2024, hackers carried out 3369 attacks, of which 1821 (54%) - in 2022-2024 (EuRepoC, 2025). The statistics include attacks on politically motivated targets and critical infrastructure facilities, regardless of whether they are carried out by states (affiliated groups) or by individual actors for political purposes. Since November 2022, the European Cyber Incident Repository (EuRepoC), as an independent consortium, has been tracking cyberattacks that have a geopolitical context and the corresponding response of states, in order to develop policies and measures to counter cyber threats based on the assessment and comparison of the "life cycle" of cyber incidents (EuRepoC, 2025).

In particular, changes in the number of cyber incidents are tracked for the period from 2021 to 2024, including in the EU. Fig. 1. clearly shows the growth of cyber incidents that preceded a full-scale invasion. In fact, targeted massive attacks in cyberspace increased sharply in 2022. It is also worth noting that since February 2023, EuRepoC has expanded its data set, which explains the sharp spike in incidents from this period on the global cyber incident graph.

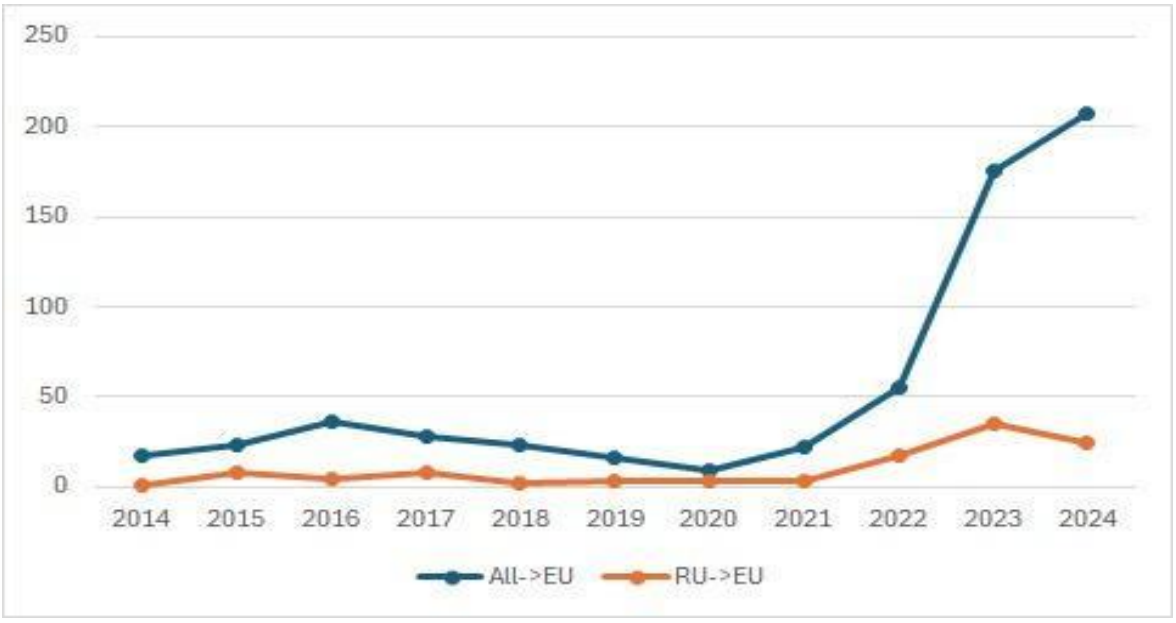

Fig. 1. Number of cyber incidents against the EU, 2014-2024, [compiled based on data from EuRepoC, 2025].

According to Fig. 2, most of the attacks that were carried out against Ukraine were of Russian origin. The total number of attacks against Ukraine is marked in red, blue - the Russian Federation against Ukraine, light blue - Ukraine against the Russian Federation. The situation with the Russian Federation as the attacking party shows that since 2021, cyberattacks have been targeted against Ukraine and reached their peak in 2022. The number of cyber incidents has increased - from 1 incident in 2020 to 27 incidents in 2022. This increase means a compound annual growth rate (CAGR) of 419.6% in two years. Ukraine during this period showed a slight surge in activity in 2014-2105, sharply increasing dynamics during 2021-2022 and a significant decrease in cyber incidents in the second half of 2023-2024 directed against the Russian Federation. For the selected period, the number of cyber incidents increased – from 1 incident in 2014 to 27 in 2022 and 16 incidents in 2024.

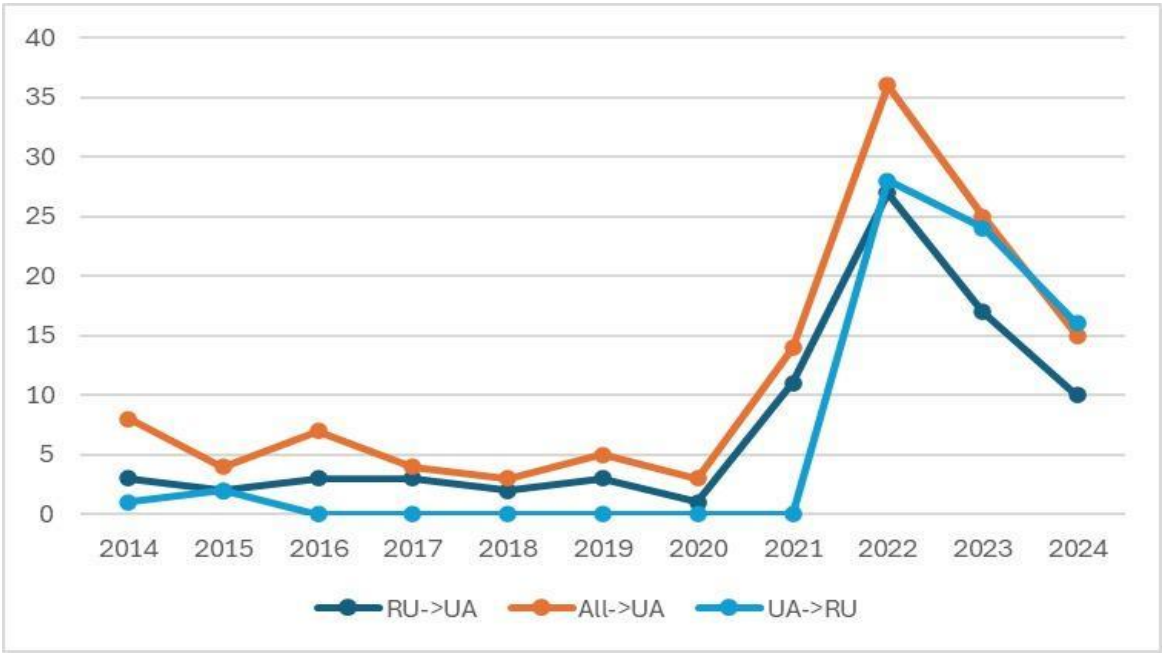

Fig. 2. Number of cyber incidents against Ukraine and the Russian Federation, 2014-2024, [compiled based on data from EuRepoC, 2025].

Based on aggregated data from national agencies, the main trends in cyberattacks by country are shown. The number of attacks reflects **recorded cyber incidents,** i.e. successful attacks on organizations, government agencies, companies or other objects or attempts.

In particular, on the eve of the Munich Security Conference (February 2025), a study on threats in the cyber and information space (CIR) was published, which also contained information on risks for the EU's foreign and security policy. Among the EU's critical infrastructure facilities in 2024, the healthcare sector, which contains confidential data, suffered the highest rate of attacks (ransomware and data theft) [Bund J., Bendiek A., Hemmelskamp J., p.3]. The largest share of cyberattacks on EU countries falls on the actively attacking Russian Federation and China, which also observe a change in the types of attacks. Within the EU, groups of Russian origin stand out for their participation in DDoS attacks, as a low-cost method of psychological influence. While Chinese groups focused on cyberespionage, avoiding detection [Bund J., Bendiek A., Hemmelskamp J, pp. 4-6].

Analysis of cyber threat statistics for 2022–2024 showed a significant increase in the number of attacks and their complexity. The presented **table 1** summarizes data on key aspects of cyber threats over the past three years (2022–2024). The data is collected from open sources, including international ones: the European Union Agency for Network and Information Security (ENISA), and Ukrainian organizations, in particular the Cyber Police of Ukraine, CERT-UA. The most attacked sector is public administration. Public institutions are a key target for cybercriminals, in particular in the context of cyber espionage, destabilization of the work of state bodies and cyberwarfare. The high proportion of attacks on the public sector also likely indicates that both cyber defense and the organization of attacks are carried out by state special services. This is confirmed by the active activities of government incident response teams (CERT-UA, ENISA and others), which record and analyze such threats. In addition to the public sector, a significant level of attacks is recorded in the financial, energy and educational sectors. The financial sector remains attractive to criminals due to the possibility of stealing funds and confidential data. Educational institutions are becoming targets due to the widespread implementation of distance learning and insufficient level of protection.

Table 1. Sectors of the economy that were attacked in 2022-2024.

Year	Sector	Attack rate (%)	Source
2022	State	30	CERT-UA, 2022, p.10
2022	Financial	25	ENISA, 2022, p.22

2022	Medical	15	ENISA, 2022, p.25
2022	Others	30	CERT-UA, 2022, p.12
2023	State	28	CERT-UA, 2023, p.11
2023	Financial	27	ENISA, 2023, p.30
2023	Energy	18	ENISA, 2023, p.35
2023	Others	27	CERT-UA, 2023, p.13
2024	State	32	CERT-UA, 2024, p.9
2024	Financial	26	ENISA, 2024, p.28
2024	Educational	20	ENISA, 2024, p.32
2024	Others	22	CERT-UA, 2024, p.11

In 2022, a significant number of attacks were recorded against government institutions with the aim of destabilizing their work; financial institutions were attacked to steal funds and confidential customer data; medical institutions were targeted due to the value of medical data and the vulnerability of their systems; other attacks included attacks on the education, energy and other sectors. In 2023, attacks on government agencies continued for the purpose of intelligence gathering, sabotage and increased attacks on the financial sector due to the development of digital services and online banking; energy companies became targets of attacks to undermine critical infrastructure; attacks on the medical, education and other sectors also did not significantly decrease. 2024 brought an increase in the number of attacks on government institutions related to the escalation of cyber conflicts; The financial sector has become an attractive target for cybercriminals due to the potential financial gain, while educational institutions are vulnerable to attacks due to the introduction of distance learning and insufficient level of protection.

In terms of tactics, it is safe to say that phishing remains effective, but attacks on supply chains, the exploitation of zero-day vulnerabilities and the use of artificial intelligence to automate hacks are coming to the fore. DDoS attacks are becoming more widespread, and ransomware is even more aggressive. At the same time, not only state-owned hacking groups are increasingly active, but also criminal groups that sell their services on the Darknet market. Hacktivists such as Anonymous and Anonymous Sudan are adding to the chaos by attacking for political motives. In addition, a third of cyberattacks were not identified by country of origin. This highlights the difficulty of attributing cyberattacks in today's cyberspace, where attackers often use techniques to hide their true location and identity.

In 2024, after three years of research by scientists from the University of Oxford and the University of New South Wales in Canberra, the Global Cybercrime Index was proposed, created to develop effective solutions to mitigate cyber threats at the national and international levels (Bruce, Lusthaus, Kashyap, Phair, Varese, 2024). The research methodology was developed in 2020 with the aim of geographically ranking cybercrime, which, according to the researchers, makes it possible to better understand and counteract it at the level of adopting relevant policies. The assessment of the participation of countries in cybercrime was carried out on the basis of a survey of 92 leading cybercrime experts during March-October 2021 according to five main categories of cybercrime and ranking by technological complexity (T-score) (Fig. 1). A negative indicator corresponds to lower technological complexity, plus - to higher. The study was published in April 2024. As can be seen from the line graph, experts who participated in this study stated that the Russian Federation and

Ukraine are the most high-tech centers of cybercrime, while British, African, and Indian cybercriminals engage in less technical forms of cybercrime.

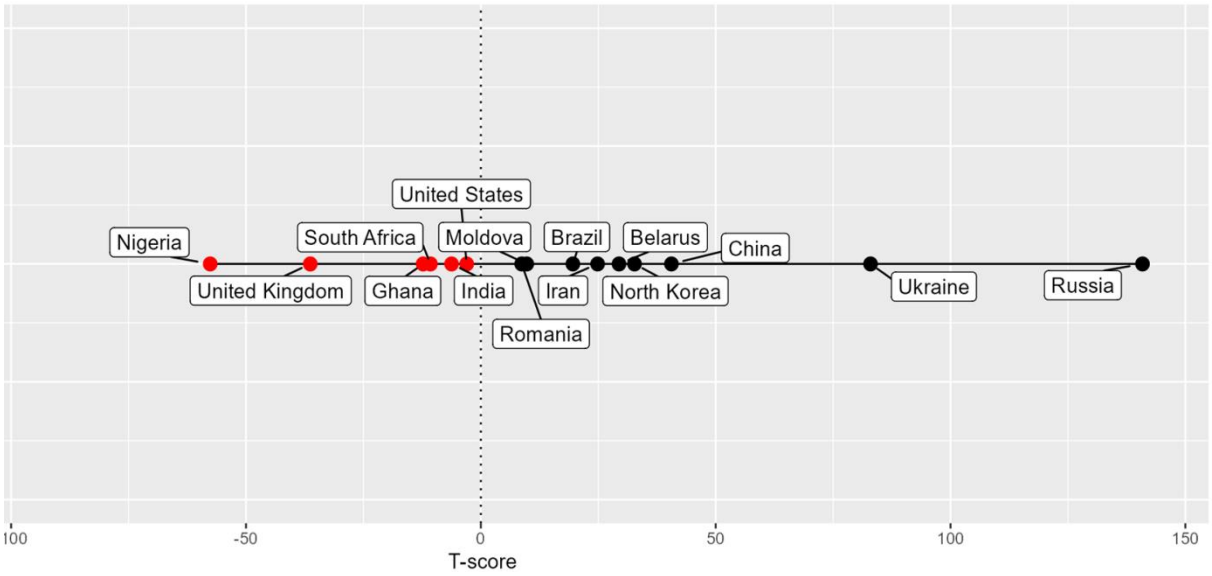

Fig. 3. Technical indicators (T-score) of the 15 best-performing countries, WCI.

This study leads to a number of conclusions and comments on the generalizations made. The scientists themselves agree that, given the small number of experts, the snowball method that was chosen for the study has limitations in terms of generalization of the results . The sample of participants also indicates a significant predominance of experts from Europe (42% of those surveyed), which could have affected the optics of the results. At the same time, the study, as well as the publication itself, did not take into account the prerequisites (including the war) that has been going on between the Russian Federation and Ukraine since 2014, and the very fact of the Russian Federation's full-scale invasion on February 24, 2022. The need to take this extremely important factor into account when preparing the study itself is clearly evidenced by official Europol (European Union Agency for Law Enforcement Cooperation) statistics and the above-mentioned EuRepoC data.

Results and Discussion

In 2020-2021, Ukraine also saw a significant increase in the level of digitalization compared to other Eastern European countries. The level of digital transformation of the public sector, the implementation of e-government (for example, the "Diya" platform), and the active development of cybersecurity infrastructure also indicate the country's high technological potential and its readiness, even in conditions of full-scale war, to preserve the principles of democracy through open data and digitalization of public services. According to the results of the UN study "E-Government Review 2024. Accelerating Digital Transformation for Sustainable Development", Ukraine significantly improved its position in the global digital governance rankings, becoming the first in the E-Participation Index (EPART), rising by 56 positions compared to 2022 **.** And in the e-government rating (E-Government Development Index, EGDI) – it took 30th place among 193 countries in the world, which is 16 positions higher than in 2022. The situation is completely opposite in the Russian Federation, which has chosen the path of authoritarianism for the past 20 years. In the e-participation rating (E-Participation Index, EPART), starting from 2012, the Russian Federation gradually moved from 19th place to 66th in 2024. And in the e-government rating (E-Government Development Index, EGDI) – it took 43rd place, which is 16 positions higher than in 2012. These data indirectly indicate differences in the trends in the use of digital technologies both in the development of the state and in its protection and defense against external cyber threats.

The European Repository of Cyber Incidents (EuRepoC) and the Cybercrime Index (WCI) discussed above, created to develop policies and measures to counter cyberattacks, require taking into account the geopolitical component, especially in the context of cyberwarfare as a component of a full-scale invasion by the Russian Federation. After all, Ukraine is forced to conduct not only defensive, but also offensive cyber operations. Therefore, such indices as the WCI require taking into

account the geopolitical prerequisites and cyber activities that preceded the full-scale invasion and took place throughout 2021, as well as the hybrid war that has been actively waged in cyberspace since 2014. On the other hand, if according to the WCI Ukraine is defined as a high-tech hub of cybercrime alongside the Russian Federation, it may indicate stereotypes that existed among European experts about Ukraine on the eve of a full-scale invasion, such as a high level of general crime, corruption, and frequent identification (merger) of the Ukrainian and Russian IT segments. It should be noted that during the survey period, Ukraine monitored significant development of the IT sector, where " compared to neighboring countries, Ukraine was considered an attractive hub" , in particular, the growth of IT services exports, which in 2021 amounted to 37% of all Ukrainian export services at $6.8 billion (compared to $5 billion in 2020). (Kondrashov, 2022).

Massive and large-scale cyberattacks require strengthening common policies and the formation of an appropriate cyber solution market for both the public and private sectors. Among the leaders of the global cybersecurity market are the USA ($81 billion), China ($15 billion), Great Britain ($11 billion), Japan ($9 billion), Germany ($8 billion), where Ukraine's share in the global market is approximately 0.07% and was mainly provided through international donor support (IT Ukraine, 2024, p. 9). In particular, US assistance to Ukraine in cybersecurity for 2022-2024 amounted to $82 million (IT Ukraine, 2024, p. 12). Significant economic losses due to cyberattacks include direct (ransoms, data recovery costs and rebuilding of destroyed systems) and hidden costs (loss of reputation, productivity, legal costs and fines for non-compliance with standards such as GDPR, NIS2 or CCPA, increased costs for cyber insurance, investments in training) (Poligenko, 2025). According to the "Cost of Data Breach" report, conducted by the independent Ponemon Institute with the support of IBM, among 604 organizations that suffered data breaches from March 2023 to February 2024 in 16 countries, The average cost of a cyber incident is expected to increase from $4.45 million in 2023 to $4.88 million in 2024, a 10% increase driven by increased recovery costs and other indirect costs (IBM Security, 2024). The public sector, financial services, and energy sectors are the most affected, highlighting the need for increased cyber security in these sectors. Attacks on energy facilities are aimed at disrupting critical infrastructure, which can have significant socio-economic consequences, especially since the start of the Russian-Ukrainian war.

In 2025 Global financial losses from cyberattacks could reach $ 10.5 trillion (the estimate consists of both direct and hidden losses (Morgan, 2024). This is due to the further increase in the number and complexity of attacks, as well as the active use of artificial intelligence by cybercriminals, which requires improving national cyber defense strategies, implementing more effective threat monitoring systems, and international cooperation in the field of cybersecurity.

Conclusions

The development of digital technologies, despite their positive impact on the economy and society, is accompanied by increasing risks associated with cyberattacks, which can lead to large-scale financial losses, disruptions to critical infrastructure, data theft, and compromise of confidential information.

Cybersecurity regulations and policies play a crucial role in safeguarding the digital landscape of the United States. the government to establish a comprehensive framework to protect critical infrastructure, sensitive data, and national security. Cybersecurity regulations and policies in the US have made significant strides in enhancing the nation's cyber resilience. The consistent surge in the cost of cybercrimes highlights the urgent need for robust cybersecurity measures. This finding implies that the current cybersecurity landscape demands a multifaceted approach to regulation, addressing a spectrum of threats.

Cybercrime as a result of illegal activity in cyberspace increasingly contains a geopolitical component, which, as a result of the full-scale invasion of the Russian Federation, has reached a new level of global scale. To counter the growing threats, coordinated actions of state, private and international organizations are required, as well as regular training and improvement of cyber hygiene among the population by overcoming digital divides, because the digitalization of a significant number of services requires an increase in relevant knowledge and skills.

Cyber threat statistics for 2022–2024 indicate a significant increase in the number of attacks and their complexity. For Ukraine, this negative trend is already part of hybrid warfare: cyber attacks paralyze the activities of critical infrastructure facilities, the banking system, the public sector, energy, healthcare, and digital services. At the same time, Ukraine continues to increase the level of digitalization and cyber defense in these extremely difficult conditions. In particular, in the direction of European integration, an active screening process is underway, i.e. the official procedure for adapting Ukrainian legislation to EU law under Chapter 10 "Digital Transformation and Media" . Despite the long war, Ukraine is demonstrating significant progress in digital development, the government has successfully transferred data and services to international cloud platforms, which guarantees their security, accessibility, and sustainability, and ensures uninterrupted access to the Internet. Such a strategic approach not only protects the country's digital assets, but also contributes to the preservation of economic activity and the functioning of public services. This strengthens Ukraine's position as a sustainable and forward-looking leader in the field of digital technologies [UN Department of Economic and Social Affairs].

The dynamics of attacks on various sectors of the economy indicate a growing role of state agencies in cybersecurity and a growing threat to critical industries. This requires improving national cyber defense strategies, implementing more effective threat monitoring systems, and international cooperation in cybersecurity. On the other hand, national security in cyberspace is largely dependent on private companies that control and develop cloud technologies. An extreme case is Microsoft's assistance to the Ukrainian government during the Russian invasion in February-March 2022. During this emergency, Microsoft helped Ukraine migrate key data, moving government ministries to the cloud to back up government data. This move had geostrategic implications for how the war unfolded and for Ukraine's resilience (Fedorov, 2022). In fact, cloud services proved to be one of the main factors hindering Russia's cyber operations during the war, leading to "widespread improvements in Ukraine's overall cybersecurity and resilience" (Bateman, 2022, 33, 42–43).

Training and Cyber Security Culture. Findings indicate the need for a cyber security culture within academic institutions, which could be achieved through regular training and mandatory security education for both staff and students.... Existing cyber security policies should be evaluated against international standards such as the ISO 27000 series to identify gaps, especially in disaster recovery and data backup protocols

The identification of activities and groups indicates the strategic nature of many attacks with geopolitical and economic motives. This emphasizes the importance of international cooperation, improving monitoring mechanisms and implementing new technologies and procedures for cyber defense. Such cyber solutions adapted to unique requirements include both technical (application security, cloud security, data security, network security, endpoint security) and organizational (risk management that supports compliance with regulatory requirements and protects against security risks) (IT Ukraine, 2024,_p. 4). The public sector can only partially counteract cyber risks, as the scale and technical level of cyber attacks increases every year.

References

1. Bruce, M., Lusthaus, J., Kashyap, R., Phair, N., & Varese, F. (2024). Mapping the global geography of cybercrime with the World Cybercrime Index. PLOS ONE, 19 (4), e0297312. https://doi.org/10.1371/journal.pone.0297312
2. Die Lage der IT-Sicherheit in Deutschland 2022. (2022). Retrieved from https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.pdf
3. ENISA. (n.d.). Threat Landscape Report. Retrieved from https://www.enisa.europa.eu
4. European Repository of Cyber Incidents. (n.d.). Cyber Incident Dashboard. Retrieved from https://eurepoc.eu/dashboard/
5. Europol. (n.d.). Cybercrime. Retrieved from https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime

6. IBM Security. (2024). Cost of a Data Breach Report 2024. Retrieved from https://table.media/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf
7. IBM X-Force Threat Intelligence. (n.d.). Retrieved from https://www.ibm.com/security/services/x-force
8. ICSA. (nd). The Impact of Cyber Threats on Modern Society: Data and Findings 2022-2024. Retrieved from https://icsa.team/701-701/
9. IT Ukraine. (2024). Ukraine Cybersecurity Market Review . Retrieved from https://itukraine.org.ua/files/Ukraine-Cybersec-Market-Review.pdf
10. Cyberpolice of Ukraine. (nd). Retrieved from https://cyberpolice.gov.ua
11. Morgan, S. (2024). Top 5 cybersecurity predictions, and statistics for 2024. Cybersecurity Ventures. Retrieved from https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2021-to-2025
12. NCSC. (2023). Annual Review 2023. Retrieved from https://www.ncsc.gov.uk/files/Annual_Review_2023.pdf
13. Kondrashov, V. (2022). Growth of 36%. Ukrainian IT industry reached $6.8 billion — IT Ukraine. NV Business. Retrieved from https://biz.nv.ua/ukr/tech/obsyag-ukrajinskogo-it-eksportu-sklav-6-8-mlrd-dolariv-novini-ukrajini-50210150.html
14. Palo Alto Networks. (n.d.). Threat Intelligence. Retrieved from https://www.paloaltonetworks.com/threat-intelligence
15. Poligenko, O. (2025). State institutions and banks under a barrage of cyberattacks. Who else is at increased risk in 2025 and what protection strategy will work? Forbes Ukraine. Retrieved from https://forbes.ua/innovations/kiberriziki-na-ponad-10-trln-zbitkiv-yaki-galuzi-biznesu-naybilshe-atakuyut-kiberzlochintsi-ta-yak-minimizuvati-naslidki-instruktsiya-vid-eksperta-u-sferi-kiberbezpeki-olega-poligenko-23012025-26534
16. Rapport Annuel Sur La Cybercriminalité 2024. (2024). Retrieved from https://www.interieur.gouv.fr/actualites/actualites-du-ministere/rapport-annuel-sur-cybercriminalite-2024
17. UN Department of Economic and Social Affairs. (2024). E-Government Survey 2024: Accelerating Digital Transformation for Sustainable Development with the addendum on Artificial Intelligence (p. 125). Retrieved from https://doi.org/10.18356/9789211067286
18. CERT-UA (Ukrainian Computer Emergency Response Team). (nd). Retrieved from https://cert.gov.ua
19. Cisco Talos Intelligence Group. (n.d.). Retrieved from https://talosintelligence.com
20. World Economic Forum. (2025). Global Risks Report 2025. Retrieved from https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf

УДК 004.056(063)(048.4)
Р 68

Роль безпеки в транскордонному та міжнародному співробітництві. Наукове видання (Збірник тез доповідей) Закарпатського угорського університету імені Ференца Ракоці II / Редактори: Степан Черничко, Маріанна Марусинець, Єлизавета Молнар Д, Оксана Мулеса та Ганна Мелеганич. Берегове: Університет Ракоці, 2025. – 384 с. (українською, англійською та угорською мовами)

ISBN 978-617-8143-50-3 (м'яка обкладинка)
ISBN 978-617-8143-51-0 (PDF)

Збірник містить тези доповідей (українською, англійською та угорською мовами) міжнародної науково-практичної конференції «Роль безпеки в транскордонному та міжнародному співробітництві», яка відбулася 8–9 жовтня 2025 року в місті Берегове. Матеріали конференції висвітлюють широкий спектр проблем, пов'язаних із забезпеченням безпеки в умовах сучасних транскордонних та міжнародних викликів. Збірник тез доповідей охоплює питання політичних, соціальних, правових і технологічних аспектів безпеки, а також інтеграцію штучного інтелекту та цифрових технологій у систему захисту інформації. Організатори конференції: Закарпатський угорський університет імені Ференца Ракоці II та Ужгородський національний університет. Співорганізатори: Кафедра ЮНЕСКО «Неперервна професійна освіта XXI століття» НАПН України, Південноукраїнський національний педагогічний університет імені К. Д. Ушинського, Черкаський національний університет імені Богдана Хмельницького, Державний університет «Київський авіаційний інститут», Університет Григорія Сковороди в Переяславі, Міжнародний гуманітарний університет, Херсонський державний університет, Берегівський навчальний центр Матіасу Корвінусу Колегіуму, Пряшівський університет у Пряшеві, Жешувський університет, Ускюдарський університет, Північний університетський центр у Бая-Маре Технічного університету Клуж-Напока.

Наукове видання

РОЛЬ БЕЗПЕКИ В ТРАНСКОРДОННОМУ ТА МІЖНАРОДНОМУ СПІВРОБІТНИЦТВІ

Міжнародна науково-практична конференція
Берегове, 8–9 жовтня 2025 року

Збірник тез доповідей

2025 р.

Рекомендовано до видання у друкованій та електронній формі (PDF)
рішенням Вченої ради Закарпатського угорського університету імені Ференца Ракоці II
(протокол №12 від «17» грудня 2025 року)

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

За редакцією:
Степан Черничко, Маріанна Марусинець, Єлизавета Молнар Д,
Оксана Мулеса та Ганна Мелеганич

Технічне редагування: *Адам Доровці, Олександр Добош та Анастасія Сенько*
Підготовка до видання у друкованій та електронній формі (PDF): *Анастасія Сенько*
Коректура: *авторська*
Дизайн обкладинки: *Вівієн Товт*
УДК: *Бібліотека ім. Опацої Чере Яноша Університету Ракоці*

Відповідальний за випуск:
Олександр Добош (начальник Видавничого відділу Університету Ракоці)

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 університет імені Ференца Ракоці II (адреса: пл. Кошута 6, м. Берегове, 90202. Електронна пошта: egyetem@kme.org.ua; office@kme.org.ua) *Свідоцтво про внесення суб'єкта видавничої справи до Державного реєстру видавців, виготовлювачів і розповсюджувачів видавничої продукції Серія ДК 8485 від 23 жовтня 2025 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. 31,2.
Формат 70x100/16.

ISBN 978-617-8143-50-3