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

ШТУЧНИЙ ІНТЕЛЕКТ ТА ЦИФРОВІ ТЕХНОЛОГІЇ У СФЕРІ БЕЗПЕКИ

ARTIFICIAL INTELLIGENCE AND DIGITAL TECHNOLOGIES IN THE FIELD OF SECURITY

MESTERSÉGES INTELLIGENCIA ÉS DIGITÁLIS TECHNOLÓGIÁK ALKALMAZÁSA A BIZTONSÁGI ÁGAZATBAN

Viktor LOBODA
Bachelor's degree student (2nd year), majoring in Cybersecurity and Data Protection (Specialty 125)
State University "Kyiv Aviation Institute"
9291605@stud.kai.edu.ua

Natalia BILOUS
PhD (Pedagogy), Associate Professor of the Professional Foreign Languages Department,
State University "Kyiv Aviation Institute"
natalia.bilous@npp.kai.edu.ua

ANALYSIS OF THE POTENTIAL OF RECURRENT NEURAL NETWORKS FOR IDENTIFICATION OF DDOS ATTACKS

In the world of cybersecurity, DDoS attacks are like a mass disease that keeps mutating. Traditional defense systems, which only look for sudden traffic spikes, are increasingly powerless against new, cunning attacks. The latest of these can behave almost like real users, "poisoning" the system slowly and unnoticed. This is why researchers are seeking more innovative solutions that can not only track the number of requests but also their underlying logic over time.

The goal of this work is to verify that specialized neural networks capable of analyzing sequences (specifically, LSTM and GRU models) are indeed a promising line of defense. The idea is that network traffic is not a set of isolated events, but a continuous "conversation". By observing this "conversation," these neural networks can learn their usual rhythm and hear the first uncertain notes when someone tries to disrupt it.

Previous research has repeatedly confirmed that such models are often more accurate than old methods. Their superpower is memory. They don't just see what's happening now, but they also remember what happened before. This makes them crucial for detecting slow, "smoldering" attacks that last for hours and go unnoticed by conventional security systems.

Our theoretical work confirms that these neural networks are a powerful tool against all kinds of DDoS attacks, from brute-force to sophisticated ones. They are flexible and can learn from new threats. Of course, they aren't perfect: training them requires powerful computers, massive datasets, and careful tuning.

In conclusion, recurrent neural networks are a serious step towards a future where security systems become not just guards with an instruction manual, but attentive and intelligent guardians. They analyze behavior over time, which gives them a significant advantage. The next step should be the creation of hybrid systems that combine the strengths of different technologies to build a truly living and resilient defender for our networks.

References

1. Buczak, A. L. & Guven, E. (2016). A Survey of Data Mining and Machine Learning Methods for Cyber Security. IEEE Communications Surveys & Tutorials, 18(2), pp. 1153-1176. DOI: 10.1109/COMST.2015.2494502.
2. Tavallaee, M., Bagheri, E., Lu, W. & Ghorbani, A. A. (2009). A detailed analysis of the KDD CUP 99 data set. Proceedings of the IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA).
3. Yin, C., Zhu, Y., Liu, S. & Fei, J. (2017). A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks. IEEE Access, 5, pp. 21954-21961. DOI: 10.1109/ACCESS.2017.2762016.

Denys TOKMENKO
Master's degree student (1 st year), majoring in Cybersecurity and Data Protection (Specialty F5)
State University "Kyiv Aviation Institute"
7411259@stud.kai.edu.ua

Nataliia BILOUS
PhD (Pedagogy), Associate Professor of the Professional Foreign Languages Department,
State University "Kyiv Aviation Institute"
natalia.bilous@npp.kai.edu.ua

USING ARTIFICIAL INTELLIGENCE FOR THREAT DETECTION IN NETWORK LOGS

In the context of the constant growth in network traffic volumes and the complication of cyberattacks, traditional threat detection methods based on signatures and manual rules (Rule-Based Systems) are becoming insufficiently effective. A huge array of unstructured or semi-structured network logs contains vital but hidden signs of malicious activity that are practically impossible to detect with the human eye or simple scripts. This determines the relevance of the topic, due to the need to increase the speed and accuracy of cybersecurity systems. The use of Artificial Intelligence (AI) technologies, particularly Machine Learning (ML) and Deep Learning (DL) methods, is a key direction for automating log analysis, which allows for the detection of anomalies and zero-day attacks that lack known signatures. This is vitally necessary to maintain the cyber resilience of critical infrastructure and corporate networks.One of the goals is to conduct a comparative theoretical analysis of the effectiveness and applicability of various Artificial Intelligence architectures (particularly ML and DL methods) for automated detection of diverse cyber threats in large arrays of network logs, and to determine the optimal models.

The scientific novelty lies in: Systematization of methods by providing a comparative analysis of the latest AI methods specifically in the context of network log processing, with a focus on pre-processing. The necessity of using ensemble AI models, which can combine the advantages of different algorithms for detecting multi-stage attacks, is substantiated.

The study involves a theoretical comparison of several key AI approaches:

AI Approach	Examples of Models	SVM, Random Forest, K-Means (Clustering)	Advantages	Limitations
Machine Learning (ML)	SVM, Random Forest, K-Means (Clustering)	Log classification by threat type, detection of anomalous users.	High training speed and interpretability of results.	Low effectiveness in detecting new (zero-day) threats.
Deep Learning (DL)	LSTM, GRU, Autoencoders	Analysis of event sequences (behavioral analysis), detection of complex temporal anomalies.	High accuracy in detecting hidden, unknown patterns; automatic feature extraction.	High computational requirements, need for large volumes of labeled data.
Ensemble /Hybrid Models	Combination of Autoencoder +	Analysis of event sequences (behavioral analysis), detection	Combining the advantages of different models	Complexity of Implementation and configuration.

	LSTM, Stacked Classifiers	of complex temporal anomalies.	for maximum accuracy.	

Based on the conducted theoretical analysis, the following main conclusions can be drawn: DL Advantage for Unknown Threats: Deep Learning (DL) models, particularly recurrent neural networks and autoencoders, demonstrate the highest potential for detecting unknown threats and complex anomalies, as they are capable of learning normal network behavior and effectively identifying deviations without the need for prior knowledge of attack signatures. Optimal Solution – Hybrid Systems: The most reliable architecture for practical application is a hybrid system, where Machine Learning (ML) algorithms quickly process known threats and filter out "noise," while DL models concentrate on the deep analysis of high-risk and anomalous sequences. Criticality of Pre-processing: The effectiveness of any AI model critically depends on the quality of log pre-processing, particularly effective vectorization and normalization. Investing resources in log format standardization is a necessary condition for the successful implementation of AI. Scalability Challenge: The main obstacle to the widespread adoption of DL models is their computational complexity and the need for powerful hardware resources, which must be taken into account when designing next-generation Security Information and Event Management systems.

References

1. Alghazzawi, A. H., El-Khatib, K. and Abed, S. A. (2023) A Survey of Machine Learning-Based Zero-Day Attack Detection: Challenges and Future Directions. Journal of King Saud University - Computer and Information Sciences, 35(2), pp. 101511. Available at: [https://pmc.ncbi.nlm.nih.gov/articles/PMC9890381/#S28] (Accessed: 14 October 2025).
2. Du, M., Li, F., Zheng, G. and Srikumar, V. (2017) DeepLog: Anomaly Detection in System Logs using Deep Neural Networks. In: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. Dallas, TX, USA: ACM, pp. 190-207. Available at: [https://www.researchgate.net/publication/320678676_DeepLog_Anomaly_Detection_and_Diagnosis_from_System_Logs_through_Deep_Learning] (Accessed: 14 October 2025).

Nataliia VOLYNETS
Bachelor's degree student (2nd year)
majoring in Software Engineering (Specialty 121),
State University "Kyiv Aviation Institute"
7881865@stud.kai.edu.ua

Vitalii SYNIAK
Bachelor's degree student (2nd year)
majoring in Software Engineering (Specialty 121),
State University "Kyiv Aviation Institute"
9302054@stud.kai.edu.ua

Larysa TEREMINKO
PhD (Pedagogy), Associate Professor of the
Professional Foreign Languages Department,
State University "Kyiv Aviation Institute"
larysa.tereminko@npp.kai.edu.ua

BIOMETRIC DATA: PROTECTION OR VULNERABILITY OF IDENTITY?

The fast spread of biometric authentication systems in the digital security infrastructure has created the basic contradictory situation of modern cyber security. Biometrics provide exceptional accuracy in identity verification through unique physiological and behavioral characteristics. However they simultaneously introduce new vulnerability vectors that challenge traditional security concepts. This research addresses the key question of whether biometric technologies strengthen or undermine the protection of personal identity in the digital age.

We aimed to conduct a study that would include conducting a thorough analysis of biometric data systems to assess defense mechanisms and potential security vulnerabilities. The relevance of the study is attributed to the rapid growth of biometric implementations in financial services, healthcare, public systems and consumer devices, which requires a rapid assessment of the risks and benefits involved.

The beginning of the research is to develop an integrated framework that quantifies the security, privacy trade-offs inherent in biometric systems, as opposed to previous works that are considered separately. That is, in contrast to traditional security research focusing solely on technical implementation, this research integrates privacy implications, social recognition factors, and the sustainable sustainability of biometric infrastructure.

The main methodology uses benchmarking of major biometric types, including fingerprints, facial recognition, iris scanning and voice authentication systems. Security vulnerability assessments investigate counterfeit attacks, template database breaches, and cross-system correlation risks. The privacy impact assessment takes into account the persistence of data, the impossibility of recall and the potential for surveillance. The study examines real-world incidents, including the 2019 Biostar 2 database breach affecting over a million users, and the Ver security camera compromise.

Key findings show that biometric systems show higher authentication accuracy compared to traditional password-based methods, with false acceptance rates below 0.001% for high-quality implementations. However, critical vulnerabilities arise from the irreversible nature of biometric compromise. Unlike passwords, compromised biometric templates cannot be reset, creating constant risks of identity theft. The study identifies pattern storage as the primary attack vector, and centralized databases represent attractive targets for attackers.

Conclusions indicate that hybrid methods of identity verification, combining biometrics with traditional methods, create an optimal balance of security and privacy. Implementing privacy-preserving techniques such as homomorphic encryption and secure multi-party computing can reduce storage risks while preserving system functionality. The regulatory framework should be developed to manage biometric data, establish clear consent mechanisms and requirements for reporting irregularities.

The data we receive shows that biometric technologies represent both the future of secure authentication and a serious privacy issue. Their protective properties are undeniable if used properly,

but the stability of biometric features requires extraordinary security measures. The study recommends decentralized storage architectures, advanced encryption protocols, and a comprehensive legal framework to maximize benefits while minimizing vulnerabilities. Future work should focus on developing quantum-resistant biometric systems and establishing international standards for biometric data protection.

References

1. Clearview AI. (2024). 'Facial recognition privacy settlement'. Illinois class-action lawsuit case study.
2. Federal Trade Commission. (2025). 'FTC warns about misuses of biometric information and harm to consumers'. FTC Press Release, March 12.
3. Identity Management Institute. (2024). 'Biometric authentication benefits and risks'. Security Analysis Report, May 14.
4. Mitek Systems. (2025). 'Advantages and disadvantages of biometrics'. Technical White Paper, January 7.
5. Nagaraj, K. (2025). 'Biometric authentication risks and best defenses'. Medium Cybersecurity, August 5.
6. SOCRadar Cyber Intelligence. (2024). 'Biometric security risks: beyond fingerprints and facial recognition'. Security Analysis, October 2.

Микола ЧЕРЕДНИЧЕНКО
здобувач вищої освіти другого (магістерського) ступеня,
1 курсу, спеціальності F7 «Комп'ютерна інженерія»,
Державний університет «Київський авіаційний інститут»,
7419525@stud.kai.edu.ua

Наталя БІЛОУС
кандидат педагогічних наук,
доцент кафедри іноземних мов професійного спрямування,
Державний університет «Київський авіаційний інститут»,
natalia.bilous@npp.kai.edu.ua

ШТУЧНИЙ ІНТЕЛЕКТ ДЛЯ КІБЕРЗАХИСТУ IOT

Інтернет речей (IoT) стає ключовим компонентом сучасної цифрової інфраструктури — від промислових систем (IoT) до «розумних» міст, транспорту й медицини. Водночас швидке зростання кількості підключених пристроїв створює нові вектори атак. Кожен IoT-пристрій, часто із мінімальними ресурсами (CPU, RAM, енергоспоживання), може стати потенційною точкою проникнення. Класичні засоби кіберзахисту, такі як антивірусні програми чи міжмережеві екрани, є занадто «важкими» для таких систем, що робить традиційні підходи неефективними.

Таким чином, актуальною є розробка автономних систем безпеки, здатних функціонувати безпосередньо на периферійних пристроях із використанням методів штучного інтелекту (ШІ).

Метою роботи є створення легкої системи виявлення аномалій у поведінці IoT-пристроїв із використанням нейронних мереж. Завданням є розробка архітектури, що дозволяє здійснювати моніторинг і реагування в реальному часі без залучення хмарної інфраструктури.

У сучасних дослідженнях кіберзахисту IoT значна увага приділяється застосуванню методів глибокого навчання для виявлення аномалій у мережевому трафіку. Зокрема, підхід N-BaIoT [1] демонструє високу точність (>99%) у виявленні ботнет-атак за допомогою глибоких автоенкодерів, хоча його практична реалізація потребує значних обчислювальних ресурсів. Подібні результати отримано і при використанні CNN- та RNN-моделей для виявлення вторгнень [2], однак їхня складність обмежує застосування на мікроконтролерах та в обмежених за функціональністю пристроях.

Для підвищення ефективності у вбудованих системах пропонуються спрощені підходи із зменшенням розмірності ознак та використанням легких моделей машинного навчання [3]. Перспективним напрямом розвитку є також квантово-підсилене машинне навчання [4], здатне подолати обчислювальні обмеження класичних алгоритмів у майбутніх поколіннях IoT-систем.

Запропонованим рішенням в цій роботі являється дворівнева архітектура кіберзахисту IoT.

Рівень 1 - модуль TinyML на мікроконтролері (наприклад, ESP32). Використовується компактний автоенкодер, навчений розпізнавати нормальну поведінку пристрою. При значному відхиленні реконструкційної помилки спрацьовує локальний тригер безпеки.

Рівень 2 - Edge-шлюз. Агреговані ознаки передаються на локальний вузол із потужнішою моделлю (наприклад, GRU+LightGBM), що уточнює класифікацію та приймає рішення про блокування чи сповіщення.

Перевагою такого підходу є низька затримка, автономність і захист приватності, адже необроблені дані не покидають пристрою. Для реалізації використовується TensorFlow Lite for Microcontrollers із квантизацією моделі до формату int8, що зменшує розмір і прискорює виконання.

Очікувана точність виявлення аномалій для полегшених автоенкодерів у контексті IoT-аналітики оцінюється у високому діапазоні (порядку 90–97%) залежно від задачі та якості ознак; при цьому реальні показники інференс-часу та споживання пам'яті значною мірою залежать від архітектури моделі та ступеня оптимізації (квантизація, pruning, knowledge distillation). Експериментальні дослідження показують, що спеціально оптимізовані TinyML-моделі здатні забезпечити інференс у мілісекундах на MCU та укладатись у десятки-сотні кілобайт пам'яті за допомогою квантизації й оптимізації моделі [5, 6]. Порівняно з класичними легковаговими алгоритмами (наприклад, Isolation Forest), автоенкодери часто дають вищу

здатність виявляти складні патерни аномалій при порівнянних витратах ресурсів після оптимізації моделі [5].

Розроблена архітектура доводить, що методи штучного інтелекту можуть бути успішно інтегровані у сферу IoT навіть на обмежених апаратних платформах. Наукова новизна полягає у практичній адаптації TinyML-підходів для задач кіберзахисту. Подальші дослідження можуть бути спрямовані на:

- застосування федеративного навчання для колективного вдосконалення моделей без передачі даних;
- впровадження апаратних NPU-модулів у мікроконтролери;
- дослідження змагальних атак і методів підвищення стійкості нейромереж до вразливостей.

Список використаних джерел

1. Meidan, Y., Bohadana, M., Mathov, Y., et al. (2018) N-BaIoT: Network-based detection of IoT botnet attacks using deep autoencoders. IEEE Pervasive Computing.
2. Korbaa, O., Jemili, F., Selem, M.S. (2024) Deep Learning for Intrusion Detection in IoT Networks. Springer.
3. Hamdan, A., Tahboush, M., Adawy, M., Alwada'n, T. & Ghwanmeh, S. (2025) Feature Reduction and Anomaly Detection in IoT using Machine Learning. International Journal of Advanced Computer Science and Applications (IJACSA), 16(1).
4. Hdaib, M., Rajasegarar, S. & Pan, L. (2024) Quantum deep learning-based anomaly detection for enhanced network security. EPJ Quantum Technology, 6(26).
5. Antonini, M., Pincheira, M., Vecchio, M. & Antonelli, F. (2023) An Adaptable and Unsupervised TinyML Anomaly Detection for Embedded Devices. Sensors, 23(4).
6. Osman, A., Abid, U., Gemma, L., Perotto, M. & Brunelli, D. (2022) TinyML Platforms Benchmarking. In: Lecture Notes in Electrical Engineering (LNEE), vol. 866. Cham: Springer, pp. 139–148.

Bohdan ILCHENKO
Bachelor's degree student (2nd year) majoring in
Computer Engineering (Specialty 123),
State University "Kyiv Aviation Institute"
8610735@stud.kai.edu.ua

Olena HURSKA
PhD (Pedagogy), Associate Professor of the
Professional Foreign Languages Department,
State University "Kyiv Aviation Institute"
olena.hurska@npp.kai.edu.ua

CYBERSECURITY IN CLOUD COMPUTING ENVIRONMENTS

In recent years, cloud computing has become one of the most rapidly developing areas of information technology. Owing to its scalability, flexibility, and cost efficiency, cloud computing has become integral to business operations, education, healthcare, and scientific research. However, as more people use cloud technology, the number and complexity of cyber threats also rise. This situation highlights the urgent need for effective cybersecurity measures in cloud computing environments. The relevance of this research lies in the growing dependency on cloud-based systems and the consequent need to secure them against evolving attacks. The novelty of the study is determined by the integration of recent technological advancements, such as artificial intelligence, blockchain, and quantum cryptography, into the field of cybersecurity. The objective of this thesis is to analyze the main risks associated with cloud computing and to examine the most effective modern and emerging methods for ensuring cybersecurity in these environments.

The transition to cloud-based infrastructure introduces new vulnerabilities and attack surfaces for cybercriminals. Unlike traditional IT systems, where organizations maintain full control over access and security policies, cloud resources are typically shared among multiple users and accessible over the Internet. This makes it easier for unauthorized people to get in and cause trouble.

The most common threats in cloud environments include:

Data leakage or loss: if cloud storage isn't set up correctly, private information such as financial documents or personal records can be exposed to unauthorized users

Unauthorized access: weak passwords, stolen credentials, or flaws in authentication mechanisms can enable attackers to infiltrate cloud systems.

Distributed Denial of Service (DDoS) attacks: attackers can flood servers with traffic, making cloud services unavailable to real users.

Vulnerabilities in Application Programming Interfaces (APIs) — APIs are important for integrating user applications with cloud services, but poorly secured interfaces can be used to gain unauthorized control over data.

Insider threats: employees or partners with authorized access may accidentally or intentionally misuse their privileges, causing security breaches.

These risks show that traditional cybersecurity methods are not enough for modern cloud technologies. To make cloud-computing systems reliable and strong, groups and service providers are using a variety of enhanced cybersecurity strategies.

The most effective methods include:

Multi-Factor Authentication (MFA): requiring multiple ways to verify users, such as passwords combined with one-time codes, significantly reduces the risk of unauthorized access.

Data Encryption: encrypting sensitive data while it's being sent and when it's stored ensures that the data remains unreadable if intercepted.

Zero Trust Architecture: this approach assumes that no user or device is trustworthy, requiring every access attempt to be verified and granting only minimal necessary privileges.

• Regular Security Audits and Continuous Monitoring: Constantly checking user activity and system operations helps detect anomalies, weaknesses, and potential breaches early.

• Backup and Disaster Recovery Planning: Keeping secure backups of important data allows for quick restoration if there are cyberattacks or system failures.

Combining these practices creates a strong defense system that greatly reduces risk in cloud environments.

Cloud service providers (CSPs) are very important in keeping and advancing cybersecurity standards. They need to do more than just provide storage or computing power; they must also follow international rules like ISO/IEC 27001 and the General Data Protection Regulation (GDPR). These standards set clear rules for handling, storing, and protecting data.

Additionally, providers must deploy advanced incident response mechanisms, including automatic detection of suspicious behavior, rapid containment of compromised systems, and timely communication with clients. How transparent and reliable these providers are in their security practices greatly affects how much people trust cloud technologies.

The future of cybersecurity in cloud computing is closely tied to new technology. Artificial Intelligence (AI) and Machine Learning (ML) are already helping automated systems analyze large amounts of data and spot anomalies faster and more accurately than people are. For example, AI monitoring tools can detect unusual network patterns that might indicate a cyberattack.

Blockchain technology also offers promising applications because it is decentralized and secure, improving data verification, authentication, and logging of secure transactions. Moreover, quantum cryptography may change the field by providing encryption methods that are difficult to break.

Cybersecurity in cloud computing is complex and constantly changing, requiring coordinated efforts from users, groups, and service providers. People and businesses must use strong authentication methods, encryption practices, and continuous monitoring. Cloud service providers must follow international standards and use advanced systems for detecting and responding to threats.

To sum up, future progress will depend on integrating new technologies like AI, blockchain, and quantum cryptography into security systems. Combining these approaches will increase trust in cloud technologies, promote their use across sectors, and ensure a secure digital transformation of the global economy. Strong cybersecurity will not only lower the risks of cyberattacks but also support sustainable growth and innovation in the digital age.

References

1. ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection. International Organization for Standardization

2. European Union. General Data Protection Regulation (GDPR), Regulation (EU) 2016/679.

3. Cloud Security Alliance. Security Guidance for Critical Areas of Focus in Cloud Computing v4.0.

4. Zissis, D., & Lekkas, D. Addressing cloud computing security issues. Future Generation Computer Systems, 28(3), 583–592.

Юрій КІШІ
аспірант кафедри інформаційних управляючих систем та технологій
Ужгородський національний університет,
yurii.kish@uzhnu.edu.ua

Ігор ЛЯХ
доктор технічних наук, професор,
професор кафедри інформатики та фізико-математичних дисциплін,
Ужгородський національний університет,
igor.lyah@uzhnu.edu.ua

FUZZY LOGIC TECHNIQUES FOR MANAGING UNCERAINTY IN CYBERSECURITY

Fuzzy logic, as a mathematical framework for handling uncertainty and incomplete data, is widely applied in risk management processes where traditional binary models fail to adequately capture the multidimensional and subjective nature of expert evaluations. The methodological foundation of the approach proposed by Swarnakar et al. [4] lies in the enhancement of the classical Kano model. This concept is employed to generate fuzzy assessments of project priority and impact, corresponding to the threat ranking or response strategy selection phase in classical risk management systems. Formally, if X denotes the universe of possible values for a given criterion , then a fuzzy set A is defined as:

$$A = \{(x, \mu_A(x)) | x \in X\}, \quad (1)$$

where μA(x) is the membership function that reflects the degree of truth of the statement "x belongs to set A." This allows for the preservation of nuanced expert judgments and prevents information loss associated with rigid categorization.

Within the framework of the "Risk House" method [2], the construction of a knowledge base begins with the identification of potential risk sources (Ri) and their associated events or issues (Ej) that may arise during production or delivery processes. For each pair (Ri, Ej), importance indices are determined, taking into account both the probability of the risk event occurring and the magnitude of its impact on the overall system performance. Analytically, this can be represented as:

$$ARPI_i = \sum_{j=1}^{n} O_i \cdot S_j \cdot C_{ij}\,, \quad (2)$$

where ARPIi denotes the Aggregated Risk Priority Index for risk source i; Oj is the estimated probability of occurrence for event j; Sj is the severity rating of the consequences of event j; and Cjj is the correlation coefficient between risk source i and event j, reflecting the strength of their interdependence.

The structured logic of the "Risk House" facilitates the prioritization of response measures, focusing managerial resources on areas where risk mitigation yields the greatest impact.

The study by Gholami et al. [3] focuses on the development of a fuzzy multi-agent model for addressing cyber threats. The core of the model lies in representing process participants - such as stakeholders, organizational units, or system component as autonomous agents, each possessing distinct goals, constraints, and levels of risk perception. This approach enables the modeling of real-world scenarios in which input data may be incomplete, inconsistent, or inherently subjective.

Mathematically, the key element involves the use of fuzzy rules of the form:

$$R_k: if\ (x_1 \in A_1^k)\ and\ (x_2 \in A_2^k)\ and\ \ldots then\ (y \in B^k), \quad (3)$$

where xi denotes the input variables (e.g., resource availability level, risk intensity, environmental vulnerability); A_i^k represents fuzzy sets that define the linguistic values of these variables; y is the output variable; and B^k is the fuzzy set that characterizes the level of the output variable. A system of such rules constitutes the model's knowledge base, which underpins its decision-making mechanism.

The study by Masoomi et al. [1] presents an integrated approach that combines interval type-2 fuzzy logic with multi MCDM methods for risk management, enhanced by blockchain technology. The mathematical foundation of this approach involves representing each risk evaluation criterion as an interval type-2 fuzzy set with a membership function μ(x,u), where the variable u reflects the degree of variation in membership values between the upper and lower membership functions. For

each risk factor R_i, an interval of importance weights W_j is defined, incorporating fuzzy boundaries. The aggregated evaluation is expressed as:

$$S_i = \sum_{i=1}^{n} \widetilde{W}_i \otimes \tilde{R}_{ij}, \quad (4)$$

where S_i is the aggregated score of alternatives i; $\widetilde{W}_i$ is the interval fuzzy weight of criterion i; $\tilde{R}_{ij}$is the interval fuzzy rating of alternative j with respect to criterion i; and the symbol $\otimes$ denotes multiplication under interval fuzziness. It demonstrates that combining interval type-2 fuzzy logic with blockchain significantly improves the accuracy of risk prioritization under conditions of high uncertainty and fragmented information.

Fuzzy logic, in its various forms, from classical fuzzy sets to interval type-2 fuzzy logic serves as a powerful mathematical tool for risk assessment and management in contexts characterized by data incompleteness, imprecision, and subjectivity. Its application, in conjunction with structured risk source identification methods, modified prioritization models, multi-agent simulations, and decentralized data storage technologies, facilitates the integration of heterogeneous information, the modeling of complex system behavior, and the formulation of balanced decisions.

References

1. Behzad Masoomi, Seyed Pendar Toufighi, Hosein Arman, Seyedeh Elham Kamali, Jan Vang, Blockchain-enabled risk mitigation in green hydrogen supply chains: an interval type-2 fuzzy MCDM approach, Cleaner Logistics and Supply Chain, Volume 16, 2025, 100238, ISSN 2772-3909, https://doi.org/10.1016/j.clscn.2025.100238.
2. Fadhil Adita Ramadhan, Agus Mansur, Nashrullah Setiawan, Mohd Rizal Salleh, An analytical risk mitigation framework for steel fabrication supply chains using fuzzy inference and house of risk, Supply Chain Analytics, Volume 10, 2025, 100122, ISSN 2949-8635, https://doi.org/10.1016/j.sca.2025.100122.
3. Hadis Gholami, Amir Azizi, Majid Sabzehparvar, Davood Jafari, A fuzzy multi-agent model of project portfolio scheduling and selection taking into account environmental resilience, Results in Control and Optimization, Volume 19, 2025, 100544, ISSN 2666-7207, https://doi.org/10.1016/j.rico.2025.100544.
4. Vikas Swarnakar, Raed Jaradat, Malik Khalfan, Maher Maalouf, Abdelrahman E.E. Eltoukhy, Niamat Ullah Ibne Hossain, Sustainable project choice: Integrating Must-Be kano and fuzzy logic for optimal project selection, Journal of Open Innovation: Technology, Market, and Complexity, Volume 11, Issue 3, 2025, 100610, ISSN 2199-8531, https://doi.org/10.1016/j.joitmc.2025.100610.

Veronika KOLIUSHEVA
Bachelor's degree student (2nd year) majoring in Computer Engineering (Specialty 123), State University "Kyiv Aviation Institute"
9227354@stud.nau.edu.ua

Olena HURSKA
PhD (Pedagogy), Associate Professor of the Professional Foreign Languages Department, State University "Kyiv Aviation Institute",
olena.hurska@npp.kai.edu.ua

THE ROLE OF ARTIFICIAL INTELLIGENCE IN MODERN CYBERSECURITY

In the digital age, cybersecurity has become one of the most critical domains influencing the stability of financial systems, government operations, and daily routines. Our reliance on connected devices, online services, and data-driven systems has made us more open to cyberattacks, which are growing in number and getting more complex. Old ways of protecting data are not enough to handle the speed, extent, and sophistication of threats we see today. This challenge underlines the relevance of integrating artificial intelligence (AI) into cybersecurity systems. AI refers to the application of intelligent algorithms and machine learning techniques that allow systems to analyze massive datasets, detect anomalies, and adapt dynamically to emerging threats. The novelty of AI lies in its ability to learn autonomously, making cybersecurity tools more proactive, adaptive, and efficient. The objective of this research is to examine how AI transforms modern cybersecurity through automation, data-driven decision-making, and predictive analytics, while also evaluating the potential risks and ethical challenges associated with its implementation.

AI helps cybersecurity by automating tasks and constantly studying data to handle huge amounts of info and react to threats as they happen. Things like machine learning and neural networks help AI systems learn from what they see and get better over time. These tools are getting better at doing what traditional tools, like firewalls and antivirus tools do. They improve how well systems can adapt and spot dangers. AI systems can study how data moves across networks, find suspicious patterns, and take action even before people notice something's wrong. These systems guard data across different cloud setups, find odd actions, and tell cybersecurity teams about possible breaches. By joining automatic threat finding with human knowledge, we can cut down the time it takes to find and fix attacks, which makes everything more secure.

The application of AI in cybersecurity provides numerous operational benefits. It helps produce more exact and important threat warnings through risk studies done by AI. Automated systems can create summaries of what happened during an issue and fix threats on their own. This cuts down on the time it takes to look into and sort out problems by a lot. AI also makes it easier to check whom users are and control who gets access by looking at how people behave and how risky each login is. These systems make it easier for approved users to get in while still guarding against things like phishing, malware, and fraud. That lowers money losses and makes things easier for users. By always watching over big data streams and finding odd things, AI lets us defend ourselves before problems happen. It turns cybersecurity from just reacting to problems into a system that can guess what will happen and adapt to changes.

Nevertheless, adding AI to cybersecurity also means we have to deal with the dangers and weaknesses that come with automatic systems. Some big risks are data poisoning, where attackers put false data into AI training sets, which makes the AI make wrong guesses and miss threats. There are also prompt injection attacks, which use flaws in AI models to change their inputs. Adversarial attacks use slightly changed data to trick AI systems. Other dangers include stealing AI models, where someone takes or copies AI models, and password hacking, where machine learning helps speed up password guessing by figuring out common password patterns. In order to handle these issues, groups need to use strong data checks, encryption, and regular model testing. This will make sure that AI defenses are safe, private, and can bounce back from problems.

Besides the technical problems, using AI in cybersecurity brings up some big moral, legal, and management questions. Since AI systems handle sensitive and personal data, it is important to follow privacy rules and moral standards. Being clear about how AI makes choices, being fair in automatic risk tests, and taking responsibility for what AI does are important for keeping user trust and following the rules. Creating ways to explain how AI works will help make it clear how algorithms make security choices. It can reduce the black box problem where it is unclear how AI comes to a decision. In addition, experts in cybersecurity, lawmakers, legal experts, and moral thinkers need to work together. They can build responsible management systems together. If there is no clear responsibility and moral control, the tools made to protect us could end up hurting privacy or being misused by attackers.

Another emerging area of innovation is the integration of AI with other advanced technologies to strengthen cybersecurity ecosystems. When AI and blockchain work together, it makes sure that all cyber events are logged in a way that is clear and cannot be changed. This makes it easier to study what happened during an event and check everything. Moreover, when AI is used with the Internet of Things (IoT), it helps protect big sensor networks in real time by guessing where problems might happen before attackers can use them. Using AI with quantum computing is also a possible next step. It could lead to unbreakable encryption but also to faster decryption if someone misuses it. These combinations not only make AI defense systems better but also mean we need new ways to work together, set standards, and team up internationally on how to manage cybersecurity.

The human factor remains a vital component in AI-driven cybersecurity systems. Even though automation helps find and fix problems faster, people give important supervision, moral thinking, and understanding of situations that machines cannot copy. If we depend too much on AI, human experts might lose their skills. This could make it harder for them to carefully judge complex situations. Therefore, the best cybersecurity plan is to join human understanding with AI's ability to study data. Human experts should stay in charge of making choices. They can double-check what AI finds and make sure it lines up with goals and moral beliefs. In addition, as AI technologies get more common, groups should put money into training programs. These programs can train people who can understand, manage, and ethically control AI systems.

In conclusion, the integration of AI into cybersecurity operations has evolved from an optional improvement to a strategic necessity. Organizations that effectively implement AI-powered defense mechanisms gain a competitive advantage in identifying, mitigating, and preventing cyber threats. However, this integration demands thoughtful planning, ethical governance, data management expertise, and continuous optimization. As cyber threats get more complex, AI is not just something that makes systems better. It is a basic evolution of cybersecurity itself. The protection of digital systems will depend on how well smart machines and human experts can work together. Automation, moral behavior, and human thinking must come together to protect digital property and keep trust in the world of digital information.

References

1. AI in Cybersecurity: Key Benefits, Defense Strategies, & Future Trends. Official website. https://www.fortinet.com/resources/cyberglossary/artificial-intelligence-in-cybersecurity

2. Understanding the Role of Artificial Intelligence in Cybersecurity. Official website. https://www.legitsecurity.com/aspm-knowledge-base/role-of-ai-in-cybersecurity

3. Artificial Intelligence Cybersecurity. Official website. https://www.ibm.com/solutions/ai-cybersecurity

Viktoria SVIASTYN
Bachelor's degree student (2nd year)
majoring in Software Engineering (Specialty 121),
State University "Kyiv Aviation Institute"
9126220@stud.kai.edu.ua

Larysa TEREMINKO
PhD (Pedagogy), Associate Professor of the
Professional Foreign Languages Department,
State University "Kyiv Aviation Institute"
larysa.tereminko@npp.kai.edu.ua

THE ROLE OF MACHINE LEARNING IN PREVENTING DATA BREACHES

The importance of machine learning in protecting systems from data breaches is well known and established through numerous industry reports and research papers such as research paper where it was accurately predicted that Machine Learning (ML) will aid in protecting systems better in 2019 It is an open question whether the recently observed technical progress in machine-learning systems can be successfully leveraged to develop Operational Technology (OT) intrusion detection systems (IDSs) that can keep up with the evolving Industrial Internet of Things (IIoT) threat landscape.

The unprecedented proliferation of data breaches in the digital age calls for a more advanced protection system that is not only knowledge-based but also capable of continuous learning. Static rules-based traditional security solutions rarely detect sophisticated or zero-day exploit-type attacks. Machine learning (ML) techniques provide the advantage of real-time processing and prediction to deal with big data technology by leveraging adaptive, scalable, intelligent concepts that can comprehend huge volumes of data and detect aberrations that might result in threats in the future (Sommer & Paxson, 2010; Buczak & Guven, 2016).

One of the most important applications of ML is Anomaly Detection. Machine learning (ML) can be used to define expectations for regular users and network behavior, which, under normal circumstances, can be compared with login activity, data movement, user-shared files, etc., and used to build models. Then it applies these models to identify activities that deviate from this behavior, detecting anomalies such as logins from unusual locations, logins at odd times, large data transfers, use of unknown company resources, or opening unknown files. This technique has been successfully used to track insider threats and hijacked accounts (Chandola, Banerjee & Kumar, 2009).

The performance of supervised learning and deep learning algorithms was better than that of traditional filters for phishing and malware detection. For instance, convolutional neural networks (CNNs) and recurrent neural networks (RNNs) can extract highly discriminative features to detect malicious URLs, phishing emails, and malware signatures [HP20, AMW20].

Predictive analytics improves risk scores by correlating software weaknesses, system misconfigurations, and external threat intelligence. This facilitates proactive patching and targeted defensive strategies to prevent major data breaches (Batarseh & Yang, 2021; Sarker et al., 2020).

ML has also been used in critical infrastructure protection and securing IoT, e.g., recurrent neural networks - based intrusion detection systems to protect healthcare, energy, and transport systems (Almiani et al., 2020). Meanwhile, blockchain and ML are being investigated to enhance trust and transparency in digital security (Clarke & Knake, 2019).

Nonetheless, there are significant obstacles for ML in cybersecurity. ML models can also be manipulated by data poisoning and adversarial machine learning attacks, tricking them into misclassifying or failing to classify malicious activity (Biggio & Roli, 2018; Rigaki & Garcia, 2018). Also, dependence on ML has ethical and legal implications, especially concerning privacy, surveillance, and accountability (Brayne, 2020; Taddeo & Floridi, 2018; ENISA, 2021).

Conclusion. Machine learning is not a silver bullet but an essential part of cybersecurity. ML mitigates data breach risk and damage through enhanced anomaly detection, phishing protection, predictive analytics, and infrastructure defense. The next advances will thus come from increased

model robustness, the integration of AI tools with human expertise, and the assurance of ethical use. In doing so, ML bolsters digital trust and is a necessary safeguard for the security of individuals and organizations in an ever-more-connected world.

References

1. Batarseh, F., & Yang, R. (2021). AI and Big Data Analytics for Smart Generation. Artificial Intelligence Review. Springer.
2. Biggio, B., & Roli, F. (2018). Wild Patterns: Ten Years After the Rise of Adversarial Machine Learning. Pattern Recognition, V. 84, 317-331. DOI: 10.1016/j.patcog.2018.07.023
3. Brayne, S. (2020). Predict and Surveil: Data, Discretion, and the Future of Policing. Information Polity, V. 26(3), 327-330. DOI: 10.3233/IP-219008
4. Buczak, F. L., Guven, E. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," in IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 1153-1176. DOI: 10.1109/COMST.2015.2494502.
5. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly Detection: A Survey. ACM Computing Surveys (CSUR), V. 41 (3), 1-58. DOI: 10.1145/1541880.1541882
6. Huang, W., Xu, F., & Gu, Q. (2020). Phishing URL Detection via CNN and Attention-Based Hierarchical RNN. Appl. Sci.,11(19), 9210. https://doi.org/10.3390/app11199210
7. Sarker, I. H., et al. (2020). Cybersecurity Data Science: An Overview from a Machine Learning Perspective. Journal of Big Data, V. 7(1). DOI: 10.1186/s40537-020-00318-5

Юлія СОКАЛ
здобувач вищої освіти другого (магістерського) ступеня,
1 курсу, спеціальності F5 «Кібербезпека та захист інформації»,
Державний університет «Київський авіаційний інститут»
sokalulia8@gmail.com

Наталя БІЛОУС
кандидат педагогічних наук, доцент кафедри
іноземних мов професійного спрямування,
Державний університет «Київський авіаційний інститут»
natalia.bilous@npp.kai.edu.ua

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ВИЯВЛЕННЯ КІБЕРЗАГРОЗ У МАЛИХ ОРГАНІЗАЦІЯХ

Малі підприємства становлять значну частку бізнесів в Україні, але більшість з них не мають спеціалістів з кібербезпеки та користуються застарілим програмним забезпеченням. Це підвищує ризик кібератак. За даними IBM X Force Threat Intelligence Index значна частина атак у світі здійснюються на малий та середній бізнес (IBM, 2024). Найпоширеніші загрози: фішинг, ransomware, атаки через соціальну інженерію, шкідливе програмне забезпечення та атаки на віддалений доступ. Навіть малі підприємства, які зберігають важливі дані на локальних серверах чи в хмарних сховищах без належного захисту, часто зазнають суттєвих фінансових збитків.

Традиційні методи захисту, такі як фаєрволи або антивіруси, не забезпечують постійний моніторинг та реагують лише на відомі загрози. Для малих організацій часто економічно не вигідно утримувати фахівця з кібербезпеки. Через це виникає потреба в таких технологіях, які автоматично аналізують підозрілу активність та повідомляють про потенційну загрозу в реальному часі.

Метою є продемонструвати, як штучний інтелект (ШІ, AI) може підвищити рівень безпеки в малих організаціях та зробити це ефективно та економічно доступно. Штучний інтелект у сфері кібербезпеки дозволяє автоматично виявляти, аналізувати та нейтралізувати загрози, зменшуючи залежність від людського фактора (NIST, 2023). Впровадження ШІ-рішень дозволить зменшити середній час виявлення загроз, що підвищить швидкість реагування навіть без участі спеціалістів з кібербезпеки. Для малих компаній це єдиний реальний спосіб отримати ефективний захист без значних фінансових витрат.

Наукова новизна полягає у використанні легких та пояснюваних моделей ШІ (Explainable Lightweight AI), які здатні працювати на стандартних робочих станціях і ефективно виявляти невідомі атаки за допомогою поведінкового аналізу та постійного самонавчання (Rahmati, 2025; Salem et al., 2024). На відміну від класичних систем захисту, які реагують лише на відомі загрози, такі моделі здатні передбачати потенційні атаки та адаптуватися до нових сценаріїв. Сучасні підходи дозволяють впроваджувати ШІ-модулі в наявну IT-інфраструктуру без значних змін у бізнес-процесах (NIST, 2023; Kulothungan, 2025).

Є три основні напрями використання ШІ для малих організацій. Перший – аномалійний аналіз, він дозволяє виявляти нетипову поведінку користувачів і процесів у мережі, що може свідчити про несанкціонований доступ або внутрішні загрози (Rahmati, 2025). Другий – обробка природної мови (NLP), що автоматично розпізнає фішингові листи, попереджаючи про потенційну шкоду (Salem et al., 2024). Третій – генеративні моделі (Generative AI), які прогнозують потенційні сценарії атак, імітуючи поведінку зловмисників, що дозволяє проактивно реагувати (AegisShield, 2025).

Практична інтеграція систем здійснюється через відкриті платформи, такі як TensorFlow Lite, SecurityBERT та Snort AI Module. Використання ШІ дозволяє автоматизувати аналіз подій у мережі, зменшити навантаження на персонал і підвищити ефективність реагування (Salem et al., 2024).

Застосування ШІ дозволяє малим організаціям прогнозувати потенційні атаки на основі поведінкових моделей, автоматично реагувати на підозрілі дії користувачів, інтегрувати захисні алгоритми без значних витрат на додаткове обладнання та підвищувати довіру клієнтів і партнерів.

Штучний інтелект забезпечує проактивний, автономний та економічний захист малих підприємств, підвищує точність виявлення загроз, мінімізує людські помилки та створює цифрову стійкість бізнесу. Легкі та пояснювані моделі ШІ роблять технології доступними навіть для компаній з обмеженим бюджетом. Використання штучного інтелекту формує основу нової стратегії безпеки – автоматизованої, навчальної та адаптивної, що гарантує стабільність і конкурентоспроможність підприємств у цифровому середовищі.

Список використаних джерел

1. AegisShield, 2025. Democratizing Cyber Threat Modeling with Generative AI. [arXiv]. Доступно за посиланням: https://arxiv.org/pdf/2509.10482.
2. IBM, 2024. IBM X Force Threat Intelligence Index 2024.
3. Kulothungan, V., 2025. Securing the AI Frontier: Urgent Ethical and Regulatory Imperatives for AI-Driven Cybersecurity. [arXiv]. Доступно за посиланням: https://arxiv.org/pdf/2501.10467.
4. NIST, 2023. Artificial Intelligence Risk Management Framework (AI RMF 1.0). Доступно за посиланням: https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.
5. Rahmati, M., 2025. Towards Explainable and Lightweight AI for Real-Time Cyber Threat Hunting in Edge Networks. [arXiv]. DOI: 10.48550/arXiv.2504.16118. Доступно за посиланням: https://arxiv.org/pdf/2504.16118.
6. Salem, A.H., et al., 2024. Advancing Cybersecurity: A Comprehensive Review of AI-Driven Approaches to Threat Detection. Journal of Big Data, SpringerOpen. DOI: 10.1186/s40537-024-00957-y.

Костянтин ГЕШУР
здобувач другого(магістерського) рівня вищої освіти
факультету інформаційних технологій
ДВНЗ «Ужгородський національний університет»
kostya.heshur@gmail.com

Володимир НІКОЛЕНКО
кандидат фізико-математичних наук, доцент кафедри
інформаційних управляючих систем та технологій,
ДВНЗ «Ужгородський національний університет»
volodymyr.nikolenko@uzhnu.edu.ua

МЕТОДИ МАШИННОГО ЗОРУ ДЛЯ РОЗПІЗНАВАННЯ АВІАЦІЙНОЇ ТЕХНІКИ

Розпізнавання авіаційної техніки за зображеннями дозволяє ідентифікувати літаки, аналізувати знімки авіабаз та аеропортів, тощо. Актуальність цієї теми особливо зростає в умовах бойових дій, коли необхідна швидка й точна обробка великих масивів даних, включно із супутниковими знімками.

Метою даної статті є демонстрація роботи розробленої системи розпізнавання авіаційної техніки: від створення моделі до її інтеграції в телеграм-бот.

Через специфіку роботи було неможливо знайти підходящий датасет. У зв'язку з цим було сформовано власний датасет, який містив у собі 370 зображень літаків(Ту-95, Ту-22, Ту-160, Су-30, А-50, Су-34, Су-35, Су-25, Су-57, Міг-31, Су-24). Датасет містить зображення перерахованих літаків з різних ракурсів: із супутника, із землі, у повітрі. Анотація даних виконана за допомогою платформи Roboflow. Roboflow — це онлайн-платформа для роботи з комп'ютерним зором. Вона допомагає розробникам і дослідникам швидко підготувати та використати датасети для навчання моделей машинного навчання. Після анотації даних потрібно виконати розподіл даних на вибірки. За допомогою інструментів платформи дані були розділені на 3 вибірки - навчальна(70%), валідаційна(20%), тестова(10%). Поділ даних відбувався за допомогою алгоритма Random Split.

Для безпосереднього розпізнавання та класифікації об'єктів була використана модель YOLO (You Only Look Once) — сучасний алгоритм детекції, який дозволяє знаходити та класифікувати об'єкти на зображеннях. Його ключова перевага полягає в тому, що аналіз виконується за один прохід нейронної мережі, що забезпечує високу швидкість та ефективність обробки навіть великих масивів даних. Проте даний підхід має і певні недоліки - недостатня точність класифікації для невеликих об'єктів на зображеннях та необхідність великих датасетів для створення моделей високої точності. Загалом моделі типу YOLO працюють наступним чином:

1. Вхідне зображення розділяють на сітку комірок (наприклад, 10x10). Кожна комірка відповідає за виявлення об'єктів, центр яких знаходиться в цій комірці.

2. Для кожної комірки сітки YOLO прогнозу кілька обмежувальних рамок, кожна з яких має показник достовірності, що вказує на ймовірність присутності об'єкта в цій рамці та на те, наскільки добре рамка відповідає об'єкту. Показник, що вказує на ймовірність того, що обмежувальна рамка містить будь-який об'єкт. Ймовірності класу: Ймовірності для кожного можливого класу об'єктів (наприклад, автомобіль, людина, собака) в межах цієї обмежувальної рамки.

3. Після початкових прогнозів NMS застосовується для фільтрації надлишкових та перекриваючих обмежувальних рамок. Якщо кілька обмежувальних рамок виявляють один і той самий об'єкт, NMS вибирає ту з найвищим показником достовірності та пригнічує інші.

Після тренування моделі було оцінено її параметри. Для аналізу було визначено 2 ключові параметри: тоочність (precision) та повнота(recall).

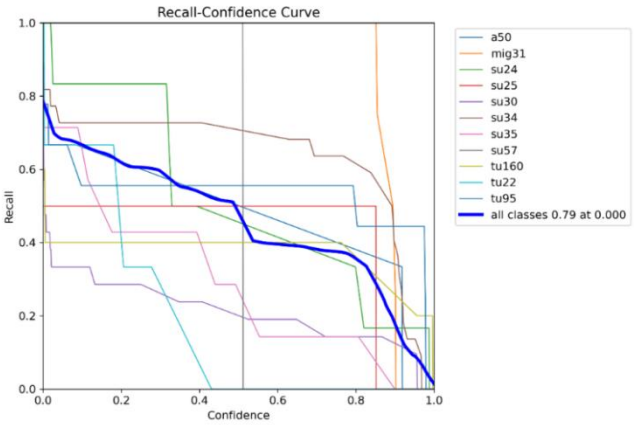


Рис.1. Повнота моделі

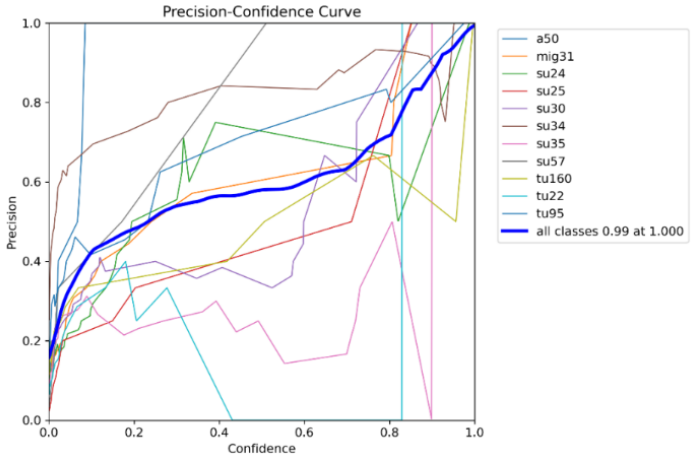


Рис.2. Точність моделі

Після тренування та оцінки моделі, використовуючи біблотку Telebot створено телеграм-бот, який буде відповідати за взаємодію між користувачем та моделлю. Також було використано бібліотеки numpy, OpenCV, Ultralytics, Pandas. Власне логіка роботи бота полягає у тому, що бот очікує від користувача медіафайл, після отримання файла фото зберігається у відведеній папці та чекає на подальші запити користувача. Користувач може обрати 2 типа детекції - стандартна детекція, яка розпізнає всі можливі літаки та детекція за параметрами(мінімальна точність, клас літака). Після вибору типу детекції відбувається розпізнавання літаків, та користувач отримує оброблене зображення з виявленими літаками.

Рис.3. Кінцевий результат роботи системи

За результатами роботи створено кастомний датасет із зображеннями відповідних літаків, який в подальшому став основою для YOLO-моделі. Моделі типу YOLO показали високу гнучкість та точність в процесі навчання та тестування та підтвердили свою надійність у системах класифікації об'єктів.

Список використаних джерел та літератури

1. OpenCV (n.d.). Deep Neural Network (dnn) module. [online] Available at: https://docs.opencv.org/4.x/d6/d0f/group__dnn.html [Accessed 22 Sep. 2025].
2. Roboflow (n.d.). Roboflow Documentation. [online] Available at: https://docs.roboflow.com/ [Accessed 18 Sep. 2025].
3. TeleBot (n.d.). TeleBot Documentation. [online] Available at: https://docs.opencv.org/4.x/d6/d0f/group__dnn.html [Accessed 18 Sep. 2025].
4. Ultralytics (n.d.). Ultralytics Documentation. [online] Available at: https://docs.ultralytics.com/ [Accessed 18 Sep. 2025].

Василь МОРОХОВИЧ
доцент кафедри інформатики та фізико-математичних дисциплін
ДВНЗ «Ужгородський національний університет»
vasyl.morokhovych@uzhnu.edu.ua

Марія КАШКА
доцент кафедри туризму
ДВНЗ «Ужгородський національний університет»
mariia.kashka@uzhnu.edu.ua

ІНФОРМАЦІЙНО-ТЕХНОЛОГІЧНІ ІНСТРУМЕНТИ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ТУРИСТІВ

На сьогодні туристична індустрія є однією з найдинамічніших і найвпливовіших галузей світової економіки. Однак, її стабільний розвиток безпосередньо залежить від рівня безпеки та комфорту для мандрівників. Глобалізація, зростання геополітичної нестабільності, епідемічні загрози та кіберзлочинність створюють нові, складніші виклики, які вимагають інноваційних підходів до захисту туристів. Традиційні методи забезпечення безпеки вже не є достатньо ефективними в умовах цифрової трансформації суспільства. Саме тому на перший план виходять інформаційно-технологічні інструменти, які здатні не лише оперативно реагувати на загрози, а й прогнозувати їх, мінімізуючи ризики для мандрівників. Метою роботи є аналіз ролі та потенціалу сучасних ІТ-рішень у підвищенні рівня безпеки в туризмі, а також ідентифікація основних викликів, пов'язаних з їх впровадженням.

Одним із ключових аспектів застосування інформаційних технологій є створення систем, що забезпечують постійний моніторинг ситуації в реальному часі. Системи геолокації та GPS-трекінгу, інтегровані в мобільні додатки та смарт-пристрої, дозволяють туристичним операторам і місцевим службам безпеки відстежувати місцезнаходження туристів, що є критично важливим у разі надзвичайних ситуацій, таких як стихійні лиха або терористичні загрози.

Системи аналізу великих даних (Big Data) відіграють центральну роль у прогнозуванні ризиків. Шляхом аналізу даних з різних джерел – соціальних мереж, новинних агентств, метеорологічних служб, політичних звітів – алгоритми можуть виявляти аномалії та тенденції, що вказують на потенційну загрозу. Наприклад, різке зростання кількості негативних відгуків або обговорень певного місця в соціальних мережах може бути сигналом про погіршення криміногенної ситуації. На основі цих даних можуть бути сформовані автоматичні попередження для туристів, що перебувають у зоні ризику, або для тих, хто лише планує подорож.

Зростання обсягів онлайн-бронювань та електронних платежів робить туристичну сферу вразливою до кіберзлочинів. Інформаційні технології є єдиним ефективним засобом захисту персональних даних туристів – від паспортних даних до фінансової інформації. Використання сучасних протоколів шифрування, багатофакторної аутентифікації та систем виявлення вторгнень (IDS/IPS) стає обов'язковим стандартом для туристичних платформ. Штучний інтелект (ШІ) використовується для аналізу поведінкових патернів і виявлення підозрілих транзакцій, що допомагає запобігти шахрайству.

Також слід зазначити, що концепція «розумних міст» активно впроваджується в туристичну інфраструктуру. Інформаційні технології в таких містах об'єднуються в єдину мережу, що дозволяє централізовано управляти безпекою. Наприклад, системи відеоспостереження з функцією розпізнавання обличчя можуть допомогти у пошуку зниклих людей або ідентифікації злочинців. Датчики, встановлені на об'єктах інфраструктури, можуть контролювати якість повітря, рівень шуму або стан доріг, що також впливає на безпеку та комфорт туристів. Крім того, інтелектуальні системи можуть надавати персоналізовані рекомендації щодо безпечних маршрутів, ґрунтуючись на поточній ситуації в місті.

Отже, інформаційно-технологічні інструменти є не просто допоміжним засобом, а фундаментальною основою сучасної системи безпеки в туризмі. Вони дозволяють перейти від реактивних методів реагування до проактивного управління ризиками. Застосування Big Data,

ШІ, IoT та мобільних додатків значно підвищує рівень захисту мандрівників, оптимізує роботу служб безпеки та створює більш надійне туристичне середовище. Однак, впровадження цих технологій супроводжується низкою викликів. Серед них – етичні аспекти, пов'язані з використанням персональних даних, необхідність уніфікації стандартів безпеки, висока вартість технологічних рішень та потреба у кваліфікованих кадрах для їх обслуговування. Подальші дослідження мають бути зосереджені на розробці збалансованих моделей, які б поєднували технологічні інновації з принципами приватності та етики. Зрештою, успішне використання ІТ-інструментів для забезпечення безпеки не лише захистить туристів, але й стане ключовим конкурентним перевагою для туристичних дестинацій у майбутньому.

Список використаних джерел

1. Омельчак Г. Цифрова доступність при формуванні безбар'єрного середовища в туризмі, International Science Journal of Management, Economics & Finance. 2024. 3 (2). С.46-55.
2. Цепенда М.М., Бурка В.Й. Інформаційні системи, комунікації і технології у туристичній індустрії: навч. посіб. Чернівці, 2024. 176 с.

Daria HURTOVA
Bachelor's degree student (2nd year)
majoring in Software Engineering (Specialty 121),
State University "Kyiv Aviation Institute"
9216651@stud.kai.edu.ua

Hanna SOROKUN
Senior Lecturer of the
Professional Foreign Languages Department,
State University "Kyiv Aviation Institute"
hanna.sorokun@npp.kai.edu.ua

EVOLVING SECURITY PARADIGMS: HOW AI TRANSFORMS THREATS AND DEFENSES

Artificial intelligence continues to reshape security landscapes around the world, enabling systems that are more adaptive, predictive, and efficient than ever before. In recent months, several breakthroughs have highlighted both the opportunities and fresh threats posed by AI in the security domain. One unexpected vulnerability discovered in ChatGPT's Deep Research agent, known as "ShadowLeak," allows attackers to siphon sensitive information without any visible user interaction. This zero-click, server-side flaw underscores the fact that AI tools themselves can be weak links in enterprises' security posture.

At the same time, generative AI attacks are accelerating at an alarming rate. A Gartner report from September 2025 found that 29% of organizations experienced attacks targeting their AI application infrastructure within the past year. Deepfake incidents – through audio, voice biometric spoofing, or video – are growing in prevalence, introducing new vectors for disinformation and fraud.

Another concern is that malware is now being developed that can evade even advanced protection tools. In one experiment, a malware strain trained via reinforcement learning managed to bypass Microsoft Defender's security checks around 8% of the time after only three months of training, using a relatively small budget. This kind of AI-generated malware shows attackers' growing ability to automate and refine their methods very quickly.

On the defense side, there are some promising developments. In Ukraine, for example, the Institute for Information Registration Problems is building an AI/ML-based system to assess the combat effectiveness of units in real time, forecast outcomes, and support decision-making under pressure. Ukraine's military AI ecosystem has also benefitted from a large number of companies and academic programs: over 243 AI-focused companies, more than 307,000 specialists in IT and software, and 106 AI/ML academic programs across 42 higher education institutions. Despite infrastructural and resource challenges, such numbers show strong local capacity and commitment.

There is also innovation in defense technologies for battlefield intelligence. A Ukrainian-Estonian firm, Farsight Vision, develops hardware and software that use UAV imagery, 3D terrain modelling, and geospatial analysis to feed actionable data to Ukrainian security services. These systems are deployed by the Armed Forces, National Guard, police, and border guard. This shows how AI combined with remote sensing can enhance situational awareness even under difficult conditions.

Another technical advance addresses adversarial machine learning: researchers proposed a defense using explainable AI (XAI) for behavior-based authentication. In this approach, the system filters out the features most vulnerable to adversarial attacks, retaining those more robust and relevant for genuine authentication. This results in improved resistance to adversarial manipulation.

These developments point to a security domain in transition. Outdated playbooks are being challenged. For example, traditional identity and access management systems are struggling with "agent sprawl" — the proliferation of AI agents operating across systems often without centralized governance. Some companies are now embedding identity security protocols directly into AI agent frameworks to maintain control, visibility, and risk oversight.

The recent period has shown that AI's role in security is more complex than ever: it offers powerful

tools for defense but also opens novel threat vectors that can be highly automated, stealthy, and adaptable. For those who design, deploy, or manage security systems, several implications are clear. First, protecting AI systems themselves is as important as using AI defensively. Vulnerabilities such as server-side flaws, model evasion, and adversarial attacks are no longer hypothetical. Second, monitoring, governance, and transparency must be built into AI tools from the start, not appended later. Explainability, oversight, and rigorous testing against adversarial scenarios are essential. Third, local, real-world deployments (as in Ukraine) illustrate that combining AI with good data, institutional capacity, and domain-specific hardware/software gives significant leverage. Finally, strategic cooperation – across sectors (industry-academic-government), across borders, and with shared threat intelligence – is necessary to keep pace with evolving AI threats. Without such cooperation, tools and systems risk being outmatched by malicious actors who are increasingly able to use AI to outthink, outpace, and outmaneuver traditional defenses.

References

1. CSIS. Understanding the Military AI Ecosystem in Ukraine. (2024). https://www.csis.org/analysis/understanding-military-ai-ecosystem-ukraine
2. Institute for Information Registration Problems of NAS of Ukraine. Artificial Intelligence for the State's Defense Capability: An Innovative Combat Capability Analysis System for the Armed Forces of Ukraine. (2024). https://www.ipri.kiev.ua/en/en-events/artificial-intelligence-for-the-states-defense-capability-an-innovative-combat-capability-analysis-system-for-the-armed-forces-of-ukraine
3. ITPro. Generative AI attacks are accelerating at an alarming rate. (2025). https://www.itpro.com/security/generative-ai-attacks-are-accelerating-at-an-alarming-rate
4. TechRadar. AI security is identity security: How Okta is weaving agents into the security fabric. (2025). https://www.techradar.com/pro/security/ai-security-is-identity-security-how-okta-is-weaving-agents-into-the-security-fabric
5. Wikipedia. Farsight Vision. (2025). https://en.wikipedia.org/wiki/Farsight_Vision
6. Windows Central. AI-powered malware eludes Microsoft Defender’s security checks 8 percent of the time. (2025). https://www.windowscentral.com/artificial-intelligence/ai-powered-malware-eludes-microsoft-defenders-security-checks-8-percent

Денис РОЗЕНВАССЕР
к.т.н., доцент,
Міжнародний гуманітарний університет
denysrozenvasser@gmail.com

Борис ГОРДЄЄВ
студент, 2 курс, магістратура
спеціальність 125 Кібербезпека та захист інформації
Міжнародний гуманітарний університет
borisgordeev2023@gmail.com

Вадим ВИСОЦЬКИЙ
студент, 2 курс, магістратура
спеціальність 172 Електронні комунікації та радіотехніка
Міжнародний гуманітарний університет
vadyanb@gmail.com

ОЦІНКА ВИКОРИСТАННЯ ЗАВАДОСТІЙКИХ КОДІВ У ШТРИХКОДАХ

Завадостійкі коди відіграють ключову роль у забезпеченні надійності штрихкодів, дозволяючи виявляти та виправляти помилки, спричинені пошкодженнями або шумом. Завадостійкі коди забезпечують фундаментальний рівень надійності, який є необхідною передумовою для застосування цифрових технологій та ШІ у сфері безпеки та простежуваності. Серед найпоширеніших таких кодів – коди Ріда-Соломона (РС) та Хеммінга, які інтегруються в формати на кшталт QR-кодів, Data Matrix та PDF417. Мета їх використання полягає в захисті даних від дефектів друку, забруднень чи механічних ушкоджень. У QR-кодах, наприклад, існують різні рівні корекції помилок: low (L), medium (M), quartile (Q) та high (H), які дозволяють адаптувати код до конкретних умов експлуатації.

Таблиця 1. Порівняння рівнів корекції помилок у QR-кодах

Рівень	Відсоток корекції	Вплив на розмір	Типове застосування
L	до 7%	Найменший	Бізнес-картки, деформації малоймовірні
M	до 15%	Середній	Роздрібна торгівля, загальне використання
Q	до 25%	Великий	Логістика, продукти з можливими пошкодженнями
H	до 30%	Найбільший	Промисловість, суворі умови, наклейки на зовнішнє пакування

Принцип роботи завадостійких кодів базується на додаванні надлишкової інформації, що дає змогу відновлювати оригінальні дані навіть при частковому пошкодженні. Виявлення помилок здійснюється за допомогою контрольних сум та перевірки парності, що є базовим механізмом. Корекція помилок передбачає використання математичних алгоритмів для реконструкції втрачених частин. Переваги таких кодів очевидні: вони підвищують ймовірність успішного зчитування штрихкодів у реальних умовах, наприклад, на складах чи в логістиці. Зменшення помилок при скануванні сприяє ефективності процесів ідентифікації товарів. Крім того, завадостійкі коди дозволяють зберігати більший обсяг даних у компактному форматі без втрати надійності. Однак, існують і обмеження: додавання надлишкової інформації збільшує розмір штрихкоду, що може бути проблемою для обмеженого простору. При значних пошкодженнях, які перевищують рівень корекції, відновлення стає неможливим. Вимоги до якості сканерів та алгоритмів декодування також зростають, що ускладнює впровадження в бюджетних системах. Оцінка ефективності завадостійких кодів проводиться за критеріями, такими як ймовірність помилки зчитування, відсоток успішного зчитування та швидкість декодування. Ймовірність помилки зчитування для кода Ріда-Соломона оцінюється за виразом:

$$p_{\text{РС}}(h_b) = \sum_{q=q_{\text{вип}}+1}^{n} C_n^q \cdot p^q \cdot (1-p)^{n-q}$$

де C_n^q – кількість комбінацій (сполучень) з n по q, $q_{\text{вип}}$ – кількість виправлених помилок, а p – ймовірність помилки в результаті дії зовнішніх факторів.

Важливо враховувати стійкість до різних типів пошкоджень, наприклад, подряпин, забруднень чи деформацій. Порівняння форматів штрихкодів показує, що QR-коди з високим рівнем корекції перевершують традиційні лінійні штрихкоди в завадостійкості. Умови експлуатації (освітлення), матеріал носія та тип сканера, суттєво впливають на результати. Сучасні тенденції включають інтеграцію завадостійких кодів з технологіями машинного зору та штучного інтелекту для покращення зчитування.

Рисунок 1. Пошкоджені QR-коди, що підлягають зчитуванню

З рисунка 1 видно, що значно пошкоджені QR-коди (зміна яскравості, стирання, написи) можна розпізнати завдяки використанню завадостійкого кодування.

Розвиток нових форматів штрихкодів спрямований на підвищення стійкості без значного збільшення розміру. У сферах з високими вимогами до надійності, таких як медицина, логістика та авіація, ці коди є незамінними. Подальші дослідження фокусуються на оптимізації алгоритмів корекції та адаптації до нових технологій сканування.

Висновок: завадостійкі коди значно підвищують надійність штрихкодів, але вимагають балансу між обсягом даних і рівнем стійкості. Їх використання дозволяє мінімізувати ризики в критичних системах. Загалом, оцінка показує, що переваги переважують недоліки в більшості застосувань. Майбутні перспективи включають комбінацію з IoT для реального часу моніторингу. Таким чином, завадостійкі коди є фундаментом сучасних систем ідентифікації.

Список використаних джерел

1. Siim Tiigimägi. Static vs Dynamic QR Codes: Key Differences. URL: https://pageloot.com/uk/qr-code-marketing/static-vs-dynamic-qr-codes/
2. Tobias Funke. Data Matrix vs. QR Codes: An Overview of the Differences. Jul 18, 2025. URL: https://www.qr-code-generator.com/blog/data-matrix-vs-qr-codes/
3. What Is the Difference Between 1D and 2D Barcode Scanning? Sep 10, 2025. URL: https://lowrysolutions.com/blog/what-is-the-difference-between-1d-and-2d-barcode-scanning/
4. Про що нам говорять штрих-коди? 30 січня 2018
5. Головне управління Держпродспоживслужби в Хмельницькій області. URL: https://consumerhm.gov.ua/544-pro-shcho-nam-govoryat-shtrikh-kodi
6. У чому різниця між кодами Data Matrix і QR-кодом. 12 жовтня 2023. URL: https://domino-kiev.com.ua/news/u-chomu-riznitsya-mizh-kodami-data-matrix-i-qr-kodom

Назар-Олексій УМАНЦІВ
здобувач другого (магістерського) рівня вищої освіти
факультету інформаційних технологій
ДВНЗ «Ужгородський національний університет»
umantsiv.nazar@student.uzhnu.edu.ua

Володимир НІКОЛЕНКО
кандидат фізико-математичних наук, доцент кафедри
інформаційних управляючих систем та технологій,
ДВНЗ «Ужгородський національний університет»

АВТОМАТИЗОВАНА КЛАСИФІКАЦІЯ РЕНТГЕНІВСЬКИХ ЗНІМКІВ ЛЕГЕНЬ НА ОСНОВІ RESNET-18 ЯК ІНСТРУМЕНТ МЕДИЧНОЇ БЕЗПЕКИ

Захворювання легень, зокрема туберкульоз, пневмонія та рак легень, становлять серйозну глобальну загрозу для здоров'я. Щорічно ці хвороби уражають мільйони людей і спричиняють мільйонні втрати життя. Так, у 2021 році на туберкульоз захворіли понад 10 млн осіб, з яких 1,6 млн померли. Пневмонія стабільно входить до п'ятірки провідних причин смертності у світі, особливо серед дітей та літніх людей, а рак легень є найлетальнішим видом раку, з близько 1,8 млн смертей у 2020 році. Вчасна діагностика цих хвороб критично важлива для ефективного лікування та стримування поширення. Однак традиційні методи діагностики (наприклад, оцінка рентгенівських знімків лікарем) обмежені людським фактором: нестача кваліфікованих радіологів, суб'єктивність оцінок та час, потрібний на аналіз великої кількості знімків. У кризових ситуаціях, як-от пандемія COVID-19, ці обмеження особливо відчутні – системи охорони здоров'я перевантажені, а швидкість ухвалення рішень стає питанням безпеки громадського здоров'я. Пандемія продемонструвала, що розробка засобів автоматизованої, швидкої діагностики має бути пріоритетом міжнародного співробітництва у сфері медичної безпеки.

Метою даної роботи є підвищення ефективності раннього виявлення легеневих захворювань шляхом розробки інтегрованої системи діагностики, що поєднує аналіз медичних зображень та анкетних даних на основі методів глибокого навчання. Задача полягала у створенні модуля автоматичної класифікації рентгенівських знімків грудної клітки з використанням глибокої нейронної мережі ResNet-18, а також додаткового модуля для оцінки ризику раку легень за допомогою опитувальників. Актуальність роботи зумовлена нагальною потребою в прискоренні та підвищенні точності діагностики інфекційних і онкологічних захворювань легень. Своєчасний скринінг та виявлення хворих дає змогу вжити заходів ізоляції і лікування, що є важливим аспектом безпеки охорони здоров'я населення.

Запропонована система складається з двох незалежних модулів, що поєднують сучасні моделі глибинного навчання та класичного ML. Перший модуль виконує аналіз рентгенограм легенів за допомогою згорткової нейромережі ResNet-18 – архітектури із 18 шарів з резидуальними зв'язками, які полегшують навчання глибоких моделей. Попередньо натреновану на ImageNet модель ResNet-18 донавчено для класифікації знімків грудної клітки на чотири класи: NORMAL (здорові), PNEUMONIA (пневмонія), TUBERCULOSIS (туберкульоз) та UNKNOWN (аномальні/немедичні зображення). Вибірка даних для навчання складалася з декількох тисяч знімків, збалансованих між цими класами. Перед навчанням всі зображення приведено до розміру 224×224 пікселів та трьохканального формату; застосовано аугментацію даних (випадкове горизонтальне віддзеркалення, обертання) для підвищення стійкості моделі. Навчання проводилося із використанням оптимізатора Adam (α=1e-4). Якість класифікації оцінювалася за точністю (precision), повнотою (recall), F1-мірою та загальною точністю (accuracy). Модель ResNet-18 продемонструвала високу ефективність: загальна точність на тестовому наборі (1527 зображень) склала 97,6%, при цьому F1-міри для класів PNEUMONIA та TUBERCULOSIS досягли 0,98, для NORMAL – 0,97. Клас UNKNOWN визначався без помилок (F1=1,0), що підтверджує здатність мережі розпізнавати нетипові випадки. Другий модуль здійснює оцінку ризику раку легень на основі 15-пунктового опитувальника (вік,

шкідливі звички, симптоми тощо). Реалізовано кілька алгоритмів класифікації (логістична регресія, наївний байєс, XGBoost), серед яких найвищу точність (91%) показав наївно-байєсівський класифікатор, дещо випередивши логістичну регресію (87,5%) і бустинг XGBoost (85,7%). Система реалізована мовою Python із використанням бібліотек PyTorch (torchvision), scikit-learn, NumPy, Pandas тощо. Для інтерактивної взаємодії користувача створено веб-додаток на базі фреймворку Streamlit: користувач може завантажити знімок для автоматичного аналізу або заповнити форму для отримання прогнозу; передбачено двомовний інтерфейс (українською та англійською) та можливість контейнерного розгортання за допомогою Docker.

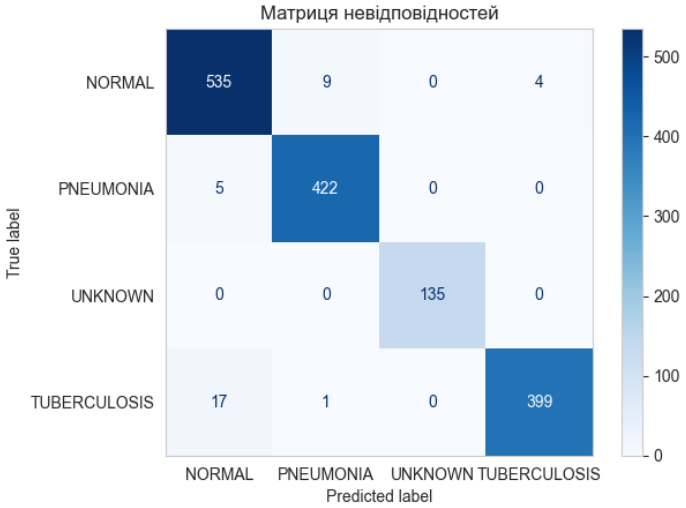


Рис. 1. Матриця невідповідностей для моделі ResNet-18 на тестовій вибірці.

Розроблений прототип інтегрованої системи автоматизовано аналізує як медичні зображення, так і анкети пацієнтів, демонструючи високу результативність застосування ШІ для ранньої діагностики легеневих захворювань. Такий комплексний підхід може слугувати у майбутньому ефективним інструментом скринінгу, підвищуючи об'єктивність і швидкість діагностики, зменшуючи ймовірність пропуску патологій та сприяючи своєчасному лікуванню. Подальший розвиток системи передбачає розширення датасетів і удосконалення моделей для підвищення її універсальності та надійності.

Список використаних джерел

1. Bush, A. & Waterer, G. (2024). World Pneumonia Day: Why Do We Still Need It? American Journal of Respiratory and Critical Care Medicine, 210(11), 1297–1299. DOI: 10.1164/rccm.202410-1883VP.

2. Hammoudi, K., Benhabiles, H., Melkemi, M., et al. (2021). Deep Learning on Chest X-ray Images to Detect and Evaluate Pneumonia Cases at the Era of COVID-19. Journal of Medical Systems, 45(7): 75. DOI: 10.1007/s10916-021-01745-4.

3. Hasan, M.R., Ullah, S.M.A., Rabiul Islam, S.M. (2024). Recent Advancement of Deep Learning Techniques for Pneumonia Prediction from Chest X-Ray Image. Medical Reports, 7, 100106. DOI: 10.1016/j.hmedic.2024.100106.

4. He, K., Zhang, X., Ren, S., Sun, J. (2016). Deep Residual Learning for Image Recognition. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR 2016), pp. 770–778. DOI: 10.1109/CVPR.2016.90.

5. Hwang, E.J., Jeong, W.G., David, P.M., et al. (2024). AI for Detection of Tuberculosis: Implications for Global Health. Radiology: Artificial Intelligence, 6(2): e230327. DOI: 10.1148/ryai.230327.

Денис КОВАЛЬЧУК
здобувач вищої освіти третього (освітньо-наукового рівня)
спеціальності 125 Кібербезпека
denys.kovalchuk1@gmail.com

Лариса ЙОНА
кандидат технічних наук, доцент кафедри
Комп'ютерної інженерії та інноваційних технологій
Міжнародного гуманітарного університету м. Одеса, Україна

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВЕКТОР КІБЕРАТАК: НОВІ ВИКЛИКИ БЕЗПЕЦІ

1. Вступ та актуальність

Соціальні мережі стали ключовою частиною цифрового простору, забезпечуючи швидку комунікацію та обмін інформацією. Водночас вони стають платформою для кібератак: фішингових кампаній, розповсюдження шкідливого ПЗ та дезінформації. Поширення використання AI-технологій, таких як створення бот-мереж та генерація deepfake-контенту, посилює масштаби цих загроз.

Особливу актуальність проблема набуває для України в умовах війни, де соцмережі використовуються у гібридних атаках та для цілеспрямованого впливу на громадську думку. В умовах транскордонного характеру атак потрібен комплексний підхід до їхнього виявлення та запобігання.

Таким чином, дослідження соціальних мереж як вектора кібератак є актуальним для розвитку національної та міжнародної кібербезпеки.

2. Аналіз проблеми

Кіберзагрози у соцмережах поєднують технічні та психологічні механізми впливу. Основні типи атак:

- Фішинг та соціальна інженерія – обман користувачів для отримання персональних даних.
- Поширення шкідливого ПЗ – заражені файли та посилання, що блокують або крадуть дані.
- Викрадення акаунтів – поширення шкідливого контенту від імені власника.
- Bot-мережі та автоматизовані кампанії – масштабне просування маніпулятивного контенту.
- Deepfake та AI-контент – створення реалістичного фейкового відео або аудіо для маніпуляцій.

Транскордонний характер атак ускладнює виявлення злочинців та їх притягнення до відповідальності. Людський фактор – низький рівень кіберграмотності користувачів – залишається головною вразливістю. AI використовується для генерації персоналізованих атак та автоматизації шкідливих кампаній.

3. Мета та завдання дослідження

Мета - виявити та систематизувати загрози соціальних мереж і визначити нові виклики безпеці.

Завдання:

- Аналіз методів атак у соцмережах.
- Визначення ролі AI у нових загрозах.
- Розгляд транскордонних аспектів кіберзлочинності.
- Формування рекомендацій щодо підвищення кіберстійкості.

4. Шляхи протидії та перспективи

Ефективна протидія кіберзагрозам у соцмережах потребує комплексного підходу:

4.1. Технологічні рішення

- AI для виявлення бот-мереж та фейкового контенту – алгоритми поведінкового аналізу та перевірки метаданих.
- Системи раннього попередження – персоналізовані сповіщення про підозрілі повідомлення або посилання.
- Автоматичне блокування шкідливого ПЗ – інтеграція антивірусних і мережевих фільтрів у соцмережі.

4.2. Правові та міжнародні аспекти

- Гармонізація законодавства у сфері кібербезпеки між країнами.
- Спільні центри реагування на кіберзагрози для обміну даними та швидкого реагування.
- Відповідальність платформ за безпеку користувачів і впровадження технологій моніторингу.

4.3. Освітні заходи

- Інтеграція курсів з кібергігієни у систему освіти.
- Інформаційні кампанії для широкого кола користувачів.
- Формування критичного мислення та навичок перевірки контенту.

4.4. Перспективи розвитку

- Транскордонні системи кіберзахисту, що поєднують моніторинг та швидке реагування.
- Використання AI як для захисту, так і для аналізу та прогнозування нових типів атак.
- Комбінований підхід: технології + законодавство + освіта забезпечують багаторівневу безпеку.

Висновки

Соціальні мережі сьогодні виступають одним із ключових векторів кібератак, поєднуючи технічні та соціальні механізми впливу. Вони забезпечують високу швидкість поширення шкідливого контенту, зокрема фішингових повідомлень, шкідливих файлів та маніпулятивної інформації. Використання технологій штучного інтелекту значно підвищує ефективність таких атак, дозволяючи створювати масштабні бот-мережі, генерувати персоналізовані фішингові повідомлення та поширювати deepfake-контент для впливу на громадську думку та політичні процеси.

Транскордонний характер загроз ускладнює їх своєчасне виявлення та притягнення винуватців до відповідальності. Атаки часто організовуються з-за кордону, а їхній ефект відчутний на національному рівні, особливо в умовах війни, що підкреслює необхідність міжнародного співробітництва. Незважаючи на розвиток технологій захисту, головною вразливістю залишається людський фактор – низький рівень кіберграмотності та недостатня обізнаність користувачів щодо потенційних ризиків.

Ефективна протидія кібератакам у соцмережах можлива лише за умови інтеграції трьох ключових компонентів:

1. Технологічного – впровадження AI-алгоритмів для моніторингу активності користувачів, виявлення ботів, блокування фейкового контенту та шкідливих файлів;
2. Правового та міжнародного – гармонізація законодавства, створення спільних центрів реагування та підвищення відповідальності платформ;
3. Освітнього – навчальні програми з кібергігієни, інформаційні кампанії та формування критичного мислення.

Подолання сучасних кіберзагроз неможливе лише технологічними засобами або лише освітніми заходами. Необхідна комплексна багаторівнева система, що поєднує захисні алгоритми, законодавчі рамки та підготовку користувачів. Перспективним напрямом є створення транскордонних систем кіберзахисту, які дозволяють не лише реагувати на атаки в режимі реального часу, а й прогнозувати появу нових типів загроз.

Таким чином, соціальні мережі залишаються водночас ефективним засобом комунікації та джерелом серйозних кіберзагроз. Комплексний підхід до їхнього захисту забезпечує стійкість на національному та міжнародному рівнях, знижуючи ризики для користувачів і державних інституцій і створюючи умови для безпечного розвитку цифрового простору.

Список використаної літератури

1. Cyble. (2024). Ukraine's Cyberthreat Landscape 2024. URL: https://cyble.com/blog/ukraine-cyberthreat-landscape-2024/
2. European Parliament. (2025). Cybersecurity: main and emerging threats. URL: https://www.europarl.europa.eu/topics/en/article/20220120STO21428/cybersecurity-main-and-emerging-threats
3. PwC. (2024). Cyber Threats 2024: A Year in Retrospect. URL: https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect.html

Veronika HAVRYLENKO
Bachelor's degree student (2nd year), majoring in Cybersecurity and Data Protection (Specialty 125)
State University "Kyiv Aviation Institute"
9098351@stud.kai.edu.ua

Natalia BILOUS
PhD (Pedagogy), Associate Professor of the Professional Foreign Languages Department,
State University "Kyiv Aviation Institute"
natalia.bilous@npp.kai.edu.ua

ARTIFICIAL INTELLIGENCE AS A TOOL FOR COUNTERING CYBERATTACKS: CURRENT STATUS AND PROSPECTS FOR UKRAINE

The current state of cybersecurity in Ukraine faces unprecedented challenges due to the complexity and scale of cyberattacks. Traditional protection systems based on signatures and static rules are proving obsolete against targeted attacks (Advanced Persistent Threats), zero-day vulnerabilities, and artificially created malware. Of particular relevance during numerous attacks is the protection of critical infrastructure in wartime.

The current goal is to analyze modern methods of applying artificial intelligence (AI) to counter cyberattacks and develop practical recommendations for their implementation in Ukraine. The importance of the study is due to the critical need to create an effective and adaptable cybersecurity system capable of effectively countering modern cyber threats.

This study proposes to consider topics such as: a combined approach to integrating AI into cybersecurity systems at various levels, specialized algorithms for protecting critical infrastructure, and practical methods for using AI in electronic warfare systems.

Modern methods of using AI in cybersecurity involve analyzing the application of artificial intelligence, which has shown promise in the following areas:

Machine learning-based intrusion detection systems are highly effective in detecting abnormal network activity. Algorithms analyze behavioral patterns and detect deviations from normal activity, allowing potential threats to be identified at an early stage.

Natural language processing technologies are used in the analysis of cyberattacks. They allow automating the process of processing threat reports, extracting key information from unstructured data, and classifying incidents by level of danger.

Particular attention is paid to the protection of critical infrastructure facilities. Specialized approaches have been developed for monitoring industrial control systems (ICS/SCADA), which differ from traditional IT systems. AI-based systems monitor technological processes in real time, analyzing equipment performance parameters and detecting anomalies that may indicate a cyberattack. This helps prevent or minimize the consequences of interference with the operation of critical facilities.

Research has shown the promise of AI in electronic warfare (EW) systems. Machine learning algorithms can be used for automatic classification of radio signals, identification of radiation sources, and improvement of electronic countermeasure strategies.

This will increase the effectiveness of ECE and reduce the response time to threats.

The implementation of AI in Ukraine's cybersecurity systems faces a number of challenges. High data quality requirements for model training require the creation of specialized datasets that reflect the specifics of the Ukrainian cyberspace. The shortage of qualified specialists hinders the development of educational programs and the professional development of existing specialists. The need for integration with existing systems requires the development of adapters and interaction standards.

Thus, the study has shown the high effectiveness of AI in countering modern cyber threats. For the successful implementation of these technologies in Ukraine, it is necessary to first develop a strategy for the use of AI in cybersecurity, form an infrastructure for collecting and analyzing data on

cyberattacks, ensure the training of qualified specialists and encourage them, as well as develop international cooperation in this field.

References

1. Buczak, A. L. & Guven, E. (2016). A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. IEEE Communications Surveys & Tutorials, 18(2), 1153–1176.

2. Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P. & Ng, A. (2020). Cybersecurity Data Science: An Overview from Machine Learning Perspective. Journal of Big Data, 7(1), 41.

3. Євсеєв, О. О. & Мацієвський, Ю. В. (2021). Штучний інтелект у системах кібербезпеки: виклики та можливості для України. Кібербезпека: освіта, наука, техніка, 3(15), 6–18.

4. Про стратегію кібербезпеки України: Указ Президента України від 26 серпня 2021 р. № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013

Максим ПОНОМАР
здобувач вищої освіти другого (магістерського) ступеня,
1 курсу, спеціальності F7 «Комп'ютерна інженерія»,
Державний університет «Київський авіаційний інститут»,
7347796@stud.kai.edu.ua

Наталя БІЛОУС
кандидат педагогічних наук,
доцент кафедри іноземних мов професійного спрямування,
Державний університет «Київський авіаційний інститут»
natalia.bilous@npp.kai.edu.ua

ЗАСТОСУВАННЯ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ ДЛЯ ВИЯВЛЕННЯ ЗГЕНЕРОВАНОГО ТА МАНІПУЛЯТИВНОГО КОНТЕНТУ В СОЦІАЛЬНИХ МЕРЕЖАХ

У сучасному інформаційному суспільстві соціальні мережі стали одним із основних каналів комунікації, впливаючи на суспільну думку, політичні процеси та рівень інформаційної безпеки. Зі зростанням обсягів контнту та поширенням технологій генерації штучного медіа (deepfake, текстові генератори, синтетичні зображення) актуальним постає питання автоматизованого виявлення маніпулятивної та згенерованої інформації [1].

Метою роботи є розробка інтелектуальної системи для аналізу та класифікації контенту в соціальних мережах із використанням методів штучного інтелекту, машинного навчання та обробки природної мови (NLP) [2].

У рамках дослідження передбачено створення програмного модуля, здатного розпізнавати потенційно небезпечний контент на основі таких характеристик:

- мовні та стилістичні патерни, притаманні для синтетичних текстів, створених генеративними моделями (наприклад, GPT або Claude);
- емоційне забарвлення та полярність повідомлень, що дозволяє виявити маніпулятивні формулювання [1];
- структурні та часові особливості поширення повідомлень, які можуть свідчити про скоординовану дезінформаційну кампанію [2].

Для реалізації системи планується використання сучасних архітектур глибинного навчання, зокрема трансформерів (BERT, RoBERTa), що забезпечують високу точність аналізу текстових даних. Алгоритм класифікації базується на поєднанні лінгвістичних ознак та метаданих користувацької активності. На етапі моделювання використовуються методи супервізованого навчання з формуванням навчальної вибірки, яка містить приклади достовірного та маніпулятивного контенту [2].

Розроблена система може бути інтегрована у платформи моніторингу соціальних мереж для автоматичного виявлення потенційних інформаційних загроз. Її застосування дозволяє:

- підвищити рівень цифрової безпеки користувачів та інформаційного простору [1];
- зменшити ризики поширення дезінформації та фейкових новин;
- надати аналітичні інструменти для органів влади, ЗМІ та організацій, що займаються кіберзахистом [2].

Отримані результати підтверджують перспективність використання інтелектуальних систем для автоматичного аналізу контенту. Впровадження таких рішень сприятиме формуванню більш безпечного цифрового середовища, що є важливим елементом національної інформаційної безпеки.

Ключові слова: штучний інтелект, інтелектуальні системи, машинне навчання, маніпулятивний контент, згенерований контент, соціальні мережі, інформаційна безпека.

Список використаних джерел

1. Петрів, О. (2023). Дезінформація та штучний інтелект: (не)видима загроза. Центр демократії та верховенства права. URL: https://cedem.org.ua/analytics/dezinformatsiya-shtuchnyi-intelekt/

2. Артеменкова, О. (2025). Використання штучного інтелекту в соціальних мережах як інструменту ведення інформаційної війни. Вісник (…): URL: https://visnyk.ukrbook.net/article/view/339525

Єлизавета ПРИЙМАК
здобувач вищої освіти другого (магістерського) ступеня,
1 курсу, спеціальності F7 «Комп'ютерна інженерія»,
Державний університет «Київський авіаційний інститут»
7495937@stud.kai.edu.ua

Наталя БІЛОУС
кандидат педагогічних наук,
доцент кафедри іноземних мов професійного спрямування,
Державний університет «Київський авіаційний інститут»
natalia.bilous@npp.kai.edu.ua

ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ВИЯВЛЕННЯ КІБЕРЗАГРОЗ У РЕАЛЬНОМУ ЧАСІ

У сучасних умовах цифрової трансформації зростає потреба у високоефективних засобах забезпечення кібербезпеки, здатних виявляти та нейтралізовувати загрози в реальному часі. Кількість кібератак щорічно збільшується на 25–30 %, а їх складність та інтелектуальність постійно зростають. Традиційні методи захисту, засновані на сигнатурному аналізі або статичних правилах, уже не відповідають динаміці сучасного кіберпростору. У цьому контексті використання технологій штучного інтелекту (ШІ) стає ключовим напрямом у підвищенні ефективності систем кіберзахисту.

Метою дослідження є обґрунтування доцільності застосування штучного інтелекту для виявлення, класифікації та прогнозування кіберзагроз у реальному часі, а також аналіз його ефективності порівняно з традиційними методами.

Застосування ШІ у сфері кібербезпеки базується на трьох основних складових: машинному навчанні, глибинному навчанні та аналізі поведінкових патернів. Машинне навчання (ML) забезпечує можливість автоматичного виявлення аномалій у мережевому трафіку та поведінці користувачів, тоді як глибинні нейронні мережі (DNN) здатні розпізнавати складні багатовимірні залежності між подіями. Поведінкові моделі дозволяють системам прогнозувати потенційні атаки на основі історичних даних та поточних дій користувачів.

Серед найефективніших сучасних рішень варто відзначити системи Darktrace, CrowdStrike Falcon та IBM QRadar Advisor with Watson, які використовують комбінацію методів машинного навчання та когнітивної аналітики. За результатами досліджень компанії Gartner (2024), використання таких систем дозволяє скоротити середній час виявлення інцидентів на 43 % та знизити кількість хибнопозитивних спрацювань на 30–35 %.

Наукова новизна даного дослідження полягає у розробленні концептуальної моделі інтеграції штучного інтелекту в архітектуру систем моніторингу безпеки. Запропонований підхід передбачає використання гібридної системи, яка поєднує алгоритми кластеризації (наприклад, k-means або DBSCAN) для виявлення нетипових патернів та рекурентні нейронні мережі (LSTM) для прогнозування розвитку атаки у часі.

Аналіз результатів експериментального моделювання показав, що використання ШІ у процесі виявлення загроз дає змогу зменшити час реагування системи безпеки до 1,8 с у порівнянні з 4,5 с у традиційних системах. Крім того, точність класифікації атак підвищується до 96,4 %, що свідчить про високу ефективність запропонованого підходу.

Важливою складовою впровадження ШІ є також питання інтерпретованості моделей та етичної відповідальності за прийняті ними рішення. Зокрема, існує потреба у створенні прозорих механізмів контролю за алгоритмами, щоб запобігти хибним діям системи або її використанню для зловмисних цілей.

У перспективі подальших досліджень доцільно зосередитись на розвитку самонавчальних систем безпеки, які зможуть автономно оновлювати свої моделі без участі людини, адаптуючись до нових типів атак. Поєднання ШІ з технологіями великих даних (Big Data) та розподілених обчислень (Edge AI) відкриває нові можливості для створення комплексних систем кіберзахисту, що реагують у режимі реального часу.

Використання штучного інтелекту у виявленні кіберзагроз у реальному часі є одним із найефективніших напрямів розвитку сучасних систем безпеки. ШІ дозволяє значно підвищити рівень автоматизації, знизити людський фактор і забезпечити адаптивність до нових загроз. Практична реалізація таких підходів сприятиме створенню інтелектуальних, динамічних і надійних систем захисту, що є необхідною умовою кіберстійкості цифрового суспільства.

Список використаних джерел

1. Bishop, C. M. (2006). Pattern Recognition and Machine Learning. Springer.
2. Sommer, R., & Paxson, V. (2010). Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. IEEE Symposium on Security and Privacy. DOI: 10.1109/SP.2010.11

Олександр ЮСУПОВ
здобувач вищої освіти другого (магістерського) ступеня,
1 курсу, спеціальності F7 «Комп'ютерна інженерія»,
Державний університет «Київський авіаційний інститут»
6233541@stud.kai.edu.ua

Наталя БІЛОУС
кандидат педагогічних наук,
доцент кафедри іноземних мов професійного спрямування,
Державний університет «Київський авіаційний інститут»
natalia.bilous@npp.kai.edu.ua

ШТУЧНИЙ ІНТЕЛЕКТ ТА ЦИФРОВІ ТЕХНОЛОГІЇ У СФЕРІ КІБЕРБЕЗПЕКИ ЯК ІНСТРУМЕНТИ ДЛЯ ВИЯВЛЕННЯ ЗАГРОЗ, ЗАПОБІГАННЯ КІБЕРАТАКАМ ТА ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЗАХИСНИХ СИСТЕМ

Стрімкий розвиток цифрової інфраструктури державних, корпоративних та персональних сервісів супроводжується зростанням складності кіберзагроз і збільшенням обсягів подій, що потребують аналізу. Традиційні інструменти захисту, орієнтовані переважно на сигнатурні методи та ручний аналіз, не завжди забезпечують достатню швидкість виявлення інцидентів у гібридних середовищах. У цьому контексті застосування штучного інтелекту (ШІ) та сучасних цифрових технологій розглядається як доцільний напрям підвищення ефективності моніторингу, кореляції подій та реагування на інциденти [1].

Одним із базових напрямів застосування ШІ є виявлення аномалій у мережевій і системній активності. Моделі машинного навчання формують профілі нормальної поведінки користувачів, сервісів і пристроїв, після чого фіксують статистично значущі відхилення. Практичне значення цього підходу полягає у можливості раннього виявлення ознак компрометації (зокрема нетипових входів, аномального обміну даними, незвичних маршрутів доступу), а також у пріоритизації сповіщень для центрів моніторингу безпеки. Така автоматизована аналітика зменшує частку хибних спрацювань порівняно з виключно правил-орієнтованими системами та підтримує більш структурований triage інцидентів [2].

Іншим важливим напрямом є прогнозування загроз та оцінювання ризиків на основі історичних даних про інциденти, тактик нападників і відомих вразливостей. Використання нейронних мереж, методів класифікації та підходів до аналізу графів дозволяє формувати ймовірні сценарії розвитку атак і уточнювати пріоритети усунення вразливостей. Завдяки цьому організації можуть переходити до більш превентивних практик захисту, зокрема коригувати політики доступу, посилювати сегментацію та оптимізувати розподіл ресурсів реагування [3].

Паралельно з розвитком інтелектуальних методів захисту посилюється роль цифрових технологій, насамперед хмарних платформ, Інтернету речей (IoT) та edge-обчислень. Їх впровадження підвищує гнучкість і масштабованість сервісів, але одночасно збільшує площу атаки та ускладнює контроль конфігурацій. У таких умовах раціональним є поєднання інтелектуального моніторингу з архітектурними принципами безпеки, зокрема Zero Trust, централізованим управлінням ідентичностями та політиками мінімальних привілеїв [4]. Важливою залишається також інтеграція ШІ-рішень у загальну систему управління ризиками, що передбачає формалізовані процедури верифікації моделей, оцінювання їх надійності та забезпечення відстежуваності рішень.

Разом із тим застосування ШІ у сфері кібербезпеки має низку обмежень. По-перше, ефективність моделей залежить від якості даних, повноти журналювання та коректності навчальних вибірок. По-друге, складні моделі можуть демонструвати недостатню інтерпретованість, що ускладнює аудит рішень і визначення відповідальності у разі помилок. По-третє, існують ризики зловмисного використання ШІ для автоматизації соціальної інженерії та створення більш адаптивних атак. Відтак впровадження ШІ має супроводжуватися дотриманням етичних і правових принципів, зокрема пропорційності моніторингу, мінімізації обробки персональних даних і прозорого управління ризиками моделей [5].

Отже, ШІ та цифрові технології є перспективною основою для підвищення результативності кіберзахисту, передусім у задачах виявлення аномалій, кореляції подій і підтримки превентивних стратегій. Водночас практична цінність цих підходів визначається не лише якістю алгоритмів, а й рівнем їх інтеграції в архітектуру безпеки організації, регламентами управління ризиками та дотриманням норм конфіденційності й відповідального використання.

Список використаної літератури та джерел

1. Frontex, “European Border and Coast Guard Agency (Frontex),” Official website. https://www.frontex.europa.eu/.
2. European Commission, Directorate-General for Migration and Home Affairs, “EUROSUR (European Border Surveillance System),” [Online]. Available: https://home-affairs.ec.europa.eu/policies/schengen/eurosur_en.
3. M. O. Farooq and T. Kunz, “Combining supervised and reinforcement learning to build a generic defensive cyber agent,” Journal of Cybersecurity and Privacy, vol. 5, no. 2, art. 23, 2025, doi: 10.3390/jcp5020023.
4. Z. Ou et al., “DRUM: Diffusion-based runoff model for probabilistic flood forecasting,” arXiv preprint, arXiv:2412.11942, 2024. [Online]. Available: https://arxiv.org/abs/2412.11942. arXiv
5. C. R. Landolt, C. Würsch, R. Meier, A. Mermoud, and J. Jang-Jaccard, “Multi-agent reinforcement learning in cybersecurity: From fundamentals to applications,” arXiv preprint, arXiv:2505.19837, 2025. [Online]. Available: https://arxiv.org/abs/2505.19837. arXiv

Ярослав ЧУХРАЙ
бакалавр освітньої програми «Інформаційні системи та технології»
Ужгородський національний університет
chukhrai.yaroslav@student.uzhnu.edu.ua

Тарас ДИТКО
старший викладач кафедри програмного забезпечення систем
Ужгородський національний університет
taras.dytko@uzhnu.edu.ua

ПРОГНОЗУВАННЯ ТРАНСКОРДОННИХ ЗАГРОЗ ЗА ДОПОМОГОЮ МУЛЬТИАГЕНТНИХ СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ

Сучасне середовище міжнародної безпеки характеризується фундаментальною трансформацією природи та характеру загроз. На зміну класичним викликам приходять складні, динамічні явища, що не визнають державних кордонів. Такі загрози як: нелегальна міграція, торгівля людьми, контрабанда, гібридні кібератаки та транскордонні екологічні катастрофи (наприклад, поширення лісових пожеж чи паводків), вирізняються децентралізованою структурою та високою адаптивністю. Ключова проблема полягає в тому, що більшість існуючих систем безпеки функціонують на основі централізованих моделей аналізу, які є недостатньо гнучкими для обробки різнорідних, асинхронних потоків даних з прикордонних територій. Це створює нагальну потребу в розробці нових, децентралізованих підходів, здатних до комплексного моделювання та проактивного реагування.

В контексті євроінтеграційних процесів України, це питання набуває особливої актуальності на кордонах з країнами ЄС. Формування спільного безпекового простору вимагає не лише гармонізації законодавства, а й досягнення високого рівня оперативної сумісності між українськими та європейськими прикордонними і митними службами, зокрема з агентством Frontex [1]. Крім того, система прогнозування транскордонних ризиків може бути інтегрована з існуючими європейськими ініціативами, такими як EUROSUR (це спільна система для обміну інформацією та співпраці між країнами-членами ЄС і агентством Frontex), що підсилить здатність до колективного реагування [2]. Ефективна співпраця у боротьбі зі спільними загрозами, такими як організована злочинність та нелегальна міграція, неможлива без єдиної, динамічної картини обстановки та здатності до спільних прогнозуючих дій. Розробка інтелектуальних систем, здатних аналізувати транскордонні ризики в режимі реального часу, є ключовим елементом для зміцнення східного кордону ЄС та поглиблення практичної співпраці у сфері безпеки.

Перспективним напрямом вирішення цієї проблеми є застосування мультиагентних систем – обчислювальних моделей, що складаються з множини взаємодіючих «розумних агентів». Кожен такий агент є автономним програмним модулем, здатним сприймати зміни у своєму оточенні, обмінюватися інформацією з іншими агентами та спільно вирішувати поставлені завдання. У контексті транскордонної безпеки, такий підхід дозволяє імітувати складну поведінку реального світу, де численні зловмисники взаємодіють між собою. Особливість представленої концепції полягає у використанні децентралізованого підходу до аналізу, де замість централізованої обробки даних функціонує мережа взаємодіючих агентів. Це дозволяє точніше враховувати локальні умови та швидше реагувати на зміни середовища. Роль ШІ в таких системах є ключовою: він забезпечує обробку великих обсягів даних у реальному часі, виявлення прихованих паттернів та аномалій, а також прогнозування подальшого розвитку ситуації [3].

Така система може базуватися на трирівневій архітектурі, яка представлена у таблиці 1. Перший рівень складають агенти-збирачі (collectors), функція яких – агрегація даних з максимально широкого спектра джерел: супутникові знімки (оптичні, інфрачервоні), сигнали з наземних сенсорів (акустичних, сейсмічних), дані систем моніторингу, а також інформація з відкритих джерел (OSINT), включаючи соціальні мережі та новинні ресурси. Другий рівень

представлений агентами-аналітиками (analysts). Ці агенти застосовують алгоритми машинного навчання для обробки отриманої інформації. Серед перспективних технологій – використання геоінформаційних систем (GIS), глибинного навчання для аналізу супутникових зображень та reinforcement learning для симуляцій. Вони виявляють кореляції, класифікують події та ідентифікують аномальні патерни. Наприклад, розглядаючи ризик паводків у Закарпатській області, такий агент може одночасно обробити дані про інтенсивні опади у верхів'ях річки Тиса на території України та отримати від агентів суміжних країн (Угорщини, Словаччини) інформацію про критично високий рівень води у нижній течії. Поєднавши це з даними супутникового моніторингу про швидке танення снігу в Карпатах, система з високою точністю прогнозує формування та проходження паводкової хвилі через кордон, розраховуючи її час та потенційні зони затоплення [4]. Третій рівень – це агенти-рішень (decision-makers). На основі аналітичних висновків вони запускають тисячі симуляцій для моделювання можливих сценаріїв розвитку подій. Результатом їхньої роботи є не єдиний прогноз, а набір імовірнісних сценаріїв з пропозиціями щодо оптимального реагування для відповідних служб [5].

Таблиця 1 Мультиагентна система прогнозування транскордонних рішень

Рівень	Назва агентів	Основні функції	Використовувані технології	Приклад застосування
1	Агенти-збирачі (collectors)	Агрегація даних з різноманітних джерел: супутникові знімки, наземні сенсори, моніторингові системи, OSINT	Супутникова зйомка, сенсорні системи, соцмережі, новини	Збір даних про опади, рівень води, моніторинг природних умов
2	Агенти-аналітики (analysts)	Обробка даних, виявлення кореляцій, класифікація подій, пошук аномальних патернів	GIS, deep learning, reinforcement learning	Прогнозування паводків
3	Агенти-рішень (decision-makers)	Генерація імовірнісних сценаріїв, моделювання розвитку подій, рекомендації для служб	Моделювання, симуляції на основі AI	Надання кількох сценаріїв реагування на транскордонні загрози

Практична цінність такого підходу полягає у створенні технологічного фундаменту для якісно нового рівня транскордонної співпраці України з її західними сусідами – Угорщиною, Словаччиною та Румунією. Така інтелектуальна система може стати спільним цифровим простором для прикордонних, митних та екологічних служб цих країн. Вона дозволяє перейти від практики реактивного обміну інформацією про інциденти, що вже сталися, до спільного прогностичного моніторингу та синхронізації превентивних дій. Вироблення узгоджених стратегій на основі єдиної, об'єктивної картини ризиків, змодельованої штучним інтелектом, є не лише фактором зміцнення регіональної стабільності, але й потужним інструментом для поглиблення взаємної довіри та ефективної інтеграції України в європейський безпековий простір. Мультиагентні системи із ШІ мають потенціал стати ключовим елементом безпекової архітектури майбутнього, а впровадження їх в Україні може стати показовим прикладом для всього східного кордону ЄС.

Список використаної літератури та джерел

1. Frontex. https://www.frontex.europa.eu
2. Eurosur. Migration and Home Affairs. https://home-affairs.ec.europa.eu/policies/schengen/old-border-crossing/eurosur_en

3. Farooq, M. O. & Kunz, T. (2025) Combining Supervised and Reinforcement Learning to Build a Generic Defensive Cyber Agent, Journal of Cybersecurity and Privacy, 5(2), 23. https://doi.org/10.3390/jcp5020023
4. Ou, Z., Nai, C., Pan, B., Pan, M., Shen, C., Jiang, P., Liu, X., Tang, Q. & Zheng, Y. (2024) DRUM: Diffusion-based runoff model for probabilistic flood forecasting, arXiv, https://arxiv.org/abs/2412.11942
5. Landolt, C. R., Würsch, C., Meier, R., Mermoud, A. & Jang-Jaccard, J. (2025) Multi-Agent Reinforcement Learning in Cybersecurity: From Fundamentals to Applications, arXiv, https://arxiv.org/abs/2505.19837

Oleksandr SOKOLETS
First-year applicant for the Master's degree in Cybersecurity and Data Protection (Specialty F5), State University "Kyiv Aviation Institute"
5243956@stud.kai.edu.ua

Natalia BILOUS
PhD (Pedagogy), Associate Professor of the Professional Foreign Languages Department, State University "Kyiv Aviation Institute"
natalia.bilous@npp.kai.edu.ua

OPTIMIZATION OF FIREWALLS IN MODERN CYBERSECURITY SYSTEMS

In the era of increasing digitalization and the expansion of network infrastructures, cybersecurity has become one of the key priorities for organizations of any scale. Firewalls, as one of the oldest yet most fundamental components of protection systems, play a crucial role in filtering network traffic and preventing unauthorized access. However, with the growing volume of data, the complexity of attacks, and the proliferation of cloud technologies, traditional firewall configurations are often unable to ensure both high performance and sufficient security levels. Therefore, the optimization of firewalls—their architectures, policies, and operational algorithms—becomes a decisive factor in achieving a balance between speed, scalability, and protection efficiency. Modern enterprises deploy dozens or even hundreds of firewalls across hybrid infrastructures, including on-premises and cloud segments. Without optimization, such systems can experience:

- Network latency due to excessive or conflicting security rules;
- Vulnerabilities caused by outdated configurations;
- Overhead in traffic inspection and logging processes.

Optimizing firewalls helps not only to increase packet-processing performance but also to reduce attack surfaces and simplify policy management. Moreover, with the integration of AI, ML, and automated orchestration, optimization becomes part of an adaptive cybersecurity framework that can self-tune in response to real-time threats.

The main goal is to analyze and systematize approaches to firewall optimization in modern cybersecurity systems, including:

- identification of key bottlenecks in traditional firewall operation;
- evaluation of optimization techniques based on rule management, load balancing, and automation;
- analysis of modern solutions such as Next-Generation Firewalls (NGFWs) and cloud-native firewall architectures.

Optimization Methods

1. Rule Set Optimization:
   - Eliminate redundant or conflicting rules.
   - Use top-down rule sorting by frequency of use.
   - Employ tools for automatic rule analysis and compression.
2. Performance Optimization:
   - Parallel packet inspection using multi-core processing.
   - Load balancing between multiple firewalls.
   - Hardware acceleration with FPGA or ASIC chips.
3. Automation and Orchestration:
   - Integration with SDN (Software-Defined Networking) for dynamic policy updates.
   - Automated policy enforcement through Ansible, Terraform, or Firewall Manager APIs.
4. Machine Learning-Based Optimization:
   - Detection of inefficient rules based on real-time traffic analytics.
   - Dynamic prioritization of rule sets using AI to minimize latency.
5. Monitoring and Continuous Improvement:

- Implementation of KPI metrics: latency, throughput, false positive rate, CPU/memory utilization.

- Periodic audits and automated compliance checks.

The use of optimization technologies enables:

- Reduced CPU usage by 30–40% through intelligent caching and rule pruning;
- Latency reduction in high-load environments (data centers, enterprise networks);
- Enhanced scalability when adding new network segments or users;
- Improved incident response due to integration with SIEM and SOAR platforms.

For example, Fortinet FortiGate and Palo Alto NGFWs implement AI-based optimization engines that adapt filtering policies according to traffic patterns and threat intelligence feeds.

Overall, firewall optimization is not merely a technical improvement—it is an integral part of a proactive cybersecurity strategy, ensuring resilience, efficiency, and adaptability in the face of evolving threats.

References

1. Alghazzawi, A. H., El-Khatib, K., & Abed, S. A. (2023). A Survey of Machine Learning-Based Zero-Day Attack Detection: Challenges and Future Directions. Journal of King Saud University - Computer and Information Sciences, 35(2), 101511.
2. Du, M., Li, F., Zheng, G., & Srikumar, V. (2017). DeepLog: Anomaly Detection in System Logs using Deep Neural Networks. ACM CCS 2017, Dallas, TX, USA. Available from [https://www.researchgate.net/publication/320678676_DeepLog_Anomaly_Detection_and_Diagnosis_from_System_Logs_through_Deep_Learning]
3. Scarfone, K., & Hoffman, P. (2009). Guidelines on Firewalls and Firewall Policy. NIST Special Publication 800-41 Revision 1.
4. Palo Alto Networks (2024). Firewall Optimization Best Practices Guide. Palo Alto Technical Documentation.
5. Fortinet (2023). Performance Optimization in FortiGate Firewalls. Fortinet Whitepaper.
6. Gupta, S., & Bhushan, B. (2022). Next-Generation Firewalls: Architecture, Security, and Performance Analysis. IEEE Access, 10, 98455–98467.
7. Check Point Software Technologies (2023). Best Practices for Firewall Rule Base Optimization. Check Point Tech Library.

Sofiia PALAMARENKO
Master's degree student (1 st year), majoring in Cybersecurity and Data Protection (Specialty F5)
State University "Kyiv Aviation Institute"
sophia.palamarenko@gmail.com

Natalia BILOUS
PhD (Pedagogy), Associate Professor of the Professional Foreign Languages Department,
State University "Kyiv Aviation Institute"
natalia.bilous@npp.kai.edu.ua

ARTIFICIAL INTELLIGENCE IN THE FIGHT AGAINST SPAM AND PHISHING

In the modern digital environment, the volume of electronic communications is growing exponentially, creating favorable conditions for the spread of spam and phishing. These types of cyber threats pose a serious danger to users, as they can lead to the leakage of confidential data, financial losses, and infection of computer systems with malicious software [1].

Traditional approaches to combating spam, such as keyword-based filtering or blacklists, are insufficiently effective, since attackers constantly adapt the text and structure of messages. In this context, artificial intelligence (AI) and machine learning (ML) methods play an important role, as they are capable of analyzing large volumes of data and identifying hidden patterns [1].

To improve the accuracy of message classification, machine learning models are trained on examples of "spam" and "ham" emails. Additionally, the system's efficiency can be enhanced through the use of similarity hashing algorithms (SimHash, TLSH, ssdeep) [2]. These algorithms make it possible to detect similar messages even when their text is partially modified, which makes them particularly useful for identifying large-scale phishing campaigns.

Practical experiments show that combining similarity hashing with natural language processing (NLP) methods provides spam detection accuracy of over 90% [2]. This approach increases the effectiveness of email filtering systems and minimizes the number of false positives.

At the same time, the issue of continuous model updating remains relevant, since spammers are increasingly using generative AI technologies to create new variants of phishing messages. This necessitates the ongoing improvement of detection methods and the integration of hybrid analysis systems [3].

Artificial intelligence is a powerful tool in countering spam and phishing. Its use allows for the automation of analysis processes, improving detection accuracy and reducing risks associated with social engineering attacks. Further development in this field should focus on creating comprehensive cybersecurity systems that combine machine learning, similarity hashing, and behavioral analytics of users [3].

References

1. Liu X. Deciphering Spam Through AI: From Traditional Methods to Deep Learning Advancements in Email Security. International Conference on Engineering Management, Information Technology and Intelligence, Shanghai, China, 14–16 June 2024. 2024. P. 553–558. URL: https://doi.org/10.5220/0012958700004508.

2. Buchanan B. Malware/Spear Phishing Detection: Meet TLSH and ssdeep. Security and So Many Things. URL: https://asecuritysite.com/blog/2025-01-01_Malware-Spear-Phishing-Detection--Meet-TLSH-and-ssdeep-2b9249c28805.html.

3. Artificial Intelligence and Machine Learning in Phishing Detection and Prevention - 2025 - PhishGrid. PhishGrid. URL: https://phishgrid.com/blog/ai-and-machine-learning-in-phishing-detection/.

Aleksandra LEVRINTS
Bachelor's student,
specializing in Accounting and Taxation
Ferenc Rákóczi II Transcarpathian Hungarian University

Nataliya STOIKA
Associate Professor
Department of Accounting and Audit
Ferenc Rákóczi II Transcarpathian Hungarian University

THE APPLICATION OF ARTIFICIAL INTELLIGENCE IN INTERNAL AUDITING

In modern business environments, internal audit is crucial for effective enterprise management, providing a diagnostic function and prioritizing the achievement of the entity's strategic goals. The internal audit department evaluates the performance of the enterprise's business processes, contributes to the improvement of the risk management system, assists in achieving core business objectives, and enhances the control function within the enterprise.

As noted by Rudnytskyi V.S., internal audit is a system of observation and expert evaluation of the economic activities of an enterprise and its structural units for the purpose of substantiating and adopting optimal tactical and strategic decisions [1, p. 363].

Furthermore, here is the definition provided by the international Institute of Internal Auditors: "Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes" [2, p. 38].

Internal audit within the enterprise is essential for an objective assessment of its operations, management system, and control function, as well as for assisting management and the governing body in improving processes and achieving strategic operational goals.

Therefore, the internal audit system is undeniably effective and necessary within enterprise management, and its development and automation are crucial. Today, amid transformational changes and the rapid development of information technologies, one of the key areas is the implementation of Artificial Intelligence (AI) technologies into the enterprise management system.

Naturally, AI cannot replace the internal auditor, but it can become a powerful assistant, a tool for information processing and analysis, document generation, and informational support.

AI rapidly processes large volumes of textual documents (policies, procedures, contracts, internal regulations), which can help identify inconsistencies and evaluate compliance with internal standards (for example, whether contracts conform to established templates). AI analyzes and summarizes audit results, deviation reports, and multi-period review findings, which can quickly orient the auditor regarding key trends and potential risks. When AI is supplied with data, it can detect atypical transactions or patterns indicative of an error. Auditors can also apply AI to develop audit programs and plans, determine business process performance indicators, and model enterprise activity risks.

Therefore, the listed capabilities of AI for internal audit purposes are not exhaustive. The directions of AI use will depend on the tasks the auditor sets for artificial intelligence technologies. The application of AI increases the speed and efficiency of work, but at the same time, its use requires consideration that it entails a loss of information confidentiality, as data is uploaded to the AI system, and the final management decision always rests with the professional specialist.

References

1. Rudnytskyi V.S. (2000). Internal Audit: Methodology, Organization [Monograph]. Ternopil: "Ekonomichna Dumka", 106 p.
2. Chuyenkov A. Ye. (2011). Internal audit in the enterprise management system. Agrosvit, (19). Retrieved from: http://www.agrosvit.info/pdf/19_2011/10.pdf
3. Makarovych V.K., Stoika N.S. (2025). Integration of Artificial Intelligence into Accounting Information Systems: Challenges and Prospects. Acta Academiae Beregsasiensis. Economics, (9). Retrieved from: https://aab-economics.kmf.uz.ua/aabe/article/view/293/286

Yehor SELIUCHENKO
Bachelor's degree student (1st year) majoring in Cybersecurity and Data Protection (Specialty 125), State University "Kyiv Aviation Institute"
9121906@stud.kai.edu.ua

Larysa TEREMINKO
PhD (Pedagogy), Associate Professor of the Professional Foreign Languages Department, State University "Kyiv Aviation Institute"
larysa.tereminko@npp.kai.edu.ua

THE IMPACT OF CYBERCULTURE ON THE MODERN EDUCATIONAL PROCESS

The rapid development of digital technologies has profoundly changed the way people learn, teach, and communicate. Domestic and international scientific sources demonstrate the uniqueness and multifaceted nature of cyberculture. Determining the essential characteristics of cyberculture, information and communication technologies, and the creation of one's own electronic educational resources during professional activities are significant, as they are practical tools in the information society. In the process of forming the cyberculture of all subjects of the educational environment, special attention should be paid to the formation of the behavioral component, namely: communicative behavior in the digital environment, netiquette, ethical rules and norms of behavior, as well as safe behavior in the digital environment (Bescorsa, 2021:220).

Cyberculture, which combines the Internet, social media, and digital communication, has created a new educational environment where learning is more open and interactive. Students and teachers can now share information instantly and access global resources with just one click.

This study aims to analyze how cyberculture influences the modern educational process and what opportunities and challenges it brings. On the one hand, digital tools such as online courses, educational platforms, and virtual classrooms make learning more flexible and accessible. They help students develop digital literacy and connect with people around the world. Cyberculture also supports creativity and independent learning, allowing students to explore topics at their own pace and according to their own interests (Castells, 2010; Buckingham, 2013).

However, the digital environment also introduces new problems. Constant online communication may reduce attention, increase screen dependency, and make it difficult to concentrate. Moreover, the risk of misinformation, plagiarism, and data privacy issues has become more serious. Teachers need to adapt their teaching methods and guide students in using digital tools responsibly (Selwyn, 2016).

Cyberculture also changes the role of the teacher. Instead of being the only source of knowledge, the teacher becomes a mentor and facilitator who helps students navigate through the large amount of online information. This shift requires new skills in both pedagogy and technology (Selwyn, 2016).

In conclusion, cyberculture has a strong and lasting impact on education. It makes the learning process more dynamic, inclusive, and innovative, but it also demands digital responsibility and critical thinking. To fully benefit from cyberculture, schools and universities must combine technology with human values and ethical education.

References

1. Bescorsa O. (2021). Content characteristics of digital culture of future primary school teachers of English. SHEI "Donbas State Pedagogical University", 1, 209-220. DOI 10.31494/2412-9208-2021-1-1. URL: https://pedagogy.bdpu.org.ua/wp-content/uploads/2021/05/24.pdf
2. Castells, M. (2010). The Rise of the Network Society. Wiley-Blackwell.
3. Selwyn, N. (2016). Education and Technology: Key Issues and Debates. Bloomsbury Academic.
4. Buckingham, D. (2013). Media Education: Literacy, Learning and Contemporary Culture. Polity Press.

Maksym ZAIETS
Bachelor's degree student (2nd year) majoring in Computer Engineering (Specialty 123), State University "Kyiv Aviation Institute"
9220506@stud.kai.edu.ua

Olena HURSKA
PhD (Pedagogy), Associate Professor of the Professional Foreign Languages Department, State University "Kyiv Aviation Institute"
olena.hurska@npp.kai.edu.ua

BALANCING HUMAN EXPERTISE AND AI IN CYBERSECURITY

In our interconnected world, digital infrastructure is the backbone of almost everything we do. From banking and shopping to how we communicate, educate ourselves, and even govern our nations, we depend on digital systems. This growing dependence has turned cyberspace into a vital area that supports our social, economic, and political well-being. However, this reliance also creates more ways for cybercriminals to attack. Today's cyberattacks are often carried out by automated systems that use artificial intelligence (AI). This makes them quicker, more complex, and harder to spot. Basic security tools and human monitoring are no longer enough to deal with these changing threats. The relevance of this study lies in addressing this imbalance by exploring how AI can be integrated with human expertise to strengthen cybersecurity. The novelty of this research is reflected in its focus on achieving synergy between AI automation and human analytical judgment to create adaptive, intelligent, and ethical security systems. The objective of this research is to analyze the role of AI in threat detection, incident response, and predictive defense, while also evaluating its limitations, risks, and the irreplaceable role of human expertise in maintaining balance and accountability.

One of the biggest ways AI can help cybersecurity is by finding unusual behavior in complex networks. Security analysts have to deal with huge amounts of data every day, like network traffic, login attempts, emails, and file transfers. It is almost impossible for people to find malicious patterns in real time on their own. However, AI systems can process this data, find hidden connections, and quickly send alerts when something seems out of the ordinary. For example, if someone uses an employee's login information from a different country, or if data starts moving in ways it shouldn't, AI can detect this within seconds and take action. This allows companies to find and stop threats early, which can greatly reduce the damage. Therefore, AI not only makes security operations more efficient but also allows companies to be proactive instead of reactive.

AI is also very important in responding to incidents. In the past, when a system was hacked, human analysts had to manually investigate the breach, find out what caused it, and decide what to do. This could take hours or even days. During that time, attackers could take advantage of weaknesses and cause more problems. AI tools have changed this by allowing for quick analysis and automated responses. Modern AI systems can suggest the best ways to contain a breach or take preventive actions automatically, like blocking malicious IP addresses or isolating infected devices. This reduces downtime, limits damage, and prevents analysts from getting overwhelmed by too many alerts. By filtering out irrelevant information and focusing on critical incidents, AI helps people stay focused and make better decisions.

Beyond just finding and responding to threats, AI is also being used to predict and prevent cyberattacks. By studying threat information from different industries and regions, AI can spot new patterns and predict which weaknesses are most likely to be exploited. This allows security teams to prioritize their defenses and use their resources more wisely. It changes cybersecurity from just reacting to attacks to preparing for them in advance. However, how well AI can predict attacks depends on the quality of the data it's trained on. If the data is inaccurate, biased, or incomplete, it can lead to false alarms, missed threats, and unreliable results. The fact that many AI algorithms are like black boxes also raises concerns about transparency and accountability. Companies may not fully trust automated decisions if they don't understand how they are made. To make things even more

complex, cybercriminals are also using AI to create more convincing phishing frauds, malware that can change its form and intrusion strategies that can adapt to defenses.

Despite all these advances, people are still essential. While AI is good at speed, dealing with large amounts of data, and finding patterns, it doesn't have the ability to understand context, think ethically, or be creative like humans do. If we rely too much on automation, we risk losing the critical thinking and analytical skills of security professionals. Additionally, setting up AI systems can be expensive, technically complex, and raise ethical questions about privacy and data protection. Therefore, the best approach is a combination where AI supports human expertise but doesn't replace it. In this partnership, AI does quick data analysis and automates repetitive tasks, while human analysts handle strategic decisions, interpret unclear data, and make sure everything is ethical and legal. The key to building strong cybersecurity systems is finding the right balance between human intuition and machine intelligence.

Looking ahead, AI will play an even bigger role in cybersecurity. New technologies will make it more transparent and ethically sound. The development of explainable AI (XAI) will make it easier to understand and trust how algorithms make decisions. Privacy-preserving techniques will allow AI models to learn from different data sources without compromising privacy. As attackers use AI to develop new offensive tools, those defending against attacks must also innovate. The growing use of the Internet of Things (IoT), edge computing, and cloud platforms will increase the need for AI-driven defense systems that can adapt to changing threats. Future studies should focus on creating guidelines for using AI responsibly in cybersecurity, balancing automation with accountability and efficiency with ethics.

In conclusion, AI is changing the cybersecurity field by allowing for faster threat detection, more effective incident response, and the ability to predict attacks. But the success of these depends on keeping a balance between automation and human oversight. AI should be a tool that helps people, not replaces them. Combining human expertise with AI systems will define the next generation of cybersecurity, which will be proactive, transparent, and ethical. The future of digital defense is not about humans competing with machines but about them working together to ensure security, resilience, and trust in an increasingly complex digital world.

References

1. The Role of AI in Cybersecurity: How Artificial Intelligence Transforms Threat Detection.Official website. https://www.eccu.edu/blog/the-role-of-ai-in-cyber-security/

2. The Role of Artificial Intelligence (AI) in Cybersecurity: A Comprehensive Guide. Official website. https://www.valoremreply.com/resources/insights/guide/role-of-ai-in-cybersecurity/

3. The Role of Artificial Intelligence (AI) in Modern Cybersecurity. Official Website https://www.ninjaone.com/blog/role-of-ai-in-cybersecurity/?utm_source=chatgpt.com

Володимир БАЛАБАН
здобувач вищої освіти другого (магістерського) ступеня,
1 курсу, спеціальності F7 «Комп'ютерна інженерія»,
Державаний університет "Київський авіаційний інститут"
vova.balaban.341@gmail.com

Наталія БІЛОУС
кандидат педагогічних наук,
доцент кафедри іноземних мов професійного спрямування,
Державний університет «Київський авіаційний інститут»
natalia.bilous@npp.kai.edu.ua

АВТОМАТИЗАЦІЯ РОЗМІТКИ ДАНИХ ДЛЯ СИСТЕМ КОМП'ЮТЕРНОГО ЗОРУ У СФЕРІ БЕЗПЕКИ

Сучасні інформаційні технології відіграють ключову роль у сфері безпеки. В умовах зростання кількості цифрових загроз, розвитку безпілотних систем, автоматизації виробничих процесів та посилення ризиків для інфраструктури особливого значення набуває застосування штучного інтелекту та систем комп'ютерного зору.

Одним із найбільш поширених підходів у цій сфері є використання нейронних мереж для автоматичного виявлення та класифікації об'єктів[1]. Такі технології активно застосовуються у:

- Відеоспостереженні (ідентифікація підозрілої поведінки, відстеження об'єктів у реальному часі);
- Транспортній безпеці (розпізнавання номерних знаків, контроль за дорожнім рухом);
- Військовій сфері (аналіз зображень із дронів, виявлення потенційних цілей);
- Промисловій безпеці (контроль за станом обладнання, виявлення небезпечних ситуацій).

Основою для роботи систем штучного інтелекту є якісні датасети, які забезпечують точність і надійність моделей[2]. Підготовка таких датасетів потребує значних ресурсів і часу, адже для навчання нейронних мереж важлива не лише кількість, а й якість даних. Саме тому актуальною задачею стає автоматизація та напівавтоматизація процесів розмітки даних.

Автоматизація процесу розмітки зображень є важливим напрямом досліджень у сфері комп'ютерного зору. Сучасні програмні рішення дозволяють напівавтоматично розмічати дані для навчання моделей штучного інтелекту, що значно скорочує час на підготовку датасетів. Такі інструменти зазвичай мають зручний інтерфейс для користувача та підтримують різні типи анотацій – від класичної розмітки об'єктів до складніших варіантів, таких як сегментація чи визначення ключових точок.

Такі рішення сприяють більш продуктивному впровадженню штучного інтелекту у сфері безпеки, адже дозволяють швидше створювати системи моніторингу, відеоаналітики та автоматичного виявлення загроз. Наприклад, алгоритми на основі YOLO можуть працювати у реальному часі, що робить їх надзвичайно корисними для оперативного реагування на потенційні небезпеки[3].

Таким чином, розвиток інформаційних технологій у сфері безпеки нерозривно пов'язаний із вдосконаленням інструментів для роботи з даними. Автоматизовані рішення для підготовки датасетів, системи комп'ютерного зору та алгоритми штучного інтелекту вже сьогодні допомагають підвищувати рівень захисту в багатьох галузях, а в майбутньому їх роль лише зростатиме.

Список використаних джерел

1. Goodfellow, I., Bengio, Y. and Courville, A. (2016) Deep Learning. MIT Press. URL: https://www.deeplearningbook.org.
2. Everingham, M., Van Gool, L., Williams, C.K.I., Winn, J. and Zisserman, A. (2015) The PASCAL Visual Object Classes Challenge: A Retrospective. International Journal of Computer Vision, 111(1), pp.98–136. DOI: 10.1007/s11263-014-0733-5;
3. Redmon, J. and Farhadi, A. (2018) YOLOv3: An Incremental Improvement. arXiv preprint arXiv:1804.02767. DOI: 10.48550/arXiv.1804.02767;

Василь БАРАНЕЦЬ
аспірант кафедри міжнародних відносин та суспільних комунікацій, Чернівецький національний університет імені Юрія Федьковича, Чернівці, Україна,
baranets.vasyl@chnu.edu.ua

Іван ОСАДЦА
кандидат політичних наук, доцент кафедри міжнародних відносин та суспільних комунікацій, Чернівецький національний університет імені Юрія Федьковича, Чернівці, Україна,
i.osadtsa@chnu.edu.ua

ШТУЧНИЙ ІНТЕЛЕКТ ЯК КАТАЛІЗАТОР ГІБРИДНИХ ЗАГРОЗ: ПОЛІТИЧНІ ВИКЛИКИ ДЛЯ НАЦІОНАЛЬНОЇ ТА МІЖНАРОДНОЇ БЕЗПЕКИ

Поява і швидке поширення систем штучного інтелекту (ШІ) стали переломним моментом для міжнародної та національної безпеки. Якщо раніше питання цифрової безпеки обмежувалися здебільшого класичними кіберзагрозами (вірусами, фішингом, DDoS-атаками), то сьогодні вони безпосередньо включають ризики, що виникають із застосуванням генеративних і прогностичних моделей. ШІ дедалі частіше застосовується в операціях моніторингу мережевого трафіку, аналізу соціальних медіа, виявлення дезінформаційних кампаній, що створює новий рівень технологічних можливостей для урядів і приватного сектору. Водночас ці ж самі інструменти здатні використовувати і зловмисники, що призводить до якісно нової гонки озброєнь у сфері кібербезпеки.

Актуальність дослідження визначається кількома чинниками. По-перше, швидке зростання кількості атак на системи, у яких ШІ є ключовим елементом. По-друге, невизначеність у правовому регулюванні: міжнародне право ще не виробило універсальних норм щодо застосування ШІ у сфері безпеки. По-третє, важливість міждисциплінарного підходу: без поєднання знань із кібернетики, міжнародних відносин та права ефективна стратегія безпечного використання ШІ неможлива [3]. Таким чином, ШІ постає не лише як інструмент захисту, але й як потенційний «каталізатор» нових загроз.

Використання ШІ у сфері цифрової безпеки надає низку переваг. Алгоритми глибинного навчання дозволяють швидше виявляти шкідливі патерни у масиві трафіку, який раніше вимагав значних людських ресурсів для обробки. Наприклад, моделі аномалій уже активно застосовуються для запобігання фішинговим кампаніям та автоматизованим атакам на банківські системи. У багатьох країнах створюються національні центри кіберзахисту, які інтегрують ШІ у системи раннього попередження [6]. Окрім того, генеративні моделі здатні виконувати роль «цифрових тренажерів», відтворюючи сценарії потенційних атак і дозволяючи тестувати надійність інфраструктур у контрольованому середовищі [4].

Однак основна проблема полягає у вразливості самих моделей ШІ. Атаки на великі мовні моделі (prompt injection, data poisoning, model inversion) стали новим напрямом діяльності зловмисників. Такі атаки дозволяють отримати конфіденційні дані, змінювати відповіді моделі або навіть використовувати її як інструмент дезінформації [7]. Дослідження Ye та ін. підтверджують, що управління персональними даними у генеративних моделях залишається одним із найбільш слабких місць: витоки навчальних корпусів становлять реальну загрозу для державних установ та міжнародних організацій [10].

Ще однією проблемою є інформаційні війни. Використання ШІ для масового виробництва фейкового контенту призводить до того, що звичайний користувач не здатен відрізнити правдиві повідомлення від підроблених. Harvard Misinformation Review наголошує: під час президентських виборів у США 2024 року саме «ШІ-розкручені» наративи стали одним із

чинників суспільної поляризації [9]. Це доводить, що генеративні моделі стають не лише технологічним, а й політичним викликом, який вимагає адаптації демократичних інститутів.

Урядові та експертні спільноти пропонують низку підходів для вирішення цих проблем [5]. Модель SecGenAI, що розроблена в Австралії, орієнтується на інтеграцію технічних контролів у хмарні сервіси, які використовують генеративний ШІ. Вона включає перевірку даних, аудит доступу, тестування моделей і контроль над використанням API [4]. Модель flexHEGs, представлена Aarne & Petrie, передбачає апаратні та нормативні механізми, які мають запобігати зловживанням високопродуктивними ШІ-системами, зокрема у військовій сфері [1].

Окремим аспектом є розвиток міжнародного співробітництва. Документи CISA та UK Government пропонують кодекси практик із кібербезпеки для ШІ, що можуть стати прототипом для європейських і глобальних стандартів [2; 8]. Це підкреслює необхідність поєднання правових інструментів із технічними механізмами контролю. Без цього жодна країна не зможе забезпечити стійкість у новій цифровій екосистемі.

Висновки. ШІ уже сьогодні є невід'ємним елементом кіберзахисту, забезпечуючи швидший і точніший аналіз загроз. Проте водночас він створює абсолютно новий клас ризиків – від атак на моделі до масового використання для поширення дезінформації. Актуальні дослідження 2024–2025 років доводять, що комплексний підхід – поєднання інженерних рішень (red teaming, аудит моделей, моніторинг дрейфу) з нормативними рамками (кодекси практик, етичні стандарти) – є єдиним шляхом до забезпечення стійкості. Міжнародні концепції на кшталт SecGenAI та flexHEGs свідчать про глобальний тренд: інтеграцію правових і технічних гарантій у сфері цифрової безпеки. Їхній досвід може бути адаптований до національних умов України з урахуванням особливостей війни та загроз гібридного типу. Ключовим завданням для держави є створення власних стандартів безпечного використання ШІ, гармонізованих із європейськими та глобальними нормами. Не менш важливим є розвиток людського капіталу – експертів, здатних працювати на перетині технологій і міжнародної політики. Саме такий підхід дозволить розглядати ШІ не лише як джерело ризиків, але і як фактор зміцнення національної безпеки та міжнародної стабільності.

Список використаних джерел

1. Aarne, O. & Petrie, J. (2025) International security applications of flexible hardware-enabled guarantees (flexHEGs). arXiv preprint. Available at: https://arxiv.org/abs/2506.15100
2. CISA (2025) AI Data Security: Best Practices for Securing Data Used to Train & Operate AI Systems. U.S. Cybersecurity and Infrastructure Security Agency. Available at: https://www.cisa.gov
3. ENISA (2024) ENISA Threat Landscape 2024. European Union Agency for Cybersecurity. Available at: https://www.enisa.europa.eu
4. Haryanto, C.Y., Hendrickx, P., Foo, E. & Morrison, J. (2024) SecGenAI: Enhancing security of cloud-based generative AI applications within Australian critical technologies of national interest. arXiv preprint. Available at: https://arxiv.org/abs/2407.01110
5. NCSC UK (2024) AI and Cyber Security: What You Need to Know. National Cyber Security Centre, UK. Available at: https://www.ncsc.gov.uk
6. Polito, C. & Pupillo, L. (2024) 'Artificial intelligence and cybersecurity', Intereconomics, 59(1), pp. 50–55. https://www.intereconomics.eu/contents/year/2024/number/1/article/artificial-intelligence-and-cybersecurity.html
7. Sun, Y., Li, H., Wu, J. & Wang, X. (2024) 'AI hallucination: towards a comprehensive classification of hallucination in large generative models', Humanities and Social Sciences Communications, 11. https://doi.org/10.1057/s41599-024-03811-x
8. UK Government (2025) Code of Practice for the Cyber Security of AI. Department for Science, Innovation and Technology & NCSC. Available at: https://www.gov.uk/government/publications/ai-cyber-security-code-of-practice

9. Yan, H.Y., Kim, S., Perra, N. & Menczer, F. (2025) 'The origin of public concerns over AI supercharging misinformation in the 2024 U.S. election', Harvard Misinformation Review, 6(1). Available at: https://osf.io/preprints/osf/cpy7v_v1

10. Ye, X., Zhang, L. & Lin, J. (2024) 'Privacy and personal data risk governance for generative AI', Telematics and Informatics, 88, 102020. https://www.sciencedirect.com/science/article/pii/S0308596124001484?ssrnid=4867063&dgcid=SSRN_redirect_SD

Тетяна ГОВОРУЩЕНКО
Доктор технічних наук, професор
Хмельницький національний університет
hovorushchenko@khmnu.edu.ua

Юрій ВОЙЧУР
Доктор філософії
Хмельницький національний університет
voichury@khmnu.edu.ua

ВИЗНАЧЕННЯ РІВНЯ БЕЗПЕКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ НА ОСНОВІ СПЕЦИФІКАЦІЇ ВИМОГ

Сьогодні розробка програмного забезпечення (ПЗ) стала однією з найбільш витратних галузей [1]. У зв'язку з цим будь-які недоліки чи збої в процесі проєктування та розроблення ПЗ можуть спричинити серйозні наслідки [2]. Відповідно до стандарту ISO 25010, безпека ПЗ формується на основі п'яти підхарактеристик – конфіденційності, цілісності, автентичності, відповідальності та безвідмовності і, подібно до інших характеристик, оцінюється за сукупністю визначених атрибутів якості (15 атрибутів), що наведені у стандарті ISO 25023. Усі атрибути, необхідні для такої оцінки, слід передбачити ще на етапі специфікації вимог до ПЗ [3]. Таким чином, виходячи зі значень атрибутів, закладених у вимогах, можна заздалегідь прогнозувати рівень безпеки майбутнього ПЗ.

На рис. 1 представлено концептуальну модель процесу прогнозування безпеки ПЗ (як однієї з характеристик якості ПЗ), що базується на атрибутах якості.

Рис. 1. Концептуальна модель процесу прогнозування безпеки ПЗ

Метод прогнозування рівня безпеки ПЗ включає такі етапи:

вхідні дані: значення 15 атрибутів якості, що визначають безпеку ПЗ;

1) аналіз спеицфікації вимог до ПЗ для виявлення значень 15 атрибутів, які впливають на безпеку;

3) підготовка отриманих значень атрибутів для подачі на вхід штучної нейронної мережі (ШНМ) – формується набір вхідних векторів з урахуванням того, що підхарактеристики безпеки залежать від 23 атрибутів, з яких 15 є різними, а входи ШНМ структуровані у 5 множин (для кожної з 5 підхарактеристик безпеки) – з 1, 2, 8, 10 та 2 атрибутів;

4) обробка значень атрибутів ШНМ;

5) аналіз результатів роботи ШНМ – прогнозованого кількісного показника безпеки ПЗ *pnvss*;

6) формування висновку щодо рівня безпеки ПЗ на основі правил (порогові значення для правил були встановлені емпіричним шляхом): якщо $pnvss \in [0; 0,22)$, то ПЗ прогнозовано матиме початковий рівень безпеки; якщо $pnvss \in [0,22; 0,49)$, то ПЗ прогнозовано матиме середній рівень безпеки; якщо $pnvss \in [0,49; 0,89)$, то ПЗ прогнозовано матиме достатній рівень безпеки; якщо $pnvss \in [0,89; 1]$, то ПЗ прогнозовано матиме високий рівень безпеки;

вихідні дані: прогнозований рівень безпеки ПЗ.

Розглянемо 10 специфікацій вимог до ПЗ, підготовлених десятьма різними компаніями м. Хмельницького (Україна) на етапі збору та аналізу вимог до одного й того ж ПЗ. Кожна з них була проаналізована щодо визначення 15 атрибутів якості, що впливають на безпеку ПЗ. Після цього сформовано вхідні вектори для ШНМ. ШНМ, опрацювавши значення атрибутів, згенерувала прогнозовані кількісні показники безпеки ПЗ (*pnvss*) для 10 розглянутих специфікацій, а саме: *pnvss1 = 0.12; pnvss2 = 0.93; pnvss3 = 0.45; pnvss4 = 0.67; pnvss5 = 0.34; pnvss6 = 0.09; pnvss7 = 0.78; pnvss8 = 0.98; pnvss9 = 0.41; pnvss10 = 0.53*. Після цього здійснено аналіз отриманих прогнозованих кількісних показників безпеки ПЗ (*pnvss1–pnvss10*), на основі якого сформульовано висновки щодо прогнозованого рівня безпеки ПЗ для кожної з 10 розглянутих специфікацій. Таким чином, очікується, що програмне забезпечення комп'ютерних систем, розроблене на основі специфікацій вимог №2 та №8, характеризуватиметься високим рівнем безпеки (за умови відсутності помилок на подальших етапах життєвого циклу). Відтак замовнику доцільно доручити розроблення ПЗ саме компаніям, які підготували ці специфікації.

При подальшому застосуванні розробленого методу було проаналізовано ще 150 різних специфікацій (наборів) вимог, створених ІТ-компаніями м. Хмельницького (Україна) для вирішення різноманітних завдань. Система визначила високий рівень безпеки майбутнього ПЗ для 41 специфікації; достатній рівень – для 29; середній рівень – для 55; низький рівень – для 25 наборів вимог. Таким чином, лише для 27% проаналізованих специфікацій потенційно можлива реалізація ПЗ із високим рівнем безпеки (рис. 2).

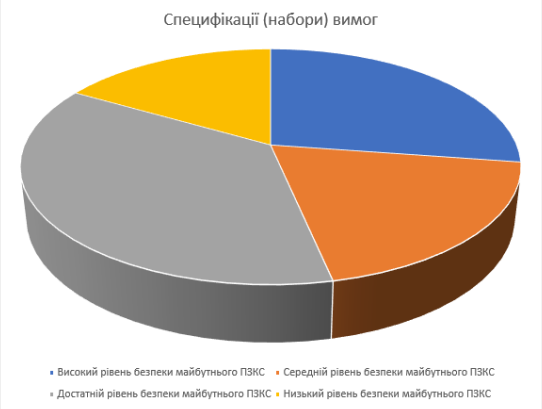


Рис. 2. Розподіл прогнозованого рівня безпеки ПЗ для 150 досліджених специфікацій вимог

Як показав аналіз прогнозів, лише для 27% проаналізованих наборів вимог потенційно можливе створення ПЗ із високим рівнем безпеки, для 19% – із достатнім рівнем безпеки, тоді як для 37% наборів вимог передбачуваний рівень безпеки ПЗ є середнім, а для 17% – низьким.

Розроблено метод прогнозування рівня безпеки ПЗ, який, на відміну від відомих, визначає залежність безпеки ПЗ від атрибутів якості та формує числовий прогноз безпеки на основі цих атрибутів. Метод дозволяє прогнозувати рівень безпеки ПЗ за отриманим числовим значенням, порівнювати специфікації вимог до ПЗ за прогнозованим рівнем безпеки та відсіювати невдалі специфікації.

Список використаних джерел

1. Software. URL: https://www.statista.com/markets/418/topic/484/software/ (Accessed: September 21, 2025).

2. TAMURA, Y. and YAMADA, S., 2023. Deep Learning Based on Fine Tuning with Application to the Reliability Assessment of Similar Open Source Software. International Journal of Mathematical, Engineering and Management Sciences, 8(4), pp. 632–639. http://dx.doi.org/10.33889/IJMEMS.2023.8.4.036

3. ГОВОРУЩЕНКО, Т.О., 2018. Теоретичні та прикладні засади інформаційної технології оцінювання достатності інформації щодо якості у специфікаціях вимог до програмного забезпечення. Дисертація доктора технічних наук. Львів.

Davyd HRYTSENOK
Bachelor's degree student (2nd year)
majoring in Software Engineering (Specialty 121),
State University "Kyiv Aviation Institute"
9145627@stud.kai.edu.ua

Larysa TEREMINKO
PhD (Pedagogy), Associate Professor of the
Professional Foreign Languages Department,
State University "Kyiv Aviation Institute"
larysa.tereminko@npp.kai.edu.ua

THE ROLE OF AI AND DIGITAL TECHNOLOGIES IN SHAPING A SAFE ENVIRONMENT

In recent years, the integration of artificial intelligence (AI) and digital technologies has significantly transformed the way societies approach safety, security, and sustainability. The rapid growth of computational power, machine learning algorithms, and smart data systems has enabled the creation of intelligent environments that not only respond to threats but also predict and prevent them. The relevance of this topic lies in the increasing reliance of critical infrastructure, transportation, healthcare, and urban management on intelligent digital solutions that ensure human and environmental safety.

The 21st century is characterized by the digitalization of nearly every aspect of human life. Technologies such as the Internet of Things (IoT), big data analytics, and AI-driven automation play a key role in creating safe and resilient systems. The global shift toward "smart" technologies has enabled the detection of natural disasters, the identification of cybersecurity threats, and the real-time monitoring of public spaces. These capabilities are essential for modern societies, especially in contexts where security risks evolve rapidly.

The significance of AI in this domain stems from its ability to analyze large volumes of heterogeneous data, recognize patterns, and generate predictive insights. For instance, machine learning models can identify potential industrial hazards, detect sources of environmental pollution, or forecast the spread of infectious diseases. Such applications directly contribute to shaping a safer and more sustainable environment, both physically and digitally.

Despite substantial progress, several challenges remain in implementing AI for safety purposes. The main problem lies in the lack of standardized frameworks for integrating AI systems into existing safety infrastructures. Issues of data privacy, algorithmic transparency, and human oversight limit the efficiency and trustworthiness of intelligent systems. Moreover, the digital divide between technologically advanced and developing regions results in unequal access to AI-driven safety tools.

The objective of this study is to examine the role of AI and digital technologies in shaping a safe environment, identify the key areas of their application, and assess their impact on the prevention and management of safety-related risks. The research also aims to outline the ethical and regulatory considerations required to ensure the responsible use of these technologies.

The scientific novelty of this research lies in the comprehensive analysis of how AI and digital technologies simultaneously influence both physical and digital safety environments. While existing studies often focus on cybersecurity or environmental monitoring separately, this work integrates both aspects under a unified perspective of technological safety ecosystems.

From a practical standpoint, the study emphasizes the importance of cross-sector collaboration among governments, industry, and academia in deploying AI solutions. For example, in the aviation industry, intelligent monitoring systems use predictive analytics to identify technical faults before they escalate into accidents. In urban management, AI-enabled surveillance, combined with facial recognition, helps authorities detect criminal activity and locate missing persons more efficiently. Furthermore, AI-based disaster response systems analyze satellite imagery to predict floods, earthquakes, or fires, allowing emergency services to act preemptively.

AI contributes to environmental and human safety through three primary dimensions: **prediction**, **prevention**, and **protection**.

1. **Prediction:** Machine learning models can process data from environmental sensors, weather stations, and social networks to predict potential risks. For instance, AI-driven meteorological systems forecast natural disasters with greater accuracy than traditional models.
2. **Prevention:** In industrial settings, AI-powered automation prevents equipment malfunctions and workplace accidents by monitoring sensor data in real time. Predictive maintenance technologies in the manufacturing and transportation sectors exemplify how AI prevents failures before they occur.
3. **Protection:** In the digital domain, AI strengthens cybersecurity by detecting anomalies, identifying phishing attacks, and preventing unauthorized access. Algorithms based on deep learning are used in threat intelligence systems to recognize malicious activities that might bypass human oversight.

A significant case study illustrating the social impact of AI is the use of intelligent surveillance in "Safe City" projects. These systems integrate video analytics, facial recognition, and behavioral modeling to enhance urban safety. Similarly, in healthcare, AI-driven diagnostic tools detect early signs of diseases, protecting patient safety and reducing medical errors.

However, while the benefits are clear, implementing such technologies raises ethical concerns about data ownership, surveillance overreach, and potential algorithmic bias. Therefore, transparent governance frameworks and ethical guidelines are essential to ensure that technological safety does not compromise individual rights.

In conclusion, we can state that the role of AI and digital technologies in shaping a safe environment is multifaceted and transformative. These technologies enhance the prediction and management of risks across environmental, industrial, and digital domains. AI's capacity to process vast data streams in real time allows for the creation of adaptive systems that ensure human well-being and ecological balance.

Nevertheless, the pursuit of safety through digital transformation must be accompanied by responsible governance, ethical compliance, and continuous monitoring. Future research should focus on developing explainable AI models, improving data protection mechanisms, and ensuring equitable access to safety technologies. The integration of human-centered design principles with intelligent systems will ultimately determine how effectively AI can contribute to a truly safe and sustainable world.

References

1. https://www.sciencedirect.com/science/article/abs/pii/S0264275118315968?via%3Dihub
2. https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai
3. https://www.sciencedirect.com/science/article/abs/pii/S0360835219304838?via%3Dihub
4. https://ieeexplore.ieee.org/document/7307098

Daria HURTOVA
Bachelor's degree student (2nd year)
majoring in Software Engineering (Specialty 121),
State University "Kyiv Aviation Institute"
9216651@stud.kai.edu.ua

Hanna SOROKUN
Senior Lecturer of the
Professional Foreign Languages Department,
State University "Kyiv Aviation Institute"
hanna.sorokun@npp.kai.edu.ua

THE ROLE OF ARTIFICIAL INTELLIGENCE IN MODERN SECURITY TECHNOLOGIES

Artificial intelligence continues to reshape security landscapes around the world, enabling systems that are more adaptive, predictive, and efficient than ever before. In recent months, several breakthroughs have highlighted both the opportunities and fresh threats posed by AI in the security domain. One unexpected vulnerability discovered in ChatGPT's Deep Research agent, known as "ShadowLeak," allows attackers to siphon sensitive information without any visible user interaction. This zero-click, server-side flaw underscores the fact that AI tools themselves can be weak links in enterprises' security posture.

At the same time, generative AI attacks are accelerating at an alarming rate. A Gartner report from September 2025 found that 29% of organizations experienced attacks targeting their AI application infrastructure within the past year. Deepfake incidents—through audio, voice biometric spoofing, or video—are growing in prevalence, introducing new vectors for disinformation and fraud.

Another concern is that malware is now being developed that can evade even advanced protection tools. In one experiment, a malware strain trained via reinforcement learning managed to bypass Microsoft Defender's security checks around 8% of the time after only three months of training, using a relatively small budget. This kind of AI-generated malware shows attackers' growing ability to automate and refine their methods very quickly.

On the defense side, there are some promising developments. In Ukraine, for example, the Institute for Information Registration Problems is building an AI/ML-based system to assess the combat effectiveness of units in real time, forecast outcomes, and support decision-making under pressure. Ukraine's military AI ecosystem has also benefitted from a large number of companies and academic programs: over 243 AI-focused companies, more than 307,000 specialists in IT and software, and 106 AI/ML academic programs across 42 higher education institutions. Despite infrastructural and resource challenges, such numbers show strong local capacity and commitment.

There is also innovation in defense technologies for battlefield intelligence. A Ukrainian-Estonian firm, Farsight Vision, develops hardware and software that use UAV imagery, 3D terrain modelling, and geospatial analysis to feed actionable data to Ukrainian security services. These systems are deployed by the Armed Forces, National Guard, police, and border guard. This shows how AI combined with remote sensing can enhance situational awareness even under difficult conditions.

Another technical advance addresses adversarial machine learning: researchers proposed a defence using explainable AI (XAI) for behavior-based authentication. In this approach, the system filters out the features most vulnerable to adversarial attacks, retaining those more robust and relevant for genuine authentication. This results in improved resistance to adversarial manipulation.

These developments point to a security domain in transition. Outdated playbooks are being challenged. For example, traditional identity and access management systems are struggling with "agent sprawl" — the proliferation of AI agents operating across systems often without centralized governance. Some companies are now embedding identity security protocols directly into AI agent frameworks to maintain control, visibility, and risk oversight.

The recent period has shown that AI's role in security is more complex than ever: it offers powerful tools for defense but also opens novel threat vectors that can be highly automated, stealthy, and adaptable.

References

1. CSIS. Understanding the Military AI Ecosystem in Ukraine. (2024). https://www.csis.org/analysis/understanding-military-ai-ecosystem-ukraine
2. Institute for Information Registration Problems of NAS of Ukraine. Artificial Intelligence for the State's Defense Capability: An Innovative Combat Capability Analysis System for the Armed Forces of Ukraine. (2024). https://www.ipri.kiev.ua/en/en-events/artificial-intelligence-for-the-states-defense-capability-an-innovative-combat-capability-analysis-system-for-the-armed-forces-of-ukraine
3. ITPro. Generative AI attacks are accelerating at an alarming rate. (2025). https://www.itpro.com/security/generative-ai-attacks-are-accelerating-at-an-alarming-rate
4. TechRadar. AI security is identity security: How Okta is weaving agents into the security fabric. (2025). https://www.techradar.com/pro/security/ai-security-is-identity-security-how-okta-is-weaving-agents-into-the-security-fabric
5. Wikipedia. Farsight Vision. (2025). https://en.wikipedia.org/wiki/Farsight_Vision
6. Windows Central. AI-powered malware eludes Microsoft Defender's security checks 8 percent of the time. (2025). https://www.windowscentral.com/artificial-intelligence/ai-powered-malware-eludes-microsoft-defenders-security-checks-8-percent

Mykyta DUZHYK
Bachelor's degree student (2nd year), majoring in Cybersecurity and Data Protection (Specialty 125), State University "Kyiv Aviation Institute"
9121906@stud.kai.edu.ua

Larysa TEREMINKO
PhD (Pedagogy), Associate Professor of the Professional Foreign Languages Department, State University "Kyiv Aviation Institute"
larysa.tereminko@npp.kai.edu.ua

ARTIFICIAL INTELLIGENCE FOR CYBERSECURITY ENHANCEMENT

The rapid digitalization of society has fundamentally transformed how individuals, organizations, and governments operate. While digital technologies facilitate global interconnectedness, efficiency, and speed, they also introduce vulnerabilities that cybercriminals exploit. Traditional cybersecurity methods, although effective in many cases, are no longer sufficient to confront increasingly sophisticated and large-scale cyberattacks. This underscores the need for new approaches that can adapt to dynamic environments, anticipate potential threats, and respond in real time. Artificial Intelligence (AI) is emerging as one of the most promising tools in this regard.

This study aims to explore the potential of AI to enhance cybersecurity in the digital environment. By analyzing the functions and mechanisms of AI applications, the paper highlights how intelligent algorithms can be used not only for threat detection but also for prevention, mitigation, and adaptive protection of digital infrastructures. This research is vital because cyber threats like phishing, ransomware, and state-sponsored cyber operations are worsening, so we need new, proactive ways to protect ourselves.

AI-based systems can process and analyze vast amounts of data faster and more accurately than human specialists. For example, machine learning models can spot unusual trends in user behavior or network traffic that may indicate malicious activity. Unlike traditional signature-based methods, AI does not require prior knowledge of a threat to detect it. Alternatively, it is predicated on the identification of anomalies, which facilitates the implementation of early warning systems that significantly reduce response time. This capacity to learn and adapt makes AI a unique solution in combating new and previously unknown cyberattacks.

Another vital contribution of AI is its ability to automate routine security processes. Tasks such as scanning for vulnerabilities, filtering out spam, or verifying user access can be effectively delegated to intelligent systems, freeing cybersecurity professionals to focus on more complex analytical work. Furthermore, AI technologies can facilitate predictive analysis, helping organizations anticipate potential attack vectors and enhance their digital resilience before incidents occur.

Nevertheless, integrating AI into cybersecurity is not without challenges. Issues such as algorithmic bias, the need for quality training data, and the risk of adversarial attacks against AI systems themselves remain significant obstacles. In addition, cybercriminals may exploit a false sense of security created by excessive reliance on automated systems. Therefore, AI shouldn't be seen as a replacement for human knowledge, but as a powerful assistant that makes people more intelligent and more capable.

In conclusion, artificial intelligence is a transformative force in cybersecurity. Because it can detect anomalies, handle incidents quickly, and anticipate new threats, it can help make digital ecosystems safer. Nevertheless, successful implementation necessitates a balanced approach that integrates professional expertise, ethical considerations, and technological innovation. Strengthening cybersecurity in the digital environment through AI is not merely a technical task but a strategic priority that will define the resilience of societies in the twenty-first century.

References

1. Emmanuel, Ok. (2024). Artificial Intelligence and Cybersecurity: Strengthening Defenses in the Digital Age. URL: https://www.researchgate.net/publication/383291847_Artificial_Intelligence_and_Cybersecurity_Strengthening_Defenses_in_the_Digital_Age
2. The Role of AI in Strengthening Cybersecurity Defenses, 2024. URL: https://pecb.com/en/article/the-role-of-ai-in-strengthening-cybersecurity-defenses#:~:text=AI%20analyzes%20historical%20data%20to,actionable%2C%20data%2Ddriven%20insights
3. Cybersecurity and AI: The Future of Digital Defense, 2024. URL: https://cybersecurity-magazine.com/ cybersecurity-and-ai-the-future-of-digital-defense/

Олексій КОЛОМІЄЦЬ
здобувач вищої освіти другого (магістерського) ступеня,
1 курсу, спеціальності F7 «Комп'ютерна інженерія»,
Державний університет «Київський авіаційний інститут»,
7448072@stud.kai.edu.ua

Наталя БІЛОУС
кандидат педагогічних наук,
доцент кафедри іноземних мов професійного спрямування,
Державний університет «Київський авіаційний інститут»,
natalia.bilous@npp.kai.edu.ua

ПРОГРАМНА СИСТЕМА МОНІТОРИНГУ РОБОТИ КОМПОНЕНТІВ IOT-СИСТЕМ

Сучасні IoT-системи (Internet of Things) являють собою складні розподілені мережі, до складу яких входять різнорідні пристрої — сенсори, контролери, виконавчі механізми та аналітичні модулі. Зростання кількості таких пристроїв, а також обсягів даних, що ними генеруються, зумовлює необхідність створення ефективних засобів моніторингу, діагностики та управління компонентами системи. Програмна система моніторингу забезпечує централізоване спостереження за роботою всіх елементів IoT-мережі, своєчасне виявлення збоїв і відхилень у роботі, а також оптимізацію використання ресурсів.

Основною метою розроблення програмної системи моніторингу є підвищення надійності, безпеки та продуктивності функціонування IoT-середовища. Система повинна забезпечувати збір, обробку, аналіз і візуалізацію телеметричних даних у режимі реального часу. До ключових завдань відносяться: визначення критичних станів пристроїв, попередження про можливі відмови, виявлення аномалій у потоці даних, а також прогнозування технічного стану на основі історичних показників.

Архітектура розробленої системи передбачає три основні рівні: рівень збору даних, рівень обробки та рівень представлення результатів. На першому рівні відбувається взаємодія із сенсорами та іншими пристроями за допомогою стандартних протоколів зв'язку, таких як MQTT, CoAP чи HTTP. Другий рівень забезпечує зберігання даних у базі, їх первинну обробку, агрегацію та фільтрацію. Третій рівень реалізує інтерфейс користувача, що дає змогу переглядати графіки, отримувати сповіщення та формувати звіти про стан системи.

У розробці програмної системи використано сучасні технології, зокрема мови програмування Python і JavaScript, фреймворки Flask та React, а також базу даних InfluxDB, оптимізовану для часових рядів. Для обміну повідомленнями між компонентами застосовано брокер повідомлень Mosquitto MQTT. Такий підхід забезпечує гнучкість системи, легкість масштабування та можливість розподілення навантаження між вузлами.

Особлива увага приділена питанню інформаційної безпеки. Для захисту переданих даних використовується шифрування TLS, автентифікація користувачів та розмежування прав доступу. Крім того, передбачено модуль контролю цілісності даних і журналювання подій. Це дозволяє своєчасно виявляти спроби несанкціонованого доступу або втручання в роботу системи.

Експериментальні дослідження показали, що впровадження системи моніторингу дозволяє знизити час простою обладнання на 25–30%, своєчасно виявляти понад 90% потенційних збоїв і зменшити витрати на обслуговування. Такі результати підтверджують ефективність розробленої моделі та доцільність її подальшого вдосконалення.

Подальший розвиток системи передбачається у напрямі впровадження модулів штучного інтелекту, які аналізуватимуть поведінку пристроїв для прогнозування відмов і оптимізації енергоспоживання. Також планується інтеграція з хмарними платформами, що дозволить масштабувати рішення на рівень промислових систем і розширити можливості віддаленого керування компонентами.

Таким чином, створена програмна система моніторингу компонентів IoT-систем демонструє високу практичну цінність для підвищення ефективності та безпеки сучасних розподілених середовищ. Її використання дає змогу покращити контроль за технічним станом

пристроїв, мінімізувати ризики відмов та забезпечити стабільне функціонування інфраструктури IoT.

Список використаних джерел

1. Ashton, K. (2009). That ‘Internet of Things’ Thing. RFID Journal.
2. Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. Business Horizons, 58(4), 431–440. https://doi.org/10.1016/j.bushor.2015.03.008
3. Minerva, R., Biru, A., & Rotondi, D. (2015). Towards a Definition of the Internet of Things (IoT). IEEE Internet Initiative.
4. Rose, K., Eldridge, S., & Chapin, L. (2015). The Internet of Things: An Overview. The Internet Society (ISOC).

Sofiia LYSIUK
Bachelor's degree student (2nd year), majoring in Cybersecurity and Data Protection (Specialty 125), State University "Kyiv Aviation Institute"
9097546@stud.kai.edu.ua

Larysa TEREMINKO
PhD (Pedagogy), Associate Professor of the Professional Foreign Languages Department, State University "Kyiv Aviation Institute"
larysa.tereminko@npp.kai.edu.ua

THE ROLE OF GOOGLE DORKING IN DETECTING PERSONAL DATA LEAKS

The modern digital world is developing incredibly fast, leading to the mass digitalisation of various services, communications, and information storage. However, this progress has a downside, which is the growth in cyber threats, among which personal data leaks occupy a special place.

It is essential for cybersecurity specialists to be equipped with tools that enable them to detect leaks at an early stage in order to decrease damage and quickly take countermeasures. Google dorking can be helpful in this case. It is important to be aware that this tool can be used by both malicious attackers to search for vulnerabilities and security specialists to identify issues.

Google dorking is simply a method of targeted analysis and highly accurate online search. It is based on using special operators and commands in the Google search system that allow you to filter results according to specific criteria.

The purpose of such a search is to find information that is technically public and indexed by a search robot, but according to the plan, should be hidden from the general public. For instance, these could be temporary files, documents with incorrect access settings, or the contents of web server directories where confidential information has accidentally ended up. As a result, Google dorking is a powerful open source intelligence (OSINT) tool that reveals not only security gaps but also traces of careless data handling.

The object of such searches is mostly personal data. Today, this concept covers a much wider range of information than just a name or address. Personal data includes any information relating to an identified individual. This can be identification numbers, email addresses, biometric data, location data, IP addresses, health information, financial transactions, and even cookies. The leakage of these categories of data poses the most serious risks, including fraud, identity theft, and phishing attacks, making their protection a priority.

When organisations place confidential information in the public domain due to server configuration errors, employee unawareness, or the use of outdated software, search engines will index it sooner or later. Google dorking as part of an audit involves analysing this indexing to identify anomalies and potential leaks: for example, accidentally published documents, open lists, or configuration files. Such analysis helps form a general idea of how the organisation is represented in the information field, classify the objects found according to risk criteria, and determine the priority measures to fix problems.

An ethical specialist can systematically check the network for such leaks using specially formulated queries. For example, searching for different types of files containing the words 'password' or 'personal file' on the domains of institutions or establishments can reveal critical security breaches. This role of Google dorking is crucial for preventing serious incidents before attackers can exploit them, making it an essential component of the modern cybersecurity arsenal.

The process of detecting leaks does not end with discovery. It moves into the critically important phase of responsible discovery. After finding a critical vulnerability, an ethical researcher does not copy or distribute the data but documents the leak and reports it to the responsible administration, giving them time to fix the problem. In this way, Google dorking transforms from a potentially dangerous tool into a key security system element. It allows you to find and patch gaps in the digital

space before attackers do, effectively performing the function of a public security audit. In a world where data is growing vastly, these methods aren't just useful; they're vital for keeping trust in digital institutions and protecting the fundamental human right to privacy.

In conclusion, Google dorking is a powerful tool in the digital era. Although its potential for misuse by malicious attackers is significant, its value as a defensive mechanism for cybersecurity professionals is undeniable. Using this OSINT technique, professionals can systematically scan vast amounts of publicly indexed material to identify and document critical data leaks caused by human mistakes and misconfigurations. Thus, when used responsibly and ethically, it serves not as a tool for attack but as an effective tool for detecting the level of information openness. It enables organisations to detect unintentional personal data leaks early and take actions to protect privacy in a timely way. This process of early detection, followed by responsible disclosure, is crucial for reducing risks. Therefore, the future of effective cybersecurity lies in the careful use of tools such as Google dorking to check for open "doors" that are often overlooked.

References

1. https://www.bytesnipers.com/en/cybersecurity-blog/google-dorks
2. https://www.riskinsight-wavestone.com/en/2020/01/dorking-exploiting-search-engine-capabilities-discover-security-gaps/
3. https://www.splunk.com/en_us/blog/learn/google-dorking.html
4. https://www.maltego.com/blog/using-google-dorks-to-support-your-open-source-intelligence-investigations/
5. https://www.researchgate.net/publication/368787532_GOOGLE_DORKING_OR_LEGAL_HACKING_FROM_THE_CIA_COMPROMISE_TO_YOUR_CAMERAS_AT_HOME_WE_ARE_NOT_AS_SAFE_AS_WE_THINK

Роман МЕТЕЛЯ
здобувач вищої освіти другого (магістерського) ступеня,
1 курсу, спеціальності F5 «Кібербезпека та захист інформації»,
Державний університет «Київський авіаційний інститут»
5783203@stud.kai.edu.ua

Наталя БІЛОУС
кандидат педагогічних наук, доцент кафедри
іноземних мов професійного спрямування,
Державний університет «Київський авіаційний інститут»
natalia.bilous@npp.kai.edu.ua

ШТУЧНИЙ ІНТЕЛЕКТ У КІБЕРБЕЗПЕЦІ: КЛАСИФІКАЦІЯ, ПРИКЛАДИ ВИКОРИСТАННЯ ТА НАПРЯМИ ДОСЛІДЖЕНЬ

Штучний інтелект (ШІ) все частіше визнається як революційний стимул у сфері кібербезпеки, оскільки він може автоматизувати рутинні завдання, пришвидшити виявлення загроз та підвищити точність захисних заходів. За словами Каур та ін. (2023), «ШІ — це потужна технологія, яка допомагає командам кібербезпеки автоматизувати повторювані завдання, пришвидшувати виявлення загроз та реагування на них, а також підвищувати точність своїх дій для посилення захисту від різних проблем безпеки та кібератак.» (с. 1).

У цій статті коротко підсумовано систематичний огляд літератури, проведений Каур та ін., де було розглянуто 236 первинних досліджень, опублікованих у період з 2010 року по лютий 2022 року. Огляд літератури представлено з точки зору п'яти основних функцій Структури кібербезпеки NIST — Ідентифікація, Захист, Виявлення, Реагування та Відновлення - та пропонує багаторівневу структуру, що пов'язує тематичні дослідження застосування ШІ з деякими категоріями рішень у сфері кібербезпеки.

Функція «Ідентифікація» є основою та включає управління активами, аналіз впливу на бізнес, управління, оцінку ризиків та управління ризиками ланцюга поставок. Методи кластеризації, класифікації та навчання з підкріпленням ШІ застосовуються для інвентаризації активів, виявлення вразливостей та оцінки ризиків. Наприклад, Промислов та ін. використовували кластеризацію к-середніх для класифікації активів на атомній електростанції на основі рівня їхніх вимог до кібербезпеки (с. 5). Також Лю та ін. використовували модель випадкового лісу для прогнозування інцидентів на основі неправильних конфігурацій DNS та BGP (с. 6).

В області «Захист» ШІ посилює управління ідентифікацією, контроль доступу, захист даних та навчання. Сіам та ін. розробили платформу біометричної автентифікації на основі фотоплетизмографії та глибокого навчання (с. 10), а Алобайді та ін. досліджували автентифікацію на основі ходьби в неконтрольованих середовищах (с. 10). ШІ також сприяє адаптивним навчальним системам, таким як веб-середовище навчання Тана та ін., яке адаптує контент на основі попередніх знань учня (с. 11).

Найдосконалішим аспектом впровадження ШІ є функція «Виявлення». Системи виявлення вторгнень (IDS) розгортаються на основі бінарних та багатокатегорійних моделей класифікації. Вчені використовували стандартні набори даних, такі як NSL-KDD, CICIDS2017 та UNSW-NB15, для навчання моделей з метою виявлення аномалій, вилучення ознак та корекції дисбалансу класів (с. 13). Розслідування темного вебу та вилучення автоматизованої інформації про загрози ШІ можуть здійснюватися із соціальних мереж, таких як Twitter, а також із баз даних CVE (с. 14-15).

Під час процесу «Реагування» ШІ сприяє динамічному управлінню випадками, пріоритизації сповіщень, технічному аналізу та автоматизованому усуненню загроз. Наприклад, Краєва та Як'яєва запропонували систему рекомендацій для вирішення інцидентів на основі нейронної мережі (с. 16), тоді як Несполі та ін. розробили штучну імунну систему для вибору оптимальних контрзаходів (с. 17).

Функція «Відновлення» залишається недостатньо вивченою, оскільки лише небагато досліджень присвячено післяінцидентному аналізу та агрегуванню звітів про інциденти.

Майєрс та Менілі застосували методи обробки природної мови (NLP) для післяінцидентного аналізу вразливостей (с. 18), тоді як Карріегос та ін. запропонували процедури накопичення даних про інциденти, щоб допомогти у майбутньому відновленні (с. 18).

У статті зазначається низка галузей досліджень, зокрема багатомовну розвідку загроз, пояснювальний ШІ (XAI) та бази даних у реальному часі. Як зазначають автори, «майбутні дослідження ШІ для кібербезпеки можуть розглядати, як інтерпретований та пояснимий ШІ може покращити продуктивність алгоритму та розкрити його «чорну скриньку», щоб зменшити ці обмеження» (с. 22). Крім того, нездатність обмінюватися національною та міжнародною розвідувальною інформацією про загрози перешкоджає механізмам реагування скоординованим чином (с. 23).

Загалом, інтеграція ШІ в кібербезпеку має великі перспективи в усіх функціях NIST. Структуру та можливості використання, які пропонують Каур та ін., можуть служити організованим керівництвом для майбутніх досліджень та практичного застосування. Вирішуючи виявлені прогалини, особливо в сферах представлення даних, інфраструктури та партнерства між людиною та І, дослідники та фахівці можуть підвищити стійкість та інтелект механізмів кібербезпеки.

Список використаних джерел

1. Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial Intelligence for Cybersecurity: Literature Review and Future Research Directions. Information Fusion, 97, Article 101804. https://doi.org/10.1016/j.inffus.2023.101804

Микола ПРОЦЕНКО
кандидат технічних наук, доцент
Державний університет інформаційно-комунікаційних технологій
m.procenko@duikt.edu.ua

МОДЕЛІ МАШИННОГО НАВЧАННЯ ДЛЯ ВИЯВЛЕННЯ АНОМАЛІЙ МЕРЕЖЕВОГО ТРАФІКУ: СТАН І ПЕРСПЕКТИВИ

Безпека функціонування комп'ютерних мереж, напряму залежать від наявності засобів вчасного виявлення аномалій мережевому трафіку. Джерелами аномалій можуть бути різноманітні зловмисні дії: атаки типу "Відмова в обслуговуванні" (DoS/DDoS), несанкціонований доступ, сканування портів та зондування, спроби впровадження шкідливого коду, використання вразливостей захисту. Аномалії можуть створювати технічні збої чи нетипові закономірності в роботі обладнання. Традиційний захист брандмауери та системи IDS/IPS, сигнатурні системи виявлення атак мають суттєві обмеження, оскільки здебільшого орієнтовані на відомі патерни зловмисної активності.

У цьому контексті машинне навчання та методи штучного інтелекту відкривають нові можливості для аналізу мережевого трафіку, виявлення невідомих типів атак і, що важливо, створення адаптивних систем безпеки комп'ютерних мереж.

Статистичні методи аналізу трафіку ґрунтуються на статистичних показниках середніх значеннях, дисперсії, щільності розподілу. Аномалією вважається будь-яка подія, яка статистично значуще відхиляється від встановленого базового рівня. Методи прості в реалізації і не потребують значних обчислень, Деякі з них використовують часові ряди для прогнозування майбутніх рівнів трафіку та ідентифікації середньо- або довгострокових тенденцій. Недоліком методів слід вважати низьку стійкість до нестабільних умов роботи мережі, слабку здатність до виявлення складних атак із поступовою ескалацією.

Використання інтелектуальних алгоритмів значно розширило можливості визначення нетипових, а отже, потенційно небезпечних процесів в мережі. Інтелектуальні алгоритми стали основою сучасних систем виявлення вторгнень, заснованих на аномаліях (Anomaly-based Intrusion Detection Systems).

Машинне навчання (Machine Learning, ML) – це галузь штучного інтелекту, яка створює комп'ютерні моделі, здатні навчатися на зібраних даних, виявляти патерни та складати прогнозні рішення. Процес створення моделі проходить три етапи.

1. Вилучення ознак (Feature Engineering). Вручну вибираються ключові характеристики мережевого трафіку: обсяг трафіку за одиницю часу, кількість пакетів, середня тривалість сесії, кількість унікальних IP-адрес призначення.
2. Навчання моделі. Модель, наприклад, метод опорних векторів, навчається на великому обсязі нормального трафіку, щоб зрозуміти, що є «здоровою» поведінкою мережі.
3. Виявлення. Модель порівнює ознаки поточного трафіка з вивченою нормою. Якщо нові дані розміщуються далеко від визначених кластерів або виходять за встановлені статистичні межі, вони класифікуються як аномалія.

Клас методів класичного машинного навчання складають методи: «Опорних векторів» (Support Vector Machine, SVM) добре справляється зі структурованими даними, здатний відокремлювати нормальний трафік від аномального у багатовимірному просторі, використовує ядра для нелінійного розділення; «Дерева рішень, Випадковий ліс» (Decision Trees, Random Forest) забезпечує інтерпретацію моделей, здійснює аналіз важливості окремих ознак, що вказують на аномалію; «Найближчих сусідів» (k-NN) ефективний при роботі з відносно невеликими наборами даних або для виявлення локальних аномалій; «Кластеризації» (k-means, DBSCAN) дозволяє формувати групи «нормальних» та «аномальних» зразків без учителя, розглядаючи аномалії як точки, що не належать до жодного кластера (DBSCAN, ізоляція) або далекі від центру нормального кластера (k-means).

Позитивними сторонами методів є відносна простота реалізації, наявність апробованих бібліотек та алгоритмів. Водночас методи потребують ретельний підбір патернів, на їхні можливості негативно впливає зростання інтенсивності та нестабільна динамічність трафіку.

Глибинне навчання (Deep Learning, DL) це підмножина ML. Для обробки даних DL використовує глибинні нейронні мережі (Deep Neural Networks, DNN) – мережі з кількома прихованими (проміжними) шарами. На сьогоднішній день, в сфері виявлення аномалій трафіку, методи DL є найперспективнішими. До класу мереж DNN відносяться: «Рекурентні нейронні мережі» (RNN, LSTM, GRU) ефективні для аналізу часових послідовностей пакетів у трафіку; «Автокодери» (Autoencoders) здійснюють відновлення нормальних патернів з реального трафіку; великі відхилення між параметрами реального і відновленого трафіка вказують на аномалії; «Нейронні мережі на графах» (Graph Neural Networks, GNN) враховують топологію мережі та зв'язки між вузлами; «Генеративно-змагальні мережі» (Generative Adversarial Network, GAN) створюють нові зразки трафіку чим підвищують точність виявлення рідкісних атак.

Позитивні сторони DNN: висока точність, здатність обробляти дані великих обсягів та виявляти складні нелінійних залежності. Негативні: значні обчислювальні витрати, потреба у великих обсягах даних для навчання, складність інтерпретації результатів.

Практика показала, що моделі глибинного навчання мають вищу точність у порівнянні з класичними алгоритмами. Водночас дослідники стикаються з проблемою узагальненості: алгоритми, добре навчені на певних вибірках, часто втрачають ефективність у випадку застосуванні до реального трафіку, де характер атак і поведінка користувачів постійно змінюються. Серед позитивних аспектів моделей DL слід відзначити підвищену здатність виявляти невідомі раніше аномалії, гнучкість і масштабованість, можливість використання у хмарних сервісах і на розподілених обчислювальних платформах. Водночас моделі DL мають високу потребу в обчислювальних ресурсах, допускають значну кількості хибних спрацювань, характеризуються складністю налаштування для реальних мережевих середовищ.

Підводячи підсумок, можна сказати, що моделі машинного навчання є потужним інструментом виявлення аномалій мережевого трафіку, на даний час вони демонструють високу ефективність у дослідницьких експериментах. Водночас на шляху до їх широкого практичного впровадження існує низка проблем: брак актуальних даних, складність адаптації до мінливих умов і недостатня інтерпретаційність. Подальший розвиток галузі пов'язаний із гібридними та адаптивними підходами, інтеграцією пояснюваного AI (Explainable AI, XAI) та розробкою методів, здатних працювати в реальному часі у високонавантажених розгалужених мережах.

Фахівці в галузі ML зазначають, що моделям машинного навчання притаманна здатність до вдосконалення і розвитку. В цьому аспекті визначені наступні перспективні напрямки:

1. Інтеграція гібридних моделей. Поєднання статистичних методів, класичного ML та глибинного навчання для досягнення балансу між точністю та швидкістю.
2. Адаптивне навчання. Використання онлайн- та інкрементального навчання для динамічного підлаштування під зміни в трафіку.
3. Федеративне навчання. Об'єднання локальних моделей із різних організацій без обміну самими даними, що дозволить враховувати ширший спектр сценаріїв атак.
4. Пояснюваний штучний інтелект (XAI). Розробка методів, які не лише виявляють аномалії, а й пояснюють причини їх класифікації.
5. Оптимізація під IoT та 5G. Легковагові моделі для пристроїв із обмеженими ресурсами та мереж нового покоління.
6. Використання генеративних моделей. GAN можуть допомогти створювати реалістичні сценарії атак для тестування систем.

Таким чином, майбутнє моделей ML полягає у поєднанні інтелектуальних алгоритмів і практичних механізмів їх використання, що дасть змогу ефективніше протидіяти новим кіберзагрозам та підвищити стійкість комп'ютерних мереж.

Владислав ПАВЛЕНКО
здобувач вищої освіти другого (магістерського) ступеня,
1 курсу, спеціальності 125 «Кібербезпека та захист інформації»,
Державний університет «Київський авіаційний інститут»
7328430@stud.nau.edu.ua

Наталя БІЛОУС
кандидат педагогічних наук, доцент кафедри
іноземних мов професійного спрямування,
Державний університет «Київський авіаційний інститут»
natalia.bilous@npp.kai.edu.ua

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У КІБЕРБЕЗПЕЦІ

У сучасному цифровому світі інформація перетворилася на найцінніший ресурс, а її захист - на ключовий фактор стабільності держав, бізнесу та суспільства. Зростання обсягів даних, розвиток хмарних технологій і глобальна цифровізація створили безпрецедентні можливості, але водночас - і нові загрози. Кібератаки стають дедалі складнішими, їх масштаби - глобальними, що в свою чергу вимагає впровадження нових підходів до безпеки.

Одним із найперспективніших напрямів є використання штучного інтелекту (ШІ) - технології, здатної аналізувати величезні масиви даних, виявляти закономірності та швидко реагувати на інциденти. ШІ у сфері кібербезпеки відкриває нові можливості для прогнозування, запобігання та мінімізації наслідків атак.[1]

Системи на основі ШІ широко використовуються для виявлення вторгнень, аналізу аномалій, моделювання поведінки та автоматизованого реагування. Зокрема, алгоритми машинного навчання шукають нестандартну активність у мережевому трафіку чи поведінці користувачів, що може свідчити про можливе вторгнення. Такі системи аналізують шаблони активності й виявляють ознаки кібератак у реальному часі, автоматично реагуючи на загрози та блокуючи їх. [1]

Крім того, ШІ також допомагає розпізнавати фішингові атаки. Системи обробки природної мови та аналізу зображень сканують електронні листи чи веб-сторінки на предмет підозрілих патернів, що характерні для фішингу. Крім того, використовуються моделі поведінкового моделювання. Однією з таких платформ є CrowdStrike Signal, яка має можливість створення індивідуальних профілів користувачів і відслідковування навіть найменших відхилень в їхній активності.Завдяки цьому «сигнали» атаки виявляються ще на ранніх етапах.[2]

Не менш важливим є автоматизоване реагування на атаки за допомогою ШІ. Наприклад, Microsoft Defender для кінцевих пристроїв використовує «AI-powered security». Згідно з заявою Microsoft, їхнє рішення за допомогою ШІ здатне в середньому зупиняти атаки-вимагальники вже через три хвилини після початку. Ця технологія базується на безперервному навчанні моделей, що дає змогу швидко адаптуватись до нових варіантів атак.[3]

Яскравим прикладом впровадження технологій ШІ на українському IT-ринку є LetsData. Даний стартап створив рішення на базі ШІ для миттєвого виявлення загроз і аналізу даних у реальному часі. Від моменту запуску їхня система на основі ШІ продемонструвала динамічний розвиток: компанія розпочала роботу на ринку США, водночас зберігаючи основний центр розробки технологій і продуктів у Європі. Окрім цього, цей проєкт вже залучений до міжнародної акселераційної програми AI for Cybersecurity.[4]

Ще одним вітчизняним стартапом, що використовує ШІ, є Mantis Analytics, що спочатку функціонував як волонтерський проєкт, побудував платформу ситуаційної обізнаності: її система в реальному часі збирає дані з соцмереж, визначає тенденції російської пропаганди і готує аналітичні звіти для Ради нацбезпеки. Ця платформа допомагає розпізнавати дезінформаційні кампанії та координувати превентивні заходи. Таким чином, українські рішення на основі ШІ доповнюють традиційні засоби захисту та дозволяють стрімко реагувати на ворожі кіберзагрози[5]

Отже, ШІ стає ключовим ресурсом у сучасній кібербезпеці, спрямовуючи захист у нове русло швидкої адаптації та автоматизації. Завдяки алгоритмам машинного та глибокого навчання підвищується точність виявлення атак і зменшується кількість хибних спрацювань, а автономні системи реагування забезпечують майже миттєве блокування загроз.

Список використаних джерел

1. Розуміння штучного інтелекту для кібербезпеки https://www.microsoft.com/uk-ua/security/business/security-101/what-is-ai-for-cybersecurity#:~:text=%D0%A8%D0%86%20%D0%B4%D0%BB%D1%8F%20%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8%C2%A0%E2%80%93%20%D1%86%D0%B5%20%D0%B2%D0%B8%D0%BA%D0%BE%D1%80%D0%B8%D1%81%D1%82%D0%B0%D0%BD%D0%BD%D1%8F,%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8%20%D0%B2%20%D1%80%D0%B5%D0%B6%D0%B8%D0%BC%D1%96%20%D1%80%D0%B5%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D0%B3%D0%BE%20%D1%87%D0%B0%D1%81%D1%83
2. CrowdStrike Signal - новий рівень виявлення загроз на основі ШІ https://iitd.ua/crowdstrike-signal-novyj-riven-vyyavlennya-zagroz-na-osnovi-shi/#:~:text=CrowdStrike%20Signal%20%E2%80%93%20%D0%BD%D0%BE%D0%B2%D0%B8%D0%B9%20%D1%80%D1%96%D0%B2%D0%B5%D0%BD%D1%8C,%D0%B2%D0%B8%D1%8F%D0%B2%D0%BB%D0%B5%D0%BD%D0%BD%D1%8F%20%D0%B7%D0%B0%D0%B3%D1%80%D0%BE%D0%B7%20%D0%BD%D0%B0%20%D0%BE%D1%81%D0%BD%D0%BE%D0%B2%D1%96%20%D0%A8%D0%86
3. Microsoft Defender Get ahead of threat actors with integrated security solutions https://www.microsoft.com/en-us/security/business/microsoft-defender#:~:text=AI,for%20Endpoint
4. 17 стартапів використовують штучний інтелект, щоб змінити майбутнє кібербезпеки https://ukraine.googleblog.com/2024/02/17.html#:~:text=%D0%92%D1%96%D0%B9%D0%BD%D0%B0%2C%20%D1%89%D0%BE%20%D1%82%D1%80%D0%B8%D0%B2%D0%B0%D1%94%20%D0%B2%20%D0%A3%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D1%96%2C,%D0%B2%D0%BE%D0%BD%D0%B8%20%D1%80%D0%BE%D0%B7%D0%BF%D0%BE%D1%87%D0%B0%D0%BB%D0%B8%20%D0%B4%D1%96%D1%8F%D0%BB%D1%8C%D0%BD%D1%96%D1%81%D1%82%D1%8C%20%D1%83%20%D0%A1%D0%A8%D0%90
5. Хай вам бот помога. Як ШІ-розробки в Україні та світі змінюють хід війни https://www.platfor.ma/topic/haj-vam-bot-pomoga-yak-shi-rozrobky-v-ukrayini-ta-sviti-zminyuyut-hid-vijny/#:~:text=%D0%86%D1%81%D0%BD%D1%83%D1%94%20%D1%87%D0%B8%D0%BC%D0%B0%D0%BB%D0%BE%20%D0%BF%D0%BE%D1%82%D1%83%D0%B6%D0%BD%D0%B8%D1%85%20%D1%81%D1%82%D0%B0%D1%80%D1%82%D0%B0%D0%BF%D1%96%D0%B2%20%D0%B2%D1%96%D0%B4,%D1%80%D0%B5%D0%B0%D0%B3%D1%83%D0%B2%D0%B0%D1%82%D0%B8%20%D1%82%D0%B0%20%D0%BE%D1%80%D0%B3%D0%B0%D0%BD%D1%96%D0%B7%D0%BE%D0%B2%D1%83%D0%B2%D0%B0%D1%82%D0%B8%20%D0%BF%D1%80%D0%B5%D0%B2%D0%B5%D0%BD%D1%82%D0%B8%D0%B2%D0%BD%D1%96%20%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D1%96

Василь БАРТКО
адвокат, партнер Адвокатського об'єднання «МВМ ЛІГАЛ»
eno5orladvocat@gmail.com

ПРОБЛЕМИ ПРАВОВОГО РЕГУЛЮВАННЯ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ У КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Швидкий розвиток технологій штучного інтелекту привів людство до переломного моменту, коли інновації розвиваються швидше, ніж можуть за ними встигати право та етика. Україна, як і багато інших країн, зараз стоїть перед викликом адаптації своєї правової системи до явищ, які ще кілька десятиліть тому були немислимими.

Штучний інтелект вже проник у економічну, соціальну та політичну сфери, впливаючи не тільки на бізнес-процеси та комунікацію, а й на основи прийняття рішень людиною.

На національному рівні українська держава вже визнала важливість регулювання штучного інтелекту. У нині недіючому Державному стандарті України ДСТУ 2938-94 «Системи обробки інформації» штучний інтелект визначається як «здатність систем обробки даних виконувати функції, пов'язані з людським інтелектом, такі як логічне мислення, навчання та самовдосконалення».

Більш комплексне та орієнтоване на політику розуміння з'явилося пізніше в Концепції розвитку штучного інтелекту в Україні, затвердженій наказом Кабінету Міністрів України № 1556-р від 2 грудня 2020 року, яка визначає ШІ як організований комплекс інформаційних технологій, що дозволяє виконувати складні завдання за допомогою наукових методів дослідження та алгоритмів обробки інформації, отриманої або самостійно створеної під час роботи [4].

Таке ж тлумачення було підтверджено в Постанові Кабінету Міністрів України № 320-р від 13 квітня 2024 року «Концепція державної цільової науково-технічної програми використання технологій штучного інтелекту в пріоритетних галузях економіки на період до 2026 року» [5].

Як неодноразово зазначали дослідники, саме поняття «інтелект» є нечітким, а в застосуванні до технічних систем стає ще більш неоднозначним. Українська термінологія значною мірою запозичена з англійської мови, де штучний інтелект означає імітацію когнітивних здібностей людини, але не їх повне відтворення. Когут Ю. І., відзначив, що, незважаючи на тривалу історію розвитку штучного інтелекту, досі немає єдиного розуміння його сутності та чіткого визначення терміну [3 с. 30].

Коли автономна система діє незалежно — наприклад, при прийнятті фінансових рішень, діагностуванні пацієнтів або керуванні транспортними засобами — стає незрозумілим, хто несе відповідальність за можливу шкоду.

Існуюче українське цивільне право передбачає, що суб'єктом відповідальності є фізична або юридична особа. Однак штучний інтелект ставить під сумнів цю традиційну логіку, функціонуючи у спосіб, який не може бути передбачений або повністю контрольований його творцями.

В результаті науковці та законодавці стикаються з дилемою: чи слід визнати ШІ особливою юридичною особою, чи вся відповідальність має і надалі покладатися на його розробників та користувачів. О. А. Баранов визначив ШІ як «сукупність методів, засобів і технологій, переважно комп'ютерних, що імітують (моделюють) когнітивні функції, які мають критерії, характеристики та показники, еквівалентні тим, що притаманні інтелектуальній діяльності людини» [1].

Штучний інтелект не залишається пасивним; він діє, налаштовує, вирішує. Автономність робить штучний інтелект сильним. Таким чином, існує небезпека в силі автономних систем штучного інтелекту, оскільки технічна помилка є не єдиним місцем, звідки можуть виходити загрози, а й соціальними та політичними алгоритмічними рішеннями.

Маніпулювання громадською думкою за допомогою контенту, створеного ШІ, поширення дезінформації та потенційне використання ШІ в кібервійні становлять реальну загрозу національній безпеці. Для України, яка вже діє в умовах гібридної війни, регулювання технологій на основі ШІ повинно включати механізми моніторингу та запобігання їх зловживанню.

Однак поточні національні стратегії вирішують питання безпеки переважно через посилання на міжнародні стандарти, а не через конкретні внутрішні норми.

У резолюції Європейського парламенту від 16 лютого 2017 року штучний інтелект характеризується як інтелектуальний робот, що володіє автономністю завдяки сенсорним датчикам і обміну даними, здатний вчитися на досвіді та взаємодії, адаптувати свою поведінку до навколишнього середовища і функціонувати незалежно, хоча і не є біологічно живим [8].

Штучний інтелект кидає виклик людським цінностям, свободі вибору та тому, якою мірою технологічний прогрес може проникати в особисте життя. При використанні в правоохоронних органах, підборі персоналу чи навіть у сфері охорони здоров'я ці системи безперечно впливають на людей – у більшості випадків без прозорості та підзвітності. Таким чином, створення етичних норм як частини самої правової системи, а не просто рекомендаційного принципу [6].

Ідея розробки Кодексу етики для ШІ в Україні є перспективною, але вона повинна бути підкріплена обов'язковими правовими механізмами, що забезпечують справедливість, пояснюваність та повагу до людської гідності в усіх рішеннях, що базуються на ШІ.

Український контекст, що характеризується швидким цифровим зростанням, постійними викликами у сфері безпеки та обмеженим інституційним потенціалом, вимагає адаптивних моделей регулювання, що поєднують інновації з суворим наглядом. Правові рамки повинні гарантувати, що ШІ служить суспільним інтересам, не підриваючи людський контроль над технологіями [7].

Проблеми правового регулювання та безпеки використання штучного інтелекту в Україні відображають більш широку необхідність переосмислити відносини між людьми та інтелектуальними системами. ШІ стає як об'єктом, так і суб'єктом правової рефлексії — інструментом, що виявляє обмеження традиційної юриспруденції.

Головне завдання сьогодні — забезпечити, щоб розвиток штучного інтелекту сприяв суспільному благу, одночасно захищаючи національну безпеку та права людини.

У довгостроковій перспективі створення узгодженої системи регулювання ШІ в Україні вимагає не тільки законодавчої точності, а й етичного передбачення та координації з міжнародними партнерами для забезпечення безпечного, відповідального та орієнтованого на людину використання штучного інтелекту.

Список використаних джерел

1. Baranov, O.A. (2023) 'Vyznachennia terminu "shtuchnyi intelekt" [Definition of the term "artificial intelligence"]', Informatsiia i pravo, 1(44), pp. 32–49. Available at: https://ippi.org.ua/sites/default/files/5_28.pdf
2. Derzhavnyi Standart Ukrainy (1994) DSTU 2938-94. Systemy obroblennia informatsii [Information Processing Systems]. Available at: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=77434
3. Kohut, Yu.I. (2024) Shtuchnyi intelekt i bezpeka [Artificial Intelligence and Security]. Edited by A.S. Dovhopolyi. Kyiv: SIDKON; Dakor, 294 p. Available at: https://jurkniga.ua/contents/shtuchniy-intelekt-i-bezpeka.pdf?srsltid=AfmBOooNL35wjNRt5sRunK-hlZMmJZf4peXn-spr3aPFFhJnX5JUPGgm
4. Cabinet of Ministers of Ukraine (2020) Rozporiadzhennia vid 2 hrudnia 2020 r. No. 1556-r "Pro skhvalennia Kontseptsii rozvytku shtuchnoho intelektu v Ukraini" [Order No. 1556-r of December 2, 2020, On Approval of the Concept for the Development of Artificial Intelligence in Ukraine]. Available at: https://zakon.rada.gov.ua/laws/show/1556-2020-p#Text
5. Cabinet of Ministers of Ukraine (2024) Rozporiadzhennia vid 13 kvitnia 2024 r. No. 320-r "Kontseptsiia Derzhavnoi tsilovoi naukovo-tekhnichnoi prohramy z vykorystannia tekhnolohii shtuchnoho intelektu v priorytetnykh haluziakh ekonomiky na period do 2026 roku" [Order No. 320-r of April 13, 2024, On the Concept of the State Target Scientific and Technical Program on the Use of Artificial Intelligence Technologies in Priority Economic Sectors until 2026]. Available at: https://zakon.rada.gov.ua/laws/show/320-2024-p#Text

6. Skitsko, O., Skladanyi, P., Shyrshov, R., Humeniuk, M. and Vorokhob, M. (2023) ‘Zahrozy ta ryzyky vykorystannia shtuchnoho intelektu [Threats and risks of using artificial intelligence]’, Kiberbezpeka: osvita, nauka, tekhnika, (2). Available at: https://csecurity.kubg.edu.ua/index.php/journal/article/view/520/408

7. Tiuria, Yu.I. (2022) ‘Analiz filosofsko-pravovykh pidkhodiv do vyznachennia poniattia “shtuchnyi intelekt” [Analysis of philosophical and legal approaches to defining the concept of “artificial intelligence”]’, Naukovyi visnyk Mizhnarodnoho humanitarnoho universytetu. Seriia: Yurysprudentsiia, (56). Available at: https://www.vestnik-pravo.mgu.od.ua/archive/juspradenc56/12.pdf

8. European Parliament (2017) Resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)) Official Journal of the European Union, 252 C, pp. 242–257. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017IP0051

Róbert VARGA
Third year Bachelor student,
"Informatics" major,
Ferenc Rakoczi II Transcarpathian Hungarian University

Katalin KUCHINKA
PhD, Associate professor,
Department of Mathematics and Informatics,
Ferenc Rakoczi II Transcarpathian Hungarian University

COMPARATIVE PERFORMANCE OF LARGE LANGUAGE MODELS IN SOLVING MATHEMATICAL AND COMPUTER SCIENCE PROBLEMS

The rapid adoption of Large Language Models (LLMs) in technical domains necessitates a rigorous, comparative assessment of their core computational abilities. Despite architectural advances, a performance gap persists in tasks requiring true mathematical reasoning and error-free algorithmic generation. This study addresses this gap by quantifying the proficiency differential across leading LLMs (ChatGPT, Claude, Gemini, Mistral) in complex Computer Science and Mathematics problems to identify specific systemic limitations.

This research aims to compare the performance of various large language models (LLMs) — such as ChatGPT, Claude, Gemini, and Mistral — in solving mathematical and computer science problems. Findings indicate that LLMs demonstrate significant differences in logical reasoning, algorithmic thinking, and programming task performance. According to Moon [1], more advanced models show improved accuracy in mathematical derivations but still exhibit frequent logical and syntactic errors. Zhao [2] emphasizes that despite architectural advancements, consistent mathematical reasoning remains a challenge for current LLMs. Noveski [3] highlights that code generation success largely depends on prompt structure and task complexity. In educational contexts, the study by Emerging Investigators [4] shows that LLMs can effectively support mathematics learning but still require improvements in explanation depth and accuracy. Overall, large language models are promising tools for enhancing algorithmic and problem-solving skills, though their performance remains context-dependent and cannot yet substitute human expertise.

Conclusion. While LLMs show a promising ability to enhance algorithmic and problem-solving skills and serve as effective, though imperfect, educational support tools, their performance remains fundamentally context-dependent. The persistent occurrence of logical and syntactic errors in complex mathematical derivations and the variability of code generation success confirm that current LLM architectures cannot yet reliably substitute the human capacity for domain-specific expertise and rigorous logical verification.

References

1. Moon, I. H. (2025). Performance Comparison of Large Language Models on Advanced Calculus Problems. arXiv. Available at: https://arxiv.org/abs/2503.03960

2. Zhao, W. X. (2023). A Survey of Large Language Models. arXiv. Available at: https://arxiv.org/abs/2303.18223

3. Noveski, G. (2024). Comparison of Large Language Models in Generating Code Solutions. Electronics, 13(20). Available at: https://www.mdpi.com/2079-9292/13/20/4109

4. Comparison of Three Large Language Models as Middle School Math Tutoring Assistants. (2024). Emerging Investigators. Available at: https://emerginginvestigators.org/articles/23-253

Katalin KUCHINKA
PhD, Associate professor,
Department of Mathematics and Informatics,
Ferenc Rakoczi II Transcarpathian Hungarian University

THINKING AS A TOOL FOR DEFENSE AGAINST DIGITAL DISINFORMATION

The proliferation of digital disinformation represents a critical threat to informed citizenship, necessitating novel cognitive defense mechanisms. This research investigates the hypothesis that the integration of critical, mathematical, and algorithmic thinking fundamentally strengthens individuals' cognitive resilience against manipulative digital content. Drawing on the Information Disorder framework [2], the study proposes educational interventions focused on recognizing algorithmic biases and logical contradictions inherent in manipulative narratives.

One of the greatest challenges of the digital age is recognizing and countering disinformation. The aim of this research is to explore how critical, mathematical, and algorithmic thinking can strengthen cognitive resilience against digital manipulation. The theoretical foundation builds on the work of Lewandowsky, Ecker, and Cook [1], who analyze the "post-truth" era and demonstrate how information overload and cognitive biases distort human judgment. Wardle and Derakhshan's [2] Information Disorder framework expands this by categorizing misinformation into three types (disinformation, misinformation, and malinformation) and emphasizing the role of educational interventions in developing resistance.

The methodological framework focuses on integrating algorithmic and critical thinking into education. According to Wing [3], computational thinking is not only a technological skill but also a universal problem-solving framework that helps identify patterns, logical contradictions, and manipulative structures. This study applies such principles through educational practice — data analysis, source comparison, and algorithmic simulations — enabling learners to interpret information logically and systematically.

The expected results show that enhancing structured thinking increases individuals' cognitive resilience, reduces susceptibility to manipulation, and fosters conscious digital citizenship. Krekó's [4] social-psychological research supports this conclusion, showing that the best defense against irrational beliefs and conspiracy theories lies in education and information literacy. This research contributes to strengthening digital security, media awareness, and cognitive defense in the complex informational environment of the 21st century.

Conclusion. This research demonstrates that developing structured, algorithmic thinking significantly boosts cognitive resilience and defense against digital manipulation. By applying principles of computational thinking (e.g., pattern recognition, logical decomposition) to information analysis, individuals can systematically counter cognitive biases and enhance their digital citizenship. The findings support the shift toward integrating these quantitative and logical frameworks into media literacy education to combat 21st-century informational challenges.

References

1. Lewandowsky, S., Ecker, U. K., & Cook, J. (2017). Beyond Misinformation: Understanding and Coping with the "Post-Truth" Era. Journal of Applied Research in Memory and Cognition, 6(4), 353–369.

2. Wardle, C., & Derakhshan, H. (2018). Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making. Council of Europe Report, Strasbourg.

3. Wing, J. M. (2006). Computational Thinking. Communications of the ACM, 49(3), 33–35.

4. Krekó, P. (2020). Mass Paranoia: The Social Psychology of Conspiracy Theories and Fake News. Athenaeum Publishing.

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.

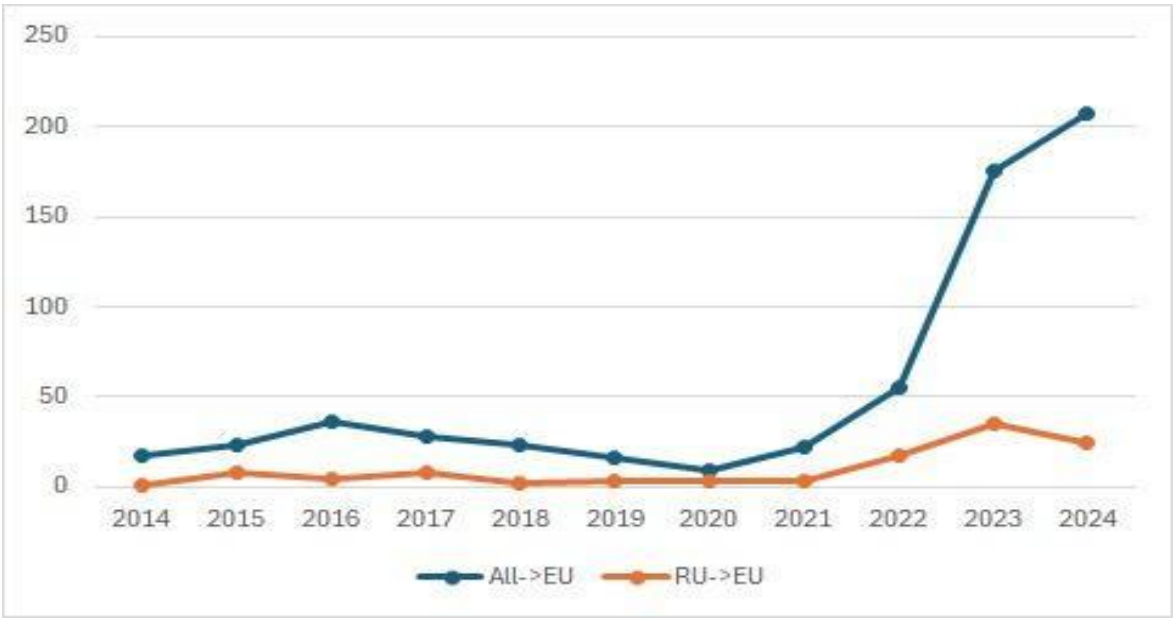


Fig. 1. Number of cyber incidents against the EU, 2014-2024, [compiled based on data from EuRepoC, 2025].

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.

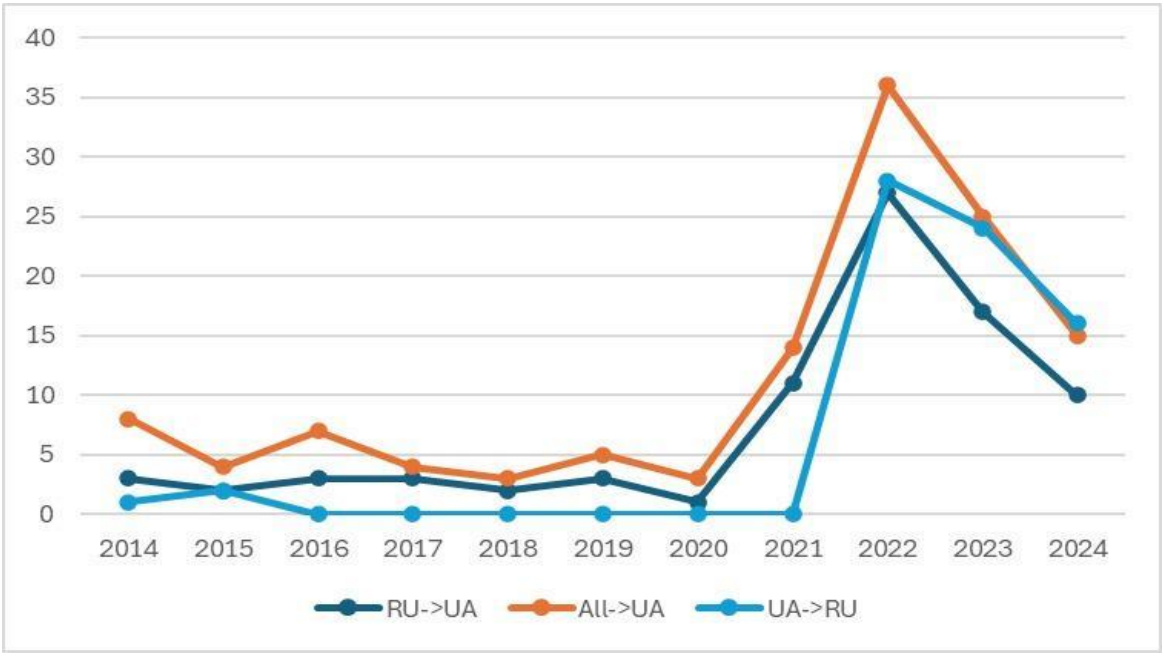


Fig. 2. Number of cyber incidents against Ukraine and the Russian Federation, 2014-2024, [compiled based on data from EuRepoC, 2025].

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.

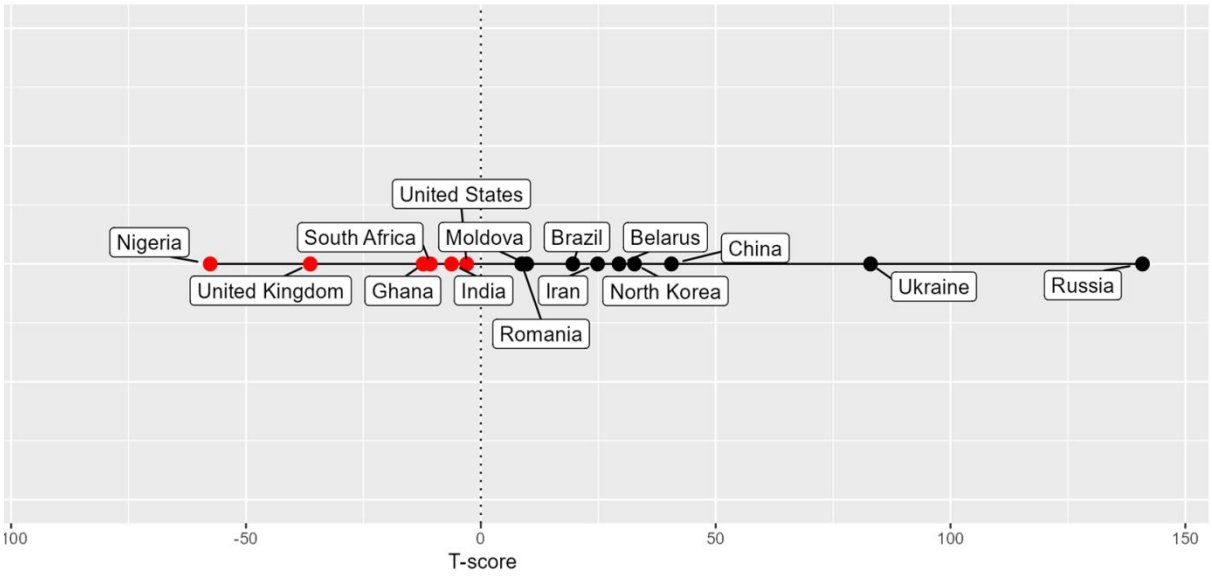


Fig. 3. Technical indicators (T-score) of the 15 best-performing countries, WCI.

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

József HOLOVÁCS
Doctor of Technical Sciences, Professor,
Department of Mathematics and Informatics,
Ferenc Rakoczi II Transcarpathian Hungarian University,

Adam DOROVTSI
PhD (Applied mathematics),
Department of Mathematics and Informatics,
Ferenc Rakoczi II Transcarpathian Hungarian University

DATABASE PROTECTION IN WEB APPLICATIONS

Web applications are widely used in business, science, and everyday life. The main element that ensures the storage and processing of information is the database (DB). However, the database is often the weakest link in the structure of information systems. Attackers use various methods that can lead to data leakage, forgery, or destruction. Therefore, ensuring the security of databases in web applications is of critical importance.

Main Threats to Database Security

- SQL Injections. This is one of the most common attacks, in which an attacker inserts specially crafted SQL code into a form or URL that is then executed by the database. As a result, the attacker may gain unauthorized access, modify, or delete data.
- XSS (Cross-Site Scripting). In this case, a malicious JavaScript script is embedded into a web page. When a user opens the page, the script executes in their browser, which can lead to the theft of cookies, passwords, or session data.
- DoS/DDoS Attacks. These attacks aim to overload the server with a large number of requests. In the case of DDoS, requests come simultaneously from many devices, making the web application and its database inaccessible to legitimate users.
- Unauthorized Access. Attackers often try to guess or steal administrator and user passwords. Weak passwords and the absence of multi-factor authentication significantly increase the risk of system compromise.
- Data Leakage. Misconfigured servers or lack of encryption during data transmission (for instance, absence of HTTPS) can result in sensitive information being intercepted.

Methods for Database Protection

- Parameterized Queries. The use of prepared statements instead of dynamically generated SQL queries effectively prevents SQL injections.
- Validation and Filtering of Input Data. Checking the format, length, and data type helps reduce the risk of injecting malicious code.
- Protection Against XSS. Implemented through HTML character escaping, Content Security Policy (CSP), and input sanitization.
- Access Control. Applying the principle of least privilege and multi-factor authentication protects the system from both internal and external threats.
- Encryption. Employing TLS/SSL for data transmission and storing passwords in a hashed and salted form enhances data confidentiality.
- Monitoring and Auditing. Continuous analysis of access logs, detection of suspicious activities, and the use of intrusion detection and prevention systems (IDS/IPS) help respond promptly to threats.

Conclusions

Database protection in web applications is a multifaceted task requiring a comprehensive approach. The key areas include preventing SQL injections, XSS, and DoS/DDoS attacks, as well as implementing modern encryption and access control methods. A robust security system not only preserves data integrity but also strengthens user trust in the web application.

References

1. Halfond, W.G.J., Viegas, J. and Orso, A. (2006) A classification of SQL-injection attacks and countermeasures. Proceedings of the IEEE International Symposium on Secure Software Engineering, pp. 13–15.
2. OWASP (2021) OWASP Top Ten Web Application Security Risks. Available at: https://owasp.org/www-project-top-ten/ (Accessed: 23 September 2025).
3. Stallings, W. (2017) Network Security Essentials: Applications and Standards. 6th edn. Pearson.
4. Шелест, О. (2020) Інформаційна безпека: навчальний посібник. Київ: Кондор.
5. Яковенко, В. (2021) Захист інформації у комп’ютерних системах та мережах. Харків: ХНУРЕ.

Нікіта ПАЛІНКАШ
магістр 2 курсу спеціальності 126 Інформаційні системи і технології
ДВНЗ «Ужгородський національний університет»
palinkash.nikita@student.uzhnu.edu.ua

Василь КУТ
завідувач кафедри інформатики та фізико-математичних дисциплін
ДВНЗ «Ужгородський національний університет»
kut.vasyl@uzhnu.edu.ua

ПРОЄКТУВАННЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ ДЛЯ ФОТОСТУДІЇ: АНАЛІЗ ТА ІНТЕГРАЦІЯ АРХІТЕКТУРНИХ РІШЕНЬ ІЗ ЗАБЕЗПЕЧЕННЯМ БЕЗПЕКИ ДАНИХ

В умовах тотальної цифровізації бізнес-процесів впровадження спеціалізованих інформаційних систем (ІС) є критичною передумовою для забезпечення конкурентоспроможності та ефективного функціонування сучасних фотостудій. Актуальність проєктування інформаційної системи для фотостудії визначається критичним збігом стратегічних економічних та технологічних чинників. На ринку послуг, де клієнт очікує миттєвої реакції та високоперсоналізованого підходу, використання ручних або неінтегрованих методів управління бізнес-процесами стає суттєвим стримуючим фактором. З економічної точки зору, впровадження ефективної ІС є не просто автоматизацією, а стратегічним інструментом для оптимізації управління ресурсами, бронюванням, графіками роботи фахівців та фінансовим обліком. Це дозволяє мінімізувати операційні помилки, пов'язані з конфліктами графіків та ресурсів, та забезпечує керівництво студії оперативними аналітичними даними для ухвалення ефективних управлінських рішень, що безпосередньо впливає на рентабельність та конкурентоспроможність [2].

Розширення спектру послуг фотостудії, від приватних фотосесій до великих комерційних проєктів, висуває жорсткі технологічні вимоги до гнучкості та масштабованості ІС. Традиційні монолітні архітектурні рішення, що не здатні швидко адаптуватися до нових функціональних вимог, стають неефективними. Тому актуальним є аналіз та впровадження сучасних архітектурних патернів, таких як мікросервісна архітектура, яка забезпечує декомпозицію ризиків, дозволяючи незалежно оновлювати та масштабувати окремі функціональні модулі, підвищуючи загальну відмовостійкість системи.

Метою роботи є обґрунтування комплексної архітектурно-технологічної моделі інформаційної системи для фотостудії, яка має забезпечити не лише високоефективну автоматизацію ключових бізнес-операцій, але й підтримувати високу швидкодію, гнучкість, а також гарантований рівень безпеки даних на архітектурному рівні. Досягнення цієї мети вимагає послідовного аналізу бізнес-вимог сучасної фотостудії, включаючи управління клієнтським досвідом, планування ресурсів та фінансову звітність. Необхідно здійснити критичний огляд і порівняльний аналіз існуючих архітектурних патернів, таких як монолітна, багаторівнева та мікросервісна архітектура, для визначення найбільш адаптивної моделі, здатної забезпечити необхідну декомпозицію функціоналу та відмовостійкість при зростанні навантаження. На основі цього аналізу буде розроблено структурно-функціональну модель ІС, включаючи модулі, API-інтерфейси та логічну схему бази даних.

Наукова новизна дослідження полягає у систематизації та інтеграції принципів проєктування гнучкої, ймовірно мікросервісної, архітектури ІС із систематичним вбудовуванням механізмів «Security by Design» безпосередньо у базові елементи системи, що є інноваційним підходом для галузевих рішень у сфері послуг.

На методологічному рівні робота ґрунтується на системному аналізі, теорії баз даних та сучасних принципах кібербезпеки. Виходячи з необхідності незалежного масштабування та розподілу ризиків, мікросервісна архітектура розглядається як найбільш доцільна основа, що дозволяє створювати автономні сервіси для бронювання, галереї, фінансового обліку тощо. Інтеграція безпеки реалізується на трьох ключових рівнях: на рівні доступу – через

використання контролю доступу на основі ролей (RBAC) та сучасних механізмів автентифікації; на рівні передачі даних – через застосування протоколу TLS; і на рівні зберігання – через обов'язкове криптографічне перетворення (шифрування AES-256) конфіденційних полів у базі даних та забезпечення захищеного сховища для медіа-файлів [1]. Фінальним завданням є техніко-економічне обґрунтування обраного рішення, яке продемонструє його ефективність порівняно з існуючими альтернативами.

Практична значущість дослідження полягає у створенні методологічної основи, яка може бути використана для розробки функціональних, високопродуктивних та, головне, надійних інформаційних систем для малих та середніх підприємств у сфері фотографічних послуг. Очікувані результати включають значне зменшення операційних витрат та підвищення клієнтської довіри за рахунок гарантованої безпеки даних та відповідності ІС міжнародним та національним вимогам щодо захисту персональних даних. Таким чином, пропонована модель проєктування забезпечує не лише технологічну ефективність, але й стратегічну стійкість бізнесу фотостудії до сучасних викликів.

Список використаних джерел

1. Бакай О.В. Особливості побудови системи та застосування криптографічного алгоритму AES. Комп'ютерні системи та мережі. 2014. №806. С.3-10.

2. Вдовичин Т.Я., Лазурчак Л.В. Проектування інформаційно-пошукових систем як засіб використання сучасних технологій. Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки. 2022. Т. 33(72). № 4. С. 66-71.

Михайло ТЯСКО
магістр освітньої програми «Управління ІТ проєктами»
Ужгородський національний університет
tiasko.mykhailo@student.uzhnu.edu.ua

Ігор ЛЯХ
доктор технічних наук, професор,
професор кафедри інформатики та фізико-математичних дисциплін
Ужгородський національний університет
igor.lyah@uzhnu.edu.ua

АДАПТИВНИЙ АЛГОРИТМ ТРАНСКОРДОННОГО ОБМІНУ ІНФОРМАЦІЄЮ ПРО КІБЕРЗАГРОЗИ

Транскордонна співпраця у сфері кіберзахисту залишається складним завданням через поєднання технічних, правових та організаційних бар'єрів. Взаємодія між державами чи організаціями часто ускладнюється нерівномірним рівнем довіри, адже навіть у межах домовленостей партнери можуть по-різному оцінювати ризики та ступінь відкритості даних. Додатковим обмеженням виступають відмінності у правових режимах, зокрема вимоги до захисту персональних даних як GDPR (General Data Protection Regulation) чи національні регуляції, що обмежують передачу чутливої інформації. Не менш значущим є питання технічної сумісності, оскільки інфраструктури кіберзахисту часто базуються на різних стандартах і протоколах. У сукупності ці чинники створюють потребу у спеціальному алгоритмі, здатному адаптивно координувати обмін інформацією про кіберзагрози з урахуванням довіри, юридичних вимог і технічних можливостей.

Концепція підходу TACB-CDA (Trust-Adaptive Cross-Border Cyber Defense Algorithm) полягає у створенні адаптивного механізму транскордонного обміну інформацією про кіберзагрози, який інтегрує фактори довіри, юридичних обмежень та технічної сумісності у єдиний процес прийняття рішень. На відміну від класичних моделей, орієнтованих на фіксовані протоколи взаємодії, запропонований алгоритм враховує контекст ситуації та динамічно обирає оптимальний формат обміну – від повного розкриття даних до передачі агрегованих метаданих чи сигнатур загроз. Такий підхід забезпечує не лише підвищення рівня безпеки й оперативності реагування, а й мінімізує ризики витоку чутливої інформації, формуючи підґрунтя для більш стійкої та довгострокової співпраці між державними та міжорганізаційними структурами.

Ключові параметри алгоритму TACB-CDA охоплюють багатовимірну систему критеріїв, що визначають можливості та формат обміну інформацією між сторонами. Передусім враховується рівень довіри, який може коливатися від високого до низького і безпосередньо впливає на ступінь відкритості даних. Важливими є і типи кіберзагрози, такі як: локальна подія, потенційно транскордонний інцидент або активна атака, що поширюється за межі однієї юрисдикції, вимагають різних стратегій реагування. Значущим параметром виступає конфіденційність інформації, адже від її чутливості залежить допустимий обсяг переданих відомостей. Крім того, алгоритм враховує юридичні обмеження, зокрема вимоги як GDPR чи національних регуляцій, що можуть обмежувати або модифікувати умови обміну. Завершальним фактором є технічна сумісність, тобто наявність у партнерів спільних протоколів і стандартів, що дозволяє забезпечити ефективну інтеграцію уніфікованих рішень.

Алгоритм TACB-CDA реалізує поетапну процедуру взаємодії, де кожен крок формує основу для прийняття подальших рішень. Початковим етапом є виявлення кіберзагрози та її класифікація за рівнем серйозності й потенційною транскордонністю. Далі відбувається оцінка рівня довіри до партнера, що визначає допустимий формат обміну даними – від повного розкриття інформації до передачі агрегованих метаданих чи сигнатур загроз.

На наступному етапі здійснюється перевірка правових та технічних обмежень, які можуть модифікувати чи звузити можливості співпраці. Після цього інформація передається або

синхронізується через захищений канал зв'язку, із можливістю отримання зворотного зв'язку обміну інформацією для уточнення чи доповнення даних. Завершальною фазою виступає адаптація політик безпеки обох сторін, що дозволяє поступово гармонізувати підходи до реагування та підвищувати стійкість транскордонного кіберзахисту. Для графічного сприйняття, розроблена та спроєктована блок-схема даного алгоритму на рисунку 1.

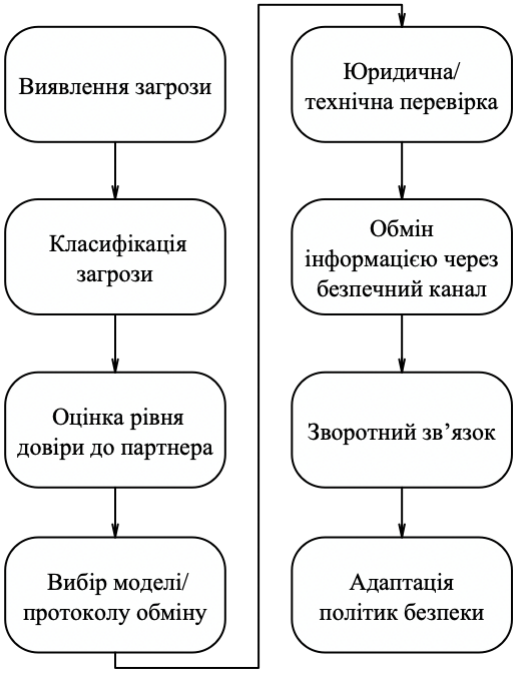


Рисунок 1. Блок-схема TACB-CDA

У межах TACB-CDA передбачено кілька варіантів обміну інформацією, які обираються залежно від рівня довіри та правових обмежень. За умов високої довіри та відсутності юридичних бар'єрів можливе повне розкриття даних про загрозу. Якщо довіра середня, доцільним стає обмін агрегованими метаданими, що дозволяє зберегти баланс між інформативністю та безпекою. У випадках низької довіри чи суворих регуляцій обмежуються передачею сигнатур або індикаторів атаки, достатніх для виявлення подібних загроз без розкриття чутливої інформації. Запропонований підхід TACB-CDA забезпечує адаптивність до різних рівнів довіри та правових чи технічних бар'єрів, мінімізуючи ризик витоку чутливих даних. Він створює умови для поступової гармонізації політик кіберзахисту та підвищення стійкості транскордонної співпраці.

Таким чином, алгоритм TACB-CDA формує основу для безпечної та ефективної транскордонної співпраці, забезпечуючи баланс між оперативністю реагування, конфіденційністю та технічною сумісністю.

Список використаних джерел

1. Fang, J., Tang, Y., & Guo, M. (2024). Comprehensive Review of Cyber Threat Intelligence Sharing: Challenges and Methodologies. In Proceedings of the 4th Asia-Pacific Artificial Intelligence and Big Data Forum. 455-461. https://doi.org/10.1145/3718491.3718565

2. Nweke, L. O., & Wolthusen, S. (2020, May). Legal issues related to cyber threat information sharing among private entities for critical infrastructure protection. In 2020 12th international conference on cyber conflict (cyCon) 1300, 63-78. IEEE.

3. Neisse, R., Hernández-Ramos, J. L., Matheu-Garcia, S. N., Baldini, G., Skarmeta, A., Siris, V., ... & Nikander, P. (2020). An interledger blockchain platform for cross-border management of cybersecurity information. IEEE Internet Computing, 24(3), 19-29. https://doi.org/10.1109/MIC.2020.3002423

Валентин ЗАДЕРА
здобувач вищої освіти другого (магістерського) ступеня,
1 курсу, спеціальності F5 «Кібербезпека та захист інформації»,
Державний університет «Київський авіаційний інститут»
ValikZadera@gmail.com

Наталя БІЛОУС
кандидат педагогічних наук, доцент кафедри
іноземних мов професійного спрямування,
Державний університет «Київський авіаційний інститут»
natalia.bilous@npp.kai.edu.ua

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ДОСЯГНЕННЯ БЕЗПЕЧНОГО ЦИФРОВОГО ПРОСТОРУ

В сучасному світі, де цифрові технології все прогресивніше інтегруються в усі сфери життєдіяльності - від освіти до охорони здоров'я, від фінансів до державного управління – в цифровому просторі набуває критичного значення питання безпеки. З кожним днем ми стикаємося з новими викликами: кіберзлочинністю, витоком даних, дезінформацією та порушенням конфіденційності. Саме штучний інтелект - не як загроза, а як потужний інструмент захисту, який має здатність аналізувати великі обсяги даних, виявляти аномалії, прогнозувати ризики та автоматизувати реагування на загрози відкриває нові горизонти для створення безпечного цифрового середовища.

На перший погляд використання штучного інтелекту може здаватися надмірно дорогим і складним рішенням, яке під силу лише великим технологічним корпораціям. Проте в умовах стрімкого зростання цифрових загроз така інвестиція стає не розкішшю, а необхідністю для будь-якої організації - незалежно від її розміру чи галузі діяльності. Через те, що кількість кібератак невпинно зростає, а їхні методи еволюціонують з неймовірною швидкістю. Так, згідно зі статистикою компанії Kaspersky, щоквартально фіксується понад 700 мільйонів онлайн-інцидентів, а Cisco щодня блокує близько 20 мільярдів атак у мережах.[1] Це може свідчити про активне застосовування автоматизованих інструментів кіберзлочинцями, зокрема алгоритми штучного інтелекту, з метою вдосконалення своїх атак, обходу традиційних систем захисту та підвищення ефективності. Одним із прикладів складної загрози є шкідливе програмне забезпечення Emotet, яке поширюється через фішингові повідомлення. [1] Група, яка розробила його, потенційно могла інтегрувати штучний інтелект для підвищення точності та масштабності атак.

У сфері кібербезпеки штучний інтелект почали застосовувати наприкінці 1980-х років, і з того часу технологія пройшла кілька ключових етапів еволюції.[2] Спочатку фахівці з безпеки використовували системи, засновані на жорстко заданих правилах, які реагували на заздалегідь визначені параметри та генерували сповіщення при їх порушенні.[2] З початку 2000-х років розвиток машинного навчання - одного з напрямів ШІ, що дозволяє аналізувати великі обсяги даних і виявляти закономірності - відкрив нові можливості для кіберзахисту.[2] Завдяки цьому фахівці змогли краще розпізнавати типові моделі поведінки користувачів і мережевого трафіку, виявляти аномалії та оперативно реагувати на потенційні загрози.

Серед найсучасніших досягнень - генеративний штучний інтелект, здатний створювати новий контент на основі існуючих даних.[2] Такі системи підтримують взаємодію в форматі природної мови, що дозволяє спеціалістам з безпеки формулювати запити без використання складної технічної термінології. Ще одним перспективним напрямом є впровадження штучно інтелектуальних агентів, які працюють у тісній взаємодії з окремими користувачами, командами та організаціями. Вони здатні автоматизувати значну частину рутинних завдань і процесів, підвищуючи загальну ефективність роботи в сфері кіберзахисту.[2] Найчастіше штучний інтелект в кібербезпеці застосовують в таких сферах як: система керування ідентичністю та доступом, захист кінцевих точок і керування ними, хмарна безпека, безпека даних, виявлення кіберзагроз та розслідування та реагування на інциденти.[2]

У системах керування ідентичністю та доступом штучний інтелект аналізує поведінку користувачів при вході в систему, виявляє аномалії, ініціює двофакторну автентифікацію або скидання пароля, а в разі підозри на компрометацію облікового запису - блокує доступ.[2] У сфері захисту кінцевих точок штучний інтелект допомагає ідентифікувати пристрої в мережі, забезпечити їх актуальними оновленнями, а також виявити шкідливе програмне забезпечення чи сліди атаки.[2] Для хмарної безпеки штучний інтелект об'єднує дані з різних хмарних сервісів, формуючи цілісну картину ризиків і вразливостей, що дозволяє оперативно реагувати на загрози. [2] У контексті безпеки даних штучний інтелект автоматизує процеси ідентифікації конфіденційної інформації, незалежно від місця її зберігання, та контролює спроби несанкціонованого переміщення даних за межі організації. [2] У виявленні кіберзагроз рішення на основі штучного інтелекту, такі як XDR і SIEM, аналізують поведінку користувачів, корелюють інциденти, запобігають атакам і формують рекомендації щодо покращення захисту.[2] Під час розслідування та реагування на інциденти штучний інтелект допомагає швидко обробляти великі обсяги даних, виявляти ключові події та формулювати висновки у зручному форматі, зокрема за допомогою генеративних моделей, що підтримують природну мову.[2]

Перевагами застосування можна виділити: швидке виявлення загроз - він аналізує тисячі подій, виокремлюючи критичні інциденти та встановлюючи зв'язки між ними; Оптимізація звітності - створює зрозумілі аналітичні документи з різних джерел, у виявленні вразливостей ідентифікує слабкі місця, як-от невідомі пристрої чи незахищені дані; Для розвитку навичок - допомагає аналітикам працювати без знання запитів, надає рекомендації та покрокові інструкції; Менше хибних сповіщень - завдяки розпізнаванню шаблонів і контексту, штучний інтелект знижує навантаження на команди; Масштабованість - автоматизує процеси, адаптується до складності загроз і підтримує стабільність систем безпеки.[2]

У підсумку, штучний інтелект відіграє ключову роль у формуванні сучасної системи кібербезпеки, перетворюючись із технологічної новинки на стратегічно важливий інструмент захисту. В умовах стрімкого зростання цифрових загроз, зловмисного використання штучного інтелекту та постійного розширення цифрового простору, його впровадження стає не просто бажаним, а необхідним для організацій будь-якого масштабу. Завдяки здатності аналізувати великі обсяги даних, виявляти аномалії, прогнозувати ризики та автоматизувати реагування, штучний інтелект забезпечить швидке виявлення загроз, ефективне управління ідентичністю, захист кінцевих точок, хмарну безпеку, контроль над конфіденційними даними та підтримку в розслідуванні інцидентів. Його переваги - від зменшення хибних сповіщень до масштабованості - дозволяють командам безпеки діяти проактивно, швидко адаптуватися до нових викликів і створювати стійке цифрове середовище, здатне протистояти сучасним кіберризикам.

Список використаних джерел

1. Коваленко, О. В. (2022) «Використання штучного інтелекту в системі кібербезпеки», Державне управління: удосконалення та розвиток, Доступно за адресою: http://www.dy.nayka.com.ua/pdf/1_2022/4.pdf (Дата звернення: 10 жовтня 2025).

2. Microsoft (n.d.) What is AI for cybersecurity?. Available at: https://www.microsoft.com/ukua/security/business/security-101/what-is-ai-for-cybersecurity#Use-cases(Accessed: 10 October 2025).

Неллі СОРОЧАН
здобувачка першого (бакалаврського) рівня вищої освіти
факультету інформаційних технологій
ДВНЗ «Ужгородський національний університет» м. Ужгород
sorochan.nelli@student.uzhnu.edu.ua

Володимир НІКОЛЕНКО
Кандидат фізико-математичних наук, доцент, доцент кафедри
інформаційних управляючих систем і технологій
ДВНЗ «Ужгородський національний університет» м. Ужгород
volodymyr.nikolenko@uzhnu.edu.ua

РОЗПІЗНАВАННЯ ДАКТИЛЬНОЇ АБЕТКИ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

Доступність засобів комунікації для людей з порушеннями слуху є важливим складником соціальної та інформаційної безпеки: в умовах критичних або адміністративних ситуацій оперативна взаємодія зменшує ризики помилок і затримок у прийнятті рішень. Розвиток цифрових рішень для розпізнавання української дактильної абетки (USL) створює можливість для побудови прикладних систем перекладу та навчальних інструментів, орієнтованих на локальний контекст. Існуючі міжнародні датасети (зокрема ASL-орієнтовані) можуть бути використані для попереднього навчання моделей з подальшою адаптацією до мовних особливостей USL, що визначає завдання розробки ефективних інтерфейсів для інклюзивної комунікації.

Мета

Метою роботи є дослідження розробки інтерфейсу, що розпізнає українську дактильну абетку з фото або відео вхідних даних із показаними жестами руки, та забезпечує текстовий вивід і режим навчання для користувача. Практичний фокус – створити pipeline, який дозволяє отримати прийнятну точність у реальному часі на доступному обладнанні.

План збору даних

У відкритому доступі є обмежена кількість наборів даних з українською дактильною абеткою, натомість доступні великі набори з американськими чи міжнародними зразками, які можна використати для попереднього тренування моделі. Використання цих ресурсів – часткове рішення. Із ASL(American Sign Language) в українській абетці співпадають шість літер, що доцільно використати для початкового навчання власної моделі. Решту букв необхідно отримати шляхом збору власних зразків. Для забезпечення вищої якості та репрезентативності необхідно забезпечити варіативність даних – зокрема, узяти зразки рук різних розмірів, форм, у різних умовах освітлення. Щоб отримати більший обсяг корисних даних, можна застосувати на вже зібраних зразках техніки аугменації: перетворити існуючі кадри, обертаючи, обрізаючи, масштабуючи їх, збільшуючи чи зменшуючи контрастність, яскравість, додаючи шум тощо [2].

Захоплення положення руки відбуватиметься з камери. У якості стабільного та ефективного рішення для виділення ключових точок кисті пропонується використовувати Google MediaPipe Hands, що повертає до 21 hand-landmark у нормалізованих координатах (x, y, z) та визначає handedness (ліва/права рука). MediaPipe доступний як для десктопних, так і для веб та мобільних середовищ, і оптимізований для роботи на CPU, що робить його придатним для прототипів, орієнтованих на реальний час [1]. Для перших етапів реалізації прототипу буде використано Jupyter Notebook, у якому раніше було реалізовано задачу розпізнавання якості вина, описану в моїй статті у збірнику «Науковий пошук молодих дослідників» [4].

Існуючі цифрові рішення та місце AI-автоматизації

В Україні вже доступні ліцензійні цифрові сервіси для обслуговування людей з порушенням слуху (наприклад, сервіси, перераховані на ресурсі ГО «Соціальна єдність»: Connect PRO, Connect WEB, «Перекладач ЖМ»), що забезпечують доступ до перекладачів жестової мови в режимі 24/7 та онлайн-зв’язок з живими перекладачами [3]. Такі рішення важливі і вже

приносять користь у взаємодії установ з користувачами з обмеженим слухом. Проте вони покладаються на людський ресурс (онлайн-перекладачів), що створює оперативні та економічні вимоги на постійне чергування фахівців. Впровадження автоматизованих компонентів на базі штучного інтелекту (автоматичний розпізнавач дактилю/жестів) може пришвидшити первинну комунікацію та забезпечити миттєвий переклад у простих сценаріях, надаючи можливість вибору між цифровими інструментами комунікації. Крім ресурсів для перекладу, системи розпізнавання української жестової мови на базі штучного інтелекту можуть слугувати освітніми прикладними програмами, що підвищить обізнаність суспільства про дактильну абетку та жестову мову. Тому розробка інструменту, який виконує функцію розпізнавання та навчання (інтерактивний інтерфейс з візуальним фідбеком), має подвійне практичне значення: надати нові можливості спілкування тут і зараз та сприяти поширенню знань у суспільстві.

Технічно очікується створення робочого прототипу інтерфейсу, що розпізнає дактильну абетку з точністю, достатньою для демонстрацій і навчання. Практично – інструмент можна використати як основу для навчання дактилю у навчальних закладах, а також додатковий автоматизований сервіс для організацій та екстрених служб, що доповнює існуючі 24/7 сервіси перекладу.

Висновки. Існуючі цифрові сервіси вже надають важливі можливості для людей з порушеннями слуху. Запропонований підхід показує, що сучасні методи машинного навчання дозволяють реалізувати автоматизований компонент перекладу й навчання, який розширює канали комунікації та підвищує їх доступність та вносячи вагомий вклад у соціальну та інформаційну безпеку

Список використаних джерел

1. Google AI for Developers, (2025). Hand landmarks detection guide. [Електронний ресурс] Google for Developers. Доступ за посиланням: https://ai.google.dev/edge/mediapipe/solutions/vision/hand_landmarker [Звернено 24 вересня 2025].

2. Walsh, H., Ivashechkin, M. & Bowden, R., (2025). Using Sign Language Production as Data Augmentation to enhance Sign Language Translation. [Електронний ресурс] Arxiv, Доступ за посиланням: https://arxiv.org/html/2506.09643v1 [Звернено 24 вересня 2025].

3. ГО «Громадський рух «Соціальна єдність»». (2025). Цифрові рішення для людей з порушенням слуху. [Електронний ресурс] Доступ за посиланням: https://se.org.ua/cifrovirishennya/ [Звернено 24 вересня 2025].

4. Сорочан, Н.(2025). Використання Jupyter Notebook в задачах розпізнавання. «Науковий пошук молодих дослідників» - Збірник наукових праць студентів, магістрантів та викладачів, випуск 18, с. 143-147 за ред. Постової С.А.. [Електронний ресурс] Доступ за посиланням: https://eprints.zu.edu.ua/44884/ [Звернено 24 вересня 2025].

Sofiia KYKHTAN
Bachelor's degree student (2nd year), majoring in Cybersecurity and Data Protection (Specialty 125), State University "Kyiv Aviation Institute"
9214304@stud.kai.edu.ua

Larysa TEREMINKO
PhD (Pedagogy), Associate Professor of the Professional Foreign Languages Department, State University "Kyiv Aviation Institute"
larysa.tereminko@npp.kai.edu.ua

METHODS OF OSINT AND THEIR INTEGRATION WITH ARTIFICIAL INTELLIGENCE TECHNOLOGIES FOR STRENGTHENING INFORMATION SECURITY

In the modern digital environment, the rapid growth of cyber threats has become one of themost pressing challenges for governments, organizations, and individuals. Cyberattacks are increasingly sophisticated, targeting critical infrastructures, private users, financial institutions, and the information space in general. Traditional security measures, such as signature-based detection systems or manual information analysis, are no longer enough to guarantee robust protection. So, integrating Open-Source Intelligence (OSINT) methods with artificial intelligence (AI) technologies has emerged as a highly effective approach to strengthening information security.

OSINT in the Cybersecurity Context. OSINT refers to collecting and analyzing information from publicly available sources, such as websites, social media platforms, online databases, government reports, and technical registries. These techniques enable security professionals to obtain valuable insights into potential risks, threat actors, and vulnerabilities without compromising legal or ethical norms. However, the volume of data available in open sources is growing rapidly, which poses a serious challenge. Processing such information manually requires enormous time and human resources, increasing the probability of overlooking significant details.

Aim and Relevance of the Research. This research aims to explore the possibilities of integrating OSINT tools with artificial intelligence algorithms to improve the efficiency of cybersecurity processes. This approach is highly relevant due to the growing demand for intelligent systems capable of collecting open-source data and classifying, organizing, and analyzing it in real time. These systems can offer early warning capabilities and strengthen proactive defense measures against cyber threats by minimizing human effort and errors.

Scientific Novelty. The study introduces a groundbreaking approach by integrating machine learning, natural language processing (NLP), and big data analysis into the field of OSINT. While OSINT is a well-established methodology, combining it with AI unlocks advanced automation and predictive capabilities. Unlike traditional manual OSINT investigations, which rely heavily on the expertise and intuition of analysts, AI-driven methods enable scalable, rapid, and systematic processing of extensive datasets. This approach facilitates the identification of hidden patterns, unusual correlations, and anomalies that may signal malicious activities or potential vulnerabilities.

Tools and Integration with AI. Several modern OSINT tools are considered within the scope of this research, such as Maltego, which specializes in link analysis and network visualization; Shodan, which scans and indexes internet-connected devices; and Recon-ng, a modular framework for reconnaissance tasks. These tools provide analysts with powerful opportunities to collect raw data. However, when integrated with AI technologies, their capabilities are significantly expanded. For example, machine learning models can enhance Maltego by automatically classifying relationships between entities; deep learning algorithms can improve Shodan scans by detecting unusual device behaviors; and NLP systems can help Recon-ng process large volumes of unstructured text from forums or social media.

Proposed Approach. The proposed method integrates pipelines where OSINT tools supply data to AI systems for preprocessing, clustering, and predictive analysis. This synergy enables the creation of dynamic risk profiles for organizations or individuals, the prediction of potential attack vectors, and the identification of threat actors' tactics, techniques, and procedures (TTPs). Additionally, AI-driven automation significantly accelerates threat hunting processes and enhances result accuracy compared to manual methods.

Research Results. The results of the research indicate that the combination of OSINT and AI has the potential to revolutionize information security practices. Automated systems can continuously monitor the digital environment, detect suspicious activity at an early stage, and support decision-making processes with accurate and timely intelligence. Such systems minimize the risks of human error, increase the scalability of security operations, and improve the resilience of organizations against cyberattacks.

Conclusions and Perspectives. In conclusion, integrating OSINT methods with artificial intelligence technologies is a promising direction for the future of cybersecurity. This synergy allows for the creation of comprehensive monitoring systems capable of collecting, processing, and interpreting vast amounts of open-source data. The practical outcomes of such integration include more efficient threat detection, enhanced predictive capabilities, and better protection of critical infrastructures and digital assets. Further research should focus on developing frameworks for combining specific OSINT tools with AI algorithms and addressing ethical and legal aspects of automated intelligence gathering.

References

1. Artificial Intelligence in OSINT - hackyourmom. https://hackyourmom.com/en/kibervijna/shtuchnyj-intelekt-v-osint-yak-pokrashhyty-rozsliduvannya-u-2024-roczi/
2. Best AI Knowledge Graph Tools in 2025. https://reviewtools.ai/category/ai-knowledge-graph
3. Ethics in OSINT Usage - Zona Hacking. https://www.areahacking.com/2024/10/ethics-in-osint-usage.html
4. Integration of AI with OSINT - Medium. https://medium.com/@nitikapoudel2/integration-of-ai-with-osint-8cabeee45868
5. What Is an AI-Powered Attack? How It Works & Examples - Twingate. https://www.twingate.com/blog/glossary/ai-powered-attack

Illya PYLYPCHUK
Second-year applicant for the Bachelor's degree in Computer Science (Specialty 122),
State University "Kyiv Aviation Institute"
9096826@stud.kai.edu.ua

Nataliia DENYSENKO
Senior Lecturer of the Professional Foreign Languages Department,
State University "Kyiv Aviation Institute"
nataliia.denysenko@npp.kai.edu.ua

THE ROLE OF AI AND DIGITAL SOLUTIONS IN ENSURING NATIONAL AND GLOBAL SECURITY

Introduction. The world is experiencing a rapid digital transformation that touches nearly every aspect of life, including security. Modern challenges—such as cyberattacks, terrorism, hybrid warfare, and information manipulation—require innovative responses. In this context, artificial intelligence (AI) and digital technologies are increasingly essential for national and global security systems [1, p. 105]; [2, p. 16].

Relevance of Digital Technologies in Security. Digital technologies allow for more efficient monitoring, forecasting, and neutralization of threats. By automating processes and analyzing large volumes of data, authorities, law enforcement, and the military can make faster and more accurate decisions [2, p. 16; 4, p. 16]. This also helps reduce response times and minimize human errors [6, p. 1].

The Role of Artificial Intelligence in Protection Systems. AI can process diverse data sources—from satellite imagery to social media—within unified platforms, identifying patterns and anticipating potential risks [1, p. 105; 6, p. 1]. On a global scale, AI is applied in missile defense, counterterrorism, intelligence analysis, and cyber defense [10, p. 199; 3, p. 133].

AI Applications in Security. Machine-learning algorithms can detect unusual network activity, identify cyberattacks, and block them in real time. This is critical for protecting essential infrastructure such as energy networks, banking systems, and transport hubs [2, p. 17; 6, p. 25].

AI in the Military Sphere. AI is increasingly used to operate unmanned aerial vehicles, automatically recognize targets, and forecast combat scenarios. This reduces risks for personnel and improves operational precision [10, p. 199; 1, p. 105].

Data Analysis Technologies in Law Enforcement. Law enforcement agencies employ facial recognition, voice analysis, and behavioral analytics to monitor suspects, process surveillance footage, and anticipate crime trends [1, p. 45; 6, p. 1].

Direction	Application Example	Expected Effect
Video Analytics	Detecting suspicious behavior in public areas	Crime prevention
Biometrics	Identification via fingerprints and facial recognition	Rapid identification
Data Analytics	Analysis of social media, calls, and transactions	Detecting organized crime groups

Table 1. Main Directions of AI Use in Law Enforcement; Source: [6, p.25]

Digital Technologies in Security. Big Data and Threat Analytics

Big Data allows authorities to detect complex threats at regional and global levels, including cyberattacks and terrorism financing [4, p. 16; 2, p. 17].

Cloud Technologies and Security. Cloud solutions offer flexible data storage and processing but also pose risks of data breaches, making encryption and strong operational security essential [1, p. 105].

IoT and Critical Infrastructure. Integrating IoT devices into transport, energy, and healthcare systems improves efficiency but also introduces vulnerabilities to attacks [4, p. 16; 6, p. 1].

Blockchain and Cryptography. Blockchain provides transparency and ensures data integrity, which is crucial for safeguarding sensitive information and financial transactions [3, ch. 4; 10, p. 199].

Risks and Challenges of AI and Digital Technologies. Ethical and Legal Issues

AI can raise concerns about human rights, particularly in mass surveillance or opaque decision-making systems. Establishing legal frameworks and safeguards is necessary to prevent misuse [5, ch. 1; 12, ch. 1].

Cyberwarfare and Hybrid Threats. Both state and non-state actors increasingly use cyberattacks as political and economic tools. Dependence on digital systems creates new vulnerabilities and risks escalation [4, p. 16; 2, p. 17].

Personal Data and Privacy. The use of biometrics and behavioral monitoring must be strictly regulated to protect privacy [1, p. 45; 12, ch. 1].

Conclusions. AI and digital technologies are transforming the security landscape, offering new ways to manage risks and protect society. At the same time, they bring ethical, legal, and technical challenges [1, p. 105; 5, ch. 1].

Key Trends in AI and Digital Security

- Integrating AI into cybersecurity [2, p. 16]
- Expanding the role of IoT in critical infrastructure [4, p. 16]
- Using blockchain to secure data [3, ch. 4]
- Increasing focus on privacy and human rights [5, ch. 1; 12, ch. 1]

Prospects for Ukraine

For Ukraine, which faces hybrid warfare, developing AI and digital technologies is essential. Investment in domestic solutions and adoption of international best practices is crucial [10, p. 199; 4, p. 16].

References

1. Ventre, D. *Artificial Intelligence, Cybersecurity and Cyber Defence*. Hoboken, NJ: John Wiley & Sons, 2020.
2. Sarker, I. H. *AI-Driven Cybersecurity and Threat Intelligence: Cyber Automation, Intelligent Decision-Making and Explainability.* Cham: Springer, 2024.
3. Shah, R. M., & Kirchhoff, C. *Unit X: How the Pentagon and Silicon Valley Are Transforming the Future of War.* New York: Simon & Schuster, 2024.
4. Jahankhani, H., Kendzierskyj, S., Chelvachandran, N., & Ibarra, J. (Eds.). *Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity.* Cham: Springer, 2020.
5. Yampolskiy, R. V. (Ed.). *Artificial Intelligence: Safety and Security.* Boca Raton, FL: Chapman & Hall/CRC, 2018.
6. Chio, C., & Freeman, D. *Machine Learning and Security: Protecting Systems with Data and Algorithms.* Sebastopol, CA: O'Reilly Media, 2018.
7. O'Neil, C. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy.* New York: Crown Publishing Group, 2016.

Semyon PYKHTEYEV
Second-year applicant for the Bachelor's degree in Computer Science (Specialty 122),
State University "Kyiv Aviation Institute"
9144285@stud.kai.edu.ua

Nataliia DENYSENKO
Senior Lecturer of the Professional Foreign Languages Department,
State University "Kyiv Aviation Institute"
nataliia.denysenko@npp.kai.edu.ua

ARTIFICIAL INTELLIGENCE AND DIGITAL TECHNOLOGIES IN THE FIELD OF SECURITY

The rapid development of digital technologies is reshaping the global security landscape. Among these innovations, artificial intelligence (AI) occupies a leading position. Its applications span numerous domains, but one of the most critical areas remains security. The rise of cyber threats, information warfare, and the increasing reliance on autonomous systems highlight the urgent need to study the potential and risks of AI. The aim of this paper is to analyze the opportunities for implementing AI in the field of security, identify its key risks, and consider the implications for Ukraine and the international community.

Artificial Intelligence in Cybersecurity. Artificial intelligence plays a central role in modern cybersecurity solutions. Machine learning algorithms are capable of analyzing vast datasets and detecting patterns that indicate potential threats. AI-based intrusion detection systems monitor user behavior, identify anomalies, and respond in real time to suspicious activity. Neural networks are increasingly used to classify malware, detect phishing attempts, and prevent data breaches. For instance, Microsoft Defender employs AI to adaptively detect previously unknown threats, while DARPA in the United States has initiated several programs integrating AI into proactive cyber defense. Such developments demonstrate the transformative role of AI in protecting critical infrastructure.

AI in National and Military Security. AI technologies are also becoming essential in national defense and military operations. Autonomous drones and robotic systems can conduct reconnaissance, provide real-time intelligence, and support logistics in combat zones. Drones equipped with Ai-powered vision system can independently recognize objects, identify potential targets, and adjust their flight paths in real time. This reduce the burden on human operators and significantly increases the efficiency of surveillance and reconnaissance missions. Predictive analytics helps optimize supply chains and anticipate enemy movements. AI is also employed in monitoring hybrid threats, disinformation campaigns, and large-scale information flows. For Ukraine, which faces ongoing military aggression, AI-enabled technologies such as automated satellite image analysis, open-source intelligence platforms, and drone swarm control have proven invaluable. These tools enhance national defense capabilities and allow more efficient resource allocation.

Threats and Ethical Challenges of AI. Despite the evident advantages, AI introduces new risks that cannot be ignored. DeepFake technologies make it possible to create hyper-realistic fake videos and audio, which can be exploited for propaganda and psychological operations. Autonomous lethal weapons raise concerns regarding accountability and the possibility of machines making life-or-death decisions without human supervision. Cybercriminals increasingly adopt AI tools for password cracking, generating phishing messages, and exploiting vulnerabilities. These challenges require robust legal frameworks and international cooperation to prevent the misuse of AI technologies. Equally important are ethical discussions surrounding privacy, transparency, and the necessity of maintaining human oversight in all critical decisions involving AI.

International and Ukrainian Experience Global practice shows a growing reliance on AI in security. Palantir Technologies develops AI-powered platforms for analyzing big data to support government agencies and security services. Clearview AI employs facial recognition technologies

that have raised both security benefits and privacy concerns. NATO has emphasized the integration of AI in its 2030 security strategy, recognizing its potential in collective defense. In Ukraine, startups and defense technology initiatives focus on AI-based monitoring of social media, image recognition for drone operations, and real-time battlefield intelligence. These experiences demonstrate both the opportunities and risks associated with the adoption of AI in defense and security contexts.

Conclusions. Artificial intelligence represents a dual-use technology: on one hand, it provides unprecedented opportunities to strengthen cybersecurity, enhance military capabilities, and ensure national safety. On the other hand, it creates significant risks related to ethical dilemmas, misuse by malicious actors, and the potential loss of human control over critical decisions. For Ukraine, the integration of AI in defense is not just a matter of technological innovation but a necessity for survival in the context of ongoing hybrid warfare. Future security strategies must focus on balancing innovation with regulation, ensuring that AI is applied responsibly and ethically to support both national and global stability.

References

1. Russell, S., Norvig, P. Artificial Intelligence: A Modern Approach. – New York: Pearson, 2021.
2. Floridi, L. AI and Security. – Oxford: Oxford University Press, 2021.
3. Palantir Technologies. Official website. – Available at: https://www.palantir.com
4. NATO. NATO 2030: Emerging Security Challenges. – Brussels: NATO Publications, 2020.
5. DSTU 8302:2015. Information and documentation. Bibliographic references. – Kyiv: SE "UkrNDNC", 2016.

Oleksandr HUSAK
Second-year applicant for the Bachelor's degree in Computer Science (Specialty 122),
State University "Kyiv Aviation Institute"
741065@stud.kai.edu.ua

Roman MOROZ
Second-year applicant for the Bachelor's degree in Computer Science (Specialty 122),
State University "Kyiv Aviation Institute"
9155820@stud.kai.edu.ua

Nataliia DENYSENKO
Senior Lecturer of the Professional Foreign Languages Department,
State University "Kyiv Aviation Institute"
nataliia.denysenko@npp.kai.edu.ua

AI SECURITY

Introduction. The 21st century has brought unprecedented challenges in the field of security. The digitalization of society, the growing number of cyberattacks, hybrid conflicts, and the globalization of threats have transformed the traditional understanding of safety and defense. Artificial Intelligence (AI) and digital technologies are no longer optional but mandatory instruments in ensuring stability and resilience of states, corporations, and individuals.

The importance of AI in security is evident in its wide adoption across sectors such as banking, transportation, military defense, and healthcare. For instance, AI-driven systems monitor global financial transactions to detect fraud, while predictive algorithms are applied in law enforcement to forecast crime hotspots. Similarly, digital technologies like Big Data, the Internet of Things (IoT), and Cloud Computing provide the backbone for collecting, analyzing, and securing massive streams of information.

The objective of this research is to explore the opportunities and limitations of AI and digital technologies in security, as well as to outline the ethical and legal considerations that accompany their development.

Artificial Intelligence in Security. Artificial Intelligence represents a transformative force in modern security strategies. Its ability to process unstructured data from multiple sources (e.g., CCTV cameras, network logs, social media) allows organizations to anticipate risks more effectively than ever before.

In cybersecurity, AI is integrated into Intrusion Detection Systems (IDS) and Security Information and Event Management (SIEM) platforms. These tools analyze real-time traffic, flag anomalies, and autonomously respond to potential breaches [1, p. 105]. By applying supervised and unsupervised machine learning, systems can adapt to new forms of malware and phishing attempts.

In physical security, AI enhances video surveillance by applying image recognition to identify suspicious behavior. Facial recognition technologies have been deployed in airports, border control, and smart cities to ensure the identification of individuals of interest. AI also supports defense applications such as autonomous vehicles, drones, and robotic systems used in hazardous environments.

Table 1. Key areas of AI application in security

Domain	Applications
Cybersecurity	Intrusion detection, anomaly detection, threat prediction

Physical security	Biometric systems, video analytics, facial recognition
Defense	Autonomous systems, unmanned aerial vehicles, strategic simulations

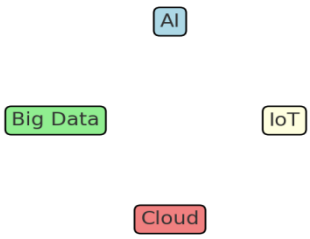
Digital Technologies in Security. Digital technologies are equally vital in addressing contemporary security challenges.

Big Data technologies provide the analytical power to detect hidden patterns across billions of records. Governments use these capabilities for counter-terrorism and intelligence gathering, while businesses apply them for fraud detection and risk management [2, p. 77].

Cloud Computing supports scalable and cost-effective infrastructure. It allows secure storage and real-time access to critical information across geographically dispersed units. However, it also demands strong encryption, access controls, and compliance with international data protection standards.

The Internet of Things (IoT) connects billions of devices – from household appliances to industrial machinery. While IoT enhances situational awareness and efficiency, every new device becomes a potential entry point for cybercriminals. Consequently, IoT security has become a top priority for policymakers and engineers.

Figure 1. Interaction of digital technologies in security systems



Source: author's own elaboration

Advantages and Risks of AI and Digital Technologies. The integration of AI and digital technologies in security brings several advantages. Firstly, they enable rapid detection of threats and automation of incident response. Secondly, predictive analytics allows for the anticipation of risks, ensuring proactive measures. Thirdly, these technologies significantly reduce the influence of human error, which has traditionally been one of the weakest points in security systems.

However, the risks must also be acknowledged. AI systems may inherit biases from the data they are trained on, raising ethical and legal concerns. Autonomous systems operating without human oversight can cause unintended harm. Moreover, adversaries can exploit AI itself, developing malicious algorithms to bypass defenses [3, p. 142].

Another pressing risk is the vulnerability of IoT devices, which are often deployed without sufficient protection. As the number of devices grows, so does the likelihood of coordinated cyberattacks. These risks highlight the necessity for robust legal frameworks, ethical guidelines, and international cooperation.

Conclusions. Artificial Intelligence and digital technologies are shaping the future of global security. Their ability to collect, process, and analyze information in real time transforms both cyber and physical protection systems. Nevertheless, successful implementation requires not only technological innovation but also legal regulation and ethical responsibility.

In the near future, we may witness deeper integration of AI with digital ecosystems, the emergence of fully autonomous defense platforms, and the adoption of quantum computing in encryption. These

trends will further increase the resilience of societies but also introduce new risks. Therefore, governments, private companies, and research institutions must collaborate to ensure that technological progress serves humanity while minimizing potential dangers.

References

1. Gavrylenko S. Artificial Intelligence in Cybersecurity. - Kyiv: Naukova Dumka, 2022. - 220 p.
2. Ivanenko O. Digital Technologies in Information Security. - Lviv: LNU Press, 2021. - 180 p.
3. Smith J. Artificial Intelligence and Security. - London: Springer, 2020. - 310 p.
4. Brown K. Cybersecurity and Big Data. - New York: Routledge, 2019. - 250 p.
5. Petrov V. Internet of Things and Security. - Kharkiv: KhNU, 2023. - 190 p.
6. Russell S., Norvig P. Artificial Intelligence: A Modern Approach. - New Jersey: Pearson, 2021. - 1152 p.
7. Zeng Y., Lu E., Huang T. Linking Artificial Intelligence Principles. - Nature Machine Intelligence, 2019, 1(1), pp. 18-19.
8. Brundage M. et al. The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. - Oxford University Press, 2018.
9. Clarke R., Knake R. Cyber War: The Next Threat to National Security. - New York: HarperCollins, 2019. - 320 p.
10. Bostrom N. Superintelligence: Paths, Dangers, Strategies. - Oxford: Oxford University Press, 2014. - 352 p.

КІБЕРКУЛЬТУРА ТА ЦИФРОВА ГІГІЄНА В ОСВІТНЬОМУ ПРОЦЕСІ

CYBERCULTURE AND DIGITAL HYGIENE IN EDUCATION

KIBERKULTÚRA ÉS DIGITÁLIS HIGIÉNIA AZ OKTATÁSI FOLYAMATBAN

Андріана КЕЛЕМЕН
кандидат педагогічних наук,
начальник відділу освіти,
культури, молоді та спорту
Хустської РДА- РВА

Роман КЕЛЕМЕН
кандидат педагогічних наук,
адвокат, викладач юридичних
дисциплін КЗПО"ЦДЮТ" Сузір'я"

БЕЗПЕЧНЕ ОСВІТНЄ СЕРЕДОВИЩЕ: НОВІ ВИМІРИ, ПРАВОВІ ТА СОЦІАЛЬНІ АСПЕКТИ

Анотація. Безпечне освітнє середовище — це не лише правова вимога, а й соціальна необхідність для розвитку здорового суспільства. У контексті сучасних викликів — війни, цифрових загроз, соціальної напруги — формування безпечного середовища є запорукою збереження освітньої системи та розвитку майбутніх поколінь.

Ключові слова: безпека, освітнє середовище, інформаційна безпеки , заклади освіти, воєнний стан.

Освітній процес укотре зазнає змін. У першу чергу більш актуальними стають питання безпечного простору та освітнього середовища.

В умовах воєнного стану формування безпечного освітнього середовища є надзвичайно складним завданням для всіх учасників освітнього процесу. Освіта розглядається не лише як процес передачі знань та формування компетенцій, а й як простір для особистісного розвитку, де кожен повинен почуватися захищеним фізично, психологічно та соціально. Безпечне освітнє середовище є фундаментальною умовою якісного викладання та навчання. Його забезпечення включає правові механізми, соціальні підходи та практичні дії вчителів, адміністрації та широкої громадськості.

Студенти переживають стресові реакції від інформаційних впливів внаслідок травматичних подій та втрат, що безпосередньо впливає на навчальний процес.

Створення безпечного освітнього середовища є одним із першочергових завдань навчального закладу, реалізація якого має реалізувати право на безпечні та нешкідливі умови для розвитку, навчання та виховання у воєнних умовах. Це має здійснюватися спільними зусиллями керівника навчального закладу, педагогічного колективу, батьків учасників освітнього процесу, громадськості.

Правова основа створення безпечного освітнього середовища в Україні ґрунтується на міжнародних і національних нормативно-правових актах. Основними документами залишаються:

Конституція України [ст.53, с. 49], яка гарантує право на освіту та безпечні умови навчання.

Закон України «Про освіту» [2017], де зазначено, що освітнє середовище має бути безпечним і комфортним для всіх учасників. Стаття 26 цього закону підкреслює обов'язок закладів освіти забезпечувати захист від будь-яких форм насильства.

Закон України «Про повну загальну середню освіту» [2020], який регулює організацію освітнього процесу в школах.

Закон України «Про запобігання та протидію домашньому насильству» [2017], що має значення для захисту дітей від насильства, в тому числі в освітньому контексті.

Конвенція ООН про права дитини [1989], яка наголошує на праві дитини на захист від усіх форм насильства, дискримінації та порушення її гідності.

Декларація про безпечні школи, до якої Україна приєдналася, що встановлює зобов'язання щодо запобігання нападам на освітні установи та їх використанню у військових цілях.

У 2025 році правова база була суттєво посилена. 18 вересня 2025 року Верховна Рада України ухвалила законопроєкт №11543 «Про запровадження заходів безпеки в закладах

загальної середньої освіти», який вносить зміни до Закону «Про повну загальну середню освіту».

Цей закон, розроблений у співпраці з Міністерством внутрішніх справ, Національною поліцією та Міністерством освіти і науки, спрямований на створення безпечного освітнього середовища в умовах воєнного часу та після перемоги.

Соціальні аспекти безпеки в освіті стосуються створення атмосфери взаємоповаги, толерантності та психологічного комфорту. Вони включають: Протидія булінгу та дискримінації; Психологічна підтримка; Інклюзивна культура; Співпраця з батьками та громадою; Цифрова безпека.

Під час військових дій та ще тривалий час після їх закінчення заклади освіти в Україні працюватимуть у нових для себе вимогах до безпечного освітнього середовища.

Безпечне освітнє середовище — це не лише вимога часу, а й індикатор якості освіти та рівня соціальної відповідальності держави.

Список використаних джерел

1. Питання кібербезпеки у світі юриспруденції . Судово-юридична газета. 2019. Вип. 3. С. 19-22.
2. Міністерство освіти і науки України«Про затвердження Положення про організацію роботи з охорони праці та безпекижиттєдіяльності учасників освітнього процесу в установах і закладах освіти» від 26.12.2017 №1669
3. Нагайчук О.В. «Організація безпечного освітнього середовища». Навчально-методичний посібник. Умань: Візаві, 2024

Євгенія ГАЙОВИЧ
аспірант кафедри загальної педагогіки
та педагогіки вищої школи,
начальник відділу електронного навчання
центру інформаційних технологій
ДВНЗ «Ужгородський національний університет»,
y.haiovych@uzhnu.edu.ua

Оксана ПОВІДАЙЧИК
доктор педагогічних наук, професор,
завідувач кафедри загальної педагогіки
та педагогіки вищої школи
ДВНЗ «Ужгородський національний університет»,
oksana.povidaichyk@uzhnu.edu.ua

ВИКЛИКИ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ КІБЕРКУЛЬТУРИ ТА ЦИФРОВОЇ ГІГІЄНИ В ОСВІТНЬОМУ ПРОЦЕСІ

Стрімкий розвиток технологій штучного інтелекту зумовлює глибокі зміни в освітній практиці, культурі спілкування та способах сприйняття інформації. ШІ не лише оптимізує процеси, а й створює нові соціальні, етичні та психологічні виклики.

У цих умовах актуалізується поняття кіберкультури – як сукупності норм, цінностей і моделей поведінки у цифровому просторі, а також цифрової гігієни – як системи знань і навичок безпечного та усвідомленого користування цифровими технологіями. Попри очевидні переваги використання технологій штучного інтелекту в освіті, залишається недостатньо дослідженим їхній культурний, етичний і психологічний вплив на учасників навчального процесу.

ШІ трансформує освітній простір, змінює комунікативні практики, структуру мислення й моделі поведінки, що ставить під сумнів традиційні уявлення про академічну доброчесність, авторство, інформаційну безпеку та відповідальність користувача. Отже, наукова проблема полягає у пошуку теоретичних і методичних засад формування кіберкультури та цифрової гігієни в умовах зростаючої інтелектуалізації освітнього середовища.

Інтеграція ШІ в освітній процес змінює структуру взаємодії між учасниками навчання. Алгоритми персоналізують навчання, автоматизують оцінювання, створюють контент, водночас формуючи нові культурні звички: делегування інтелектуальних завдань технологіям, зниження потреби у власному аналізі, перенесення довіри з людини на систему. Інтелектуальні репетитори та віртуальні помічники, інклюзивність освітнього середовища, віртуальна та доповнена реальність модернізують освітній процес і змушують переосмислити підходи [1, 243].

Такі зміни вимагають нового типу цифрової грамотності, який включає елементи алгоритмічного та критичного мислення, розуміння етичних меж використання технологій.

Трансформаційний потенціал технологій ШІ створює як безпрецедентні ризики, так і неперевершені можливості для кібербезпеки. Оскільки організації поспішають запровадити штучний інтелект, кіберзлочинці з шаленою швидкістю використовують уразливості, одночасно підвищуючи ефективність своїх методів. Кіберзахисники також докладають усіх зусиль, щоб використати потенціал цих технологій і змінити баланс у зростаючій гонці озброєнь ШІ [2, 40].

Але передусім штучний інтелект створює низку загроз для цифрової гігієни:

- розповсюдження дезінформації, фейкових зображень і симуляцій;
- втрату авторства та розмивання меж між людським і машинним контентом;
- порушення конфіденційності даних при роботі з відкритими моделями;
- зростання цифрової залежності та когнітивного перевантаження.

Крім того, серед основних викликів та загроз впровадження штучного інтелекту в освітній процес сучасного закладу освіти, які можуть негативно позначатися на якості освіти, можуть бути: стандартизація навчання, втрата контакту між учасниками освітнього процесу, зниження мотивації до навчання, порушення академічної доброчесності, алгоритмічні помилки та

недостовірність даних, соціальна ізоляція, недостатня підготовка кадрів, кіберзагрози та безпека даних [1].

У цьому контексті цифрова гігієна набуває нового змісту – як етико-технологічна компетентність, що поєднує технічну обізнаність, критичне мислення та відповідальне ставлення до власної присутності в мережі.

Одним із головних викликів ШІ у сфері освіти є збереження академічної доброчесності. Автоматизовані інструменти полегшують створення текстів, розв'язання завдань і навіть наукових робіт, що породжує ризики плагіату й зниження якості мислення. Викладачі мають не лише контролювати використання технологій, а й виховувати культуру відповідального користування ШІ, формуючи в здобувачів розуміння меж між допомогою інструменту та власною інтелектуальною діяльністю.

Важливо розробляти внутрішні політики етичного використання штучного інтелекту в освітніх закладах. Вирішення означених проблем потребує системного підходу, який охоплює:

- включення теми етики ШІ, медіаграмотності та цифрової гігієни в навчальні програми;
- підготовку викладачів до роботи з інтелектуальними системами;
- створення умов для розвитку AI-компетентності як складової громадянських і професійних навичок XXI століття.

Ключовим завданням освіти стає формування усвідомленої кіберкультури, заснованої на принципах критичності, етичності й безпеки.

Штучний інтелект виступає не лише технологічним інструментом, а й новим культурним чинником, який трансформує соціальні відносини, навчальні практики та уявлення про знання.

Його вплив на кіберкультуру та цифрову гігієну потребує усвідомленої педагогічної відповіді – через розвиток етичної, критичної та інформаційної компетентності всіх учасників освітнього процесу. Лише за умови поєднання інноваційності й етики можливо сформувати безпечне, стале та гуманістичне цифрове середовище освіти.

Список використаних джерел

1. Ілійчук Л. (2024). Штучний інтелект і якість освіти: можливості, виклики та загрози. Науково-педагогічні студії, (8), 232 – 248. https://doi.org/10.32405/2663-5739-2028-8-232-248
2. Яненкова І. (2025). Штучний інтелект у сфері кіьербезпеки: виклики, регулювання, впливи. Матеріали конференцій МЦНД, (21.03.2025; Тернопіль, Україна), 40 – 49. https://doi.org/10.62731/mcnd-21.03.2025.001

Enikő JAKAB
Doctor of Philosophy (PhD)
Senior Lecturer, Department of Mathematics and Informatics,
Ferenc Rákóczi II Transcarpathian Hungarian University,
e-mail: jakab.eniko@kmf.org.ua

MEASURING THE EFFECTIVENESS OF A SHORT INTERACTIVE MODULE ON PHISHING DETECTION AMONG SECONDARY SCHOOL STUDENTS

Phishing attacks pose a significant and growing threat to the digital safety of secondary school students. As young people increasingly rely on digital technologies for learning, communication, and entertainment, they are frequently exposed to manipulation attempts that aim to exploit their inexperience and trust. Phishing is recognized as one of the most widespread cybersecurity risks affecting adolescent users (Impact Networking, 2024), manifesting through various channels that are part of their daily digital routines — such as fake in-game offers, fraudulent discount links, or social media scams impersonating influencers, peers, or trusted services. These deceptive practices often aim to extract login credentials, financial data, or personal information that can later be misused for identity theft or further targeted cyberattacks.

Research indicates that adolescents' cybersecurity awareness and critical evaluation skills are often insufficient to effectively identify manipulation attempts (Hadlington & Murphy, 2018), and simple warnings alone do not effectively prevent deception in social engineering attacks (Junger et al., 2017). This reveals the need for practical, age-appropriate educational interventions that strengthen students' ability to recognize suspicious content and make safer decisions online.

The aim of this study is to determine whether a short (maximum 20-minute), interactive educational module can improve students' ability to detect phishing attempts across commonly used digital platforms. Two groups of students are compared: one participates in the interactive education, while the other does not. Students' performance is assessed before and after the lesson to detect improvement. The research involves students from grades 9–11 and focuses on two key performance aspects: the accuracy of phishing recognition and the quality of justifications provided for their decisions. The intervention uses real examples that are relevant to students' everyday online activities, and it includes short interactive decision-making tasks with immediate feedback to help them learn how to stay safe online.

The expected results suggest that even a brief and focused teaching intervention can significantly improve students' cybersecurity awareness and phishing-detection skills. The novelty of this research lies in evaluating the impact of a practice-oriented learning module in a real school environment, and thereby contributing to the pedagogical advancement of cybersecurity education and the development of digital safety competencies aligned with modern curriculum requirements.

Keywords: phishing, cybersecurity, cybersecurity awareness, informatics education, interactive learning, digital competence development

References

1. Hadlington L, Murphy K. (2018): Is Media Multitasking Good for Cybersecurity? Exploring the Relationship Between Media Multitasking and Everyday Cognitive Failures on Self-Reported Risky Cybersecurity Behaviors. Cyberpsychol Behav Soc Netw, 21(3):168-172. DOI: 10.1089/cyber.2017.0524.
2. Impact Networking. (2021). Cybersecurity in education is lagging behind other industries. Find out 15 stats that will act as a wake-up call to schools & organizations. URL: https://www.impactmybiz.com/blog/cybersecurity-in-education-stats/

Enikő JAKAB
Doctor of Philosophy (PhD)
Senior Lecturer, Department of Mathematics and Informatics,
Ferenc Rákóczi II Transcarpathian Hungarian University,
e-mail: jakab.eniko@kmf.org.ua

Gabriella PAPP
Senior Lecturer, Department of Mathematics and Informatics,
Ferenc Rákóczi II Transcarpathian Hungarian University,
e-mail: papp.gabriella@kmf.org.ua

MAPPING DIGITAL CITIZENSHIP AMONG FUTURE IT PROFESSIONALS

The rapid development of digital technologies has fundamentally transformed how people learn, work, communicate and carry out everyday tasks. As more and more aspects of our lives move into the online environment, it becomes increasingly important not only to use digital tools effectively, but also to behave safely, responsibly and ethically in digital spaces. In recent years, the concept of digital citizenship has gained significant attention, as it encompasses the protection of personal data, the critical evaluation of online information, responsible and respectful communication, and the ability to maintain a healthy balance between online and offline activities.

IT students play a particularly important role in this context. They are the ones who will design and operate the digital infrastructures of the future, shaping how technology supports society. At the same time, a considerable proportion of them will become IT teachers in secondary education, where they will influence the habits, thinking and attitudes of young people who are already active participants in the digital world. These students represent the next generation of digital citizens, and they will rely on the knowledge and example set by their teachers. Therefore, it is essential that future IT professionals develop not only high-level technical skills but also strong awareness of responsible digital behaviour.

The aim of this research is to examine how IT students manage their personal data and digital security, whether they behave critically when consuming online information, and how they support their own digital well-being. It is particularly relevant to understand how they deal with risks such as weak passwords, privacy issues on social media, misinformation or manipulation by digital content-selection algorithms, and how aware they are of the importance of maintaining personal boundaries and healthy screen-time habits. The research is based on an online questionnaire conducted among IT students at the Ferenc Rákóczi II Transcarpathian Hungarian University and provides empirical data on their current level of digital citizenship competencies.

The scientific novelty of the study lies in the approach that digital citizenship is examined not only from a technological perspective but also from ethical, social and pedagogical viewpoints. Since IT students will serve both as professionals developing new digital solutions and as future educators guiding younger users, their personal practices have a direct impact on the digital culture of future generations. If they lack sufficient awareness, security knowledge or critical thinking skills, they may not be able to support students effectively in navigating the challenges of the digital world.

The expected results of the study can contribute to improving higher education programmes in the field of informatics. They may highlight specific areas where curriculum development or targeted training interventions are needed, especially in relation to digital safety and digital well-being. Strengthening students' ethical awareness, sense of responsibility and critical thinking can ensure that they become trustworthy and exemplary role models in the digital society. Ultimately, the research supports the development of a modern educational approach that promotes not only technological competence but also responsible participation in the digital environment, which is fundamental for both individual and community well-being in the future.

Keywords: education, digital citizenship, digital safety, data protection; critical information

Gabriella PAPP
Senior Lecturer, Department of Mathematics and Informatics,
Ferenc Rákóczi II Transcarpathian Hungarian University,
e-mail: papp.gabriella@kmf.org.ua

DIGITAL TECHNOLOGIES AND DIGITAL HYGIENE IN MEASURING MATHEMATICAL KNOWLEDGE

Nowadays, in the higher education context, digital transformation represents not merely a technical shift, but also a pedagogical paradigm shift. This holds particularly true for disciplines built upon abstract conceptual systems, such as mathematics education. Digital technologies fundamentally alter the process of knowledge transfer and acquisition. They enable the dynamic visualization of abstract mathematical structures, inquiry-based learning, and the deepening of conceptual understanding. Alongside these technological innovations, digital assessment (e-tests) is becoming an integral part of the educational process, which, through immediate, automated feedback, can accelerate student development and support formative assessment strategies.

The focus of our present research is the synthesis of these two areas—digital technology and digital hygiene—examined through the development of custom-designed electronic assessment tests (e-tests) applied in higher mathematics education. The primary target population of the research consisted of pre-service teachers in the Secondary Education (Mathematics) and Secondary Education (Informatics) programs, who, as future educators, play a key role in the transmission of digital pedagogical culture.

The specific goal of our research was to create a quasi-standardized and reliable e-test suitable for the longitudinal measurement of knowledge acquired in the topic of combinatorics. The measurement was carried out at the end of the semester in the form of a delayed post-test, thus examining the existence of durable, structured knowledge rather than short-term memory.

The e-test was developed, incorporating multiple reviews from both content and subject-didactic (pedagogical content) perspectives. For the test implementation, we chose an online platform that not only allowed for administration and automated evaluation—thereby maximizing the assessment's objectivity—but also ensured the conditions of digital hygiene (e.g., secure access, transparent data handling, a test-focused, low-stimulus user interface).

The success of the testing goals was examined by further analyzing fundamental psychometric properties of Classical Test Theory (CTT):

- Reliability: To measure the test's internal consistency, we calculated the Cronbach's alpha coefficient, which shows the extent to which the items in the test measure the same latent construct.
- Item Discrimination: During the analysis of individual items, we examined their discrimination index, i.e., their ability to differentiate between students with higher and lower knowledge of the subject.
- Validity: The test's validity was primarily ensured from the perspective of content validity, guaranteeing that the test questions representatively cover the defined pedagogical objectives and curriculum of the course.

The aim and task of our research was to develop a methodological framework through which reliable and valid digital tests, providing rapid feedback, can be created for measuring the mathematical knowledge level of students in higher education. The development of such tools is essential for aligning technical advancement with increased pedagogical effectiveness, ensuring that digital instruments genuinely support the deeper levels of mathematics acquisition.

Keywords: mathematics education, digital technologies, digital hygiene, e-test

Gabriella PAPP
Senior Lecturer, Department of Mathematics and Informatics
Ferenc Rákóczi II Transcarpathian Hungarian University,
papp.gabriella@kmf.org.ua

Ádám PISTA
Student, Department of Mathematics and Informatics
Ferenc Rákóczi II Transcarpathian Hungarian University,
pista.adam@kmf.org.ua

THE USE OF DIGITAL TECHNOLOGIES IN TEACHING ABOUT INEQUALITIES

Digital technologies play a crucial role in the teaching of mathematical inequalities, as they are capable of bridging the gap between abstract algebraic notations and concrete visual representations. Students often face cognitive difficulties when they must interpret the solution of an inequality in a coordinate system. Dynamic geometry software, such as GeoGebra, provides an interactive learning environment that enables the bridging of this conceptual gap and the development of a deeper understanding. These tools provide immediate, real-time visual feedback, enabling students to actively explore the half-planes that represent the solution set.

The present pedagogical research aims to develop and investigate the impact of technology-supported instruction. The study will be conducted among 9th-grade secondary school students while covering the curriculum unit on inequalities and systems of inequalities. The intervention is centered on the purposeful application of the GeoGebra software, which we integrate into the mathematics lessons we conduct, for solving targeted tasks. We place particular emphasis on displaying the solution set of systems of inequalities as a visually interpretable intersection region (feasible region). Our assumption is that this interactive, visual approach significantly increases the students' intrinsic motivation towards the topic.

This study contributes to the identification of pedagogical practices that most effectively support the integration of algebraic and geometric thinking in 9th-grade students.

Keywords: mathematics education, digital technologies, inequalities

Miroszláv SZTOJKA
Phd, Associate Professor
Head of the Department of Mathematics and Informatics
Ferenc Rakoczi II Transcarpathian Hungarian University
Berehove, Ukraine,
sztojka.miroszlav@kmf.org.ua

Ádám TEMETŐ
2nd year student majoring in Mathematics MSc degree
Ferenc Rakoczi II Transcarpathian Hungarian University
Berehove, Ukraine,
adamtemeto11@gmail.com

DIGITAL HYGIENE CRISIS: WHY 73% OF EDUCATIONAL INSTITUTIONS ARE AT RISK IN 2025

What is digital hygiene and why it matters in 2025?

Digital hygiene crisis poses a severe threat to educational institutions, with studies showing 73% risk of cybersecurity breaches by 2025. As schools become more digitally dependent, understanding digital hygiene - practices that maintain secure digital environments - is crucial.

What is digital hygiene and why it matters in 2025? "Learners in the internet age don't need more information. They need to know how to efficiently use the massive amount of information available at their fingertips – to determine what's credible, what's relevant, and when it's useful to reference." — Anna Sabramowicz, eLearning designer and digital learning expert

Digital hygiene encompasses proactive practices that institutions, staff, and students adopt to maintain online security and digital well-being. On May 2, 2025, countries began implementing formal approaches, including the Concept of Digital Hygiene for Preschoolers, aimed at creating safe digital infrastructure in schools [4]. Digital citizenship and cyber hygiene work together to create secure educational environments. While cyber hygiene focuses on technical safety practices, digital citizenship covers broader behavioral standards [5].

Schools lacking proper digital hygiene face significant risks, particularly regarding sensitive data protection [2]. Key impacts include:

- Compromised sensitive information: Exposure of personal data [2]
- Identity theft risks: Targeted attacks by cybercriminals [2]
- Academic integrity issues: Unauthorized access can compromise academic records [2]
- Significant reputational damage: Security breaches harm institutional reputation [1]
- Financial and operational disruption: Data breaches cause financial losses [1]

Poor digital hygiene can impact students' mental health through inappropriate content exposure. This risk is higher for younger students [6].

Core digital hygiene practices for educational institutions

Implementing digital hygiene requires clear protocols. Schools face unique challenges due to vast data and diverse users. Here are the essential practices. Schools should enforce 10-character passwords for standard accounts and 16 for administrative ones [7]. Long passphrases are more effective than complex symbols. Two-factor authentication (2FA) blocks 99% of untargeted attacks [8] and should be mandatory for administrator and financial accounts [8]. With 96% of school apps sharing student data [9], institutions need strict vetting protocols. Schools should prioritize FERPA-compliant apps and implement mobile device management systems [9]. Phishing threatens schools, with 60% experiencing attacks in 2020 [10]. Schools should deploy email security with malware detection and language processing [10]. Regular phishing awareness training and simulations are essential for staff and students. Automated device updates during off-hours prevent security gaps [11]. Microsoft Defender provides crucial malware protection for educational settings [11]. Schools should use Identity Pre-Shared Key (IPSK) for unique Wi-Fi credentials [12]. Network segmentation creates isolated zones, containing potential breaches [13].

Curriculum integration and teacher training

"To understand their world, we must be willing to immerse ourselves in that world. We must embrace the new digital reality. If we can't relate, if we don't get it, we won't be able to make schools relevant to the current and future needs of the digital generation." — Ian Jukes, Director, InfoSavvy Group; global education futurist

Integrating digital hygiene across subjects enables contextual learning. Italy mandates digital citizenship education within civics, requiring 33 teaching hours yearly [20]. This cross-curricular approach focuses on digital information evaluation, data security, and ethical communication.

Educators need proper cybersecurity training to guide students effectively. The Cyber Hygiene Academy offers specialized programs for K-12 teachers [21], covering:

- Digital platform design techniques
- Mental health impacts
- Facilitating digital well-being discussions [5]

Monitoring, metrics, and long-term impact

School cybersecurity audits provide insights into digital hygiene practices and help obtain cybersecurity insurance. Documentation through screenshots and policies simplifies future audits. Studies show high satisfaction rates and knowledge improvement through digital hygiene training programs. Long-term digital hygiene improvement requires cultural shifts throughout educational institutions. Interactive digital education leads to lasting improvements in knowledge and practices. Recognizing good cybersecurity behavior, like acknowledging staff who report phishing, reinforces positive habits and transforms mindsets. A strong digital safety culture builds technology trust while enhancing school processes. When everyone understands their prevention role, safety becomes routine.

Conclusion

Educational institutions face critical cybersecurity threats as digital dependence grows. Schools hold sensitive data, making them prime targets. Without safeguards, they risk breaches, theft, and disruption. Students face additional online risks.

Strong authentication, safe browsing, training, and network security provide essential protection. These work best with behavioral changes through engaging education.

Regular audits and metrics help track digital hygiene progress. Schools must act now on cybersecurity or risk devastating breaches by 2025.

References

1. Podlinyayeva O.O. and Sytnyk L.G. (n.d.). CYBER HYGIENE PRACTICES AND PROVIDING PROPER EDUCATION . [online] Available at: https://www.researchgate.net/publication/374094554_CYBER_HYGIENE_PRACTICES_AND_PROVIDING_PROPER_EDUCATION [Accessed 15 Oct. 2025].

2. Securus360.com. (2023). Building a Cybersecurity Culture: Essential Cyber Hygiene for K-12 Schools. [online] Available at: https://www.securus360.com/blog/building-a-cybersecurity-culture-essential-cyber-hygiene-for-k-12-schools.

3. Good-start.eu. (2016). Digital Hygiene Practices and Skills Gap Current Situation Report – Good Start. [online] Available at: https://good-start.eu/digital-hygiene-practices-and-skills-gap-current-situation-report/ [Accessed 16 Oct. 2025].

4. Iitlt.gov.ua. (2025). The Concept of Digital Hygiene for Preschoolers has been approved. – Institute for Digitalisation of Education of the NAES of Ukraine. [online] Available at: https://iitlt.gov.ua/en/skhvaleno-kontseptsiiu-tsyfrovoi-hihieny/ [Accessed 15 Oct. 2025].

5. Europass Teacher Academy. (2025). Digital Wellbeing: A New Challenge for Teachers and Students. [online] Available at: https://www.teacheracademy.eu/course/digital-wellbeing/ [Accessed 17 Oct. 2025].

Ildiko GREBA
PhD
Ferenc Rakoczi II Transcarpathian Hungarian University,
greba.ildiko@kmf.org.ua

Tetiana SHCHERBAN
Doctor of Psychological Sciences, Professor
Ferenc Rakoczi II Transcarpathian Hungarian University,
scserban.tetjana@kmf.org.ua

BULLYING AND CYBERBULLYING IN THE EDUCATIONAL ENVIRONMENT: THE ROLE OF THE EDUCATIONAL PROCESS IN FORMING A CULTURE OF DIGITAL HYGIENE

Problem Statement. The contemporary educational environment is increasingly shaped by digitalization, offering new learning opportunities while simultaneously exacerbating the risks of bullying and cyberbullying. These phenomena compromise psychological safety and negatively affect the socialization of participants in the educational process. Insufficient digital awareness complicates the detection and prevention of cyberbullying, highlighting the need to cultivate responsible digital behavior, tolerance, and safe interaction both online and offline.

Analysis of Current Research. Bullying and cyberbullying are recognized as key threats to a safe educational environment and have been actively studied by both international and Ukrainian scholars. Early research was conducted by Scandinavian scientists such as D. Olweus, E. Roland, A. Picasso, and P. Heinemann, while significant contributions to counteracting the phenomenon were made by A. Brown, M. Klein, E. Miller, and D. Thompson. In Ukraine, researchers including M. Alekseenko, T. Tytarenko, T. Yatsenko, I. Dorozhko, O. Drozdova, and V. Shakhrai have focused on psychological and pedagogical aspects of bullying. In the context of modern digitalized education, increasing attention is paid to cyberbullying, which requires new preventive approaches. The role of the educational process in forming a culture of digital hygiene remains underdeveloped and warrants further scientific inquiry and practical solutions (Greba & Havryliuk, 2023).

Main Content. Bullying and cyberbullying represent complex socio-psychological phenomena manifested through various forms of aggressive behavior within educational settings. Scientific sources reveal several synonymous terms – "violence," "harassment," "child cruelty," "aggression," "mobbing," and "persecution" – with "aggression" and "bullying" being the most commonly used. According to Shcherbatiuk (2022), aggression refers to destructive behavior that causes physical or psychological harm, inducing fear, anxiety, or tension, and may be overt or covert, individual or group-based.

Bullying is defined as the systematic and deliberate humiliation, intimidation, or harassment of another person aimed at dominance or control (Prokopenko et al., 2019). Under the Law of Ukraine No. 2657-VIII "On Amendments to Certain Legislative Acts of Ukraine Regarding Counteraction to Bullying" (2018), such acts may be physical, psychological, economic, or sexual in nature, including the use of electronic communication means.

Within educational institutions, bullying is considered a form of institutional violence encompassing physical, psychological, spiritual, and social actions that undermine a child's status and cause suffering. Forms of bullying include indirect, physical, behavioral, verbal, and cyberbullying (Hluza, 2022). With digitalization and hybrid learning, cyberbullying has intensified due to reduced physical interaction and the manifestation of aggression in virtual environments (Karpinska, 2022). Cyberbullying is characterized by perpetrator anonymity, rapid information dissemination, and prolonged psychological impact on the victim, underscoring the importance of fostering a culture of digital hygiene.

Research indicates that bullying and cyberbullying are closely interrelated, with the same individuals often becoming victims of both. Therefore, combating cyberbullying is impossible without systematic anti-bullying measures within educational institutions. Pedagogical interventions in digital environments should be based on proven anti-bullying approaches, consider the specific features of online aggression, and utilize digital tools in educational work with students.

Implementation of structured anti-bullying programs, such as Kenneth Shore's 12-step program, and active collaboration with law enforcement through meetings and discussions on the legal aspects of bullying and cyberbullying, are particularly effective. It is crucial to ensure conditions for safe, responsible, and ethical use of digital resources while fostering an atmosphere of support and protection for all participants in the educational process.

A key component is informing participants that incidents of bullying and cyberbullying will receive appropriate responses from educators and the administration in accordance with Ukrainian legislation and Ministry of Education regulations. Reporting mechanisms should be known, confidential, and adapted to different age groups. School personnel should monitor bullying incidents, evaluate the effectiveness of preventive measures, and develop comprehensive action plans to prevent and address bullying and cyberbullying based on such analysis.

Conclusions. Bullying and cyberbullying in the contemporary educational environment are closely interrelated phenomena that negatively impact the psychological and social development of participants. Effective prevention requires a systemic approach within the educational institution, including preventive measures, the cultivation of a culture of digital hygiene, and responsible use of digital resources. Ensuring a safe and supportive environment, active information sharing, and collaboration among educators, students, and law enforcement agencies are key factors in fostering responsible online behavior.

References

1. Глюза, М. П. (2022): Булінг як актуальна проблема соціалізації сучасної молоді. / Режим доступу: https://openarchive.nure.ua/server/api/core/bitstreams/47853876-c83d4e4a-93a4-f1a62c85ec5c/content
2. Греба, І. & Гаврилюк, І. (2023). Булінг та його прояви в освітньому середовищі початкової школи. / Режим доступу: https://doi.org/10.59694/ped_sciences.2023.05.095
3. Карпінська, Л. В. (2022): Булінг як соціально-психологічний феномен девіантної поведінки шкільної молоді. In The 9 th International scientific and practical conference "Modern research in world science" SPC "Sci-conf. com. ua", Lviv, Ukraine. / Режим доступу: https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/48191/1/%D0%A2%D0%B5%D0%B7%D0%B8%20%D0%9B%D1%8C%D0%B2%D1%96%D0%B2.pdf#page=1064
4. Прокопенко Л. І., Тетьоркіна В. А., Оловаренко О. І., Пальчик О. О., (2019): Дослідження булінгу в просторі організованого дитячого колективу. / Режим доступу: http://repository.khpa.edu.ua:8080/jspui/bitstream/123456789/229/1/Palch_st_1.pdf
5. Шахрай, В. М. (2025). Провідні педагогічні умови запобігання і подолання булінгу в цифровому освітньому середовищі. «Суспільство та національні інтереси», 2(10), 461-474.
6. Щербатюк, О. В. (2022): Багатовимірність у вивченні агресивності. Режим доступу: https://www.researchgate.net/profile/Vadym-Sulitskyi/publication/363468599

Ildiko GREBA
PhD
Ferenc Rakoczi II Transcarpathian Hungarian University,
greba.ildiko@kmf.org.ua

Marina BEVZIUK
Candidate of Pedagogical Sciences
Ferenc Rakoczi II Transcarpathian Hungarian University,
bevzjuk.marina@kmf.org.ua

CYBERBULLYING IN THE EDUCATIONAL PROCESS: TYPES AND PREVENTIVE MEASURES

Problem Statement. In the contemporary educational environment, cyberbullying is becoming increasingly widespread due to the active use of digital technologies, social networks, and online communication among children and adolescents. Unlike traditional bullying, cyberbullying is characterized by anonymity, rapid information dissemination, and continuous psychological pressure, which complicates its detection and mitigation. Cyberbullying negatively affects the emotional well-being, learning motivation, and social adaptation of participants in the educational process. Despite growing attention to the issue, prevention systems remain insufficiently developed, and educators, parents, and students often lack effective strategies for responding. This highlights the need to identify types of cyberbullying, analyze their features, and develop comprehensive preventive measures within the educational process.

Analysis of Current Research. Research indicates that cyberbullying and its prevention are actively studied by both international and Ukrainian scholars. International researchers (K. Barrett, R. Kowalski, S. Limber, P. Smith, J. Finkel, J. Yunoven) focus on the factors contributing to cyberbullying, participant roles, and psychological mechanisms. Ukrainian scholars (L. Naidionova, V. Bedan, K. Ivanyuk, A. Tyshchenko, et al.) examine the nature of the phenomenon, classification of its types, and developmental dynamics. Significant attention is given to the destructive impact of cyberbullying on children's and adolescents' mental health (Yu. Lehar, M. Ozhevan, O. Petrunko). Other studies (H. Yefremova, Z. Zalibovska, K. Chaban) analyze the role structure of participants and behavioral models in online spaces. Legal aspects of countering cyberbullying are discussed by P. Bilenchuk, M. Dzyuba, V. Lipkan, among others, emphasizing the interdisciplinary nature of the problem.

Main Content. Bullying in educational settings remains one of the most pressing social issues. Globally, the term "bullying" refers to systematic humiliation, aggression, or violent acts against others. Ukrainian legislation, specifically the Law of Ukraine "On Amendments to Certain Legislative Acts Regarding Counteraction to Bullying" № 2657-VIII (2018), defines bullying as actions by participants in the educational process – including physical, psychological, economic, and sexual violence, as well as actions via electronic communications – that may cause harm to victims (Греба, Гаврилюк, 2023). Bullying is characterized by systematicity, intentionality, a desire to dominate, and instill fear in the victim, with motives including revenge, self-assertion, or sadistic satisfaction (Савельєв, Салата, 2009).

Cyberbullying, a modern form of traditional bullying, emerged with the development of digital technologies. The term was first introduced by Canadian educator B. Belsey and American lawyer N. Willard in the late 1990s. Cyberbullying is defined as the deliberate humiliation, intimidation, or harassment of an individual using electronic communication tools – such as smartphones, social networks, messaging apps, and email. Its distinguishing features include perpetrator anonymity and the constant accessibility of the victim, which increases psychological pressure and complicates identification of the aggressor.

Scholars P. Smith and R. Slonje define cyberbullying as aggressive, repeated, and intentional actions directed at a person who is unable to defend themselves over time (Нестеренко, 2019). Such actions may include spreading offensive messages, publishing humiliating photos or videos, creating fake accounts, cyberstalking, or socially isolating the user online.

Several classifications of cyberbullying exist in the academic discourse. A widely recognized classification by R. Kowalski, S. Limber, and P. Agatston in Cyberbullying: Bullying in the Digital Age (2011) identifies key forms of cyberbullying: flaming (aggressive messages in public chats), harassment (persistent offensive messages), griefing (intentional disruption of games or digital processes), cyberstalking (persistent online pursuit), trolling (provocative communication style), sexting (sending or sharing intimate photos or videos without consent), cyber defamation (posting false or humiliating information), outing (disclosure of private or confidential information), happy slapping (sharing videos of violent scenes), and virtual exclusion/ignoring (boycott in digital spaces) (Мафтин, 2024). With the advancement of digital technologies, the prevalence and forms of cyberbullying continue to expand, including new methods of psychological pressure via artificial intelligence, fake news, manipulative content, and chatbots.

Preventing cyberbullying in the educational process requires a systematic approach involving all participants – teachers, students, parents, and administrators. Key areas include fostering digital literacy and a culture of safe online behavior, which encompasses teaching ethical internet and social media use. It is essential to conduct training sessions, educational hours, and interactive activities aimed at developing empathy, tolerance, and non-violent communication skills. Enhancing the digital competence of teachers and parents ensures timely recognition and response to cyberbullying. Educational institutions should establish clear incident response systems, provide confidential channels for reporting cyberbullying, and collaborate with psychologists, social services, and law enforcement.

Conclusion. Cyberbullying in the educational process poses a significant threat to students' psychological and social development, necessitating a systematic approach for its detection and prevention. Effective prevention requires comprehensive collaboration among educators, parents, and administrators, fostering digital literacy, cultivating empathy, and implementing clear mechanisms for responding to incidents within the educational environment.

References

1. Греба, І. & Гаврилюк, І. (2023). Булінг та його прояви в освітньому середовищі початкової школи. / Режим доступу: https://doi.org/10.59694/ped_sciences.2023.05.095
2. Мафтин Л. (2024) Психолого-педагогічні умови профілактики кібербулінгу в освітньому середовищі / Педагогічні науки: теорія, історія, інноваційні технології : науковий журнал № 5 (139). – С. 383–394. – DOI: 10.24139/2312-5993/2024.05/383-394
3. Нестеренко, А. (2019). Адміністративно-правова протидія кібербулінгу стосовно дітей. Вісник Національного університету «Львівська політехніка». Серія: Юридичні науки, 21, 170-175.
4. Савельєв Ю. & Салата Т. (2009): Виключення та насильство: чи існує булінг в українській школі? / Режим доступу: https://ekmair.ukma.edu.ua/server/api/core/bitstreams/5b87c979-11c1-4cc9-a7a3-e3dfb0b4af1b/content

Ildiko GREBA
PhD
Ferenc Rakoczi II Transcarpathian Hungarian University,
greba.ildiko@kmf.org.ua

Emőke BERGHAUER-OLASZ
PhD, Associate Professor
Ferenc Rakoczi II Transcarpathian Hungarian University,
berghauer.olasz.emoke@kmf.org.ua

CYBER HYGIENE IN THE EDUCATIONAL ENVIRONMENT: FOSTERING SAFE DIGITAL BEHAVIOR AMONG PARTICIPANTS IN THE EDUCATIONAL PROCESS

Problem Statement. In the contemporary educational environment, digital technologies and online communication have become an integral part of the learning process, providing new opportunities for instruction, interaction, and socialization for both students and educators. At the same time, the active use of digital resources generates risks to the safety of educational participants, including cyberbullying, information manipulation, excessive psychological strain, privacy violations, and uncontrolled use of personal data. The absence of systematic digital security training and insufficient digital competence among students, teachers, and parents increases the likelihood of negative consequences arising from the use of information and communication technologies. This underscores the urgent need to cultivate principles of cyber hygiene among all participants in the educational process – skills for safe and responsible digital behavior, the ability to critically evaluate information, avoid risks, and counteract harmful phenomena online.

Analysis of Current Research. Research on cyber hygiene has emphasized issues of cybersecurity and safe digital behavior within educational contexts. Studies by Yu. Bilyavska, Ya. Shestak, and others explore cyber hygiene as a key component of digital culture, particularly in the context of active digitalization in education. Ukrainian researchers such as V. Bykov, O. Burov, and N. Dementievska focus on cybersecurity mechanisms in digital learning environments, directly related to the prevention of cyberbullying. O. Chernykh's research on fostering safe online behavior in children further confirms the necessity of a systematic approach to digital hygiene education (Лунгол, 2024), (Гончарова, 2022).

Main Content. Cyber hygiene constitutes a crucial element in ensuring user safety in digital environments. It encompasses knowledge and skills related to protecting personal data, creating strong passwords, using two-factor authentication, updating software and antivirus programs, and exercising caution in social networks and online banking. Adherence to cyber hygiene principles enhances the information security of individual users and society as a whole, reducing the risks of cyberattacks, data breaches, and cybercrime, which is particularly critical during wartime and in the context of distance learning (Гончарова, 2022).

Both domestic and international scholars emphasize the importance of cultivating digital culture among children and youth by integrating cybersecurity into educational processes. Learning platforms, online courses, quizzes, and simulations facilitate the development of practical skills for safe online behavior. In Ukraine, the Ministry of Digital Transformation has implemented the platform "Diia. Digital Education," which hosts educational series for students, educators, and parents, including "Fundamentals of Cyber Hygiene," "Personal Cyber Hygiene," "Cyber Nannies," "Cyberbullying for Teenagers," and "Beware of Cyber Fraud," among others. The platform also provides interactive tools – simulators, tests, and gamified exercises – that allow users to practice digital safety skills in a hands-on manner (Diia. Education Portal).

Public organizations also play a significant role in promoting cyber hygiene. The NGO "MINZMIN" runs the "Children's Online Safety School" and the online course "Digital Rights and Child Safety," offering video lessons, checklists, assessments, lesson plans, and materials for parents. The NGO "Stop Sexting" has developed educational materials for different age groups, online courses for educators and school directors, and interactive lessons for high school students (e.g., "Billboard

Test and Online Love," "Intimate Selfies Online," "(Non)Child Relationships Online"), aimed at preventing sexual violence and cyberbullying.

The integration of government initiatives, public projects, interactive teaching methods, and systematic implementation of cyber hygiene in schools enables students to develop comprehensive competencies for safe digital behavior, thereby raising the overall level of digital culture in Ukrainian society.

International massive open online courses (MOOCs) on platforms such as EdX also contribute significantly to enhancing educators' digital competence. The course "Get Started Teaching Computing in Primary Schools" (ages 5-11) focuses on the safe use of computers and the internet, while the course "Teach Teens Computing: Cybersecurity" (ages 14-16) covers cybersecurity concepts, types of cyberattacks, and tools for protecting data, devices, and networks. The online course "Cyberbullying" trains teachers to identify, prevent, and respond to instances of online harassment, including collaboration with parents and law enforcement. The curriculum includes modules on the forms, causes, and consequences of cyberbullying, as well as strategies for prevention and incident reporting (Наумова, Бульвінська, 2024).

Conclusion. In conclusion, fostering cyber hygiene in the educational environment is an essential component of contemporary digital culture and the security of participants in the educational process. The combination of government initiatives, educational platforms, public projects, and international online courses ensures systematic preparation of students, educators, and parents for safe digital behavior. Interactive teaching methods and practical exercises support the development of skills for protecting personal data, preventing cyberbullying, and responsibly using digital resources. Ultimately, implementing cyber hygiene contributes to enhancing the digital culture and information security of Ukrainian society as a whole.

References

1. Basic Knowledge of Cyber Hygiene. Diia. Education Portal. Available at: https://osvita.diia.gov.ua/courses/basic-knowledge-of-cyber-hygiene
2. Гончарова, І. П. (2022). Формування основ кібергігієни здобувачів освіти як один з головних пріоритетів освітньої діяльності в умовах дистанційного навчання у воєнний час.
3. Лунгол О. М. (2024). Роль кібергігієни у безпеці та розвитку українського суспільства / Сучасна українська держава: вектори розвитку та шляхи мобілізації ресурсів матеріали VII Всеукраїнської науково-практичної конференції. – С. 268-270.
4. Наумова, В., & Бульвінська, О. (2024). Управління безпекою учнів в інтернеті: відкриті освітні ресурси на допомогу освітянам. Освітологія, 13(13), 78-90.

Ildiko GREBA
PhD
Ferenc Rakoczi II Transcarpathian Hungarian University,
greba.ildiko@kmf.org.ua

Valentina BILAN
Candidate of Pedagogical Sciences, Associate Professor
Ferenc Rakoczi II Transcarpathian Hungarian University,
bilan.valentina@kmf.org.ua

BULLYING AND CYBERBULLYING PREVENTION IN THE EDUCATIONAL ENVIRONMENT: PEDAGOGICAL CONDITIONS FOR FORMING SAFE DIGITAL BEHAVIOR

Problem Statement. Bullying and cyberbullying are widespread phenomena in contemporary educational environments, negatively affecting the development of children and adolescents. The problem has persisted even during the war: in 2023, 96 cases of bullying were registered in Ukraine, with a total of 614 cases over the past five years. Cyberbullying poses particular danger due to the widespread use of digital technologies, as children and adolescents make up one-third of global internet users. International studies indicate increasing online victimization, while traditional bullying is decreasing. This underscores the need to develop effective pedagogical strategies for preventing bullying and fostering safe digital behavior among participants in the educational process.

Analysis of Current Research. The issue of cyberbullying and its prevention is actively studied by both international and Ukrainian scholars. International researchers, including K. Barrett, R. Kowalski, S. Limber, P. Smith, J. Finkel, and J. Yunoven, investigate factors contributing to cyberbullying, role structures, and behavioral characteristics of participants in digital harassment. Ukrainian scholars, such as H. Yefremova, Z. Zalibovska, O. Motlyakh, T. Tsyuman, K. Chaban, and B. Petrenko, analyze the psychological and pedagogical aspects of cyberbullying, its consequences for educational participants, and the role of digital technologies in the spread of aggression.

Main Content. The internet has become an integral part of modern life, providing broad opportunities for communication, information search, learning, and various activities through social networks, online courses, video lessons, virtual libraries, and educational projects (Біда, Кучай, Сироєжко, 2023). At the same time, digitalization introduces new threats, with cyberbullying being particularly dangerous – deliberate, repeated actions using digital technologies to humiliate, intimidate, or psychologically pressure victims. Cyberbullying is characterized by perpetrator anonymity, rapid information dissemination, and prolonged psychological impact. A safe educational environment requires not only material and technical protection but also psychological and informational security, development of information culture, legal competence, and skills for safe communication (Мафтин, 2024).

V. Shakhray proposed a classification of prevention levels for bullying and cyberbullying in digital educational environments:

High (socially harmonious) – no signs of bullying; educators are well-informed, systematically conduct educational work, and possess digital competence; students demonstrate empathy, assertiveness, and self-protection skills; parents have high digital and pedagogical literacy and actively cooperate with educators.

Medium (socially acceptable) – bullying is minor and unsystematic; educators and students have sufficient knowledge and skills for prevention, but educational work is periodic; parents are partially informed and collaborate with teachers.

Low (socially inhibiting) – bullying and cyberbullying appear occasionally; educators are insufficiently aware of the problem and apply preventive measures unsystematically; participants exhibit low empathy, assertiveness, and digital culture; parents are poorly informed and unprepared to cooperate with educators (Шахрай, 2024).

Effective counteraction to cyberbullying requires a comprehensive approach, including pedagogical, technological, and socio-educational measures. Building on ideas from J. Patchin and

S. Hinduja regarding bullying prevention – creating a safe environment, engaging students, parents, teachers, and specialists, enhancing parental digital competence, improving school prevention methods, and developing skills to resist bullying via support groups – the following methods are recommended:

1. Educational activities and upbringing work – training sessions, lectures, and interactive activities to develop empathy, assertiveness, and digital culture;
2. Enhancing digital competence – training teachers and parents to use digital tools for prevention and detection of cyberbullying;
3. Internal rules and procedures – protocols for responding to cyberbullying incidents, confidential reporting channels, and accountability for perpetrators;
4. Collaboration with social services and law enforcement – consultations, legal and psychological support for victims;
5. Creating a safe microclimate – active involvement of students, teachers, and parents in educational work and promoting mutual respect online and offline.

Conclusion. Bullying and cyberbullying remain pressing issues in educational environments, adversely affecting participants' development. Cyberbullying is complicated by perpetrator anonymity, rapid information dissemination, and prolonged psychological impact. Effective prevention requires a comprehensive approach: pedagogical, technological, and socio-educational measures, enhanced digital competence of teachers and parents, and clear internal procedures for responding to incidents. Cooperation with social services, law enforcement, and active engagement of all educational participants fosters a safe digital environment and promotes a culture of responsible online behavior.

References

1. Біда, Олена, Кучай, Тетяна, Сироєжко, Ольга. (2023) Необхідність застосування інтернет-ресурсів при підготовці вчителів. Перспективи та інновації науки. Серія «Педагогіка», 16 (34), 27-35.
2. Мафтин Л. (2024) Психолого-педагогічні умови профілактики кібербулінгу в освітньому середовищі / Педагогічні науки: теорія, історія, інноваційні технології : науковий журнал № 5 (139). – С. 383–394. – DOI: 10.24139/2312-5993/2024.05/383-394
3. Шахрай, В. М. (2024). Запобігання булінгу в цифровому освітньому середовищі: стан і способи вдосконалення. Теоретико-методичні проблеми виховання дітей та учнівської молоді, 2(28), 245-259.
4. Шахрай, В. М. (2025). Провідні педагогічні умови запобігання і подолання булінгу в цифровому освітньому середовищі. "Суспільство та національні інтереси", 2(10), 461-474..

Chobo HEI
Bachelor's degree student in Secondary Education, specializing in Mathematics
Ferenc Rákóczi II Transcarpathian Hungarian University

Myroslav STOIKA
Associate Professor
Department of Mathematics and Informatics
Ferenc Rákóczi II Transcarpathian Hungarian University

CYBERCULTURE AS A COMPONENT OF PROFESSIONAL TRAINING OF MATHEMATICS AND INFORMATICS TEACHERS

Problem Statement. Bullying and cyberbullying are widespread phenomena in contemporary educational environments, negatively affecting the development of children and adolescents. The problem has persisted even during the war: in 2023, 96 cases of bullying were registered in Ukraine, with a total of 614 cases over the past five years. Cyberbullying poses particular danger due to the widespread use of digital technologies, as children and adolescents make up one-third of global internet users. International studies indicate increasing online victimization, while traditional bullying is decreasing. This underscores the need to develop effective pedagogical strategies for preventing bullying and fostering safe digital behavior among participants in the educational process.

Analysis of Current Research. The issue of cyberbullying and its prevention is actively studied by both international and Ukrainian scholars. International researchers, including K. Barrett, R. Kowalski, S. Limber, P. Smith, J. Finkel, and J. Yunoven, investigate factors contributing to cyberbullying, role structures, and behavioral characteristics of participants in digital harassment. Ukrainian scholars, such as H. Yefremova, Z. Zalibovska, O. Motlyakh, T. Tsyuman, K. Chaban, and B. Petrenko, analyze the psychological and pedagogical aspects of cyberbullying, its consequences for educational participants, and the role of digital technologies in the spread of aggression.

Main Content. The internet has become an integral part of modern life, providing broad opportunities for communication, information search, learning, and various activities through social networks, online courses, video lessons, virtual libraries, and educational projects (Біда, Кучай, Сироєжко, 2023). At the same time, digitalization introduces new threats, with cyberbullying being particularly dangerous – deliberate, repeated actions using digital technologies to humiliate, intimidate, or psychologically pressure victims. Cyberbullying is characterized by perpetrator anonymity, rapid information dissemination, and prolonged psychological impact. A safe educational environment requires not only material and technical protection but also psychological and informational security, development of information culture, legal competence, and skills for safe communication (Мафтин, 2024).

V. Shakhray proposed a classification of prevention levels for bullying and cyberbullying in digital educational environments:

High (socially harmonious) – no signs of bullying; educators are well-informed, systematically conduct educational work, and possess digital competence; students demonstrate empathy, assertiveness, and self-protection skills; parents have high digital and pedagogical literacy and actively cooperate with educators.

Medium (socially acceptable) – bullying is minor and unsystematic; educators and students have sufficient knowledge and skills for prevention, but educational work is periodic; parents are partially informed and collaborate with teachers.

Low (socially inhibiting) – bullying and cyberbullying appear occasionally; educators are insufficiently aware of the problem and apply preventive measures unsystematically; participants exhibit low empathy, assertiveness, and digital culture; parents are poorly informed and unprepared to cooperate with educators (Шахрай, 2024).

Effective counteraction to cyberbullying requires a comprehensive approach, including pedagogical, technological, and socio-educational measures. Building on ideas from J. Patchin and S. Hinduja regarding bullying prevention – creating a safe environment, engaging students, parents,

teachers, and specialists, enhancing parental digital competence, improving school prevention methods, and developing skills to resist bullying via support groups – the following methods are recommended:

1. Educational activities and upbringing work – training sessions, lectures, and interactive activities to develop empathy, assertiveness, and digital culture;
2. Enhancing digital competence – training teachers and parents to use digital tools for prevention and detection of cyberbullying;
3. Internal rules and procedures – protocols for responding to cyberbullying incidents, confidential reporting channels, and accountability for perpetrators;
4. Collaboration with social services and law enforcement – consultations, legal and psychological support for victims;
5. Creating a safe microclimate – active involvement of students, teachers, and parents in educational work and promoting mutual respect online and offline.

Conclusion. Bullying and cyberbullying remain pressing issues in educational environments, adversely affecting participants' development. Cyberbullying is complicated by perpetrator anonymity, rapid information dissemination, and prolonged psychological impact. Effective prevention requires a comprehensive approach: pedagogical, technological, and socio-educational measures, enhanced digital competence of teachers and parents, and clear internal procedures for responding to incidents. Cooperation with social services, law enforcement, and active engagement of all educational participants fosters a safe digital environment and promotes a culture of responsible online behavior.

References

1. Arney, C., Vanatta, M., & Nelson, J. (2016). Cyber education via mathematical education. Cyber Defense Review.
2. Sacristán, A. I. (2024). Digital technologies, cultures and mathematics education. In Proceedings of the 14th International Congress on Mathematical Education.
3. Hörmann, C. (2024). Digital education training for teachers—Learnings from Austria. Frontiers in Education.
4. Ajala, O. A., & Soladoye, D. A. (2025). Introducing the principles of cybersecurity, artificial intelligence, and IoT applications into the STEM curriculum. In Proceedings of the 14th International Conference on STEM Education.
5. TeachCyber.org. (2024). Teacher professional development.
6. Martin, F. (2024). Teacher professional development and collaboration to integrate cybersecurity into mathematics and science instruction. CADRE K12.
7. Cyber.org. (2024). Empowering educators to teach cyber.

Олена ПЕТРУШЕВИЧ
студентка 4-го курсу
кафедра математики та інформатики,
Закарпатський угорський університет ім. Ференца Ракоці II

Еніке ЯКОБ
доктор філософії (PhD)
кафедри математики та інформатики
Закарпатський угорський університет ім. Ференца Ракоці II
jakab.eniko@kmf.org.ua

ВИПРОБУВАННЯ ТА ОЦІНЮВАННЯ ВПЛИВУ ШТУЧНОГО ІНТЕЛЕКТУ НА УРОКАХ ІНФОРМАТИКИ

Штучний інтелект (ШІ) перетворився на один із впливових та визначальних факторів розвитку сучасного суспільства, який і надалі стрімко розвивається та активно застосовується. Інтеграція ШІ в навчальний процес має великий потенціал у поліпшенні якості освіти та створенні більш ефективних підходів до навчання. ШІ може спрощувати адміністративні процеси для навчальних закладів, автоматизувати рутинні завдання педагогів (оцінювання, перевірка тестів, створення завдань), розробляти програми та платформи, аналізувати дані кожного учня, враховуючи індивідуальні можливості та потреби, швидкість та стиль навчання кожного здобувача освіти, дає доступ до якісної освіти незалежно від місця проживання та фінансових можливостей учнів, та багато інших переваг, які постійно розширюються та вдосконалюються, реагуючи на потреби та вподобання користувачів та вимоги сучасного життя.

Підібравши відповідний інструмент ШІ можна використати їх для вирішення багатьох освітніх завдань у викладанні інформатики. При вивченні кодування доцільним є застосування CodeSignal Learn, Replit. MagicSchool, Eduaide.ai може допомогти у плануванні уроків. Nolej, DiffIt, MyLessonPal, Copilot, teachology.ai., Curipod можна застосовувати для створення сценарію уроку. Для виготовлення презентацій підійдуть Gamma.app, Tome, Canva, Beautiful.ai, MagicSlides. Цікавим та корисним є отримання через TeachFX, EnlightenAI зворотнього зв'язку від проведеного уроку.

Було проведено опитування серед вчителів інформатики щодо використання ШІ у викладанні предмету. Серед педагогів, які брали участь в опитуванні усі активно застосовують у викладанні різноманітні ШІ. Такі види робіт, як складання плану уроку, швидке створення завдань, перевірку вправ, тестів, контрольних робіт, моніторинг успішності, вчителі інформатики делегували б штучному інтелекту. Найнебезпечнішим недоліком штучного інтелекту вважають у наданні ШІ хибних даних. Самими поширеними серед вчителів інформатики є такі інструменти як ChatGPT, Gemini та Copilot.

Для визначення ефективності деяких інструментів ШІ ми провели тестування найбільш популярних серед них – ChatGPT, Gemini, Copilot, Perplexity. Для цих інструментів ШІ було надано завдання підготувати план уроку, тест та цікаву ідею для проведення уроку в 11 класі. Порівнюючи результати, які надали інструменти ми прийшли до висновку, що кожна модель без помилок виконала запит, проте деякі дають більш розгорнуту відповідь (Gemini, Perplexity), а інші лаконічнішу (ChatGPT, Copilot).

Отже, застосування штучного інтелекту у викладанні інформатики робить навчальний процес більш ефективним, якісним, гнучким, індивідуалізованим, дозволяє підвищити мотивацію учнів, розкриває їхній потенціал та формує інформатичну грамотність, необхідну для життя в сучасному цифровому суспільстві.

Проте, використання інструментів штучного інтелекту вимагає обережного та відповідального підходу. При його застосуванні необхідно надавати перевагу раціональному використанню, тобто зі збереженням продуктивної боротьби, результатом якої є глибоке мислення та самовираження. Під час роботи зі ШІ необхідно подбати також про конфіденційність даних учнів.

У підсумку, при застосовуванні ШІ у викладанні інформатики необхідно врахувати всі можливі наслідки та вдосконалювати стратегії його використання.

Ключові слова: штучний інтелект, уроки інформатики, тестування штучного інтелекту, інформаційна безпека, цифрова грамотність, освітні інновації.

CSEHIL Anikó
a II. Rákóczi Ferenc Kárpátaljai Magyar Egyetem,
Pedagógia, Pszichológia, Tanító, Óvodapedagógia,
Oktatási Intézményvezetés Tanszék oktatója
E-mail: orban.aniko@kmf.org.ua

A KIBERTSPORT HATÁSA A FELSŐOKTATÁSI HALLGATÓK EGÉSZSÉGÉRE

A 21. század digitális forradalma alapvetően formálta át a fiatal felnőttek életmódját, szabadidős szokásait és társas kapcsolatait. A technológiai fejlődés, az internet és a digitális platformok rohamos terjedése új kulturális és gazdasági ökoszisztémát hozott létre, amelyben a videojátékok központi szerepet játszanak. A videojáték-ipar kezdetben elsősorban szórakoztatási célt szolgált, azonban az online technológiák megjelenésével a játékhasználat átlépte a földrajzi korlátokat, és globális közösségi, illetve versenyszerű tevékenységgé fejlődött (Katona, 2015; Kuzmenko, 2021).

E folyamat eredményeként bontakozott ki a kibersport (e-sport), amely szervezett keretek között zajló, videojáték-alapú versenysporttevékenység, s mára a világ egyik leggyorsabban növekvő iparágává vált (Szabella, 2018). A globális e-sport bevétele 2019-ben meghaladta a 24,9 milliárd dollárt, a nézőszám pedig 2020 elején elérte a 495 millió főt (Scott et al., 2021). A kibersport nem csupán kulturális és gazdasági tényező, hanem társadalmi és egészségügyi hatásai miatt is jelentős vizsgálati terület.

Különösen látványos a kibersport térnyerése a felsőoktatási hallgatók körében. A fiatal generáció tagjai már digitális bennszülöttek: mindennapjaik szerves részét képezik a videojátékok, az online interakciók és a digitális közösségek. A 2020-as hazai statisztikák szerint a videojátékosok száma meghaladja a 3,8 millió főt, a hallgatók átlagos játékideje hétköznapokon 2–3 óra, hétvégén pedig ennél jóval több (Kányai – Osváth – Kósa, 2021; Bésevec et al., 2023). A kibersport népszerűsége több tényezőnek köszönhető: a digitális kultúra jelenléte, a versenyhelyzet és sikerélmény keresése, a közösségi interakciók, a gazdasági lehetőségek, valamint a stresszoldás és kikapcsolódás igénye egyaránt szerepet játszik (Kuzmenko et al., 2021).

Ezzel párhuzamosan a kibersport elterjedése komoly egészségügyi kihívásokat vet fel. A hosszú ideig tartó képernyőhasználat, a statikus ülő testhelyzet és a fizikai aktivitás csökkenése hozzájárulhat mozgásszervi rendellenességek, látásromlás, anyagcserezavarok és pszichoemocionális problémák kialakulásához (Bogár – Csukonyi, 2021; Kányai – Osváth – Kósa, 2021). A jelenség népegészségügyi jelentősége egyre nyilvánvalóbb, ugyanakkor a magyar és kárpátaljai felsőoktatási hallgatók körében kevés empirikus adat áll rendelkezésre.

A kutatás célja a kibersport és a rendszeres videojátékozás egészségi hatásainak feltárása volt a felsőoktatásban tanuló hallgatók körében, különös tekintettel a mozgásszervi, látásbeli és pszichoemocionális tényezőkre. A vizsgálat célja továbbá a potenciális kockázati tényezők azonosítása és annak feltérképezése, hogy a kibersport milyen életmódbeli különbségekkel jár együtt a rendszeresen és nem rendszeresen videojátékozó populáció között.

A vizsgálat önkitöltős kérdőív alkalmazásával zajlott a II. Rákóczi Ferenc Kárpátaljai Magyar Főiskola elsőéves hallgatói körében. A mintát 86 hallgató alkotta, közülük 21 fő jelezte, hogy rendszeresen videojátékozik szabadidejében, elsősorban szórakozás és kikapcsolódás céljából.

A kérdőív a következő területekre irányult:

- videojáték-használati szokások és játékidő,
- fizikai aktivitás gyakorisága,
- szubjektív egészségérzet és mozgásszervi panaszok,
- pszichoemocionális állapot.

Az elemzések azt mutatták, hogy a rendszeres videojátékozók és a nem videojátékozók között nem volt jelentős különbség a fizikai aktivitás gyakoriságában. Ugyanakkor a rendszeres játékosok körében egyértelmű egészségi tendenciák figyelhetők meg:

- Mozgásszervi problémák: a videojátékozók körében gyakrabban fordult elő nyaki, háti, csukló- és kézfájdalom, valamint vázizomfájdalom.

• Látásromlás és szemfáradtság: a képernyő előtt töltött idő növekedésével fokozódott a szem megerőltetése és a látásélesség panaszai.

• Pszichoemocionális problémák: a kibersport növelte a stressz, a szorongás és az önbizalomcsökkenés előfordulásának kockázatát.

Az egészségkárosító tényezők között a legmeghatározóbbnak bizonyult a monitorral való állandó interakció, a hosszan tartó statikus ülés, az ergonómiailag helytelen testtartás, valamint a kibersport és más tevékenységek közötti egyensúly megbomlása. A videojátékozók körében gyakoribb volt a passzív életmód, és kevesebb időt fordítottak egészségmegőrző rekreációs testmozgásra is, mint a nem kibersportolók.

A vizsgálat eredményei összhangban állnak a nemzetközi kutatásokkal (Bogár – Csukonyi, 2021; Kuzmenko et al., 2021; Bésevec et al., 2023; Papp et.al., 2023), amelyek a kibersport és a hosszú távú videojáték-használat kapcsán hasonló fizikai és pszichés kockázatokat azonosítottak. A mozgásszegény életmód, az ülő testhelyzet és a képernyőidő növekedése fokozott egészségügyi kockázatot hordoz: hozzájárulhat a mozgásszervi betegségek, az elhízás, a 2-es típusú diabétesz és a kardiovaszkuláris betegségek kialakulásához, valamint pszichés problémák (pl. stressz, szorongás, izoláció) megjelenéséhez. Fontos ugyanakkor kiemelni, hogy a videojátékozás bizonyos pszichológiai előnyöket is hordozhat, például stresszcsökkentést, közösségépítést vagy kognitív képességek fejlesztését. A negatív hatások elsősorban a túlzott játékidő, az ergonómiai hiányosságok és az életmódbeli egyensúly hiánya miatt jelentkeznek.

A kibersport és a videojáték-használat a felsőoktatási hallgatók életének meghatározó tényezőjévé vált. A kutatás rávilágít arra, hogy e tevékenységek komplex fizikai és pszichés hatásokkal járnak, amelyek prevenciója és kezelése multidiszciplináris megközelítést igényel. Kiemelt jelentőségű a rekreációs testmozgás integrálása a hallgatók mindennapjaiba, valamint az egészségvédő programok bevezetése, amelyek ellensúlyozzák a digitális aktivitásból eredő egészségkárosító tényezőket.

A jövőbeni kutatásoknak érdemes feltárniuk a kibersport hosszú távú egészségügyi következményeit, azonosítaniuk a legfontosabb rizikófaktorokat, valamint kidolgozniuk célzott, hallgatói populációra szabott intervenciós stratégiákat.

Felhasznált irodalom:

1. Bogár Lilla, Csukonyi Csilla, (2021): A mentális állóképesség vizsgálata e-sportolók és tradicionális sportolók körében. In: Bácsné, Bába Éva; Balogh, László; Szabados, György Norbert; Ráthonyi, Gergely Gábor; Harangi-Rákos, Mónika; Lenténé, Puskás Andrea; Biró, Melinda (szerk.). Az e-sport az élre tör: tematikus különszám. Debreceni Egyetem Sporttudományi Koordinációs Intézet, Debrecen (2021) 81-98. pp. URL: https://sportsci.unideb.hu/sites/default/files/upload_documents/e-sport_kotet_20210321_2.pdf
2. Katona György (2015): Összehasonlító kutatások a szakmai tanárképzés területén. Soproni Egyetem Kiadó, Sopron. URL: http://publicatio.uni-sopron.hu/2395/
3. Kányai Zsófia Tea, Osváth Mátyás, Kósa Karolina (2022): A gamerek és e-sportolók személyes jellemzői, motivációi, valamint életminőségük vizsgálata a játszási szokások tükrében. MENTÁLHIGIÉNÉ ÉS PSZICHOSZOMATIKA, 23 (4). pp. 400-432. ISSN 1419-8126 DOI: https://real.mtak.hu/172146/1/0406-article-p400.pdf
4. Papp, D., Győri, K., Kovács, K. E., & Csukonyi, C. (2023). A videójátékozás mint protektív megküzdési lehetőség és játékhasználati zavar jellemzőinek vizsgálata a távolléti oktatás alatt a felsőoktatási hallgatók körében. Alkalmazott Pszichológia, 25(1). DOI: https://doi.org/10.17627/ALKPSZICH.2023.1.51
5. Szabella Olivér, „Korunk virágzó biznisze? Az e-sport iparág bemutatása". Információs Társadalom XVIII, 1. szám (2018): 66–92. pp. DOI: https://doi.org/10.22503/inftars.XVIII.2018.1.5
6. Andrajeva et.al., 2021 (Кіберспорт: монографія / [Андрєєва О., Анохін Е., Бекар С. та ін. / за заг. ред. Є. В. Імаса, О. В. Борисової, О. А. Шинкарук]. – К.: Олімп. л-ра, 2021. – 616 с. ISBN 978-617-7492-15-2) DOI: https://files.znu.edu.ua/files/Bibliobooks/Inshi72/0053043.pdf
7. Bésevec et.al., 2023 (Бишевець, Н., Герасименко, С., Усиченко, В., Бишевець, Г., Ужвенко, В., & Бондарчук, С. (2023). Вплив занять кіберспортом на здоров'я здобувачів вищої

освіти. Вісник Кам'янець-Подільського національного університету імені Івана Огієнка. Фізичне виховання, спорт і здоров'я людини, №28(4), 210–215.) URL: https://reposit.uni-sport.edu.ua/handle/787878787/5562

8. Kuzmenko et.al., 2021 (Кузьменко О. В., Койбічук В. В., Яценко В. В., Гриценко К. Г. Дослідження світових тенденцій розвитку кіберспорту за допомогою методів Data Mining // Вісник Київського національного університету імені Тараса Шевченка. Серія Фізико-математичні науки. 2021. № 2. С. 117-124. DOI: https://doi.org/10.17721/1812-5409.2021/2.16)

9. Scott, M. J., Summerley, R., Besombes, N., Connolly, C., Gawrysiak, J., Halevi, T., Jenny, S., Miljanovic, M., Stange, M., Taipalus, T., & Williams, J. P. (2021). Towards a framework to support the design of esports curricula in higher education. In 26th ACM Conference on Innovation and Technology in Computer Science Education (ITiCSE 2021) (pp. 2–4). ACM. DOI: https://doi.org/10.1145/3456565.3461440

Dominik KIRÁLY
Bachelor's degree student in Secondary Education, specializing in Informatics
Ferenc Rákóczi II Transcarpathian Hungarian University

Myroslav STOIKA
Associate Professor
Department of Mathematics and Informatics
Ferenc Rákóczi II Transcarpathian Hungarian University

DIGITAL HYGIENE OF SCHOOLCHILDREN: HOW TO TEACH INTERNET SAFETY FROM AN EARLY AGE

Digital hygiene is a set of norms, skills, and habits that ensure safe, healthy, and conscious use of digital technologies. Schoolchildren, especially younger ones, are a vulnerable group due to their insufficiently developed critical thinking, socio-emotional characteristics, and inexperience in the digital environment [1].

Teaching internet safety should begin at an early age and progress gradually, taking into account the child's developmental stage. At first, it is important to teach simple rules — not to share personal information, not to open suspicious links, and not to communicate with strangers — and later move on to more complex topics such as cyberbullying, phishing, fraud, password protection, and privacy [2].

The role of parents and teachers in this process is crucial: they should not only explain the rules but also create a trusting environment where a child can discuss online experiences, report dangerous situations, and receive support [3].

It is essential to develop children's critical thinking — the ability to question the information they see online, assess the reliability of sources, and recognize manipulation and false content. According to UNICEF, about 95% of children and young people in Ukraine actively verify online information; however, a significant number still encounter cyberbullying or online fraud [4].

At school, teaching digital safety should be systematic and interdisciplinary. This can include integrated lessons, training sessions, role-playing games, projects, or case discussions. Studies show that the use of interactive methods — games, discussions, and online courses — significantly increases students' awareness and promotes behavioral change in the digital environment [5].

In Ukraine, there are educational initiatives aimed at developing digital hygiene skills, such as the "Cyber Hygiene for Youth" and "Online Safety for Children" courses on the Diia.Education platform, which provide practical advice on protecting personal data, avoiding cyber risks, and using gadgets safely [6; 7].

In addition to information security, digital hygiene also includes physical aspects — regulating screen time, maintaining ergonomic standards, and preventing eye strain. Research shows that excessive use of digital devices negatively affects the psycho-emotional state of schoolchildren; therefore, education should also promote elements of a healthy lifestyle in the digital environment [8].

Improving the level of digital safety among schoolchildren is possible only through the cooperation of schools, families, and society. Systematic education, monitoring of effectiveness, and updating learning materials in line with emerging risks and technologies will contribute to the formation of responsible, conscious, and safe online behavior among children.

References

1. Adamczyk, B. (2018). The digital generation of children and adolescents in face of internet dangers. Zhytomyr Ivan Franko State University Journal of Pedagogical Sciences. Retrieved from https://pedagogy.visnyk.zu.edu.ua
2. Sukhikh, A. S. (2020). Osoblyvosti formuvannia tsyfrovoi hramotnosti pidlitkiv v aspekti onlain-bezpeky [Features of the formation of digital literacy of adolescents in the aspect of online safety]. Retrieved from https://lib.iitta.gov.ua/id/eprint/720311
3. Vasylenko, R. M. (2022). Uchytelska robota nad bezpekoiu ditei v Interneti [Teacher's work on children's safety on the Internet]. Retrieved from https://lib.iitta.gov.ua/id/eprint/731117

4. UNICEF Ukraine. (2023). Actively check online sources. Retrieved from https://www.unicef.org/ukraine/en/press-releases/actively-check-online-sources
5. Zhurba, K. O., Kanishevska, L. V., Malynoshevskyi, R. V., Kharchenko, N. V., & Fedorenko, S. V. (2022). Raising children and young people in the digital space: A guide. Institute of Problems on Education of the National Academy of Educational Sciences of Ukraine. Retrieved from https://lib.iitta.gov.ua/id/eprint/733779
6. Diia.Education. (n.d.). Cyber hygiene for youth. Retrieved from https://osvita.diia.gov.ua/en/courses/cyber-hygiene-for-youth
7. Diia.Education. (n.d.). Online safety for children (a series for parents). Retrieved from https://osvita.diia.gov.ua/en/courses/serial-dlya-batkiv-onlayn-bezpeka-ditey
8. Characteristics of digital devices and their use by school children in modern conditions. (2023). Journal of Morphology. Retrieved from https://j-morphology.com/0016-9900/article/view/638340/Gigiena%20i%20sanitariya

Mark KOPTYAJEV
Bachelor's degree student in Secondary Education, specializing in Mathematics
Ferenc Rákóczi II Transcarpathian Hungarian University

Myroslav STOIKA
Associate Professor
Department of Mathematics and Informatics
Ferenc Rákóczi II Transcarpathian Hungarian University

THE USE OF DIGITAL HYGIENE IN THEPROFESSIONAL ACTIVITY OF FUTURE MATHEMATICS AND INFORMATICS TEACHERS

In the modern era of digital interaction and constant use of information and communication technologies, digital hygiene emerges as a critically important component of the professional activity of future mathematics and informatics teachers. It involves the systematic observance of safe, ethical, and efficient practices for using digital resources to minimize risks associated with cyber threats, information overload, and breaches of privacy.

One of the key aspects is digital literacy and safety-oriented behavior: knowledge about personal data protection, recognition of phishing and other forms of online fraud, use of strong passwords, and two-factor authentication. Studies show that among university students and staff, there is a significant proportion of individuals with insufficient knowledge and habits related to cyber hygiene, which highlights the need for specialized training [1].

A second important component is the regular updating of knowledge and skills, as technologies and threats are constantly evolving. Future teachers should incorporate self-education, participation in seminars, webinars, and cybersecurity courses into their professional practice. This will enable them not only to protect their own digital environments but also to serve as role models for their students.

The third aspect is the integration of digital hygiene into the educational process and teaching methodology. This means that mathematics and informatics teachers should not only teach their subjects but also embed elements of digital hygiene into their lessons — for instance, explaining how to search for information safely online, how to verify sources, and how to respond to suspicious content. Educational tasks may also include practical exercises in evaluating the security of web resources or adjusting privacy settings on social media platforms.

Research data obtained in different countries and contexts support the idea that the level of digital hygiene significantly correlates with age, educational background, and academic discipline. For example, a study conducted among students and staff of a Nigerian university found that while many respondents had broad access to the Internet, they lacked sufficient knowledge and behavioral skills in cyber hygiene [1]. Another study demonstrated how gender, employment status, and academic discipline influence awareness and practices of cyber hygiene among university communities [2].

In the context of professional training for future mathematics and informatics teachers, the implementation of digital hygiene should be systematic: introducing relevant modules or courses on cybersecurity and digital ethics into educational programs, organizing regular training sessions, practical workshops, and projects involving case studies of security or privacy violations. Collaboration with experts in information security and psychology is also essential for understanding risks and developing healthy digital habits.

Finally, the use of digital hygiene in the professional activity of future mathematics and informatics teachers contributes to improving the quality of education, protecting students and the learning environment, strengthening trust in digital technologies, and fostering responsible digital citizenship. It is not merely a technical competence but an essential part of a teacher's professional culture.

References

1. Ugwu, C., Ani, C., Ezema, M., Asogwa, C., Ome, U., Obayi, A., Ebem, D., & Atanda, A., Ukwandu, E. (2021, March 11). Towards determining the effect of age and educational level on cyber-hygiene. arXiv. https://arxiv.org/abs/2103.06621

2. Ugwu, C., Ezema, M., Ome, U., Ofusori, L., Olebera, C., Ukwandu, E., & others. (2023, May 30). A study on the impact of gender, employment status and academic discipline on cyber hygiene: A case study of University of Nigeria, Nsukka. arXiv. https://arxiv.org/abs/2305.19300

Dávid KOVÁCS
Bachelor's degree student in Secondary Education, specializing in Informatics
Ferenc Rákóczi II Transcarpathian Hungarian University

Myroslav STOIKA
Associate Professor
Department of Mathematics and Informatics
Ferenc Rákóczi II Transcarpathian Hungarian University

CYBERADDICTION: THE ROLE OF EDUCATION IN PREVENTING EXCESSIVE USE OF DIGITAL DEVICES

Cyberaddiction (digital addiction or problematic internet use) is a phenomenon in which the use of digital devices or online activities becomes excessive, uncontrolled, and begins to disrupt important areas of life — such as learning, social relationships, and physical or mental health. The educational system can play a key role in early identification, prevention, and the formation of a healthy attitude toward technology.

In the school context, effective prevention programs can be integrated into the curriculum or implemented as separate modules that address screen dependence, mechanisms of stimulation (e.g., reward systems, self-control, digital detox), as well as exercises for self-assessment and reflection on one's own technology use [1].

Education on cyberaddiction should include the development of self-regulation skills: setting time limits, recognizing signs of overload, taking regular breaks, keeping usage journals, and discussing digital balance in the classroom. Such activities enable students to become aware of their own digital habits, identify the risk of addiction, and adjust their behavior in time [2].

It is particularly important to note that excessive use of digital devices correlates with learning difficulties: studies show that adolescents with a high level of digital dependence often demonstrate lower concentration, reduced academic productivity, and more frequent learning challenges [3]. Therefore, the educational mission of schools should also focus on the link between digital lifestyle and academic success.

Within the framework of educational technologies, persuasive strategies and gamification can be used to promote healthy habits in device usage — for example, apps that remind users to take breaks, automatic blocking systems, or screen-time reports. Such approaches are already being studied as effective tools for reducing the risk of excessive use [4].

Another crucial component is the involvement of parents and teachers in joint discussions about gadget use: establishing shared family rules, modeling responsible adult behavior (digital hygiene within the family), and open dialogue about risks and consequences. This fosters a culture of responsible technology use and supports students' motivation to maintain a healthy balance [5].

Educational measures should be regular and age-appropriate, with adjustments for different developmental stages (for example, distinct approaches for younger pupils and teenagers). Systematic education, monitoring behavioral changes (through surveys or self-assessments), and program adjustments are key steps in reducing the risk of cyberaddiction among students.

In conclusion, the role of education in preventing cyberaddiction is strategic: it should not only inform but also shape healthy digital habits, self-regulation skills, and a culture of conscious and responsible technology use.

References

1. Throuvala, M. A., Griffiths, M. D., Rennoldson, M., & Kuss, D. J. (2019). School-based prevention for adolescent internet addiction: A review of existing evidence. Frontiers in Public Health, 7, 324. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6712298/

2. Theopilus Y, Al Mahmud A, Davis H, Octavia JR. (2024). Preventive interventions for internet addiction in young children. JMIR Mental Health. https://mental.jmir.org/2024/1/e56896

3. Seema, R., & Varik-Maasik, E. (2023). Students' digital addiction and learning difficulties: Shortcomings of surveys in inclusion. Frontiers in Education, 8, 1191817. https://www.frontiersin.org/articles/10.3389/feduc.2023.1191817/full
4. Theopilus, Y., Al Mahmud, A., Davis, H., & Octavia, J. R. (2024). Persuasive strategies in digital interventions to combat internet addiction: A systematic review. International Journal of Human-Computer Studies. https://doi.org/10.1016/j.ijhcs.2024.104950
5. American Psychological Association. (2018, November). Treating the misuse of digital devices. APA Monitor on Psychology. https://www.apa.org/monitor/2018/11/cover-misuse-digital

Attila KOZUB
Bachelor's degree student in Secondary Education, specializing in Informatics
Ferenc Rákóczi II Transcarpathian Hungarian University

Myroslav STOIKA
Associate Professor
Department of Mathematics and Informatics
Ferenc Rákóczi II Transcarpathian Hungarian University

CYBERCULTURE AND DIGITAL HYGIENE AS ESSENTIAL COMPETENCIES OF A MODERN TEACHER OF INFORMATICS

In today's digital society, where information and communication technologies (ICT) have penetrated all areas of life, cyberculture and digital hygiene have become essential competencies for informatics teachers. A modern teacher must not only possess technical skills in programming or working with digital tools, but also be capable of creating an environment where the use of technology is safe, ethical, and conscious, minimizing the risks of cyber threats, data loss, or information overload.

One of the key components is digital hygiene as a practical skill: protecting personal and student data, using strong passwords, being aware of online fraud, and regularly updating software. Without such knowledge, a teacher risks creating vulnerable situations within the educational process.

At the same time, cyberculture also encompasses ethical, social, and psychological aspects: respecting copyright, following communication ethics in social networks and forums, critically evaluating information sources, and developing what can be called digital ethics. In other words, fostering cyberculture means that a teacher does not simply master a tool, but understands how to use it responsibly and how its use affects students and the educational environment as a whole.

Research in Ukraine confirms that digital literacy—which is a component of both cyberculture and digital hygiene—is actively recognized as part of the professionally important competencies of future teachers. For example, in the article by Henseruk H. [1], it is emphasized that developing digital competencies through courses in cybersecurity, media education, and ICT use is essential.

Another source, by Stoika O. [2], indicates that postgraduate teachers often have general digital skills, but their digital hygiene and cyberethics are less developed, which reduces their ability to respond effectively to challenges related to data security and online environments.

In teaching informatics, it is advisable to implement methodological modules that combine digital hygiene and cyberethical practices: educational tasks, case analyses of privacy or ethical violations online, and projects in which students and teachers work together to protect information or create safe digital environments. This approach contributes not only to technical preparation but also to cultivating responsible digital users and citizens.

A systematic approach is also important: this competency should be integrated into teacher training programs, including both theoretical knowledge and practical exercises, self-education, the use of digital environments, and the assessment (monitoring) of teachers' digital hygiene and cyberculture levels.

Ultimately, cyberculture and digital hygiene as core competencies of modern informatics teachers contribute to improving the quality of the educational process, reducing security risks, enhancing interaction in digital environments, and fostering students' and parents' trust in the use of information technologies in learning.

References

1. Henseruk, H. (2019). Digital competence as one of the professionally important competencies of future teachers. 2019, Open Educational e-environment of Modern University, № 6.
2. Stoika, O. (2023). Formation of digital literacy for teachers in the system of postgraduate education in ukraine. Continuing Professional Education: Theory and Practice, 2(75), 61–76.

Karolina SÁRKÖZI
Bachelor's degree student in Secondary Education, specializing in Informatics
Ferenc Rákóczi II Transcarpathian Hungarian University

Myroslav STOIKA
Associate Professor
Department of Mathematics and Informatics
Ferenc Rákóczi II Transcarpathian Hungarian University

SOCIAL NETWORKS IN THE LIFE OF A SCHOOLCHILD: EDUCATIONAL OPPORTUNITIES AND RISKS

Social networks today play an increasingly significant role in the lives of schoolchildren, shaping not only their modes of communication but also providing an environment for learning, personal development, and self-identity. The use of social networks can facilitate access to a variety of educational resources—video lessons, online courses, open lectures, interest-based communities—where students exchange knowledge and experience, ask questions, and participate in project work [1].

Moreover, social networks can enhance academic motivation and a sense of belonging to school: when a student uses social platforms for educational purposes and interacts with classmates or teachers, this can improve the emotional climate and help develop collaboration and communication skills [2]. During periods of distance learning or limited offline contact, social networks often become an important link in maintaining the educational process and providing social support [3].

However, there are significant risks. The first is the potential for social media addiction, which may manifest as reduced concentration, increased distractions, and decreased academic productivity. Research shows that excessive social media use is associated with mental health problems, such as anxiety, depression, and sleep disturbances [4].

The second risk is privacy violation, the danger of phishing, and manipulation through false information or content promoting unrealistic standards of appearance and social status. These factors can undermine students' self-esteem, lead to social comparison, and cause psychological discomfort.

The third aspect is that social networks can become an environment for cyberbullying, online harassment, or isolation, where virtual interactions do not support real social skills or emotional support and, on the contrary, may create feelings of loneliness or exclusion [5].

It is essential that educational institutions, parents, and students themselves work on developing media literacy, emotional intelligence, and healthy social media habits. This includes recognizing fake content, managing screen time, setting privacy boundaries, and critically evaluating information [6].

In conclusion, social networks can be a powerful tool in a student's life if their educational potential is used consciously and if the associated risks are actively minimized through education, support, and responsible engagement in the digital environment.

References

1. Osborne, A. (2025). Balancing the benefits and risks of social media on adolescent mental health in a post-pandemic world. Child and Adolescent Psychiatry and Mental Health, 19, 92. https://doi.org/10.1186/s13034-025-00951-z

2. Sampasa-Kanyinga, H., Chaput, J.-P., & Hamilton, H. A. (2019). Social media use, school connectedness, and academic performance among adolescents. Journal of Primary Prevention, 40(2), 189–211. DOI: 10.1007/s10935-019-00543-6

3. Mulisa, F., Getahun, D.A. Perceived Benefits and Risks of Social Media: Ethiopian Secondary School Students' Perspectives. J. technol. behav. sci. 3, 294–300 (2018). https://doi.org/10.1007/s41347-018-0062-6

4. Meghari, A. (2019). Effects of using social networks on adolescents: Applied study on a sample of high school students. An-Najah University Journal for Research - B (Humanities), 33(12), 2011-2052. https://doi.org/10.35552/0247-033-012-005

5. Piccerillo, L., & Digennaro, S. (2024). Adolescent social media use and emotional intelligence: A systematic review. Adolescent Research Review, 10(2), 201–218. https://doi.org/10.1007/s40894-024-00245-z

6. Zimmermann, E., & Tomczyk, S. (2025). Using social media to promote life skills among adolescents: A debate on opportunities, challenges, and implications for health and education. Journal of Prevention, 46(2), 201–211. https://doi.org/10.1007/s10935-025-00826-1

Hajnalka FŐZŐ
Second year Bachelor student
"Mathematics" major
Ferenc Rakoczi II Transcarpathian Hungarian University

Katalin KUCHINKA
PhD, Associate professor
Department of Mathematics and Informatics
Ferenc Rakoczi II Transcarpathian Hungarian University

NUMBER THEORY GAMES IN THE SERVICE OF DEVELOPING LOGICAL AND ALGORITHMIC THINKING

This research investigates the pedagogical efficacy of number theory games (focusing on divisibility, primality, and modular arithmetic) in enhancing computational skills. The aim is to demonstrate that by embedding core mathematical concepts within a gamified framework, we can actively foster students' logical inference, combinatorial skills, and conscious algorithmic thinking. This digital approach supports abstraction and the systematic development of error correction strategies.

Number theory games can serve as effective tools in mathematics and computer science education, as they simultaneously enhance logical, combinatorial, and algorithmic thinking. This research aims to explore how divisibility, prime number, and modular arithmetic games can be used to develop students' digital literacy and systems thinking. The playful learning environment supports independent problem-solving, the development of abstraction skills, and the awareness of error correction strategies.

The methodological framework is based on the principles of discovery learning and gamification, which several studies have found effective in developing algorithmic thinking. Ihsan and Karjanto [1] emphasize that the playful teaching of combinatorial thinking promotes the understanding of algorithmization and logical consistency. According to Kovtaniuk et al. [2], digital simulations and educational games are particularly effective in enhancing algorithmic thinking, as they create interactive, feedback-based learning environments. Gundersen and Lampropoulos [3] highlight that the use of serious and digital games increases students' motivation and promotes the integration of computational thinking into education.

The research is expected to demonstrate that number theory games can strengthen deductive and inductive reasoning, develop logical inference abilities, and foster a conscious algorithmic mindset. The study contributes to understanding how elements of gamification and digital learning environments can be integrated into the development of mathematical thinking and digital competencies.

Conclusion. This study substantiates that integrating number theory games significantly strengthens deductive/inductive reasoning and the conscious application of algorithmic processes. Utilizing concepts like modular arithmetic within a gamified, discovery-based model effectively bridges theoretical mathematics with practical computational thinking and digital literacy. The findings recommend these digital playful strategies as a structured method to cultivate a deeper, systematic approach to problem-solving in educational settings.

References

1. Ihsan, I. R., & Karjanto, N. (2019). Optimizing students' combinatorial-thinking skill through design-based research. arXiv preprint, https://arxiv.org/abs/1911.07655
2. Kovtaniuk, M. S., Shokaliuk, S. V., & Stepanyuk, A. N. (2025). Game simulators as educational tools for developing algorithmic thinking skills in computer science education. CTE Workshop Proceedings, Vol. 12, 19–62,
3. Gundersen, S. W., & Lampropoulos, G. (2025). Using Serious Games and Digital Games to Improve Students' Computational Thinking and Programming Skills in K–12 Education: A Systematic Literature Review. Technologies, 13(3), 113. https://www.mdpi.com/2227-7080/13/3/113

Alexandra HAPAK
Second year Bachelor student
"Mathematics" major
Ferenc Rakoczi II Transcarpathian Hungarian University

Katalin KUCHINKA
PhD, Associate professor
Department of Mathematics and Informatics
Ferenc Rakoczi II Transcarpathian Hungarian University

TEACHING COMBINATORIAL PARADOXES AT THE INTERSECTION OF DIGITAL CULTURE AND ALGORITHMIC THINKING

This research addresses the growing need to integrate sophisticated computational thinking into teacher training. We perform a critical pedagogical and computational analysis of the LearningApps platform. The study determines which specific learning theories (e.g., behaviorist vs. constructivist) its underlying algorithmic templates support, and proposes methodologically sound strategies for future educators to leverage this structure for differentiated, complex learning outcomes.

Combinatorial paradoxes and probability curiosities can be effectively applied to the development of algorithmic thinking and digital culture, as they help learners recognize logical inconsistencies, intuitive fallacies, and the importance of systematic reasoning. The aim of this research is to explore how such paradoxes can be used to enhance critical and algorithmic thinking in mathematics and computer science education. Classic paradoxes, such as the Monty Hall problem and the Chevalier de Méré paradox, serve as excellent tools for developing probabilistic reasoning, logical deduction, and awareness of cognitive biases [1][2].

Wijayatunga [2] demonstrated that using such paradoxes improves students' critical thinking skills, especially when applied in interactive and digital learning environments. Similarly, Rezvanifard, Radmehr, and Drake [3] found that incorporating paradoxes and sophisms into higher education enhances students' reflective thinking and strengthens their ability to decompose and analyze problems algorithmically. Tillema [4], through an empirical study of secondary school students, showed that visual and 3D combinatorial structures significantly foster abstraction and logical organization.

The central argument of this thesis is that teaching combinatorial paradoxes contributes not only to mathematical understanding but also to the development of digital thinking, cognitive safety, and information literacy. The didactic use of paradoxes supports the formation of an algorithmic mindset and promotes the pedagogical advancement of digital culture and digital hygiene.

Conclusion: LearningApps templates, fundamentally rooted in simple algorithmic structures (e.g., graph-matching for pairing, finite state machines for sequencing), primarily enforce behaviorist reinforcement. This study concludes that while excellent for knowledge recall, its limited structural flexibility constrains project-based, constructivist activities. Future pedagogical utility depends on the educator's ability to use these static tools to support differentiated learning paths and to critically assess their role against the emerging capabilities of dynamic, generative AI-driven content creation.

References

1. López-Barrientos, J. D.; Silva, E.; Lemus-Rodríguez, E. (2023). Lessons from the famous 17th-century paradox of the Chevalier de Méré. Teaching Statistics, 45(1):36-44.
2. Wijayatunga, P. (2024). Probability Paradoxes for Increasing Critical Thinking Skills.
3. Rezvanifard, F.; Radmehr, F.; Drake, M. (2023). Perceptions of Lecturers and Engineering Students of Sophism and Paradox: The Case of Differential Equations. Education Sciences, 13(4):354.
4. Tillema, E. S. (2024). Combinatorial and quantitative reasoning: Stage 3 high school students' reasoning about combinatorics problems and 3-D arrays. Journal of Mathematical Behavior.

István MEGGYESI
Second year Bachelor student
"Informatics" major
Ferenc Rakoczi II Transcarpathian Hungarian University

Katalin KUCHINKA
PhD, Associate professor
Department of Mathematics and Informatics
Ferenc Rakoczi II Transcarpathian Hungarian University

DIGITAL AWARENESS FROM THE GROUND UP – SAFE DEVELOPMENT OF ALGORITHMIC THINKING THROUGH UNPLUGGED ACTIVITIES

In the 21st century, the rapid expansion of digital technologies has made the development of digital awareness and algorithmic thinking a fundamental objective of modern education. Algorithmic thinking is widely recognized as a core cognitive competence that supports logical reasoning, abstraction, decomposition, and problem-solving skills, which together form the basis of digital literacy and computational understanding across disciplines [1]. Preparing students to navigate the digital world responsibly therefore requires not only technical knowledge but also reflective, structured ways of thinking.

Recent educational research emphasizes the effectiveness of unplugged pedagogical methods—learning activities that introduce computational concepts without the use of digital devices—particularly in early and primary education [2]. Through logical and physical games such as sequencing tasks, role-based algorithms, movement-based coding, and problem-solving puzzles, learners can internalize fundamental algorithmic principles in an age-appropriate and engaging manner. These activities transform abstract computational ideas into tangible experiences, enabling students to construct mental models of algorithms before encountering formal programming languages.

Empirical studies have demonstrated that unplugged approaches lead to measurable improvements in key components of computational thinking, including decomposition, abstraction, pattern recognition, and debugging abilities among primary school learners [3]. By eliminating the cognitive load associated with digital interfaces and syntax, unplugged learning allows students to focus on reasoning processes rather than technological operation. This gradual introduction contributes to both cognitive and psychological safety, helping learners build confidence while avoiding early overexposure to screen-based environments. Beyond cognitive development, unplugged activities foster collaboration, communication, and reflective discussion—competencies closely linked to responsible digital citizenship and digital hygiene [4]. Working collaboratively to design, test, and refine algorithms encourages learners to articulate their thinking, negotiate solutions, and perceive errors as natural elements of the learning process. Such experiences reinforce the understanding that digital security and ethical technology use begin with conscious decision-making and structured problem-solving rather than mere technical proficiency.

Although unplugged pedagogy does not replace digital learning, it effectively complements it by providing a solid conceptual foundation for later engagement with coding and digital tools. Acting as a bridge between analog and digital learning environments, unplugged methods support the development of reflective, responsible digital citizens who are equipped to engage with technology safely, critically, and thoughtfully from an early age.

References

1. Wing, J. M. (2006). Computational thinking. Communications of the ACM, 49(3), 33–35.
2. Bell, T., Alexander, J., Freeman, I., & Grimley, M. (2009). Computer Science Unplugged: School students doing real computing without computers.
3. Futschek, G., & Moschitz, J. (2011). Developing Algorithmic Thinking by Inventing and Playing Algorithms.
4. Csizmadia, A., Curzon, P., Dorling, M., Humphreys, S., Ng, T., Selby, C., & Woollard, J. (2015). Computational Thinking – A Guide for Teachers. Computing at School.

SZENYKÓ Anasztázia
Mesterszakos hallgató,
Matematika szak,
Matematika és Informatika Tanszék,
II. Rákóczi Ferenc Kárpátaljai Magyar Egyetem

KUCSINKA Katalin
docens, PhD,
Matematika és Informatika Tanszék,
II. Rákóczi Ferenc Kárpátaljai Magyar Egyetem

A GEOMETRIAI GONDOLKODÁS ÉS A DIGITÁLIS ÍRÁSTUDÁS KAPCSOLATA

A modern oktatási stratégia elengedhetetlen részévé vált a digitális eszközök használata úgy tanárok, mint diákok körében. A 21. század oktatásának egyik legnagyobb kihívása, hogy a tanulók képesek legyenek eligazodni a digitális világ összetett problémáiban. Ezeknek a képességeknek az alapját a logikus és algoritmikus gondolkodás alkotja, melynek a fejlesztésében a geometriai gondolkodás játssza a fő szerepet.

A geometriai gondolkodás magába foglalja a geometriai fogalmak megértését, azok alkalmazását a problémák és feladatok megoldására. A geometriai gondolkodás fejlesztése fontos, mert segít a tanulóknak megérteni a térbeli világot és megoldani ezek során felmerülő problémákat.[4.] Ez egyfajta kognitív edzőterem, melynek köszönhetően tanulunk meg rendszerezni és lépésről lépésre gondolkodni – pont úgy, ahogy a digitális világban való problémamegoldás is megkívánja.

A geometria fontos része a tudásszerzés során, hiszen fejleszti a síkbeli és térbeli látást, logikai következtetési képességet és az absztrakciós készséget. Amikor egy geometriai feladat során be kell bizonyítani például két háromszög egybevágóságát, nem csupán képleteket alkalmazunk, hanem stratégiai döntéseket hozunk, összefüggéseket keresünk és információt rendszerezünk. Ezek a kognitív műveletek az informatikai és digitális problémamegoldás alapjaiként szerepelnek. [2.]

Dina van Hiele-Geldof és Pierre van Hiele házaspár 1950-ben kidolgoztak egy olyan rendszert, amely segít felmérni a geometriai tudást a tanulóknál. Ez a rendszer 5 szintre van osztva, melyek egymásra épülnek. Igaz, mikor vizsgálták, rájöttek, hogy nem mindenki rendelkezik fejlett geometriai tudással, így egy nulladik szint is létrejött az öt mellé. Ha az előző szintet nem sikerül teljesíteni, akkor nem tudnak tovább lépni a következőre, és a teljesített szint lesz a geometriai tudásuk szintje. [4].

0. szint: A tanuló megfigyeli a geometriai alakzatokat, de még nem ismeri fel a kapcsolato- kat közöttük.

1. szint: A tanuló képes az alakzatokat felismerni, megnevezni őket.

2. szint: A tanuló már képes értelmezni és leírni az alakzatok tulajdonságait és kapcsolatokat találni közöttük.

3. szint: A tanuló az alakzatokat a definíciókkal képes felismerni, a tulajdonságokat megne- vezni felismerni, egyszerű axiómákat bizonyítani.

4. szint: A tanuló ismeri a különbséget az axiómák, állítások, definíciók között, de nem feltétlen tudja visszavezetni bizonyítását axiómákra. Az elfogadott állításokat nem tartja fontosnak bizonyítani, így nem is teszi.

5. szint: A tanuló képes az absztrakt gondolkodásra, vagyis az axiómákat tudja használni és kombinálni őket a megoldás elérése érdekében, tudja őket bizonyítani, alátámasz- tani állításait. (ez a legmagasabb szint). [3.] [4.]

Van Hiele rendszretét alapul véve lett összeállítva a mai napig használt Usiskin-féle feladatsor, mely 25 feladatból áll, 35 perc teljesítéssel. Usiskin a kutatócsoportjával 1982-re véglegesítette a feladatsort, mely az alábbi 5 szintre bomlik:

1. Kiindulási szint: az alakzatokat, mint egészet látják, felismerik, de nem veszik észre a tulajdonságokat és azok összefüggéseit.

2. Elemző szint: megkezdődik az alakzatok tulajdonságainak vizsgálata, de a köztük levő kapcsolatokat még nem ismeri fel. Az alakzatokat ezért még nem definiálják.

3. Rendezési szint: megkezdődik az alakzatok logikai rendszerezése tulajdonságaik alapján, a tulajdonságok összefüggéseinek felfedezése, a bizonyítások kezdetei.

4. Lokális dedukciószintje: az egyes részek deduktív felépítése, alapfogalmak, axiómák, definíciók, tételek, bizonyítások.

5. Axiomatikus felépítés: az axiómákat egymás után alkalmazni megfelelően a megoldás elérése érdekében. [1.]

Ahhoz, hogy szintet lehessen lépni, az adott szinten legalább 3 feladatot helyesen kell megoldani. Ha ez nem sikerül, akkor az előző szinthez sorolják, vagy egyikhez sem.

A geometriában tanult bizonyítás módszerek és azok felépítése nagyban segít a programozás logikájának a megértésében. Mindkettő arra alapul, hogy meg kell határozni az ismert adatokat, megfogalmazni a célt és lépésről lépésre elérni a helyes eredményt. Minden lépés függ az előzőtől, és egyetlen logikai hiba is megbontja az egész rendszert – akárcsak egy hibás kód a programban.

A digitális tudás egyik kulcseleme az információ rendszerezése: az adatok, források és tartalmak rendszerezett feldolgozása. A geometriai gondolkodás ezt a képességet is fejleszti, hiszen a diák megtanulja áttekinteni a problémát, megszűrni a releváns információt, majd összekapcsolni az elemeket egy koherens megoldásban.

Aki megtanulja a geometriai rendszerezést, az a digitális térben is magabiztosabban tájékozódik: könnyebben felismeri az adatkapcsolatokat, logikai struktúrákat és hibalehetőségeket.

Felhasznált irodalom

1. Dobák Dávid, Csuta Ákos, Megyeri Krisztina, Szilágyi Brigitta, A geometriai gondol- kodás szintjeinek feltérképezése a van Hiele-elmélet segítségével, Tudományos Diákköri Konferencia Dolgozat, Budapest, Magyarország, 2021, 406-412 old.
2. Herendiné Kónya Eszter, A geometriai képességek fejlesztésének lehetőségei, Debrecen, Magyarország: KFRTKF, 2007, 6 old.
3. Herendiné Kónya Eszter, A tanítójelöltek geometriai gondolkodásának jellegzetességei, Iskolakultúra, pp. 51-61. |online dokumentum| letöltés időpontja: 2025.10.23.
URL: https://www.iskolakultura.hu/index.php/iskolakultura/article/view/19954/19744
4. Szenykó Anasztázia, A 9. osztályos tanulók geometriai gondolkodásának szintjei és fejlesztésének lehetőségei. Matematika és Informatika Tanszék, Beregszász, 2024. 57 old.

Yuliia KOVALCHUK
Master's degree student (1st year), majoring in Software engineering (Specialty F2)
State University "Kyiv Aviation Institute"
7526280@stud.kai.edu.ua

Nataliia BILOUS
PhD (Pedagogy), Associate Professor of the Professional Foreign Languages Department,
State University "Kyiv Aviation Institute"
natalia.bilous@npp.kai.edu.ua

DIGITAL HYGIENE IN EDUCATION: A MODEL FOR PROTECTING STUDENTS' PERSONAL DATA IN THE CLOUD ENVIRONMENT

Keywords: cloud services, digital hygiene, personal data, online education.

At the moment, in the world and in Ukraine, in particular, there is an intensive digitalization of the educational process. This is accompanied by the dynamic implementation and use of cloud services (Google Workspace for Education, Microsoft 365 Education, Moodle Cloud) for the processing, storage and exchange of educational information.

However, the use of such services creates significant problems for the security of students' personal data. This is due to the fact that cloud providers do not regularly provide an adequate level of access control, information privacy, and backup.

The lack of clear digital hygiene among education users (students and teachers) reinforces the problem of data leakage and increases the level of cyber threats.

The purpose of this work is to determine the structural components of digital hygiene during the use of cloud educational platforms and to develop a model for the protection of students' personal data, which will take into account the features of public cloud environments.

The relevance of the study is explained by several global factors. In today's realities, there is a rapid increase in the use of cloud technologies in educational institutions all over the world, and, accordingly, an increase in demand for online education.

Also, educational institutions are faced with the need to comply with international standards for the protection of personal data, in particular the requirements of the GDPR. Risk analysis shows that some of the most common causes of security breaches are errors in access settings (67%), phishing attacks (41%), and the use of weak passwords (34%).

The scientific novelty of this work lies in the created correlation between the level of digital literacy of users and the overall effectiveness of technical means of information protection. This makes it possible to optimize the distribution of resources between technical security infrastructure and educational programs to enhance digital culture.

Taking into account this goal, an integrated multifactorial model consisting of four interrelated components was proposed.

The first component – the technical level of protection – includes the implementation of Multi-Factor Authentication (MFA) for all users of educational platforms, the use of AES-256 encryption algorithms to protect data at rest and the TLS protocol for secure information transfer, as well as the implementation of role-based access control in compliance with the principle of minimum privileges.

The second component – the cloud service provider level – provides for checking the compliance of educational platform providers with international security standards ISO 27001 and SOC 2, as well as assessing the transparency of their policies for processing and storing users' personal data.

The third component – the organizational level – covers the development and implementation of information security policies for higher education institutions, designated data protection officers in accordance with the requirements of the GDPR, as well as the creation of a procedure for responding to security incidents.

The fourth component – the educational level – includes the development of specialized digital hygiene curricula for students, regular testing of their skills of safe online behavior and assessment of the level of digital literacy.

Conclusion

After defining the structural components of digital hygiene, a protection model was created that takes into account modern risks and types of threats, including access configuration errors, phishing attacks, as well as the use of weak passwords. The formation of such a model for increasing the level of security of educational data creates the basis for the effective adaptation of educational systems to modern information security challenges.

References

1. Datami Security Report. How phishing will change in 2025: trend analysis and recommendations [Electronic resource]. Available at: https://datami.ee/ua/blog/how-phishing-is-changing-in-2025-analysis-by-datami (accessed: 20.10.2025).

2. Google Workspace for Education: Privacy and Security Center. (2025). Available at: https://support.google.com/edu/classroom/answer/10467843 (accessed: 20.10.2025).

Viviien TOVT
Graduate student (Master's program)
in Secondary Education, specializing in Mathematics
Ferenc Rakoczi II Transcarpathian Hungarian University

Myroslav STOIKA
Associate Professor
Department of Mathematics and Informatics
Ferenc Rakoczi II Transcarpathian Hungarian University

FORMATION OF DIGITAL HYGIENE AND CYBERCULTURE AMONG FUTURE TEACHERS OF MATHEMATICS AND INFORMATICS

The process of digitalization in Ukrainian education requires a profound reorientation of teacher training. Future teachers of mathematics and informatics must not only possess digital skills but also understand the ethical, safety, and cultural aspects of technology use. An essential component of modern teachers' digital competence is the formation of digital hygiene and cyberculture, which determine their ability to interact safely, responsibly, and consciously in the digital environment [1].

Digital hygiene encompasses knowledge and skills related to personal data protection, information security, prevention of cyberbullying, and rational use of digital devices. According to Ş. Bayzan (2025), teachers' level of cyber hygiene directly affects their awareness of digital security and reduces the risks of data breaches and manipulations [2]. For future teachers, this is especially important, as they act as intermediaries between technology and students.

Cyberculture, in turn, is understood as a set of norms, values, and behavioral models in the virtual environment. It includes aspects of digital ethics, academic integrity, media literacy, and critical thinking. Developing cyberculture involves students' ability to communicate consciously in online spaces, respect intellectual property, and avoid aggression or destructive interactions [3].

Research by Termenzhy (2025) emphasizes that cyberethics, cybersafety, and cybersecurity skills are core elements of AI-related competence for future educators. These skills should be integrated into the training of teachers in natural and mathematical sciences [4].

Domestic and international experience demonstrates that the formation of digital hygiene and cyberculture is effective only under a systemic approach, combining educational courses, practical trainings, independent activities, and research work [5]. As noted by Borysova (2023), the digital culture of future education should be based on conscious technology use, critical information evaluation, and social responsibility [5].

In the Ukrainian context, this issue has gained even greater importance due to the ongoing war, where digital technologies are the primary means of communication, distance learning, and maintaining educational processes. According to Vorotnykova, Morze, and Hrynevych (2023), digital transformation in wartime education requires teachers not only to be technically proficient but also psychologically prepared for safe digital interaction [3].

For students specializing in Secondary Education (Mathematics) and Secondary Education (Informatics), it is important to create conditions where digital hygiene and cyberculture are naturally formed—through participation in projects, research activities, inter-university online courses, and digital communities. At the same time, as Verbovskyi (2023) notes, individual learning trajectories should be considered, balancing technological and humanitarian components of teacher training [6].

Thus, the formation of digital hygiene and cyberculture among future teachers of mathematics and informatics is an integral condition for their professional competence. It involves developing ethical responsibility, critical thinking, information security, and digital self-regulation skills. These qualities will ensure the resilience and human-centered orientation of the educational process in the era of artificial intelligence.

References

1. Zhernovnykova, O. A., Nalyvaiko, O. O., & Nalyvaiko, N. A. (2020). Formation of information and digital competence of future teachers in the context of the development of the New Ukrainian School. CEUR Workshop Proceedings.
2. Bayzan, Ş. (2025). Are teachers cyber hygienic? An investigation into the relationship between teachers' cyber hygiene status and digital data security awareness. Bartın University Journal of Faculty of Education, 14(3), 751–772.
3. Vorotnykova, I. P., Morze, N. V., & Hrynevych, L. M. (2023). Digital transformation of secondary education of Ukraine and the quality of teaching natural and mathematical sciences in the conditions of war. CEUR Workshop Proceedings, 3553, 130–142.
4. Termenzhy, O. (2025). Cyberethics, cybersafety, and cybersecurity skills as a core component of AI competency for educators. CEUR Workshop Proceedings, 4042, 100–110.
5. Borysova, S. (2023). Digital competencies in Ukrainian education of the future. Futurity Education Journal, 1(1), 50–60.
6. Verbovskyi, I. (2023). Modern trends in the training of future computer science teachers. Pedagogical Journal of Zaporozhye State University, 1(1), 15–22.

Emőke BERGHAUER-OLASZ
PhD, Associate professor
Ferenc Rakoczi II Transcarpathian Hungarian University

Ildiko GREBA
PhD
Ferenc Rakoczi II Transcarpathian Hungarian University,
greba.ildiko@kmf.org.ua

BULLYING AS A BARRIER TO PARTICIPATION IN INCLUSIVE EDUCATION: INTEGRATING PREVENTION INTO UKRAINE'S SCHOOL PRACTICES

This article conceptualises bullying as a systemic barrier to participation within Ukraine's inclusive education. Drawing on 2024 – 2025 empirical studies and current guidance from the Ministry of Education and Science, we argue that formal placement without deliberate design of classroom interaction leaves learners with special educational needs (SEN) vulnerable to peer victimisation and subtler forms of social exclusion. We propose a participation-oriented prevention model that (1) embeds anti-bullying measures in each learner's Individual Support Plan (ISP); (2) extends Universal Design for Learning (UDL) beyond access to the design of interaction (predictable turn-taking, rotating non-hierarchical roles, mixed-ability cooperation); (3) couples high academic expectations with warm, consistent teacher - student relationships; and (4) integrates peer support and social-emotional learning (SEL) within the base class. Evidence from inclusive classrooms indicates that such routines narrow status asymmetries, reduce opportunities for relational bullying, and strengthen belonging. At the whole-school level, routine monitoring, staff development, and coordinated engagement with families are required, particularly under hybrid and resource-uneven conditions typical of Ukrainian schools. Effective bullying prevention is therefore a necessary condition for meaningful participation of SEN learners in ordinary classes rather than an optional add-on.

Keywords: inclusive education; special educational needs (SEN); bullying prevention; participation; school climate; peer support; Universal Design for Learning (UDL); social-emotional learning (SEL)

Inclusive education in Ukraine aims to ensure that learners with special educational needs (SEN/ООП) learn alongside their peers and take part in everyday classroom life with support tailored to their profiles, rather than in segregated settings. Recent studies indicate, however, that bullying and subtler forms of social exclusion often undermine this participation even where formal inclusion is in place. In this sense, bullying functions as a structural obstacle within inclusion: unless schools address it deliberately at class and whole-school levels, placement alone will not translate into meaningful involvement (Carmona, García-Fernández, & Martín, 2025; Horton, 2025; Ručman, 2025). Comparative classroom research reports higher rates of peer victimisation, rejection and isolation among SEN learners, with corresponding declines in perceived inclusion and wellbeing. Accounts from practice frequently note relational patterns such as exclusion from group work, ridicule of learning supports and interference with assistive devices, which erode participation yet remain less visible to adults (Carmona et al., 2025; Ručman, 2025).

Three mechanisms recur across recent evidence and are directly relevant for schools in Zakarpattia and elsewhere in Ukraine. First, many inclusion efforts secure access to content and physical space but leave participation roles implicit. Where a learner with ADHD, autistic characteristics or specific learning difficulties is present yet socially peripheral, status asymmetries create opportunities for relational and verbal bullying, especially during cooperative tasks and unstructured intervals (Horton, 2025). Second, teacher modelling shapes peer responses to difference. Warm, consistent interactions coupled with clear expectations for SEN learners are associated with better social positioning and lower exposure to bullying, whereas over-protection or visibly lowered expectations are often "read" by peers as permission to distance or ridicule (Horton, 2025; Ručman, 2025). Third, support is frequently organised as individual pull-out assistance that improves task access without building peer-mediated participation in the base classroom. When the social field is under-designed in this way, exclusion dynamics fill the gap (Carmona et al., 2025).

Official guidance from the Ministry of Education and Science of Ukraine specifies that schools must ensure a safe educational environment for learners with special educational needs (ООП). In practice, this means treating bullying as a barrier in the learner's Individual Support Plan (ISP) and in routine classroom design (Міністерство освіти і науки України, 2025). At ISP level, schools can specify protected reporting routes, explicit safeguarding of assistive technology, agreed adult follow-up and concise scripts for communication with parents. At classroom level, Universal Design for Learning principles should extend beyond access to the design of interaction: predictable turn-taking, rotating cooperative roles that are not ability-ranked, and visible, low-threshold opportunities for SEN learners to contribute to shared outcomes. Evidence from inclusive classrooms suggests that when participation roles are planned in this way, peer status gaps narrow and opportunities for relational bullying decline (Carmona et al., 2025). Teacher routines that signal high expectations and unconditional regard – brief individual check-ins, clear re-entry after pull-out support, public recognition of effort –ma reduce social distance and model acceptance that peers tend to emulate (Horton, 2025). Complementing these routines with peer support embedded in the base class – structured buddying, mixed-ability collaboration with shared products, and explicit recognition of inclusive acts – offers socially valued alternatives to exclusion. Where peer support exists only on paper or is confined to tutoring, it rarely shifts bullying dynamics (Ručman, 2025).

Targeted social-emotional learning (SEL) can serve as an inclusion tool when it strengthens social-emotional competence together with peer relationships. Evidence shows that reductions in bullying are mediated through this dual pathway, which is precisely what inclusive classrooms require to stabilise participation (Doumas & Midgett, 2024). Ukrainian contributions point in the same direction. School-based analyses and syntheses since 2022 document persistent patterns of peer victimisation and relational exclusion, and recommend embedding prevention into ordinary class routines and teacher–student relations rather than relying on stand-alone programmes (Kostikova & Guzenko, 2024; Melnychenko, 2024; Shakhrai, 2024; Nypadymka, 2025). International guidance is compatible with this stance: UNESCO's whole-school approach treats safety as a precondition for participation and calls for routine monitoring, staff development and engagement with families, which can be adapted to the hybrid conditions and uneven specialist availability that characterise many Ukrainian schools (UNESCO, 2025).

In sum, current evidence supports a practical synthesis for Ukrainian settings. Bullying should be defined explicitly as a participation barrier within inclusion planning; participation roles need to be designed to reduce status asymmetries; teachers should couple warm relations with clear expectations; peer support must be visible in the base class; and SEL should be used to consolidate the competencies and relationships that sustain inclusion. These measures do not replace formal policies. They provide the social base without which formal inclusion remains vulnerable to everyday exclusion.

References

1. Carmona, Á., García-Fernández, J. M., & Martín, M. (2025). Bullying and social exclusion of students with special educational needs in inclusive classrooms. Social Sciences, 14(7), 430. https://doi.org/10.3390/socsci14070430
2. Doumas, D. M., & Midgett, A. (2024). Sense of school belonging as a mediator of the relationship between witnessing bullying and internalizing symptoms. International Journal of Environmental Research and Public Health, 21(7), 873. https://doi.org/10.3390/ijerph21070873
3. Horton, P. (2025). Inclusive education and the bullying involvement of learners with special educational needs. International Journal of Inclusive Education. Advance online publication. https://doi.org/10.1080/13603116.2025.2487471
4. Kostikova, I., & Guzenko, N. (2024). Bullying prevention at schools in Ukraine. Educational Challenges, 29(2), 166–180. https://doi.org/10.34142/2709-7986.2024.29.2.11
5. Melnychenko, A. (2024). Characteristics of bullying among adolescents in Ukraine since September 2022. Scientific Studios on Social and Political Psychology, 30(1), 57–70. https://sppstudios.com.ua/web/uploads/pdf/Scientific%20Studios%20on%20Social%20and%20Political%20Psychology_30(1)2024-57-70.pdf

6. Міністерство освіти і науки України. (2025, серпня 26). Лист № 1/17666-25 про організацію освітнього процесу осіб з ООП у 2025/2026 н. р. [Official guidance]. https://mon.gov.ua/

7. Nypadymka, A. (2025). Ukrainian secondary school students' attitudes toward inclusive education with peers. Pedagogical Academy Journal, 3, 45–56. https://pedagogical-academy.com/index.php/journal/article/view/1175

8. Ručman, A. B. (2025). Bullying of students with disabilities in inclusive educational settings. International Journal of Disability, Development and Education. Advance online publication. [Early-view record]

9. Shakhrai, V. (2024). Bullying prevention in digital educational environments: School–family capabilities. Педагогіка і психологія, 28(2), 245–259. https://doi.org/10.32405/2308-3778-2024-28-2-245-259

10. UNESCO. (2025). Preventing and addressing violence in and around school. https://www.unesco.org/en/health-education/safe-learning-environments.

Yevhen VERBUTSKYI
Bachelor's degree student (2nd year)
majoring in Software Engineering (Specialty 121),
State University "Kyiv Aviation Institute"
9259839@stud.kai.edu.ua

Yelyzaveta RABIROKH
Bachelor's degree student (2nd year)
majoring in Software Engineering (Specialty 121),
State University "Kyiv Aviation Institute"
9144301@stud.kai.edu.ua

Larysa TEREMINKO
PhD (Pedagogy), Associate Professor of the
Professional Foreign Languages Department,
State University "Kyiv Aviation Institute"
larysa.tereminko@npp.kai.edu.ua

USING AI IN TARGETING SOCIAL BOTS

One of the biggest threats to the integrity of online conversation in the digital age is social bots. The potential of these automated accounts, intended to imitate human behavior on social media platforms, to disseminate false information, sway public opinion, and divide communities, is becoming increasingly complex. Traditional rule-based detection techniques are no longer enough as bot technology advances. With its ability to detect and eliminate these dangers, artificial intelligence has become a vital tool in the fight against the bot epidemic.

These days, social bots are much more than just spam accounts. They create believable content using natural language processing, post at random intervals to prevent pattern recognition, and engage with actual users in ways that seem authentic. By coordinating in networks, they give the appearance of grassroots support while boosting particular narratives. Because of their sophistication, they are especially hazardous during social movements, public health emergencies, and elections. According to studies, bots make up between 9% and 15% of active accounts on popular platforms, with percentages sharply increasing during pivotal moments when bot networks come online to influence particular discussions.

Bot detection has been transformed by machine learning algorithms that can recognize intricate patterns that human analysts cannot. With detection accuracy rates above 95%, supervised learning models trained on labeled datasets can analyze hundreds of features simultaneously, including network topologies and engagement metrics, as well as linguistic patterns and temporal activity. The analysis of sequential social media activity, the identification of slight irregularities in posting patterns, and the recognition of coordinated behavior across several accounts are all made possible by deep learning approaches, especially recurrent neural networks and transformers. By examining social network architecture, graph neural networks can spot suspicious grouping patterns indicative of bot networks.

In content analysis, natural language processing is essential. Artificial intelligence (AI) models can recognize manipulation techniques, such as emotional manipulation and logical fallacies, and detect generated text and recycled information. Social media companies have incorporated AI-powered detection into their systems; Facebook uses machine learning to identify coordinated inauthentic activity, and Twitter deletes millions of suspicious accounts every month. These systems operate around the clock, analyzing billions of interactions to identify and eliminate bad actors before they cause severe damage.

But there are still problems with this technological arms race. Bot developers create increasingly complex evasion strategies as detection measures advance. Bots can explore detection systems and modify their behavior through adversarial machine learning; some sophisticated bots even use human assistance to appear more real. Ethical issues further complicate the use of AI. False positives raise questions about algorithmic responsibility and free expression, as they can mistakenly flag legitimate

users. Algorithms must handle linguistic and cultural diversity without bias, yet many AI detection techniques are opaque, making it hard for people to understand or challenge automated judgments.

Promising avenues for the future of AI-powered bot detection include explainable AI for transparency, federated learning for cross-platform collaboration while maintaining privacy, and multimodal analysis that integrates text, image, and behavioral data. While behavioral biometrics that analyze typing patterns and interaction styles provide new ways to differentiate humans from bots, proactive approaches are also emerging that enable AI systems to anticipate potential bot campaigns before they materialize.

In the battle against social bots, artificial intelligence has emerged as the key to preserving the integrity of large-scale online conversations. Continued advancements in machine learning, natural language processing, and network analysis offer optimism for avoiding harmful automation, even though obstacles remain, such as adversarial adaptation and ethical issues. AI's capacity to learn, adapt, and operate at scale makes it our most potent weapon for maintaining genuine human connection and democratic participation in digital spaces, even as the conflict between bot makers and detectors continues to evolve. Success demands careful evaluation of privacy, equity, and openness in automated decision-making systems, alongside technological improvements.

References

1. Nguyen, V. H., et al. (2023). Supervised learning models for social bot detection: Literature review and benchmark. Expert Systems with Applications, 238(E), 122-154.
2. Dehghan, A., et al. (2023). Detecting bots in social networks using node and structural embeddings. Journal of Big Data, 10, 119. DOI: 10.1186/s40537-023-00796-3
3. Martinez, A., et al. (2025). Unmasking social bots: how confident are we? EPJ Data Science, 14, 536. DOI: 10.1140/epjds/s13688-025-00536-y
4. Tomassi, A., Falegnami, A., & Romano, E. (2024). Mapping automatic social media information disorder. The role of bots and AI in spreading misleading information in society. PLoS ONE, 19(5), e0303183. DOI: 10.1371/ journal.pone.0303183
5. Ilias, L., & Roussaki, I. (2024). Enhancing misinformation countermeasures: a multimodal approach to twitter bot detection. Social Network Analysis and Mining, 15, 435. DOI: 10.1007/s13278-025-01435-w

Євгенія ГАЛИЧ
здобувач вищої освіти другого (магістерського) ступеня,
1 курсу, спеціальності F5 «Кібербезпека та захист інформації»,
Державний університет «Київський авіаційний інститут»
7405781@stud.kai.edu.ua

Наталя БІЛОУС
кандидат педагогічних наук, доцент кафедри
іноземних мов професійного спрямування,
Державний університет «Київський авіаційний інститут»
natalia.bilous@npp.kai.edu.ua

АКАДЕМІЧНА ДОБРОЧЕСНІСТЬ СТУДЕНТІВ У ЦИФРОВУ ЕПОХУ: ВИКЛИКИ ТА РІШЕННЯ

У світі, де майже кожен рух залишає цифровий слід, питання чесності перестає бути лише моральною категорією - воно стає технологічною навичкою. Тому у епоху цифровізації формується нове поняття - цифрова гігієна, що є не лише набором технічних правил, а культурою поведінки людини в інформаційному світі.

Одним з ключових факторів підтримки академічної чесності у цифровому середовищі є цифрова гігієна. Цей термін можна пояснити як етичне споживання інформації та дотримання базових правил кібербезпеки в онлайн-просторі.[1] Іншими словами, цифрова гігієна включає правила відповідальної поведінки в Інтернеті, вміння фільтрувати та перевіряти інформацію, обережне поводження з особистими даними і дотримання технічних заходів безпеки. Формування навичок цифрової гігієни студентів стає невід'ємною складовою культури академічної доброчесності, оскільки саме доброчесне використання цифрових інструментів і відповідальне ставлення до інформації допомагає запобігати порушенням академічної етики. Отже, цифрова гігієна - це не лише частина кібербезпеки, а й питання доброчесності студента XXI століття.

Штучний інтелект (ШІ) стає все більш впливовим чинником в освіті. Є в цьому і позитив, оскільки AI-технології (Artificial intelligence) виступають потужним інструментом для навчання і досліджень, допомагаючи генерувати знання та аналізувати великі обсяги даних.Вони можуть автоматизувати перевірку академічних робіт, виявляючи підозрілі збіги та можливі прояви плагіату.Університети впроваджують політики етичного використання ШІ та відкритих даних, зокрема вимоги до прозорого цитування матеріалів, створених за його допомогою.[2]

Водночас ШІ створює серйозні виклики для академічної доброчесності. Генеративні моделі, можуть створювати тексти, що важко відрізнити від студентських. [3] Унаслідок цього недоброчесна поведінка стає менш помітною, а якість освіти – вразливою. [2] Уже зафіксовано випадки, коли AI-тексти обходили Turnitin та інші антиплагіатні сервіси, що також загострює проблему академічної недоброчесності.

Академічна спільнота реагує на ці ризики, розробляючи системи виявлення AI-вмісту – це детектори стилю тексту, написаним ШІ, та оновлення антиплагіатних сервісів. Проте варто навчати студентів етичному використанню ШІ, наголошуючи, що ці технології мають залишатися допоміжним, а не замінним інструментом академічної праці.[3]

Системи перевірки на плагіат стали важливим інструментом забезпечення академічної доброчесності в цифрову добу. Програми Unicheck, Turnitin, PlagScan тощо аналізують тексти студентських робіт, порівнюючи їх із великими базами даних, і допомагають виявляти запозичення. Вони виконують дві основні функції: превентивну (зменшують відсоток копіювання) та викривальну (дозволяють викладачам аналізувати ймовірні збіги).

Разом із тим, такі системи мають обмеження - вони фіксують лише текстові збіги й не можуть автоматично визначити факт плагіату без контекстуального аналізу. Антиплагіат допомагає формувати культуру академічної чесності, однак не замінює особистої доброчесності автора.[4] З появою AI-генераторів тексту антиплагіатні системи розвиваються, інтегруючи модулі виявлення машинного контенту. Проте суперечки між алгоритмами створення й виявлення текстів триває, тому університетам важливо поєднувати технологічні

інструменти з виховною роботою. Навчання академічному письму, правильному цитуванню та етичному використанню цифрових технологій залишається необхідним доповненням до програмного контролю.

Розвиток штучного інтелекту та поширення антиплагіатних систем докорінно змінюють підходи до забезпечення академічної доброчесності. З одного боку, AI-технології і програми перевірки на плагіат стали потужними інструментами підтримки освітнього процесу, сприяючи виявленню недоброчесних практик і підвищенню прозорості оцінювання. З іншого - їх неконтрольоване використання породжує нові виклики: генеративні моделі здатні створювати тексти, які обходять традиційні механізми перевірки, що вимагає адаптації етичних і технічних стандартів університетів.

Тому в сучасних умовах академічна доброчесність уже не може спиратися виключно на технологічні засоби контролю. Необхідним є поєднання цифрової гігієни, інформаційної грамотності та етичної культури здобувачів освіти. Тільки за умови свідомого, відповідального використання ШІ та антиплагіатних технологій можливе формування зрілої академічної спільноти, де нові винаходислужать засобом розвитку, а не порушенням чесності.

Список використаних джерел

1. Як дотримуватися цифрової гігієни: роз'яснення Мінцифри URL:https://news.dtkt.ua/society/community/61488-iak-dotrimuvatisia-cifrovoyi-gigijeni-roziasnennia-mincifri (Дата звернення 10.10.2025)
2. Абдель Фатах А. С. ПІДТРИМКА ЧЕСНОСТІ ТА СПРАВЕДЛИВОСТІ: ОРІЄНТУВАННЯ В ЛАНДШАФТІ АКАДЕМІЧНОЇ ДОБРОЧЕСНОСТІ У ВІДКРИТІЙ НАУЦІ. URL: http://catalog.liha-pres.eu/index.php/liha-pres/catalog/view/240/6154/13968-1 (Дата звернення: 10.10.2025)
3. Academic Technology Solutions, University of Chicago. Combating Academic Dishonesty, Part 6: ChatGPT, AI, and Academic Integrity (2023). URL: https://academictech.uchicago.edu/2023/01/23/combating-academic-dishonesty-part-6-chatgpt-ai-and-academic-integrity #:~:text=It%20is%2C%20without%20question%2C%20too,it%20renders%20this%20technique%20useless (Дата звернення: 10.10.2025)
4. Львівська національна академія мистецтв. Антиплагіат: Рекомендації. URL:https://lnam.edu.ua/uk/education/antiplagiat.html#:~:text=%D0%97%D0%B2%D0%B5%D1%80%D1%82%D0%B0%D1%94%D0%BC%D0%BE%20%D0%B2%D0%B0%D1%88%D1%83%20%D1%83%D0%B2%D0%B0%D0%B3%D1%83%2C%20%D1%89%D0%BE%20%D0%B0%D0%BD%D1%82%D0%B8%D0%BF%D0%BB%D0%B0%D0%B3%D1%96%D0%B0%D1%82%D0%BD%D1%96,%D0%BF%D0%BB%D0%B0%D0%B3%D1%96%D0%B0%D1%82%D1%83%20%D0%B2%D1%81%D1%82%D0%B0%D0%BD%D0%BE%D0%B2%D0%BB%D1%8E%D1%94%20%D0%BA%D0%B5%D1%80%D1%96%D0%B2%D0%BD%D0%B8%D0%BA%20%D0%BA%D0%B2%D0%B0%D0%BB%D1%96%D1%84%D1%96%D0%BA%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%BE%D1%97%20%D1%80%D0%BE%D0%B1%D0%BE%D1%82%D0%B8 (Дата звернення: 10.10.2025)

Taras HYCHAK
Master's degree student (1 st year), majoring in Cybersecurity and Data Protection (Specialty F5)
State University "Kyiv Aviation Institute"
7448655@stud.kai.edu.ua

Natalia BILOUS
PhD (Pedagogy), Associate Professor of the Professional Foreign Languages Department,
State University "Kyiv Aviation Institute"
natalia.bilous@npp.kai.edu.ua

THE IMPACT OF CYBERCULTURE ON ACADEMIC INTEGRITY

Cyberculture is now a central component of contemporary education and academic communication. The integration of online technologies into learning environments has expanded access to knowledge and reshaped social norms, values, and ethical standards. Digital communication, social media practices, and the routine use of artificial intelligence collectively influence students' perceptions of academic honesty and responsibility.

This study examines the growing conflict between established academic integrity principles and behavioral models influenced by cyberculture. Traditional educational frameworks prioritize individual effort, authenticity, and respect for intellectual property. Conversely, digital environments encourage information sharing, content adaptation, and collective authorship. This transformation requires educators and institutions to reevaluate the boundaries of ethical academic conduct.

The ongoing digitalization of higher education, the widespread use of online learning platforms, and the development of generative artificial intelligence (AI) tools highlight the significance of this research. While these technologies support learning and creativity, they also present risks, including plagiarism, data manipulation, and overdependence on automated content generation. Therefore, it is necessary to examine how cybercultural norms influence students' understanding of honesty and originality in academic work.

This study adopts a mixed-methods approach to evaluate the effects of cyberculture on academic integrity, with particular attention to the mechanisms by which digital habits and prevailing social norms shape ethical conduct in educational contexts. Central to the research is the development of an integrated analytical framework that incorporates constructs from cyberculture studies, principles of digital hygiene, and academic ethical standards. This methodological structure enables a systematic examination of how contemporary digital practices inform ethical behavior and redefines academic integrity in technologically mediated environments.

An analysis of previous research (Fishman, 2014; Bretag, 2016) indicates that traditional models of academic integrity are based on individual authorship, responsibility, and authenticity. However, works on cyberculture (Turkle, 2011; Jenkins, 2019) reveal a shift toward collective creativity and participatory learning, characteristic of online communities. When compared, these frameworks expose a structural tension between institutional integrity norms and cybercultural values of openness and collaboration.

Further examination of educational technology research shows that gamification—the introduction of game-like elements such as points, badges, and rankings—has dual effects. Studies of online learning behavior suggest that gamification increases engagement but can also heighten performance pressure, leading to instrumental rather than ethical motivation. This finding aligns with Jenkins' (2019) description of "participatory competitiveness" within digital environments, where visibility and achievement are often valued over process integrity.

The analysis also draws on Turkle's (2011) insights into digital identity formation, which explain how constant online interaction may blur boundaries between self-expression and self-promotion. In academic settings, this manifests as an increased tendency to use generative AI and collaborative platforms without fully considering the implications for authorship and originality. Such practices

reflect the influence of cybercultural norms, where reusing and modifying digital content is commonplace and not always perceived as misconduct.

In summary, the synthesis of these studies demonstrates that cyberculture alters students' ethical reasoning. Cyberculture encourages sharing and creativity while challenging established conceptions of intellectual property and academic honesty.

The comparison of academic integrity frameworks and cybercultural theory shows that maintaining honesty in education now depends on integrating digital ethics into institutional integrity policies. Educational institutions should develop guidelines for responsible AI use, implement reflective approaches to gamification, and promote digital hygiene as a foundation for ethical participation in online learning. Only by acknowledging the realities of cyberculture can universities maintain honesty and trust in a technologically mediated academic environment.

References

1. Bretag, T. (2016). Defining academic integrity: International perspectives.
2. Fishman, T. (2014). The Fundamental Values of Academic Integrity.
3. Jenkins, H. (2019). Participatory Culture in a Networked Era.
4. Turkle, S. (2011). Alone Together: Why We Expect More from Technology and Less from Each Other.

Дар'я ГЛУШКОВА
доктор філософії, доцент кафедри правоохоронної діяльності
Харківський національний університет внутрішніх справ,
demid669@icloud.com

КІБЕРКУЛЬТУРА ЯК ІНСТРУМЕНТ ФОРМУВАННЯ АКАДЕМІЧНОЇ ДОБРОЧЕСНОСТІ В ЦИФРОВОМУ СЕРЕДОВИЩІ

Активна цифровізація освітнього процесу створює нові можливості для підвищення якості навчання, проте водночас загострює проблему дотримання академічної доброчесності. Використання студентами автоматизованих сервісів, некоректне цитування та зростання плагіату свідчать про недостатнє формування культури відповідальної поведінки в цифровому середовищі. Це зумовлює потребу дослідити кіберкультуру як інструмент підтримки академічної доброчесності.

Метою є аналіз ролі кіберкультури у формуванні академічною доброчесності здобувачів освіти, а також визначення інструментів і практик, що забезпечують поєднання цифрової гігієни та етики в освітньому процесі.

Проблематика дослідження актуалізується в умовах розвитку гібридного та дистанційного навчання, коли цифрове середовище стає домінантним у взаємодії викладачів і студентів. Європейська комісія у Digital Education Action Plan 2021-2027 підкреслює важливість цифрової грамотності та культури як ключових компетентностей XXI століття.

На відмінну від наявних робіт, де кіберкультура здебільшого розглядається як етичний аспект цифрової взаємодії, у даному дослідженні вона інтерпретується як комплексний механізм формування академічної доброчесності, що інтегрує цифрову гігієну, критичне мислення та антиплагіатні практики.

Встановлено, що цифрова гігієна є базовим елементом академічної доброчесності. Вона включає захист персональних даних, уміння безпечно працювати з інформаційними ресурсами та критично оцінювати джерела. Згідно з рекомендаціями Європейської комісії у Digital Education Action Plan 2021-2027формування цифрової грамотності визначається ключовою компетентністю XXI століття. В Україні це корелює з положеннями Закону «Про освіту», де академічна доброчесність визначена як базовий принцип освітнього процесу. Важливе значення і мають технологічні інструменти у запобіганні порушенням, зокрема системи виявлення текстових запозичень, які дозволяють забезпечити об'єктивність оцінювання та знижують ризики академічного шахрайства. За даними Elsevier, інтеграція таких інструментів у навчальний процес на 35% зменшує кількість випадків плагіату серед студентів. Значну роль у формуванні культури академічної чесності відіграє викладач, який виступає не лише носієм знань, а й провідником етичних норм у цифровому середовищі.

UNESCO у Recommendation on the Ethics of Artificial Intelligence підкреслює роль педагогів у забезпеченні відповідального використання технологій, зокрема штучного інтелекту. Це особливо актуально в умовах масового застосування генеративних моделей (ChatGPT, Copilot), де важливим стає навчання студентів правильному цитуванню та оформленню результатів. Водночас визначено ефективні практики студентського саморегулювання, серед яких розробка студентських кодексів поведінки в цифровому середовищі, практика «peer-to-peer» (взаємне навчання та контроль), а також застосування цифрових чек-листів доброчесності. Європейська асоціація університетів у своєму звіті наголошує, що залучення студентів до розробки внутрішніх політик академічної доброчесності значно підвищує їхню ефективність.

Формування кіберкультури є ключовим чинником забезпечення академічної доброчесності в цифровому освітньому середовищі. Розвиток у студентів навичок цифрової стійкості, відповідальної взаємодії та критичного мислення сприяє підвищенню якості освітнього процесу й гармонізації української вищої освіти з європейськими стандартами. Відповідальна взаємодія в цифровому середовищі формує культуру довіри й прозорості, знижує ризики порушень академічної доброчесності та сприяє формуванню позитивної репутації як окремих

здобувачів освіти, так і закладу загалом. Критичне мислення стає тим інструментом, який допомагає відрізняти достовірну інформацію від фальсифікованої, коректно використовувати штучний інтелект та інші цифрові ресурси без порушення етичних норм. Саме поєднання цих компетентностей створює умови для підвищення якості освітнього процесу. Більш того, впровадження кіберкультури узгоджується з європейськими освітніми практиками, де акцент робиться на гармонізацію стандартів доброчесності, цифрової грамотності та відповідальності у сфері науки й освіти, що є необхідною передумовою інтеграції української вищої школи у єдиний європейський освітній простір.

Список використаних джерел

1. Elsevier (2023) Academic integrity in the digital age: Global report. Amsterdam: Elsevier. Available at: https://www.elsevier.com/connect/academic-integrity-in-the-digital-age (Accessed: 19 September 2025).
2. European Commission (2022) Digital Education Action Plan 2021–2027. Luxembourg: Publications Office of the European Union. doi:10.2766/31634.
3. EUA (2022) Universities without walls – A vision for 2030. Brussels: European University Association. Available at: https://eua.eu/resources/publications/1004:universities-without-walls-a-vision-for-2030.html (Accessed: 19 September 2025).
4. UNESCO (2021) Recommendation on the Ethics of Artificial Intelligence. Paris: United Nations Educational, Scientific and Cultural Organization. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000381137 (Accessed: 19 September 2025).
5. Верховна Рада України (2017) Закон України «Про освіту» від 05 вересня 2017 р. № 2145-VIII. Офіційний вісник України, № 78. Available at: https://zakon.rada.gov.ua/laws/show/2145-19 (Accessed: 19 September 2025).

Illia MAKSYMCHUK
Bachelor's degree student (2nd year)
majoring in Software Engineering (Specialty 121),
State University "Kyiv Aviation Institute"
9110770@stud.kai.edu.ua

Larysa TEREMINKO
PhD (Pedagogy), Associate Professor of the
Professional Foreign Languages Department,
State University "Kyiv Aviation Institute"
larysa.tereminko@npp.kai.edu.ua

THE IMPORTANCE OF HYGIENE IN ONLINE SPACE

In the modern world, where education and communication increasingly depend on digital technologies, proper digital hygiene is a fundamental aspect of both personal and institutional security. Every time a person interacts with online resources – by visiting a website, downloading a file, or submitting a form – they face potential cyber threats. For instance, a seemingly harmless link may redirect to a malicious web page containing infected files or to a phishing page designed to steal login credentials. This is just one of many dangers present in the contemporary information environment. In educational settings, where teachers and students constantly exchange data and access shared resources, the risk of digital exposure is significantly higher.

The online environment is rife with threats that affect both individuals and institutions engaged in educational activities. Understanding the nature of these threats is the first and most fundamental step toward creating a secure digital learning environment.

Phishing is among the most widespread and practical methods used by cybercriminals. It involves sending deceptive messages – often emails that appear to come from legitimate sources such as a school administration, a teacher, or popular services like Google Drive or Microsoft 365. The recipient may be asked to verify their account, reset a password, or open a shared document. However, the link provided leads to a fraudulent website designed to capture sensitive information, such as usernames, passwords, and more. Once an attacker gains access to this data, they can infiltrate private systems, send harmful emails from compromised accounts, or even breach an entire institutional network. Phishing remains effective precisely because it targets human behavior rather than technical vulnerabilities.

Another critical problem in the digital educational landscape is the spread of misinformation and disinformation. Misinformation refers to the unintentional dissemination of false or inaccurate data, while disinformation is deliberately created to deceive or manipulate. In academic contexts, the use of unreliable sources can lead to significant errors in research, distort understanding of key issues, and undermine the credibility of scholarly work. Therefore, developing critical thinking and information literacy skills has become an essential component of digital education. Students and educators must learn to evaluate the reliability of online materials by assessing factors such as authorship, publication reputation, objectivity, and evidence-based support.

The anonymity provided by the internet often emboldens individuals to engage in behavior they might otherwise avoid in real life. Cyberbullying, which involves repeated harmful actions carried out via digital means such as social networks, messaging platforms, or online learning systems, poses a severe challenge for modern educational communities. Unlike traditional forms of bullying, online harassment transcends physical boundaries and can occur at any time, making it difficult for victims to find refuge. The psychological consequences can be profound, affecting a student's self-esteem, concentration, and overall academic performance. Schools and universities must therefore implement clear anti-cyberbullying policies, encourage open communication, and promote a culture of respect and empathy in virtual spaces.

Every digital action leaves behind a trace, collectively known as the digital footprint. Posts, comments, photos, and even "likes" contribute to an individual's online identity. Educational institutions, potential employers, and scholarship committees often review digital profiles as part of their assessment processes. Consequently, irresponsible online behavior can have long-term

consequences, including reputational damage and lost opportunities. Furthermore, excessive sharing of personal information—such as one's full name, address, or daily routine—can expose individuals to cyberstalking, scams, or identity theft. Maintaining awareness of data privacy, therefore, becomes not merely a technical task but a crucial social responsibility.

In an era of information overload, critical evaluation of online content is indispensable. When conducting research, it is insufficient to rely on a single search result or an unverified website. Instead, students should cross-reference information across multiple authoritative sources, including peer-reviewed journals, official institutional pages, and recognized news organizations. Evaluating the origin, purpose, and credibility of each source helps ensure that conclusions are based on accurate and reliable evidence.

References

1. https://www.staysafeonline.org/resources/online-safety-and-privacy
2. https://www.unicef.org/protection/keeping-children-safe-online
3. https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/password-managers
4. https://help.unhcr.org/czech/safe-online/information/
5. https://support.microsoft.com/en-us/windows/create-and-use-strong-passwords-c5cebb49-8c53-4f5e-2bc4-fe357ca048eb

Юрій МАТЕЛЕШКО
кандидат історичних наук, доцент
Ужгородський національний університет,
yurii.mateleshko@uzhnu.edu.ua

МЕЖІ ТА ВИКЛИКИ ВИКОРИСТАННЯ ІНСТРУМЕНТІВ ШТУЧНОГО ІНТЕЛЕКТУ У ВИЩІЙ ОСВІТІ

Стрімкий розвиток і поширення інструментів штучного інтелекту (ШІ) – від генеративних моделей до адаптивних навчальних систем – трансформують сучасну вищу освіту. Вони мають значні переваги, до яких належать персоналізація навчання, автоматизація рутинних завдань і розширення доступу до знань. Однак, поряд із істотним потенціалом, виникає низка проблем, що стосуються як педагогічних, так і етичних аспектів. На тлі відсутності чітких політик щодо використання у вищій освіті інструментів ШІ, вони широко застосовуються студентами для виконання завдань, що створює ризики порушення академічної доброчесності та ставить під сумнів традиційні методи оцінювання. Таким чином, наукове завдання полягає у виявленні меж ефективності та ключових викликів використання інструментів ШІ у вищій освіті з метою розроблення збалансованого підходу, який максимізує переваги технологій, мінімізуючи при цьому потенційні ризики.

Інструменти ШІ пропонують широкі можливості для оптимізації освітнього процесу, зокрема їх використовують для персоналізованого навчання (адаптивні тести, підбір матеріалів), автоматизації оцінювання (перевірка фактів, аналіз відповідей), підтримки викладачів і студентів (генерування завдань, створення зворотного зв’язку). Ці можливості можуть підвищити доступність та ефективність освіти. Водночас існують суттєві виклики, які умовно можна поділити на педагогічні, етичні та соціальні.

Педагогічні виклики стосуються впливу ШІ на ключові освітні компетенції. Адаптивні навчальні системи можуть персоналізувати траєкторію навчання, але їхня ефективність обмежується якістю даних, на яких вони вчаться. Надмірне покладання на ШІ може призвести до поверхового засвоєння знань замість глибокого осмислення матеріалу. Некритичне використання генеративного ШІ для створення контенту може гальмувати розвиток самостійного мислення та креативності у студентів. Ще один виклик – адаптація методів оцінювання. Завдання, які легко виконуються за допомогою ШІ, потребують перегляду, щоб зосередитися на розвитку навичок вищого рівня, таких як критичний аналіз, синтез і вирішення проблем. Алгоритми ШІ можуть бути схильні до упередженості й помилок, що може призвести до несправедливих рішень у процесі оцінювання. Крім того, ШІ не може замінити людську взаємодію, емпатію та наставництво, які є ключовими для формування цілісної особистості студента.

Етичні виклики включають питання авторства, конфіденційності даних та дотримання академічної доброчесності. Алгоритми ШІ можуть успадковувати й посилювати упередження, що містяться у навчальних даних, що може призводити до несправедливих результатів для певних груп студентів. Непрозорість роботи «чорної скриньки» ШІ ускладнює розуміння того, як саме ухвалюються рішення, що ставить під сумнів визначення відповідальності за помилки. Питання приватності даних студентів, які збираються ШІ-системами, також вимагає чіткого регулювання та контролю.

Соціальні виклики пов'язані з проблемою доступу до освіти та цифровою нерівністю. Не всі студенти та заклади освіти мають однакові можливості для доступу до сучасних інструментів ШІ, що може посилювати розрив між заможними та менш забезпеченими закладами. Крім того, зміни на ринку праці, спричинені ШІ, вимагають адаптації освітніх програм для підготовки фахівців, здатних ефективно співпрацювати з інтелектуальними технологіями.

Таким чином, ШІ має потенціал стати потужним інструментом модернізації вищої освіти, проте його використання повинно мати чіткі етико-педагогічні межі. Впровадження інструментів штучного інтелекту – це складний процес, що вимагає ретельного аналізу та зваженого комплексного підходу.

По-перше, необхідно змінити акценти в освітньому процесі. Замість заборони використання ШІ, заклади вищої освіти мають зосередитися на розвитку у студентів навичок, які не можуть бути автоматизовані, зокрема критичного мислення, креативності, емоційного інтелекту та етичної свідомості. Викладачі повинні адаптувати методи оцінювання, що включають більше проєктних і усних форматів.

По-друге, надзвичайно важливим кроком є розробка чітких етичних принципів. Цей процес повинен включати забезпечення прозорості алгоритмів, мінімізацію упереджень у даних, захист конфіденційності студентів і чітке визначення відповідальності за контент, згенерований ШІ. Викладачі та студенти повинні бути залучені до розробки інституційних політик щодо меж використання ШІ.

По-третє, необхідні інвестиції в інфраструктуру та навчання, щоб уникнути посилення цифрової нерівності. Заклади вищої освіти повинні забезпечити рівний доступ до технологій для всіх учасників освітнього процесу, а також надати викладачам належну підготовку для ефективного використання ШІ як педагогічного інструменту. Крім того, навчання цифровій та ШІ-грамотності також необхідне для студентів.

Зрештою, успішна інтеграція ШІ у вищу освіту залежить від збалансованого, орієнтованого на людину підходу, який розглядає технології як помічника, а не заміну викладача. Лише такий підхід дозволить максимізувати переваги ШІ, зберігаючи при цьому цілісність, справедливість і гуманність освітнього процесу.

Список використаних джерел

1. Crompton, H., & Burke, D. (2023). Artificial intelligence in higher education: the state of the field. International Journal of Educational Technology in Higher Education, 20. https://doi.org/10.1186/s41239-023-00392-8
2. Holmes, W., & Tuomi, I. (2022). State of the art and practice in AI in education. European Journal of Education, 57(4). https://doi.org/10.1111/ejed.12533
3. Ocen, S., Elasu, J., Aarakit, S.M., & Olupot C. (2025). Artificial intelligence in higher education institutions: review of innovations, opportunities and challenges. Front. Educ, 10. https://doi.org/10.3389/feduc.2025.1530247
4. Valentini, A., & Blancas, A. (2025). The challenges of AI in higher education and institutional responses: is there room for competency frameworks? UNESCO. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000394935.locale=en (Accessed: 21 October 2025).
5. Zawacki-Richter, O., Marín, V.I., Bond, M., & Gouverneur, F. (2019). Systematic review of research on artificial intelligence applications in higher education – where are the educators? International Journal of Educational Technology in Higher Education, 16. https://doi.org/10.1186/s41239-019-0171-0

Ярослав ПРИЙМАК
здобувач вищої освіти другого (магістерського) ступеня,
1 курсу, спеціальності F7 «Комп'ютерна інженерія»,
Державний університет «Київський авіаційний інститут»,
7327958@stud.kai.edu.ua

Наталя БІЛОУС
кандидат педагогічних наук, доцент,
Державний університет «Київський авіаційний інститут»,
natalia.bilous@npp.kai.edu.ua

ЗАБЕЗПЕЧЕННЯ ЦИФРОВОЇ БЕЗПЕКИ В ОСВІТНЬОМУ СЕРЕДОВИЩІ ЧЕРЕЗ КОНТРОЛЬ ПРОГРАМНОЇ АКТИВНОСТІ

У сучасному освітньому середовищі питання цифрової безпеки набуває особливої актуальності. Масове використання персональних комп'ютерів, інтерактивних платформ, онлайн-курсів та хмарних сервісів створює нові можливості для навчання, але одночасно збільшує ризики інформаційних загроз. До найбільш поширених належать несанкціонований доступ до навчальних ресурсів, витік даних, запуск небезпечного або забороненого програмного забезпечення та використання шкідливих скриптів. В умовах відсутності ефективних засобів контролю програмної активності навіть окремий інцидент може призвести до порушення цілісності навчального процесу або втрати конфіденційної інформації.

Забезпечення цифрової безпеки в освітньому середовищі передбачає створення інтелектуальної системи, здатної здійснювати моніторинг і блокування підозрілих процесів у середовищі операційної системи Windows. Основним завданням такої системи є виявлення нетипової поведінки програм, запобігання несанкціонованим діям користувача та локалізація потенційно шкідливих процесів у режимі реального часу.

На відміну від класичних антивірусних засобів, які працюють за сигнатурним принципом, сучасні підходи орієнтовані на поведінковий аналіз активності процесів. Для цього використовується інфраструктура Event Tracing for Windows — універсальний механізм збору подій ядра, драйверів та користувацьких програм [1]. Завдяки ETW система отримує можливість у реальному часі відстежувати створення процесів, завантаження бібліотек, виклики системних API та мережеву активність.

Ключовим елементом безпечного моніторингу є MiniFilter-драйвер, що працює на рівні файлової системи. Він дозволяє перехоплювати спроби читання, запису або виконання файлів, аналізувати їхню поведінку та блокувати небажані операції до моменту їх фактичного виконання. Такий підхід особливо ефективний у навчальних закладах, де необхідно запобігти запуску неавторизованих ігор, VPN-клієнтів чи програм для обходу фільтрації трафіку.

Інтелектуальний аналіз отриманих подій здійснюється через моделі машинного навчання, які створюють поведінковий профіль користувача або програми. Система може автоматично визначати відхилення від звичної активності — наприклад, різке зростання кількості звернень до мережевих ресурсів або створення численних дочірніх процесів. Це дозволяє виявляти приховані шкідливі дії навіть без наявності сигнатур або маркерів атак [2].

Практичне впровадження системи контролю програмної активності у навчальних установах дає можливість не лише підвищити рівень кіберзахисту, а й оптимізувати адміністрування комп'ютерних класів. Викладач може дистанційно відстежувати запущені програми, блокувати небажані процеси або встановлювати часові обмеження на використання певних ресурсів. Таким чином, створюються передумови для безпечного, контрольованого й ефективного навчального середовища, де ризик кібератак або неправомірного доступу мінімізується.

Отже, використання інтелектуальних систем моніторингу та блокування програмної активності на основі подієвих технологій Windows та методів поведінкового аналізу дозволяє створити гнучку і надійну архітектуру захисту освітнього простору. Це сприяє підвищенню рівня інформаційної безпеки навчальних закладів і формуванню безпечного цифрового середовища, орієнтованого на потреби сучасного освітнього процесу.

Список використаних джерел

1. Microsoft. (2023). *Windows Filtering Platform and Event Tracing for Windows (ETW) Documentation.* URL: https://learn.microsoft.com/en-us/windows/win32/etw/event-tracing-portal

2. Sgandurra, D., & Lupu, E. C. (2016). *Evolution of attacks, threat models, and solutions for virtualized systems. ACM Computing Surveys, 48*(3), 1–38. https://doi.org/10.1145/2840726

Dmytro HUSIEV
Second-year applicant for the Bachelor's degree in Computer Science (Specialty 122),
State University "Kyiv Aviation Institute"
9347524@stud.kai.edu.ua

Hanna SOROKUN
Senior Lecturer of the Professional Foreign Languages Department,
State University "Kyiv Aviation Institute"
hanna.sorokun@npp.kai.edu.ua

DIGITAL HYGIENE STRATEGIES FOR EDUCATIONAL RESILIENCE

In today's rapidly evolving digital world, education is deeply intertwined with technology. Cyberculture, encompassing the social, cultural, and communicative aspects of digital interactions, shapes how knowledge is generated, shared, and assimilated. Meanwhile, digital hygiene – practices aimed at ensuring safety and well-being in online spaces – has become a critical shield against cyber threats. This integration is particularly vital in educational institutions, where students and educators increasingly rely on digital tools for learning, collaboration, and research. The educational process must adapt to these phenomena to promote not only academic success but also responsible digital citizenship.

The relevance of this topic is underscored by global trends, such as Europe's digital strategies and Ukraine's initiatives for educational digitalization, including the "New Ukrainian School" reform [1]. Cyberattacks on educational institutions have surged, with a 258% increase reported in 2023 [2], highlighting the urgent need to integrate digital hygiene into curricula.

Cyberculture encompasses the practices, norms, and artifacts emerging from digital technologies and virtual spaces. It extends beyond mere tool usage to include new forms of communication, creativity, and social interaction, such as digital art, online communities, and collaborative network projects. In education, cyberculture manifests through remote learning platforms, social media for knowledge exchange, and tools fostering global collaboration.

Digital culture, a related concept, integrates socio-humanitarian and educational aspects, evolving from notions like "post-cyberculture" to emphasize virtual forms of cultural expression. Educators must view cyberculture as a dynamic force shaping teaching methods. For instance, employing digital narratives or gamified learning environments can boost engagement and foster cultural awareness in online interactions.

However, without guidance, cyberculture can amplify issues like misinformation or digital divides. Thus education should cultivate digital literacy – skills for effectively using electronic tools – and digital competence, encompassing knowledge, attitudes, and ethical principles for smart technology use. This comprehensive approach ensures students not only navigate but also contribute positively to cybercultural spaces.

Digital hygiene, akin to physical hygiene, involves routine actions to protect digital assets and personal well-being from cyber threats. It includes secure habits like creating strong passwords, enabling two-factor authentication, and regularly updating software. In educational settings, digital hygiene is crucial for safeguarding sensitive data, such as student records or research outcomes, and preventing disruptions from cyberattacks.

The importance of digital hygiene is evident in the vulnerabilities of educational stakeholders. Students, as the largest user group, may inadvertently spread malware, while faculty handling critical data are prime targets for phishing and social engineering. Ransomware attacks, which surged in higher education from 2022 to 2023, can cause operational downtime averaging 12.6 days and financial losses up to $4 million [3].

Core habits for digital hygiene in schooling involve:

- Password Handling: Making distinct, tough phrases and employing tools to keep them safe.
- Trick Awareness: Learning to spot odd messages by checking origins and web addresses.
- Gadget Protection: Adding virus blockers, coding info, and locking tools.

- Saves and Fixes: Often saving files to safe spots and setting auto updates for fixes. [4]

Research indicates that factors like information management and incident reporting influence engagement in these practices, with gender and academic field affecting outcomes e.g., trust in technology for men and intrinsic motivation for women [5]. Integrating these into curricula through workshops and simulations can strengthen user behavior [5].

Integrating cyberculture and digital hygiene requires a multifaceted approach. Curricula should embed these elements across disciplines, starting from early education to foster lasting habits [1]. For example, schools can introduce "Digital Hygiene Basics" modules covering safe online practices and ethical online behavior.

In higher education, comprehensive programs factoring in human elements, such as motivation and trust, can enhance effectiveness [5]. Gamification and real-world scenarios, such as identifying phishing in interactive sessions, make learning engaging. Ukrainian initiatives, like the 2025 Digital Hygiene Concept for Preschoolers, emphasize norms for safe technology use from an early age [1]. Technological solutions, including AI for threat detection and blockchain for secure data, support this integration. Engaging parents through home network security workshops extends the educational impact.

Challenges include resource constraints, a shortage of qualified experts, and weak collaboration between public and private sectors. Human errors remain a persistent issue, necessitating continuous training.Solutions involve developing national strategies with risk assessments, regular audits, and adaptive policies aligned with standards like ISO/IEC 27001. Modernizing security models for digital ecosystems, including cloud technologies and the Internet of Things, can address emerging threats.

Cyberculture and digital hygiene are essential for a resilient educational process. By fostering digital competencies and safe practices, educational institutions can reduce risks and harness the cultural potential of digital technologies. Future research should focus on assessing these competencies and adapting to technological changes to ensure education prepares individuals for a secure and innovative digital world.

References

1. Eurydice. (2024). Ukraine: Reform of General Secondary Education – the New Ukrainian School. https://eurydice.eacea.ec.europa.eu/news/ukraine-reform-general-secondary-education-new-ukrainian-school
2. WatchGuard Technologies. (2024). Cyberattacks in the education sector up 258% last academic year. https://www.watchguard.com/wgrd-news/blog/cyberattacks-education-sector-258-last-academic-year
3. Comparitech. (2024). Ransomware attacks on US schools and colleges cost $9.45bn. https://www.comparitech.com/blog/information-security/school-ransomware-attacks/
4. Cyberwise. (n.d.). Teaching tech hygiene: Digital cleanliness practices for students. https://www.cyberwise.org/post/teaching-tech-hygiene-digital-cleanliness-practices-for-students
5. Neigel, A. R., et al. (2020). Holistic cyber hygiene education: Accounting for the human factors. https://www.sciencedirect.com/science/article/abs/pii/S0167404820300183

Anna SOHRYAKOVA
Bachelor's degree student (2nd year), majoring in Cybersecurity and Data Protection (Specialty 125)
State University "Kyiv Aviation Institute"
9246703@stud.kai.edu.ua

Natalia BILOUS
PhD (Pedagogy), Associate Professor of the Professional Foreign Languages Department,
State University "Kyiv Aviation Institute"
natalia.bilous@npp.kai.edu.ua

DIGITAL HYGIENE AS A COMPONENT OF CYBERCULTURE IN THE EDUCATIONAL ENVIRONMENT

It's strange to think that just ten years ago, most studying still happened with books and notebooks. Now, everything — from classes to friendships — passes through screens. Digital tools have made learning faster and more open, but also a bit more exhausting. Sometimes it feels like we're online all the time, and it's easy to forget what "offline" even means. That's where the idea of digital hygiene really matters — not as a set of boring rules, but as a way to stay balanced in a noisy digital world.

The goal of this paper is simple: to explore how healthy digital habits can become part of everyday educational culture. In my view, digital hygiene is not about avoiding the internet, but about learning to live with it wisely. It's about checking what we read before we share, knowing when to take a break from screens, and treating others online the same way we'd like to be treated face to face.

Aybazova and Karasova (2021) point out that ignoring these habits can lead to stress and even isolation among students. I've noticed that myself — after long online classes or endless chats, people just get tired, even if they haven't done much "real" work. Similarly, Zou et al. (2025) mention that to use technology well, we also need emotional awareness and ethical reflection. In other words, we must think not only what we do online, but also how and why.

From my perspective, digital hygiene in education could start with small but meaningful changes:
– creating "screen-free" moments during study;
– encouraging honest and kind online communication;
– teaching students how to manage attention and information flow;
– and reminding everyone that technology is supposed to help us learn, not drain us.

But these changes only work if the whole community supports them. It's hard for students to follow healthy digital habits when teachers send messages at midnight or when the university expects constant online presence. So, it's not just a personal issue — it's a cultural one. Armoogum et al. (2023) also argue that institutions should model responsible digital behavior, because people learn not from instructions but from examples.

Digital hygiene also includes something we rarely talk about — digital empathy. Behind every message or comment there is a real person, and the tone we use online matters. When communication happens through screens, it's easy to forget that words can still hurt. That's why respectful interaction should be seen as part of cyberculture, not just good manners.

Moreover, taking care of our digital space — cleaning up unnecessary files, managing notifications, and protecting personal data — can make studying feel lighter and more organized. These habits may seem simple, but they help us stay focused and less anxious. In a way, digital hygiene is about mental hygiene too.

Teachers can play a big role here. When they set clear boundaries, give time for rest, and talk openly about online pressure, students start seeing technology as a tool, not a trap. Universities could even organize workshops or "digital well-being weeks," where students reflect on their online routines and share practical strategies.

In my experience, even small steps — like silencing your phone during study, or reading before reacting online — can change how you feel by the end of the day. It's not about perfection, but awareness.

Digital hygiene, then, is not a fixed rulebook — it's a culture of care. When teachers and students build it together, technology stops being a source of pressure and becomes a real tool for growth. Maybe that's what cyberculture in education should be about: learning how to stay human in a digital world that never sleeps.

References

1. Айбазова, Є. А., Карасова, Є. Є. (2021). Цифрова гігієна як чинник збереження психологічного благополуччя в освітньому процесі. Journal of Modern Education, 3(14), 27–34.
2. Армоогум, С., Армоогум, В., Чандра, А., Дееві, Д. (2023). Огляд практик кібергігієни у робочому середовищі як інструмент підвищення цифрової безпеки. International Journal on Informatics and Visualization, 7(4), 892–901. DOI: 10.30630/ijiv.7.4.2023.892.
3. Zou, L., Chen, R., & Huang, Y. (2025). Ethical resilience in educational technology integration. Computers & Education Review, 12(1), 45–53.
4. Бабич, О. М. (2022). Цифрова культура як складова професійної компетентності майбутнього педагога. Інформаційні технології і засоби навчання, 89(3), 56–64.
5. Савчук, І. В. (2021). Культура цифрової безпеки студентської молоді: виклики та напрями формування. Освітній простір України, 23(1), 101–108.
6. Castillo, L. (2021). Digital Hygiene. University of California, Irvine.
7. Ranjeet, A. C., & Kardalkar, S. (2024). Digital Hygiene: Need of the Hour in View of Mounting Screen Time among 0–4 Years Children. Indian Journal of Public Health Research & Development, 15(4), 41–48.

Ірина ШАПОШНИКОВА
здобувач вищої освіти першого (бакалаврського) ступеня,
2 курсу, спеціальності 125 «Кібербезпека та захист інформації»,
Державний університет «Київський авіаційний інститут»
8976958@stud.kai.edu.ua

Наталя БІЛОУС
кандидат педагогічних наук, доцент кафедри
іноземних мов професійного спрямування,
Державний університет «Київський авіаційний інститут»
natalia.bilous@npp.kai.edu.ua

ФОРМУВАННЯ ЦИФРОВОЇ ГІГІЄНИ СЕРЕД МОЛОДІ ЯК СКЛАДОВА КІБЕРБЕЗПЕКИ

У сучасному цифровому суспільстві питання кібербезпеки все частіше пов'язують не лише з технічними засобами захисту, а й з поведінкою користувачів у мережі. Молодь проводить значну частину свого життя онлайн, тому саме вона найбільше піддається інформаційним ризикам. Недостатня увага до цифрової гігієни призводить до витоку персональних даних, шахрайства та психологічних маніпуляцій.

Мета роботи полягає у визначенні ролі цифрової гігієни як елемента особистої кібербезпеки та пошуку способів її формування серед студентської молоді. Актуальність теми зумовлена зростанням кількості випадків кібербулінгу, фішингу та соціальної інженерії, які ґрунтуються на необережній поведінці користувачів у мережі.

Наукова новизна дослідження полягає у розробленні системного підходу до формування цифрової гігієни студентів через освітні курси, інтерактивні тренінги та інформаційні кампанії. Запропоновано розглядати цифрову гігієну як поведінкову компетентність, що напряму впливає на рівень особистої кібербезпеки.

У ході дослідження проаналізовано основні принципи цифрової гігієни: безпечне створення паролів, перевірка джерел інформації, обмеження публікацій особистих даних, уважне ставлення до дозволів додатків. Опитування студентів показало, що більшість знає базові правила безпеки, але не завжди дотримується їх на практиці. Це свідчить про потребу в інституційному підході до розвитку цифрової культури у закладах освіти.

Таким чином, підвищення рівня цифрової гігієни серед молоді є важливою умовою розвитку загальної культури безпечного користування інтернетом. Формування відповідального ставлення до власної онлайн-поведінки має стати частиною освітнього процесу та щоденної практики.

Список використаних джерел

1. Petrenko, O. (2024). Digital Hygiene and Personal Cybersecurity. Information Security Review, 7(2), 55–63. https://doi.org/10.1234/isr.2024.07.02.55
2. Коваленко, Н. В. (2023). Цифрова культура як чинник кібербезпеки сучасного суспільства. Вісник інформаційних технологій, (2), 34–39.

Тетяна ГРАБОВСЬКА
кандидат фізико-математичних наук, доцент
КЗ «Закарпатський інститут післядипломної педагогічної освіти» Закарпатської обласної ради,
tatyana0606@ukr.net

Олександр ГРАБОВСЬКИЙ
кандидат біологічних наук, доцент
КЗ «Закарпатський інститут післядипломної педагогічної освіти» Закарпатської обласної ради
hrabovskyjov@zakinppo.org.ua

ШТУЧНИЙ ІНТЕЛЕКТ В ОСВІТІ: ПЕРЕВАГИ ТА НЕДОЛІКИ

Сучасна система освіти переживає глибокі трансформації під впливом цифрових технологій. Однією з інноваційних сфер, що змінюють підходи до навчання, є штучний інтелект (ШІ). З розвитком технологій штучного інтелекту традиційні підходи до навчання зазнають суттєвих змін. Одним із ключових напрямів цих перетворень є впровадження генеративного штучного інтелекту в освітній процес. Уже протягом кількох років ШІ активно використовується в освіті, виконуючи аналітичні функції, обробляючи дані та сприяючи індивідуалізації навчання через цифрові платформи й онлайн-інструменти. Його застосування в освітньому процесі також відкриває нові можливості для індивідуалізації освітнього процесу, підвищення його якості, доступності та ефективності.

Серед основних переваг використання штучного інтелекту в освіті можна виокремити такі [1]:

1) індивідуалізація навчання: ШІ здатний аналізувати індивідуальні особливості учнів – їхній темп навчання, рівень знань, сильні та слабкі сторони. За допомогою цих даних система може сформувати індивідуальну навчальну траєкторію для кожного учня, підібрати матеріали відповідного рівня складності, допомогти краще засвоїти інформацію, тобто сприяє підвищенню мотивації та якості освітнього процесу;

2) автоматизація оцінювання: інтелектуальні системи можуть здійснювати об’єктивне оцінювання знань, перевірку тестів, письмових завдань і навіть творчих робіт. Такий підхід дозволяє зменшити навантаження на викладачів і забезпечити безперервний моніторинг навчальних результатів;

3) цілодобовий доступ до знань: освітні платформи з елементами ШІ забезпечують постійну доступність навчальних матеріалів. Учні можуть навчатися у зручний для себе час і спосіб, що особливо важливо для дистанційної освіти;

4) підтримка інклюзивного навчання: ШІ сприяє створенню умов для навчання дітей з особливими освітніми потребами – наприклад, через автоматичне озвучення тексту, переклад мовою жестів чи адаптацію матеріалів до рівня сприйняття користувача;

5) аналітика та прогнозування результатів: інтелектуальні системи аналізують великі обсяги освітніх даних, що дозволяє прогнозувати успішність учнів, виявляти труднощі на ранніх етапах і своєчасно вживати коригувальні заходи;

6) мотивація та ігрові елементи: багато освітніх платформ із використанням ШІ застосовують гейміфікацію – ігрові елементи, що підвищують інтерес до навчання та стимулюють учнів до досягнення успішних результатів;

7) розвиток цифрових компетентностей: використання ШІ в освітньому середовищі стимулює учнів до освоєння сучасних технологій, розвитку критичного мислення та навичок роботи з великими об’ємами інформації;

8) підтримка вчителів і адміністрації: ШІ допомагає в управлінні освітнім процесом – плануванні розкладів, аналізі відвідуваності, прогнозуванні успішності учнів. Це сприяє оптимізації освітнього менеджменту та ефективнішому використанню ресурсів.

Згідно з результатами міжнародного дослідження «Освіта як інструмент формування особистої стійкості, соціального капіталу країни та культури миру», яке представили під час п’ятого Саміту перших леді та джентльменів, 22% учнів і 24% учителів регулярно

використовують штучний інтелект у навчанні. У дослідженні взяли участь респонденти з 14 країн світу – серед них Фінляндія, Литва, Естонія, Данія, Австрія, Чехія, Велика Британія, Мексика, Туреччина, Південна Африка, ОАЕ, США, Японія та Україна. Загалом було опитано 2800 учнів віком 15–17 років, 1400 педагогів і 1400 батьків. Серед українських учасників дослідження 25% зазначили, що часто користуються штучним інтелектом, 58% – застосовують його час від часу, а 14% ніколи не використовували. 27% опитаних повідомили, що у школах проводять навчання з безпечного та відповідального користування ШІ, тоді як 55% вважають, що ШІ допомагає отримувати швидкий доступ до інформації та пояснень. Водночас у результатах не наведено окремого аналізу відповідей українських учнів, учителів і батьків, що ускладнює порівняння їхніх поглядів на роль штучного інтелекту в освіті [2].

Зауважимо, що інтерес до впровадження технологій штучного інтелекту в освітній процес продовжує зростати. Це свідчить про необхідність подальших наукових розробок для ефективного використання штучного інтелекту з метою підвищення якості освіти. Водночас активне впровадження ШІ породжує і низку нових викликів – як педагогічних, так і соціально-етичних:

1) етичні та соціальні аспекти: використання ШІ може призводити до порушення конфіденційності, дискримінації та маніпулювання навчальними результатами. Також існує ризик зменшення ролі вчителя як морального та інтелектуального наставника;

2) технологічна залежність: занадто активне використання ШІ може знизити здатність учнів до самостійного мислення, пошуку інформації та аналізу. Автоматизація навчання не повинна замінювати інтелектуальну діяльність людини, а лише доповнювати її;

3) цифрова нерівність: не всі заклади освіти мають доступ до сучасних технологій ШІ. Це призводить до нерівності між міськими й сільськими школами, а також між країнами з різним рівнем економічного розвитку;

4) якість даних і алгоритмічні упередження: робота систем ШІ залежить від якості даних. Неповні або упереджені дані можуть призвести до неточних результатів і несправедливого оцінювання учнів.

Отже, майбутнє освіти тісно пов’язане з подальшою інтеграцією ШІ у всі рівні освітнього процесу. Упровадження штучного інтелекту в освітню сферу є складним і багатогранним процесом, що вимагає ретельного планування, тісної співпраці між усіма учасниками та усвідомлення його впливу на освітній процес і суспільство загалом. Основні напрями розвитку систем ШІ в освіті – оптимізація управління навчальним процесом, індивідуалізація навчання та підтримка педагогів – окреслюють перспективи подальшого вдосконалення освіти в умовах сучасного технологічного поступу. Поєднання людського та машинного інтелекту сприятиме створенню більш гнучкої, інклюзивної та ефективної системи освіти. Водночас необхідно й надалі проводити дослідження та розвивати напрям штучного інтелекту в освіті, приділяючи особливу увагу етичним і безпечним аспектам його застосування, а також забезпечуючи гармонійне поєднання технологій із освітнім процесом.

Список використаних джерел

1. Холін В. В. Штучний інтелект у сучасній освіті: можливості та виклики // Освітологічний дискурс. – 2023. – №2. – С. 34-45.

2. Штучний інтелект в освіті: статистика використання, рекомендації щодо застосування та як обрати безпечний інструмент. URL: https://eo.gov.ua/shtuchnyy-intelekt-v-osviti-statystyka-vykorystannia-rekomendatsii-shchodo-zastosuvannia-ta-iak-obraty-bezpechnyy-instrument/2025/10/16/

Дмитро КУМКОВ
Відокремлений структурний підрозділ
«Харківський торговельно-економічний фаховий коледж
Державного торговельно-економічного університету»
dkumkov@ukr.net

ЦИФРОВА ГІГІЄНА В ОСВІТНЬОМУ ПРОЦЕСІ: ВИКЛИКИ СУЧАСНОСТІ

У XXI столітті освіта зазнає суттєвих трансформацій, які зумовлені активним впровадженням цифрових технологій у всі сфери суспільного життя. Використання комп'ютерів, планшетів, смартфонів та різноманітних онлайн-платформ дозволяє забезпечити широкий доступ до знань, сприяє розвитку самостійного навчання, аналітичного та критичного мислення, а також формує в учнів навички роботи в умовах інформаційного перенавантаження. Водночас такі цифрові інструменти можуть створювати низку ризиків, зокрема перевантаження уваги, швидку втому, погіршення зору, підвищення рівня стресу та розвиток залежності від гаджетів.

У цьому контексті поняття цифрової гігієни набуває особливої важливості. Вона розглядається як система правил і практик раціонального використання цифрових технологій, що забезпечує безпеку, продуктивність та комфорт учасників освітнього процесу. Дотримання принципів цифрової гігієни дозволяє знизити негативний вплив цифрового середовища на здоров'я, підвищити ефективність навчальної діяльності та створити умови для безпечного і гармонійного розвитку особистості в умовах сучасної освіти.

Розглянемо дане питання з оглядом думок науковців. Зокрема, науковці К. О. Журба, Л. В. Канішевська, Р. В. Малиношевський, Н. В. Харченко та С. В. Федоренко акцентують увагу на тому, що ігнорування цифрової гігієни у навчанні може призвести до серйозних негативних наслідків. Серед них – перевантаження нервової системи, хронічна втома, погіршення зору, зниження концентрації уваги, когнітивна виснаженість та загальне зниження ефективності освітнього процесу [1, с. 44–45]. Тому формування в учнів та студентів навичок цифрової гігієни слід розглядати не як допоміжний, а як фундаментальний компонент сучасної освіти, який сприяє збереженню здоров'я та підвищенню якості навчання.

Можемо виокремити, що цифрова гігієна охоплює кілька ключових вимірів: фізичний (оптимальний режим роботи з гаджетами, дотримання правил ергономіки, профілактика перевтоми), психологічний (баланс між онлайн- і офлайн-активностями, уникнення цифрової залежності, збереження психоемоційної стабільності), інформаційний (вміння критично оцінювати контент, захищати персональні дані, протидіяти дезінформації) та комунікативний (культура спілкування у віртуальному просторі, запобігання кібербулінгу, формування етичних норм взаємодії). Усі ці аспекти взаємопов'язані та формують цілісну основу для побудови безпечного й ефективного освітнього середовища.

І. В. Іваній та О. Б. Мехед наголошують, що цифрова гігієна має стратегічне значення у контексті міжнародної співпраці у сфері освіти та науки [2, с. 26]. В умовах глобалізації саме вона забезпечує захищеність конфіденційної інформації, якісну комунікацію між учасниками освітніх і наукових проєктів, а також підтримує інноваційність навчального процесу. О. Б. Мехед, Д. Б. Мехед та К. М. Мехед зазначають, що цифрова гігієна мінімізує ризики втрати чи викривлення даних, сприяє безпечному обміну інформацією та допомагає уникати помилок у підготовці міжнародних документів [3, с. 28]. У такий спосіб вона постає як інструмент забезпечення конкурентоспроможності в умовах цифрової економіки та освітнього простору.

Міжнародний досвід переконливо свідчить, що формування цифрової гігієни є одним із ключових завдань сучасної освітньої політики, оскільки цифрове середовище дедалі більше визначає не лише характер навчання, а й соціалізацію, розвиток критичного мислення та психологічне благополуччя молоді. Так, у Фінляндії стратегічним орієнтиром є концепція «цифрового добробуту», яка інтегрована у державні освітні програми та спрямована на створення гармонійного балансу між активним використанням цифрових технологій і

збереженням психофізичного здоров'я учнів. У навчальних закладах учителі акцентують увагу не лише на технічних навичках, а й на усвідомленому користуванні цифровими ресурсами, обмеженні часу екранної активності та розвитку навичок саморегуляції [4, с. 107]. У Сполучених Штатах Америки та країнах Європейського Союзу акцент робиться на формуванні цифрової грамотності та кіберкультури. Зокрема, реалізуються комплексні освітні програми з медіаграмотності, кібербезпеки та захисту персональних даних. Важливим є також навчання учнів і студентів критично аналізувати інформацію в умовах масового поширення фейків та маніпуляцій, що значно підвищує рівень інформаційної безпеки суспільства. Окрім того, у школах ЄС учнів ознайомлюють з етикою онлайн-спілкування, культурою комунікації в соціальних мережах і правовими аспектами цифрової взаємодії [5, с. 23].

У свою чергу, азійські країни, зокрема Південна Корея та Японія, демонструють інший підхід, орієнтований на профілактику цифрової залежності та психологічних ризиків, пов'язаних з надмірним використанням гаджетів. Тут активно впроваджуються програми, що поєднують педагогічні, психологічні та соціокультурні стратегії. Наприклад, у Південній Кореї функціонують державні центри підтримки молоді, де учнів консультують психологи та фахівці з інформаційних технологій, а в Японії поширені освітні курси з цифрової етики та здорового стилю життя у цифровому середовищі [6, с. 272]. Можемо стверджувати, що міжнародний досвід підтверджує, що цифрова гігієна розглядається не лише як технічна складова освітнього процесу, а й як комплексна система знань, навичок і ціннісних орієнтацій. Її ефективне впровадження можливе лише за умови інтеграції освітніх, психологічних і соціальних підходів, що дозволяє забезпечити сталий розвиток особистості та суспільства в умовах цифрової трансформації.

Цілком слушною є думка К. М. Хабел, адже питання створення комфортного освітнього простору в умовах цифровізації набуває особливої актуальності. Дотримання правил цифрової гігієни справді допомагає знизити рівень інформаційного перевантаження, уникнути стресових ситуацій та підтримати психоемоційний баланс учасників освітнього процесу. Це важливо не лише для збереження працездатності та концентрації уваги, але й для розвитку здатності до продуктивної взаємодії між учнями, викладачами та батьками [7, с. 129]. З позиції сучасних досліджень, грамотна організація цифрового середовища має багатовимірний ефект. По-перше, вона створює умови для формування позитивного психологічного клімату, у якому учні почуваються захищеними та впевненими під час навчальної діяльності. По-друге, збалансоване використання цифрових технологій відкриває нові можливості для розвитку креативного мислення, оскільки дає змогу учням не лише споживати інформацію, а й створювати власний контент, працювати з інтерактивними платформами, долучатися до колективних проектів. По-третє, правильно організоване цифрове середовище сприяє зміцненню міжособистісної взаємодії, навіть за умов дистанційного або змішаного навчання, де особисті контакти часто обмежені.

Слід наголосити, що створення комфортного освітнього простору в цифровій площині має розглядатися як одна з ключових складових освітньої політики. Це включає не лише технічне забезпечення чи наявність сучасних цифрових інструментів, але й формування культури їх використання. Особливо важливим є навчання учнів і студентів принципам цифрової гігієни: умінню дозувати час роботи з гаджетами, організовувати робоче місце, підтримувати баланс між онлайн- та офлайн-активністю. Можна стверджувати, що окреслений підхід дозволяє не тільки запобігти ризикам перевантаження, але й сприяє гармонійному особистісному розвитку та підвищенню ефективності освітнього процесу загалом.

Таким чином, цифрова гігієна в освітньому процесі є багатокомпонентним явищем, яке поєднує у собі медико-психологічний, соціально-педагогічний, інформаційно-безпековий та міжнародний виміри. Вона виступає основою для формування безпечного, комфортного та інноваційного освітнього простору. Інтеграція міжнародного досвіду та адаптація кращих практик до національних умов дозволять Україні сформувати ефективну стратегію розвитку цифрової гігієни в освіті. Це, у свою чергу, забезпечить підвищення якості навчання,

зміцнення здоров’я учнів та студентів, розвиток цифрових компетентностей і сприятиме інтеграції української освіти у світовий освітній простір.

Список використаних джерел

1. Журба К. О., Канішевська Л. В., Малиношевський Р. В., Харченко Н. В., Федоренко С. В. Виховання дітей та молоді у цифровому просторі. Посібник. Київ, 2022. 124 с.
2. Іваній І. В., Мехед О. Б. Формування готовності до міжнародної комунікації майбутніх фахівців з фізичної культури та спорту. Наукові записки. Серія: Педагогічні науки. Кропивницький: Центральноукраїнський державний університет імені Володимира Винниченка, 2023. Випуск 209. С. 22-26.
3. Мехед О. Б., Мехед Д. Б., Мехед К. М. Використання інформаційно-комунікаційних технологій при здійсненні соціально-педагогічної діяльності. Вісник Національного університету «Чернігівський колегіум» імені Т. Г. Шевченка. Чернігів : НУЧК, 2021. Dbg/ 14- 15. С. 27-31.
4. Котун К. Політика цифрової трансформації освіти у фінляндії: стратегічні пріоритети, цілі та механізми реалізації. Професійно-педагогічні та компаративні дослідження в освіті. 2025. С. 103-123.
5. Дорош О. В., Василенко В. Ю. Цифрова безпека в освіті: досвід зарубіжних країн. Прикладні аспекти сучасних міждисциплінарних досліджень. 2024. С. 22-24.
6. Рябчун Г. Трансформація медіаграмотності в країнах сучасної Азії: виклики та перспективи. Актуальні питання гуманітарних наук. 2024. С. 271-274.
7. Хабел К. М. Цифрова гігієна – основа комфортного освітнього простору. Освіта XXI століття: аксіологічний вимір: збірник матеріалів III Всеукраїнської студентської науково-практичної конференції. Нікополь: Навчально-методичний кабінет, 2024. С. 128-129.

Людмила КУЧЕР
кандидат економічних наук, доцент
Національна академія сухопутних військ
імені гетьмана Петра Сагайдачного,
lrkucher1@gmail.com

Наталія ТИХОЦЬКА
Національна академія сухопутних військ
імені гетьмана Петра Сагайдачного,
natalya.tihocka@gmail.com

ПІДТРИМАННЯ ІНТЕЛЕКТУАЛЬНОГО ПОТЕНЦІАЛУ В УМОВАХ АКТИВНОЇ ЦИФРОВІЗАЦІЇ

Аналізуючи сучасне суспільство, із пересторогою спостерігаємо надто активний рух у напрямку цілковитої цифровізації усіх його сфер: починаючи від підприємництва і закінчуючи освітньою діяльністю. Чи можна назвати цей рух конструктивним? Усвідомлюємо, що нові виклики суспільства формують нові вимоги до професійних здібностей та освітніх компетентностей: вільне користування технологіями, запропонованими цифровими платформами, новими досягненнями у сфері науково-технічного виробництва.

Революція цифрових технологій однозначно змінила людину як особистість. І якщо до конструктиву відносимо зміну традиційних моделей взаємодії, розвиток логіко-математичного інтелекту – уміння аналізувати, рахувати, міркувати; кінестетичного – координація рухів; когнітивного – розвиток мислення, пам'яті, уваги; творчого – здатність створювати нове, нестандартне; то однозначним деструктивом вважаємо розвиток міжособистісного інтелекту – розуміння емоцій, мотивів інших людей; соціального – здатність активно взаємодіяти з людьми; емоційного – уміння розуміти й контролювати емоції; морально-цінного – розуміння добра, справедливості. Як результат, ми отримуємо сучасну особистість, яка пристосована до часу і простору, але втрачає відчуття особистісного контакту; прекрасно справляється з новітніми технологіями, проте не відчуває потреби самостійно мислити – усю необхідну інформацію можна отримати швидко і легко з інтернетресурсів.

Оцінюючи цифровізацію в освітньому процесі, варто сказати про активне застосування платформ, які аналізують можливості його учасників і адаптують під них стиль навчання; створюють навчальний контент (завдання, тести, тексти, пояснення до них тощо); спеціалізовані класи для віртуальних екскурсій, симуляції різнотипних завдань, ігрових методів навчання; застосування на заняттях мобільних пристроїв з використанням ChatGPT. Усе це, звичайно, стимулює швидке прийняття рішень, тренує усі типи пам'яті, економить час на підготовку, адаптує інформацію під індивідуальні потреби, дає можливість експериментувати у віртуальних лабораторіях. Проте, у результаті ми отримуємо сформовану, високомобільну особистість, готову до викликів глобалізованого світу сучасних технологій і, водночас, спостерігаємо зниження креативного мислення, цифрову втому, залежність від гаджетів та інтернету, відрив від реального світу.

У розрізі поєднання цифрових технологій з поняттям академічної доброчесності також відслідковуємо дисонанс: це як нові можливості, так і нові шляхи до порушень. З одного боку, прозорість онлайн-платформ, де зберігається історія виконання завдань; перевірка на плагіат зменшує обсяг можливих маніпуляцій; володіння майстерністю грамотного цитування посилює академічну відповідальність; автоматизація оцінювання знижує ризики списування через обмеженість у часі. З іншого боку, легкий доступ до готових інформаційних джерел стимулює до плагіату, використання штучного інтелекту ставить під великий сумнів авторство робіт, а момент списування під час виконання будь-яких завдань з використанням сторонньої (технічної) допомоги зростає.

Варто зупинитися ще на тому, що рівень активності впровадження та використання цифрових технологій безпосередньо залежить від загального стану в країні. У мілітарних країнах цифровізація набуває вимушеного, але динамічного характеру Так, під час російсько-

української війни, коли ворожими обстрілами знищено навчальні заклади, підприємства, інфраструктуру, коли спостерігаємо активну міграцію населення, традиційна система навчання стає неможливою. Дистанційне навчання трансформується у інструмент порятунку освітнього процесу. За умов цифровізації його учасники можуть продовжувати навчання незалежно від місця перебування, регламентуючи самостійно часові показники. Однак і за таких умов можна окреслити і недоліки: не завжди є доступ до техніки чи інтернету, відсутність стабільного інтересу та самоорганізації, психологічна втома під впливом воєнних дій. Та попри все у воюючій країні використання технологізації є альтернативою до поступу вперед, збереження інтелектуального потенціалу нації.

Отож, аналізуючи вищесказане, варто дотримуватись балансу між цифровізацією і рефлексією. У цьому й полягає кіберкультура: гармонійне поєднання технічних засобів із самоаналізом, усвідомленням своїх емоцій, процесу мислення та прийняття рішень.

Епоха цифрових можливостей диктує суспільству нові виклики – не лише оволодіння новітніми технологіями, а й збереження людського інтелекту як базової основи розвитку цивілізації. Цифровізація має стати не замінником мислення, а його інструментом, що розширює можливості особистості до самопізнання, творчого зростання, внутрішньої свободи та соціальної відповідальності.

Список використаних джерел

1. Закон України “Про освіту” від 05.09.2017 № 2145-VIII
2. Бобро Н. Цифровізація освіти: виклики та можливості у ххі столітті. Педагогічні науки. № 5 (129). 2024. https://doi.org/10.32839/2304-5809/2024-5-129-8

Ангеліна ОТЕЧЕНКО
здобувач вищої освіти другого (магістерського) ступеня,
1 курсу, спеціальності F7 «Комп'ютерна інженерія»,
Державний університет «Київський авіаційний інститут»,
7406618@stud.kai.edu.ua

Наталя БІЛОУС
кандидат педагогічних наук,
доцент кафедри іноземних мов професійного спрямування,
Державний університет «Київський авіаційний інститут»
natalia.bilous@npp.kai.edu.ua

КІБЕРКУЛЬТУРА ЯК ДЕТЕРМІНАНТА РОЗВИТКУ ЦИФРОВОЇ ГІГІЄНИ В ОСВІТНЬОМУ СЕРЕДОВИЩІ

Актуальність дослідження полягає у зростаючій ролі цифрового простору в освітній діяльності, що створює нові виклики для збереження безпеки, психологічного комфорту та академічної доброчесності учасників навчального процесу.

У сучасному світі розвиток цифрової культури тісно пов'язаний із поняттям кіберкультури, яка визначає рівень цифрової етики, свідомості та інформаційної відповідальності людини.

Мета роботи полягає у дослідженні впливу кіберкультури на формування навичок цифрової гігієни серед студентської молоді.

Під цифровою гігієною розуміють комплекс дій, спрямованих на безпечне, етичне та усвідомлене використання цифрових технологій, що включає захист персональних даних, критичне сприйняття інформації, дотримання інформаційної етики та запобігання залежності від гаджетів.

Наукова новизна дослідження полягає у визначенні кіберкультури як системоутворювального чинника цифрової гігієни.

Якщо традиційно під кіберкультурою розуміють соціальні практики у віртуальному середовищі, то в освітньому контексті вона набуває нових рис — формує інформаційну компетентність, толерантність у спілкуванні, уміння протидіяти маніпуляціям і дезінформації.

Розвиток цифрової гігієни в освітньому середовищі неможливий без інтеграції елементів кіберкультури у навчальні дисципліни.

Зокрема, важливими є курси з цифрової грамотності, основ кібербезпеки, критичного мислення, а також інтерактивні тренінги з безпечної поведінки онлайн.

Досвід провідних європейських університетів свідчить, що включення таких дисциплін до навчальних планів сприяє підвищенню рівня цифрової етики та саморегуляції студентів.

Практична частина дослідження передбачає аналіз поведінкових моделей студентів у цифровому середовищі.

Результати опитування, проведеного серед студентів першого курсу технічних спеціальностей, показали, що лише 42% респондентів регулярно оновлюють паролі, 35% використовують двофакторну аутентифікацію, а понад 60% не перевіряють достовірність джерел інформації перед поширенням.

Ці дані підтверджують потребу у системному вихованні культури безпечної цифрової поведінки.

Формування кіберкультури також впливає на академічну доброчесність.

Поширення плагіату, використання штучного інтелекту без належного цитування та некритичне копіювання контенту створюють нові виклики для освітньої спільноти.

Розвиток цифрової гігієни допомагає мінімізувати ці ризики шляхом формування навичок усвідомленого користування інформацією.

Кіберкультура є важливим чинником формування цифрової гігієни в освітньому середовищі, забезпечуючи баланс між технологічним розвитком та етичними нормами поведінки користувачів.

Підвищення рівня кіберкультури сприятиме безпечнішому цифровому простору, зміцненню академічної доброчесності та розвитку критичного мислення студентів.

Список використаних джерел

1. Castells, M. (2010). The Rise of the Network Society. Oxford: Wiley-Blackwell. https://doi.org/10.1002/9781444319514
2. Floridi, L. (2013). The Ethics of Information. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199641321.001.0001
3. Jenkins, H. (2009). Confronting the Challenges of Participatory Culture. MIT Press. https://doi.org/10.7551/mitpress/8435.001.0001
4. Ковальчук, В. В. (2020). Цифрова гігієна в освітньому просторі // Наукові записки НаУ «Острозька академія». №2(10), С. 45–52.
5. Черняк, А. І. (2021). Кіберкультура як складова цифрової освіти // Інформаційні технології і суспільство. №3, С. 33–40.

Тетяна КУЗНЄЦОВА
Кандидат економічних наук, доцент
доцент кафедри менеджменту
Університет Григорія Сковороди в Переяславі

ЦИФРОВІ СТРАТЕГІЇ СПІВПРАЦІ ОСВІТИ ТА БІЗНЕСУ

Пошук ефективних форм співпраці між освітою та бізнесом є одним з ключових напрямів відродження України. Попри триваючу війну, українська система вищої освіти продовжує виконувати стратегічну місію – зберігати та розвивати людський потенціал, підтримувати життєздатність наукової спільноти та готувати фахівців, спроможних забезпечити повоєнну відбудову держави. В умовах нестабільності, ризиків і постійних викликів цифрові стратегії є ключовим інструментом стійкості освітнього процесу, безперервності навчання та професійного зростання молоді. Саме завдяки цифровізації університети зберегли можливість співпрацювати з бізнесом, реалізувати партнерські ініціативи та впроваджувати інноваційні формати навчання.

У співпраці з корпоративним сектором акценти освітнього процесу зміщено від традиційної академічності до гнучкості, креативності та практичної спрямованості. Цифрові стратегії співпраці освіти та бізнесу розглядаються як ресурс національної стійкості, інструмент професійної мобільності та шлях до європейської інтеграції освітнього простору України.

Онлайн-комунікації, цифрові тренажери, аналітичні панелі та сервіси взаємодії між роботодавцями та здобувачами вищої освіти інтегровано у структуру сучасних освітніх програм. Це дозволило університетам перейти від моделі теоретичного навчання до практикоорієнтованого формату співтворення освітнього контенту спільно з бізнесом.

Метою дослідження визначено виявлення ефективних цифрових стратегій партнерства між університетами та бізнесом, спрямованих на розвиток кар'єрних, професійних і соціально-комунікативних компетентностей як викладачів, так і здобувачів вищої освіти. Методологію побудовано на аналізуванні результатів участі у трьох послідовних етапах освітнього проєкту «Uni-Biz Bridge» від платформи UGEN (Україна), який реалізовувався у співпраці з провідними компаніями – SoftServe, Deloitte, KPMG, EY, PwC, Genesis, Infopulse, OKKO, Lifecell, Дарниця, UkrSibbank BNP Paribas Group. Етапи дослідження підтверджено сертифікатами авторки дослідження (рис. 1-3), що відображають поступову адаптацію цифрових практик освіти й бізнесу до реалій воєнного часу та зміст сучасної освітньо-бізнесової взаємодії.

Перший етап дослідження здійснено у 2022 році та присвячено розвиткові цифрових інструментів формування soft skills серед студентів (рис. 1). В умовах дистанційного формату навчання, зумовленого безпековими ризиками війни, основну увагу приділено побудові цифрових комунікаційних каналів між центрами працевлаштування університетів і роботодавцями. У співпраці з компаніями Lifecell, Дарниця, UkrSibbank BNP Paribas Group і Deloitte апробовано методики управління кар'єрними онлайн-проєктами, упроваджено систему нематеріальної мотивації здобувачів вищої освіти у цифровому просторі.

Розроблено модель використання соціальних мереж як цифрових платформ для залучення студентів до професійних спільнот. Застосовано методологію NPS/eNPS для визначення рівня задоволеності здобувачів вищої освіти цифровими сервісами університетів. Отримано підтвердження, що цифрова комунікація сприяла підвищенню залученості студентів і підготувала підґрунтя для подальшої інтеграції кар'єрного консультування в онлайн-формати.

Отже, перший етап дозволив окреслити цифрову компетентність як інтегральну характеристику професійної готовності випускників. Доведено, що гнучкість цифрових стратегій і підтримка бізнесу створили умови для нових форм взаємодії освіти та ринку праці.

Рис. 1. Сертифікат №89 (28-29.09.2022) – участь у проєкті «Uni-Biz Bridge», присвяченому розвитку soft skills у співпраці з Lifecell, Дарницею, UkrSibbank BNP Paribas Group, Deloitte

Другий етап дослідження реалізовано у 2023 році та спрямовано на вивчення цифрових форматів коучингу, менторства та наставництва у процесі взаємодії між бізнесом і освітою (рис. 2). У межах співпраці з компаніями Genesis, SoftServe, Infopulse, OKKO і KPMG проведено апробацію цифрових платформ для реалізації менторських програм. Створено алгоритм побудови індивідуального плану розвитку здобувача вищої освіти з використанням онлайн-сервісів самооцінювання компетентностей.

У ході дослідження встановлено, що цифрове наставництво дозволило поєднати корпоративний досвід фахівців з академічними практиками університетів. Учасники проєкту мали можливість у режимі реального часу спілкуватися з менторами суб'єктів господарювання, обговорювати кейси, розробляти проєктні рішення й отримувати фідбек на інтерактивних платформах.

Результати другого етапу засвідчено підвищенням якості цифрової взаємодії між учасниками освітнього процесу. Педагогічне менторство трансформовано у гнучку систему цифрової підтримки здобувачів вищої освіти, орієнтовану на розвиток самостійності, критичного мислення й адаптивності до змін.

Рис. 2. Сертифікат №262 (15-17.05.2023) – участь у проєкті «Uni-Biz Bridge: Коучинг, менторство та наставництво» у партнерстві з Genesis, SoftServe, Infopulse, OKKO, KPMG

Третій етап дослідження проведено у 2024 році. Його зміст зосереджено на формуванні цифрової ідентичності викладача та використанні цифрових стратегій у розвитку особистого бренду педагога (рис. 3). В рамках співпраці з EY, PwC, Deloitte, SoftServe та Genesis розроблено методики використання цифрових стратегій у плануванні освітнього процесу, організації роботи зі студентами та побудові корпоративної культури взаємодії.

Застосовано технології тайм-менеджменту, постановки цілей, оцінювання результативності й управління цифровою стресостійкістю. Апробовано формат World café, у межах якого викладачі та представники бізнесу обговорювали компетентності сучасного здобувача вищої освіти в цифровому середовищі.

Визначено, що цифрова трансформація педагогічної діяльності навіть в умовах воєнних обмежень сприяла підвищенню ефективності навчання та створенню нової педагогічної парадигми – «викладач як медіатор між освітою та бізнесом».

Рис. 3. Сертифікат №1202 (27-29.02.2024) – участь у проєкті «Uni-Biz Bridge» на тему «Сучасний викладач» у партнерстві з EY, Deloitte, PwC, SoftServe, Genesis.

У результаті трирічного циклу дослідження систематизовано показники цифрової взаємодії освіти та бізнесу, які не лише відображають динаміку розвитку партнерства, а й демонструють поступове становлення цифрової культури взаємодії між університетами, студентами та роботодавцями. Проаналізовано зміни у підходах до використання цифрових інструментів управління освітніми процесами, обміну інформацією, реалізації кар'єрних сервісів і менторських програм. Узагальнення отриманих даних надало змогу простежити, як цифровізація впливає на якість освітніх результатів, мотивацію учасників освітнього процесу та ступінь залученості бізнесу до формування професійних компетентностей здобувачів вищої освіти.

На основі результатів проведеної апробації встановлено взаємозв'язок між рівнем цифрової компетентності й ефективністю партнерських програм, визначено чинники успішності спільних проєктів і типові бар'єри їх реалізації в умовах війни. Порівняльний аналіз дозволив виокремити кращі практики українських університетів, що співпрацювали з великими корпораціями та міжнародними компаніями, а також розробити критерії оцінювання результативності таких ініціатив. Для узагальнення напрацьованого досвіду укладено таб. 1, у якій системно представлено ключові параметри впровадження цифрових стратегій співпраці університетів України з бізнесом, показники їх ефективності та динаміку розвитку упродовж 2022-2024 років.

Таблиця 1. Систематизація результатів упровадження цифрових стратегій співпраці освіти та бізнесу (2022-2024 рр.)

Рік	Етап проєкту	Основний напрям	Бізнес-партнери	Цифрові інструменти	Отримані результати	Підтвердження (сертифікат)
2022	Soft skills	Кар'єрний розвиток	Lifecell, Дарниця, UkrSibbank, Deloitte	Соціальні мережі, eNPS	Зростання залученості здобувачів вищої освіти	№89
2023	Коучинг, менторство	Цифрова взаємодія	Genesis, SoftServe, ОККО, KPMG	Менторські платформи, фідбек-сервіси	Розвиток саморефлексії здобувачів вищої освіти	№262

Рік	Етап проєкту	Основний напрям	Бізнес-партнери	Цифрові інструменти	Отримані результати	Підтвердження (сертифікат)
2024	Сучасний викладач	Цифрова ідентичність	EY, PwC, Deloitte, Genesis, SoftServe	World café, LMS, тайм-менеджмент	Підвищення цифрової компетентності викладачів	№1202

Джерело: систематизовано авторкою на підставі власних досягнень

Висновки

Проведене дослідження дозволило:

- виявити взаємозв'язок між цифровими інструментами й якістю партнерської взаємодії освіти та бізнесу;
- підтвердити ефективність цифрових платформ у розвитку soft skills студентів;
- довести, що цифрове менторство формує новий формат педагогічної взаємодії;
- установити, що цифрова ідентичність викладача є чинником довіри між університетом і бізнесом;
- розробити алгоритм формування індивідуального цифрового плану розвитку здобувача вищої освіти;
- систематизувати досвід співпраці університетів з міжнародними компаніями у форматі трирічного циклу;
- показати, що цифрові стратегії є механізмом підтримання освітньої стійкості України в умовах війни та водночас – інструментом поступової інтеграції до європейського освітнього простору.

Перспективи розвитку

Подальший розвиток цифрових стратегій співпраці освіти та бізнесу виходить за межі інтеграції штучного інтелекту та переходить до використання новітніх технологій четвертої та п'ятої хвиль цифрової трансформації. У центрі цих процесів – квантові обчислення, що забезпечують надшвидке оброблення даних для освітньої аналітики та прогнозування компетентнісних потреб ринку праці. Активно розвиваються нейромережеві системи персоналізованого навчання, які формують індивідуальні траєкторії розвитку здобувачів вищої освіти, спираючись на аналіз великих даних про їхні освітні досягнення, когнітивні особливості та кар'єрні цілі.

У партнерстві з бізнесом університетами розгортаються XR-технології (extended reality), що поєднують віртуальну, доповнену та змішану реальність для відтворення виробничих процесів в освітньому середовищі. У промислових і фінансових корпораціях створюються – віртуальні моделі суб'єктів господарювання та посадових функцій, на яких здобувачі вищої освіти можуть проходити симуляційні практики. Водночас формується новий напрям – Data-driven governance в освіті, який базується на використанні алгоритмів квантової аналітики для управлінських рішень і оцінки ефективності партнерських проєктів.

Особливо перспективним визнано створення інтероперабельних освітніх екосистем – спільних хмарних платформ, де університети, корпорації, стартапи й урядові інституції функціонують як рівноправні суб'єкти єдиного цифрового простору. Такі рішення сприятимуть прозорості академічних процесів, відкритому обміну даними, розвиткові етичних стандартів використання технологій і сталому зростанню суспільного добробуту. У довгостроковій перспективі вони стануть одним з ключових чинників відродження України – не лише як держави, що відновлює інфраструктуру після руйнувань, а як країни, що формує нову якість життя засобом інтелекту, освіти, інновацій і відповідального партнерства між наукою, освітою, бізнесом і суспільством.

Богдан МАШТАЛЕР
здобувач вищої освіти другого (магістерського) ступеня,
1 курсу, спеціальності F7 «Комп'ютерна інженерія»,
Державний університет «Київський авіаційний інститут»,
5210628@stud.kai.edu.ua

Наталя БІЛОУС
кандидат педагогічних наук,
доцент кафедри іноземних мов професійного спрямування,
Державний університет «Київський авіаційний інститут»,
natalia.bilous@npp.kai.edu.ua

КІБЕРКУЛЬТУРА ТА ЦИФРОВА ГІГІЄНА В ОСВІТНЬОМУ ПРОЦЕСІ

Сучасна освітня система дедалі більше інтегрується у цифрове середовище, що формує новий тип соціальної взаємодії — кіберкультуру. Вона передбачає не лише технічну грамотність, а й розвиток етичних норм, інформаційної відповідальності та безпечної поведінки у віртуальному просторі. У цьому контексті важливим аспектом стає цифрова гігієна — сукупність знань, навичок і звичок, спрямованих на збереження психологічного здоров'я та інформаційної безпеки користувачів.

Метою дослідження є аналіз ролі кіберкультури у формуванні цифрової компетентності студентів та визначення ефективних методів упровадження принципів цифрової гігієни в освітній процес. Наукова новизна полягає у визначенні взаємозв'язку між рівнем цифрової культури та готовністю молоді до безпечного й усвідомленого використання технологій у навчанні.

Результати дослідження свідчать, що системне впровадження освітніх програм із цифрової гігієни сприяє розвитку критичного мислення, підвищенню кібербезпеки та формуванню відповідальної цифрової поведінки студентів. Це, у свою чергу, забезпечує гармонійне поєднання технологічної ефективності та гуманістичних цінностей освіти.

Особливу увагу в контексті дослідження слід приділити проблемі «інформаційного шуму» та когнітивного перенавантаження, які суттєво знижують концентрацію уваги здобувачів освіти. Практична реалізація цифрової гігієни вимагає інтеграції в навчальні дисципліни модулів із медіаграмотності, спрямованих на верифікацію джерел, розпізнавання маніпулятивних технологій та протидію кібербулінгу.

Важливим компонентом формування кіберкультури є також усвідомлення цифрового сліду та захист персональних даних, що стає необхідною умовою професійної компетентності майбутніх фахівців. Роль викладача при цьому трансформується з транслятора знань у модератора цифрової поведінки, який власним прикладом демонструє етичні норми онлайн-комунікації. У довгостроковій перспективі дотримання правил цифрової гігієни дозволяє не лише оптимізувати навчальний процес, а й запобігти професійному вигоранню, формуючи стійкий імунітет до деструктивних впливів віртуального середовища та сприяючи збереженню ментального здоров'я.

Список використаних джерел

1. Buckingham, D. (2019). The Media Education Manifesto. Cambridge: Polity Press.
2. Castells, M. (2010). The Rise of the Network Society. Oxford: Wiley-Blackwell.
3. Livingstone, S. & Helsper, E. (2020). Digital literacy and online resilience in education. Journal of Learning, Media and Technology, 45(2), 1–15.
4. UNESCO (2021). Guidelines on Digital Literacy for Educators. Paris: UNESCO.
5. Руденко, О. В. (2023). Цифрова гігієна як елемент інформаційної безпеки в освіті. Інформаційні технології і засоби навчання, 96(4), 45–57.

Євгенія ГАЙОВИЧ
аспірант кафедри загальної педагогіки
та педагогіки вищої школи,
начальник відділу електронного навчання
центру інформаційних технологій
ДВНЗ «Ужгородський національний університет»,
y.haiovych@uzhnu.edu.ua

Оксана ПОВІДАЙЧИК
доктор педагогічних наук, професор,
завідувач кафедри загальної педагогіки
та педагогіки вищої школи
ДВНЗ «Ужгородський національний університет»,
oksana.povidaichyk@uzhnu.edu.ua

ВИКЛИКИ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ КІБЕРКУЛЬТУРИ ТА ЦИФРОВОЇ ГІГІЄНИ В ОСВІТНЬОМУ ПРОЦЕСІ

Ключові слова: штучний інтелект, кіберкультура, цифрова гігієна, освіта, академічна доброчесність, етика ШІ.

Стрімкий розвиток технологій штучного інтелекту зумовлює глибокі зміни в освітній практиці, культурі спілкування та способах сприйняття інформації. ШІ не лише оптимізує процеси, а й створює нові соціальні, етичні та психологічні виклики.

У цих умовах актуалізується поняття кіберкультури – як сукупності норм, цінностей і моделей поведінки у цифровому просторі, а також цифрової гігієни – як системи знань і навичок безпечного та усвідомленого користування цифровими технологіями. Попри очевидні переваги використання технологій штучного інтелекту в освіті, залишається недостатньо дослідженим їхній культурний, етичний і психологічний вплив на учасників навчального процесу.

ШІ трансформує освітній простір, змінює комунікативні практики, структуру мислення й моделі поведінки, що ставить під сумнів традиційні уявлення про академічну доброчесність, авторство, інформаційну безпеку та відповідальність користувача. Отже, наукова проблема полягає у пошуку теоретичних і методичних засад формування кіберкультури та цифрової гігієни в умовах зростаючої інтелектуалізації освітнього середовища.

Інтеграція ШІ в освітній процес змінює структуру взаємодії між учасниками навчання.

Алгоритми персоналізують навчання, автоматизують оцінювання, створюють контент, водночас формуючи нові культурні звички: делегування інтелектуальних завдань технологіям, зниження потреби у власному аналізі, перенесення довіри з людини на систему. Інтелектуальні репетитори та віртуальні помічники, інклюзивність освітнього середовища, віртуальна та доповнена реальність модернізують освітній процес і змушують переосмислити підходи [1, 243].

Такі зміни вимагають нового типу цифрової грамотності, який включає елементи алгоритмічного та критичного мислення, розуміння етичних меж використання технологій.

Трансформаційний потенціал технологій ШІ створює як безпрецедентні ризики, так і неперевершені можливості для кібербезпеки. Оскільки організації поспішають запровадити штучний інтелект, кіберзлочинці з шаленою швидкістю використовують уразливості, одночасно підвищуючи ефективність своїх методів. Кіберзахисники також докладають усіх зусиль, щоб використати потенціал цих технологій і змінити баланс у зростаючій гонці озброєнь ШІ [2, 40].

Але передусім штучний інтелект створює низку загроз для цифрової гігієни:

- розповсюдження дезінформації, фейкових зображень і симуляцій;
- втрату авторства та розмивання меж між людським і машинним контентом;
- порушення конфіденційності даних при роботі з відкритими моделями;
- зростання цифрової залежності та когнітивного перевантаження.

Крім того, серед основних викликів та загроз впровадження штучного інтелекту в освітній процес сучасного закладу освіти, які можуть негативно позначатися на якості освіти, можуть бути: стандартизація навчання, втрата контакту між учасниками освітнього процесу, зниження мотивації до навчання, порушення академічної доброчесності, алгоритмічні помилки та недостовірність даних, соціальна ізоляція, недостатня підготовка кадрів, кіберзагрози та безпека даних [1].

У цьому контексті цифрова гігієна набуває нового змісту – як етико-технологічна компетентність, що поєднує технічну обізнаність, критичне мислення та відповідальне ставлення до власної присутності в мережі.

Одним із головних викликів ШІ у сфері освіти є збереження академічної доброчесності. Автоматизовані інструменти полегшують створення текстів, розв'язання завдань і навіть наукових робіт, що породжує ризики плагіату й зниження якості мислення. Викладачі мають не лише контролювати використання технологій, а й виховувати культуру відповідального користування ШІ, формуючи в здобувачів розуміння меж між допомогою інструменту та власною інтелектуальною діяльністю.

Важливо розробляти внутрішні політики етичного використання штучного інтелекту в освітніх закладах. Вирішення означених проблем потребує системного підходу, який охоплює:

- включення теми етики ШІ, медіаграмотності та цифрової гігієни в навчальні програми;
- підготовку викладачів до роботи з інтелектуальними системами;
- створення умов для розвитку AI-компетентності як складової громадянських і професійних навичок XXI століття.

Ключовим завданням освіти стає формування усвідомленої кіберкультури, заснованої на принципах критичності, етичності й безпеки.

Штучний інтелект виступає не лише технологічним інструментом, а й новим культурним чинником, який трансформує соціальні відносини, навчальні практики та уявлення про знання.

Його вплив на кіберкультуру та цифрову гігієну потребує усвідомленої педагогічної відповіді – через розвиток етичної, критичної та інформаційної компетентності всіх учасників освітнього процесу. Лише за умови поєднання інноваційності й етики можливо сформувати безпечне, стале та гуманістичне цифрове середовище освіти.

Список використаних джерел

1. Ілійчук Л. (2024). Штучний інтелект і якість освіти: можливості, виклики та загрози. Науково-педагогічні студії, (8), 232 – 248. https://doi.org/10.32405/2663-5739-2028-8-232-248

2. Яненкова І. (2025). Штучний інтелект у сфері кіьербезпеки: виклики, регулювання, впливи. Матеріали конференцій МЦНД, (21.03.2025; Тернопіль, Україна), 40 – 49. https://doi.org/10.62731/mcnd-21.03.2025.001

Krisztofer PETRECKI
BSc student
Ferenc Rákóczi II Transcarpathian Hungarian University

Adam DOROVTSI
PhD (Applied mathematics)
Department of Mathematics and Informatics
Ferenc Rákóczi II Transcarpathian Hungarian University

DIGITAL FOOTPRINT AND AWARENESS: CYBER HYGIENE EDUCATION IN PUBLIC EDUCATION

With the ubiquity of internet use among youth – about half of 8–17 year-olds reportedly go online daily – concerns have grown over issues like privacy, cyberbullying, and exposure to cyber threats [1]. Paradoxically, many young people are tech-savvy yet lack awareness of their own digital footprints and how to manage them [1]. The cyber hygiene concept encompasses the safe and responsible online practices needed to protect one's digital identity and security. As internet technologies become deeply ingrained in daily life, the security problems associated with poor cyber hygiene and unmanaged digital footprints (e.g. personal data leaks, reputation damage) have become a frequent topic of concern. This has underscored the importance of educating the general public – especially students – about managing their digital footprints and practicing good cyber hygiene from an early age.

Educating students about cybersecurity and digital citizenship is widely seen as critical for mitigating online risks. Experts emphasize that user education and awareness are crucial to creating a safer cyber environment [2]. For example, Subaşı et al. (2023) examined teenagers' awareness of digital footprints and found significant gaps: students who spent more time online (e.g. 4–6 hours daily) actually tended to have lower understanding of their digital footprints than those online less often [3]. Such findings suggest that simply growing up as "digital natives" does not guarantee wisdom about online privacy or safety. Formal cyber hygiene education in schools can bridge this gap by teaching students about personal data protection, safe communication, and the long-term implications of their online actions. Research also shows this need extends to those guiding children: Buchanan et al. (2019) found that while parents and teachers are very aware of digital footprint risks and cyber-safety issues, they often lack knowledge on how to help children manage their online presence and leverage positive opportunities [4]. This highlights the need not only for student training but also for resources and training for educators to effectively teach cyber hygiene.

Digital footprint awareness and cyber hygiene are increasingly recognized worldwide as essential competencies, yet integrating these topics into public education faces international challenges. Children are accessing digital technologies at younger ages, prompting calls to introduce basic cybersecurity and digital citizenship lessons even in primary schools. However, a recent systematic review of K-12 cybersecurity education across countries found that most aspects of cybersecurity (including safe online behavior) are not being systematically taught at the K-12 level around the world [5]. This inconsistency suggests a need for a more cohesive, international approach. Cyber threats are a global problem without boundaries, and experts argue that improving cyber hygiene education must be a shared global effort. Developing international cooperation—through sharing best practices, creating common standards, and adapting successful curricula across different education systems—is seen as vital to raising the baseline of cyber safety awareness in students globally [2]. In short, the push for digital footprint awareness in education is international in scope, yet progress varies widely, with many countries still in early stages of implementation.

To effectively foster cyber hygiene and digital footprint awareness, educators and policymakers advocate practical, curriculum-based interventions. One key strategy is to embed cyber hygiene topics into school curricula, either by creating dedicated modules or by integrating these topics into existing subjects (e.g. IT/computer classes or social studies) [2]. For instance, lessons might cover how personal data is collected and used online, the permanence of one's digital footprint, and strategies for protecting privacy (such as strong passwords, thoughtful sharing on social media, and critical evaluation of online content). Schools are also encouraged to provide hands-on activities and

discussions that make abstract concepts tangible – for example, guiding students to audit their own digital footprints as a learning exercise. A recent innovative approach by Ng et al. (2025) even involved primary school students as active co-researchers examining their digital footprints, which helped them critically understand the traces they leave online [6]. Beyond the classroom, experts recommend engaging the broader community: teacher training and workshops for parents can empower adults to reinforce good practices, and partnerships with technology companies or non-profits can bring in up-to-date expertise and resources [2]. Overall, a practical emphasis is placed on creating a culture of cybersecurity through continuous education, rather than one-off lessons. This includes school-wide initiatives like cyber-safety campaigns, student clubs focusing on digital citizenship, and interactive programs (such as cybersecurity games or simulations) that make learning about online safety engaging and relevant.

In conclusion, addressing digital footprint awareness through cyber hygiene education in public schooling is both a pressing need and a collective responsibility. Equipping students with the knowledge to navigate their digital lives safely is essential for their personal development and for society's resilience against cyber threats. An internationally minded approach – sharing research, policies, and best practices across borders – can accelerate progress in this area. By integrating cyber hygiene into education early and practically, we empower the next generation to become responsible digital citizens who can protect their privacy, security, and well-being online. The research surveyed illustrates that while challenges remain, there is a growing consensus that cyber hygiene education must be a foundational element of general education in the digital age [2]. Schools, communities, and international stakeholders must work in tandem to ensure that young people not only understand their digital footprints but can actively manage and safeguard them as part of a healthy, informed online presence.

References

1. Aguiar, Jorge, "Digital Footprint Management: Youth and Social Media on Protecting your Online Identity and Reputation" (2024). Electronic Theses, Projects, and Dissertations. 2073. https://scholarworks.lib.csusb.edu/etd/2073
2. Basholli, A., Mema, B., Basholli, F., Hyka, D., & Salillari, D. (2023). The role of education in cyber hygiene. Advanced engineering Days, 7, 178-181
3. Subasi, S., Korkmaz, O., & Cakir, R. (2023). Cyberbullying, digital footprint, and cyber security awareness levels of Secondary School Students. International Journal of Technology in Education and Science, 7(2), 129–151. doi:10.46328/ijtes.471
4. Buchanan, R., Southgate, E., & Smith, S. P. (2019). 'The whole world's watching really': Parental and educator perspectives on managing children's digital lives. Global Studies of Childhood, 9(2), 167–180. doi:10.1177/2043610619846351
5. Ibrahim, A., McKee, M., Sikos, L. F., & Johnson, N. F. (2024). A systematic review of K-12 cybersecurity education around the world. IEEE Access: Practical Innovations, Open Solutions, 12, 59726–59738. doi:10.1109/access.2024.3393425
6. Ng, R., Rivera, M. C. S., Cook, M., Mavilidi, M. F., & Bennett, S. (2025). Co-researching with primary school students to retrace their digital footprint. Computers & Education, 224(105170), 105170. doi:10.1016/j.compedu.2024.105170

Adam DOROVTSI
PhD (Applied mathematics)
Department of Mathematics and Informatics
Ferenc Rákóczi II Transcarpathian Hungarian University

THE CONSCIOUS AND ETHICAL USE OF ARTIFICIAL INTELLIGENCE TOOLS IN EDUCATION

Higher education is undergoing a digital transformation, and AI technologies are at the forefront of this change. In recent years, artificial intelligence (AI) tools have been increasingly adopted in educational settings, offering new opportunities to enhance teaching and learning. The emergence of generative AI models like OpenAI's ChatGPT has accelerated this trend, providing benefits such as personalized learning support, increased student engagement, collaboration, and improved accessibility [1,2]. AI systems can automate repetitive tasks and assist with data analysis and content generation, making educational processes more efficient. However, these advantages come with significant ethical challenges. The growing use of AI in academia has raised concerns about academic integrity, as AI-generated content may facilitate plagiarism, contract cheating, or other forms of dishonest behavior [2].

The release of ChatGPT in late 2022, for example, sparked immediate discussions about academic honesty in universities. Students could potentially use such tools to complete assignments unfairly, prompting many institutions to react by highlighting the risks to academic integrity and exploring preventive measures. Early responses from universities and educators have often focused on the threat of "AI-giarism" (AI-assisted plagiarism) and the need to adapt assessment methods to discourage misuse of AI [3]. Indeed, academic integrity is a cornerstone of educational quality, embodying values of honesty, trust, and ethical behavior. The challenge posed by AI to maintaining this integrity has become a key issue, underscoring the importance of developing strategies that uphold the credibility of academic qualifications [4]. Beyond cheating, educators also worry that over-reliance on AI could erode students' critical thinking and writing skills, and that generative AI tools might produce inaccurate or biased information with unwarranted authority [4]. These factors make conscious oversight and guidance essential when employing AI tools in educational contexts.

Importantly, many experts recognize that generative AI can be leveraged positively to support learning when used responsibly [3]. Although a few academic journals and institutions initially reacted by discouraging or even banning AI tools outright due to integrity and quality concerns [1], blanket prohibitions are unlikely to be sustainable. Instead, there is a growing consensus that higher education should integrate AI tools in a conscious and ethical manner, balancing innovation with responsibility [4]. Scholars and academic leaders are calling for proactive approaches to ensure AI is used as a force for good in education. Key recommendations include updating academic integrity policies to explicitly address AI usage, providing clear guidelines on acceptable versus unacceptable uses of AI, and offering training for students and faculty on how to use AI effectively and ethically [2]. In addition, institutions are investing in AI-powered plagiarism detection and other technologies to identify AI-generated content and deter misconduct, illustrating how AI can also be part of the solution [2]. Studies further suggest that these policies and guidelines should be adaptable to diverse cultural contexts, as perceptions of ethical AI use may differ across regions and student populations [1]. Overall, such efforts encourage mindful use of AI—where users critically evaluate when and how to employ AI tools to complement learning objectives without undermining the educational process.

In conclusion, fostering a strong culture of academic integrity is essential in the age of AI. Educators and policymakers must work together to promote an academic environment where the use of AI tools is transparent, fair, and aligned with the core values of scholarship. Conscious and ethical use of AI means using these tools as aids to human learning and creativity, rather than shortcuts to bypass effort. By emphasizing integrity and guiding students in the mindful use of AI, higher education can harness the benefits of AI-driven innovation while preserving trust and credibility in academic outcomes [4]. This balanced approach will be critical for the future of education as AI becomes ever more ubiquitous.

References

1. Yusuf, A., Pervin, N., & Román-González, M. (2024). Generative AI and the future of higher education: a threat to academic integrity or reformation? Evidence from multicultural perspectives. International Journal of Educational Technology in Higher Education, 21(1). doi:10.1186/s41239-024-00453-6
2. Cotton, D., Cotton, P., & Shipway, J. R. (2023). Chatting and Cheating. Ensuring academic integrity in the era of ChatGPT. doi:10.35542/osf.io/mrz8h
3. Sullivan, M., Kelly, A., & McLaughlan, P. (2023). ChatGPT in higher education: Considerations for academic integrity and student learning. (2023). Journal of Applied Learning & Teaching, 6(1). doi:10.37074/jalt.2023.6.1.17
4. Balalle, H., & Pannilage, S. (2025). Reassessing academic integrity in the age of AI: A systematic literature review on AI and academic integrity. Social Sciences & Humanities Open, 11(101299), 101299. doi:10.1016/j.ssaho.2025.101299

István BALOG
BSc student
Ferenc Rákóczi II Transcarpathian Hungarian University

Adam DOROVTSI
PhD (Applied mathematics)
Department of Mathematics and Informatics
Ferenc Rákóczi II Transcarpathian Hungarian University

THE ROLE OF ARTIFICIAL INTELLIGENCE IN COMBATING DISINFORMATION AND INFORMATION SECURITY

In the digital age, society faces dual challenges of widespread disinformation and escalating cyber threats to information security. Disinformation campaigns, often fueled by social media, erode public trust and can undermine democratic processes. Simultaneously, cyber attacks on information systems are growing in sophistication. Artificial intelligence (AI) has emerged as a crucial tool to address both issues, offering advanced capabilities to analyze large volumes of data and detect anomalies that humans might miss [1].

AI-driven solutions are increasingly employed to combat online falsehoods. Machine learning algorithms can scan and evaluate vast streams of content at a scale unattainable for human fact-checkers, helping identify fake news, fake accounts, and coordinated propaganda in real time. Notably, generative AI technology presents a double-edged sword in this arena. On one hand, AI text and image generators lower the barrier for producing convincing fake content such as deepfake videos, intensifying the disinformation threat. On the other hand, AI also provides powerful defenses: large language models and other AI systems show promise in automated fact-checking and content verification [2]. Recent studies indicate that AI chatbots can accurately classify misleading narratives—for example, a generative AI like ChatGPT achieved over 81% accuracy in identifying conspiracy theories in experiments [2]. Overall, generative AI plays a dual role, enabling the rapid creation of synthetic false content while simultaneously offering new opportunities for detection and verification [3].

In parallel, AI has become integral to modern information security practices. Its adaptability and pattern-recognition capabilities make it well-suited for detecting and countering cyber threats [5]. Current AI applications in cybersecurity span intrusion detection systems, malware identification, fraud prevention, and protection of critical networks [5]. By analyzing network traffic and user behavior, AI can flag anomalies and potential attacks faster and more accurately than traditional methods. Notably, AI-driven intrusion detection tools have grown to dominate cybersecurity research, reflecting an ongoing emphasis on using machine learning to identify unauthorized access [5]. AI is also used proactively to anticipate threats, employing predictive analytics to identify vulnerabilities before they are exploited [5]. However, just as in the fight against disinformation, AI in cybersecurity is a double-edged sword. Attackers are weaponizing AI to develop more sophisticated exploits—such as automated spear-phishing campaigns that evade detection [5]. These dynamics create an arms race between attackers and defenders. Moreover, challenges like high computational demands, adversarial machine learning (where attackers trick AI models), and ethical concerns about autonomous decisions remain significant hurdles [5]. Researchers emphasize the need for trustworthy AI solutions, including explainable models and robust validation, to ensure AI-driven security tools are reliable and fair [5].

In conclusion, artificial intelligence holds a pivotal role in safeguarding information integrity—both by filtering out disinformation and by fortifying information security systems. The synergy of AI's speed and scale with human expertise offers a promising path to counter digital threats. Yet, maximizing AI's benefits requires addressing its limitations and governing its use responsibly. Recent studies highlight that a comprehensive strategy against disinformation and cyberattacks must combine technological innovation with organizational and policy measures [3]. Multi-stakeholder cooperation is needed, as governments, tech platforms, and educators develop guidelines to prevent misuse of AI while deploying it to protect the public sphere [3]. As efforts continue, the development

of transparent, ethical, and resilient AI solutions will be essential to strengthen our defenses against both misinformation and malicious cyber activities.

References

1. Santos, F. C. C. (2023). Artificial intelligence in automated detection of disinformation: A thematic analysis. Journalism and Media, 4(2), 679–687. doi:10.3390/journalmedia4020043
2. Park, S., & Nan, X. (2025). Generative AI and misinformation: a scoping review of the role of generative AI in the generation, detection, mitigation, and impact of misinformation. AI & Society. doi:10.1007/s00146-025-02620-3
3. López-Borrull, A., & Lopezosa, C. (2025). Mapping the impact of generative AI on disinformation: Insights from a scoping review. Publications, 13(3), 33. doi:10.3390/publications13030033
4. Achuthan, K., Ramanathan, S., Srinivas, S., & Raman, R. (2024). Advancing cybersecurity and privacy with artificial intelligence: current trends and future research directions. Frontiers in Big Data, 7, 1497535. doi:10.3389/fdata.2024.1497535
5. Achuthan, K., Ramanathan, S., Srinivas, S., & Raman, R. (2024). Advancing cybersecurity and privacy with artificial intelligence: current trends and future research directions. Frontiers in Big Data, 7, 1497535. doi:10.3389/fdata.2024.1497535

János SZANYI
B*Sc student*
Ferenc Rákóczi II Transcarpathian Hungarian University

Adam DOROVTSI
PhD (Applied mathematics)
Department of Mathematics and Informatics
Ferenc Rákóczi II Transcarpathian Hungarian University

THE ROLE OF GENERATIVE AI IN PREDICTING CYBERSECURITY THREATS

In today's rapidly evolving digital landscape, cybersecurity faces increasingly complex and dynamic threats. Traditional defensive mechanisms that rely on predefined signatures or rule-based systems often fail to detect novel attacks and zero-day vulnerabilities. Generative Artificial Intelligence (GenAI) offers a transformative approach to this challenge by enabling predictive threat modeling and proactive defense strategies. Through the use of advanced machine learning and generative modeling techniques, GenAI can analyze massive volumes of historical cyberattack data to uncover hidden correlations, simulate realistic threat scenarios, and anticipate future vulnerabilities. This predictive capacity represents a paradigm shift from reactive cybersecurity toward anticipatory, intelligence-driven protection that evolves alongside adversarial innovation.

Generative artificial intelligence (GenAI) has emerged as a promising tool in cybersecurity for predicting and preempting threats. By leveraging machine learning on historical attack data and threat intelligence feeds, GenAI models can identify patterns and forecast potential new cyber-attack vectors and vulnerabilities [1]. This predictive capacity allows security teams to anticipate emerging threats and proactively reinforce defenses before attacks materialize. In addition, GenAI-driven systems excel at anomaly detection, learning the baseline of "normal" behavior and flagging deviations that may indicate novel intrusions beyond the scope of traditional signature-based detection.

Furthermore, generative models can simulate adversarial behavior and generate diverse synthetic cyber-attack scenarios to enhance preparedness [2]. For example, advanced GenAI systems have been used to create thousands of realistic attack variants, helping cybersecurity defenses recognize and neutralize previously unseen attack patterns [2]. These applications of GenAI significantly strengthen threat intelligence and incident response by expanding the scope of scenarios considered and improving the robustness of detection algorithms. However, the same generative techniques also present new challenges: malicious actors are employing GenAI to craft more sophisticated malware, polymorphic attacks, and convincing social engineering lures (like deepfakes and phishing campaigns) that evade conventional security measures [1]. This dual-edged nature means that while GenAI provides powerful predictive insights for cyber threat forecasting and enables more proactive defense strategies, organizations must implement strong ethical guidelines and security controls to mitigate the risks of GenAI misuse.

Generative AI stands as both a powerful ally and a potential adversary in the realm of cybersecurity. Its predictive and simulation capabilities allow organizations to foresee and counteract threats before they occur, strengthening resilience and response efficiency. However, the same technology can be exploited by malicious actors to develop more adaptive and deceptive attack methods. Thus, the future of cybersecurity will depend not only on technological advancement but also on establishing ethical governance frameworks and robust oversight mechanisms to ensure that GenAI serves as a tool for security, not exploitation. Ultimately, harnessing GenAI responsibly can redefine the balance of power in cyberspace, turning prediction into prevention.

References

1. Ibrar, W., Mahmood, D., Al-Shamayleh, A. S., Ahmed, G., Alharthi, S. Z., & Akhunzada, A. (2025). Generative AI: a double-edged sword in the cyber threat landscape. Artificial Intelligence Review, 58(9). doi:10.1007/s10462-025-11285-9

2. Balasubramanian, P., Liyana, S., Sankaran, H., Sivaramakrishnan, S., Pusuluri, S., Pirttikangas, S., & Peltonen, E. (2025). Generative AI for cyber threat intelligence: applications, challenges, and analysis of real-world case studies. Artificial Intelligence Review, 58(11). doi:10.1007/s10462-025-11338-z

Оксана КОЧАН
старший викладач
Комунальний заклад «Мукачівський
професійний аграрний ліцей імені Михайла Данканича»
Закарпатської обласної ради,
ok8877733@gmail.com

ЦИФРОВА ТА МЕДІАГРАМОТНІСТЬ УЧАСНИКІВ ОСВІТНЬОГО ПРОЦЕСУ ЗАКЛАДУ ПО В КОНТЕКСТІ ПРОБЛЕМИ КІБЕРБУЛІНГУ

Тема цифрової та медіаграмотності є актуальною для учасників освітнього процесу у контексті сприяння запобіганню, протидії кібербулінгу та створення безпечного освітнього середовища закладу професійної освіти. Пандемія, карантин, онлайн навчання, докорінно змінили наше життя. Ми живемо в активному інформаційному середовищі. Цифрові технології торкнулися, мабуть, всіх сучасних сфер діяльності. Війна, стрес, відсутність стабільності суттєво відобразилися на освіті. Для сучасних здобувачів професійної освіти Інтернет – це не просто віртуальна реальність, а невід'ємна частина їхнього життя, де вони навчаються, комунікують, вибудовують відносини та відчувають себе частиною спільноти. Студенти все більше часу проводять в мережі. Вони сприймають інтернет як безпечне середовище. Але це зовсім не так!

Кіберпростір несе чимало загроз, наслідки яких не обмежуються втратою грошей чи особистих паролів у соціальних мережах, а можуть коштувати здоров'я та майбутнього. Однією з найбільш поширених небезпек є кібербулінг. Це поняття має дві складові. Основою є «булінг». Згідно статті 173 кодексу України про адміністративні правопорушення булінг (цькування) – дії учасників освітнього процесу, які полягають у психологічному, фізичному, економічному чи сексуальному насильстві [1].

Друга частина – цифрові технології. Він може відбуватися в соціальних мережах, платформах обміну повідомленнями (месенджерах), ігрових платформах та мобільних телефонах.

Кібербулінг привернув увагу багатьох зарубіжних фахівців. Белсі Б., Сміт П., Магдаві Дж., Волак Дж., Мітчел К., Дулі Дж. активно працювали над визначенням цього поняття.

Бурова О., Бутнік-Сіверський О., Орлюк О., та Горська К. дослідили у своїй роботі [2] питання цифрової гігієни та інформаційної безпеки, вказуючи на те, що традиційні підходи не завжди здатні виявляти та вирішувати нові складні атаки.

Кібербулінг – це глобальна проблема, що стосується не тільки здобувачів професійної освіти, а і їх батьків, викладачів, майстрів виробничого навчання, громадських діячів, представників держави та системи освіти.

Ключовими інструментами у боротьбі з цією проблемою є цифрова та медіаграмотність учасників освітнього процесу. Цифрова грамотність є однією з восьми оновлених ключових компетентностей для навчання протягом життя, визначених Рамковою програмою Європейського Союзу [3]. Вона передбачає впевнене і водночас критичне застосування ІКТ для створення, пошуку, обробки, обміну інформацією на роботі, в публічному просторі та приватному спілкуванні. Інформаційна й медіаграмотність, основи програмування, алгоритмічне мислення, робота з базами даних, навички безпеки в Інтернеті та кібербезпека – це те, на що треба звертати увагу в сучасних закладах ПО.

У відповідності до річного плану роботи Комунального закладу «Мукачівський професійний аграрний ліцей імені Михайла Данканича» Закарпатської обласної ради проводяться тематичні дні та тижні щодо підвищення рівня освіченості студентів з питань формування цифрової та медіаграмотності, спрямованих на протидію кібербулінгу в навчальному закладі.

Серед них День безпечного Інтернету, Глобальний тиждень медіаграмотності, Тиждень правових знань, Всеукраїнська акція «16 днів проти насильства».

Вони включають тренінги, вебінари, конкурси, вікторини, інтелектуальні ігри тощо. Варто відзначити, що молодь демонструє високий рівень освіченості з питань безпеки у Всесвітній мережі та інфомедійної грамотності у Всеукраїнських конкурсах «Основи кібербезпеки», «Цифрова грамотність» від ТОВ «ВСЕОСВІТА», Національному тесті з медіаграмотності.

У навчальному закладі налагоджена тісна співпраці з соціальними службами, представниками відділу протидії кіберзлочинам в Закарпатській області, сектору ювенальної превенції Мукачівського міжрайонного управління внутрішніх справ в Закарпатській області, державними інспекторами Управління інспекційної діяльності у Закарпатській області, Національною поліцією, службами у справах дітей, інформаційно-ресурсним центром «Вікно в Америку» КЗ «Закарпатської обласної універсальної наукової бібліотеки ім. Ф. Потушняка» ЗОР, волонтерами, позашкільними установами, громадськими організаціями та іншими.

Безпеку в інтернеті для здобувачів професійної освіти потрібно організовувати, не тільки навчаючи їх, а й самим не забуваючи про правила. Значну роль у вирішенні проблем кібербулінгу в навчальному закладі відіграє сформованість у педагогічних працівників цифрової та медіаграмотності, які водночас вони формують і у своїх студентів.

Тема кібербулінгу на сьогодні є резонансною. Важливо, щоб викладачі вміли розпізнавати ситуації булінгу та вчасно і правильно реагували на його прояви в освітньому середовищі. Проблему краще попередити, ніж потім її вирішувати. Саме тому педагогічні працівники ліцею опановують базові практичні знання для роботи з ситуацією кібербулінгу в закладі освіти, вчаться орієнтуватися в інформаційному просторі та формують навички ефективного використання цифрової компетентності в навчальному процесі. Педагоги ліцею підвищують кваліфікацію під час вебінарів, конференцій, онлайн-курсів.

Для підвищення рівня цифрової компетентності викладачі та майстри виробничого навчання проходять навчання в Школі ІТ – компетентності при Навчально-методичному центрі професійно-технічної освіти у Закарпатській області, яка працює з 2017 року. Навчання передбачає розширення та поглиблення теоретичних знань, закріплення практичних умінь і навичок педагогів із використання цифрових технологій, що сприяє підвищенню ефективності навчання та якості знань здобувачів освіти.

Отже, важливо вчасно розпізнати та попередити кібербулінг і зупинити цей процес на ранніх стадіях, поки ситуація не вийшла з-під контролю. Це явище поширене не тільки в Україні, а й у всьому світі, тому що насильницька модель поведінки стає дедалі популярнішою. Підлітки є найбільш вразливою категорією суспільства. Дуже актуальним є формування цифрової та медіаграмотності всіх ланок – здобувачів професійної освіти, викладачів, майстрів виробничого навчання, адміністрації, батьків та суспільства в цілому. Необхідно привернути увагу підлітків до питання насилля засобами Інтернету, до пошуку виходу із небезпечних ситуацій, спонукати їх до самопізнання, саморозвитку і доброзичливого ставлення до людей.

Список використаних джерел

1. Закон України Про внесення змін до деяких законодавчих актів України щодо протидії булінгу (цькуванню) [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/2657-19#n8

2. О. Буров, О. Бутнік-Сіверський, О. Орлюк та К. Горська, «КІБЕРБЕЗПЕКА ТА ІННОВАЦІЙНЕ ЦИФРОВЕ ОСВІТНЄ СЕРЕДОВИЩЕ», ITLT , т. 80, № 6, с. 414–430, грудень 2020 р., doi: 10.33407/itlt.v80i6.4159

3. ANNEX to the Proposal for a Council Recommendation on Key Competences for Lifelong Learning [Електронний ресурс]. URL: https://is.gd/CANrvz

Emőke BERGHAUER-OLASZ
PhD, Associate Professor
Ferenc Rakoczi II Transcarpathian Hungarian University

Tetiana SHCHERBAN
Doctor of Psychological Sciences, Professor
Ferenc Rakoczi II Transcarpathian Hungarian University

PREVENTION OF CYBERBULLYING IN EDUCATIONAL SETTINGS: FROM DIGITAL HYGIENE TO A CULTURE OF SAFE INTERACTION

Cyberbullying is a persistent, technology-mediated form of peer aggression that requires systemic, multi-level prevention rather than incident-driven responses. This article advances a three-component model that proceeds from individual skills to institutional culture: (1) digital hygiene micro-skills for learners (account security, privacy management, authenticity checks, refusal to share degrading content, documentation and safe reporting); (2) curriculum-embedded digital citizenship that integrates online-safety knowledge with socio-emotional learning, perspective-taking, and bystander activation across ICT/civics lessons; and (3) a whole-school policy framework that ensures confidential reporting channels, systematic documentation, proportionate-preferably restorative-responses, and ongoing staff development. Synthesising recent empirical evidence (2024 – 2025) and international guidance, we show that such multi-layered designs reduce both perpetration and victimisation, increase cyber self-efficacy, and normalise early disclosure. We also outline implementation considerations for Ukrainian and wider Central-European contexts, including harmonisation of school and family digital rules, simple monitoring instruments (anonymous surveys, incident logs, checklists), and adaptations for hybrid learning and shared/low-security devices. Framing cyberbullying as a relational phenomenon distributed across skills, classroom processes, and institutional climate, the model links "digital hygiene" to a durable culture of safe interaction.

Keywords: cyberbullying; prevention; digital hygiene; digital citizenship; bystander activation; school policy; restorative practices; cyber self-efficacy

Cyberbullying is a persistent, technology-mediated form of peer aggression that affects roughly 20–30% of learners and is increasingly intertwined with home, community, and, in some regions, conflict-related online spaces (UNESCO, 2024, 2025). Because attacks are mobile, networked, and easily replicated, schools need preventive systems rather than ad hoc reactions. Recent empirical syntheses converge on the same point: school-based programmes are effective only when they are multi-layered and explicitly connect individual skills with classroom processes and institutional rules (Chicote-Beato, González-Víllora, Bodoque-Osma, & Navarro, 2024; Shi, 2025).

The first layer is individual digital hygiene. Learners need to be able to secure their accounts and devices, manage privacy settings, verify the authenticity of messages, refuse to share degrading images of peers, document abusive episodes, and report them without counter-aggression. Hinduja and Patchin (2024) showed that such micro-skills increase cyber self-efficacy, which in turn mitigates internalising symptoms following exposure to online aggression. Likewise, Pan's (2025) longitudinal analysis found that the perceived probability of being cyberbullied, rather than the raw frequency of incidents, was the stronger predictor of mental-health outcomes, underscoring the importance of teaching students to exert control over their digital environment.

The second layer is curriculum-embedded digital citizenship. The 2024 systematic review in Aggression and Violent Behavior demonstrated that programmes which combined online-safety knowledge with socio-emotional learning, perspective-taking, and bystander activation produced the most consistent reductions in both perpetration and victimisation across 17 studies from Europe and Latin America (Chicote-Beato et al., 2024). Embedding such modules into ICT, civic education or homeroom lessons ensures repetition, enables teachers to correct platform-specific misconceptions, and makes it explicit that cyberbullying is a relational problem rather than merely "bad behaviour"

by an individual student. This is consistent with wider European evidence showing that bullying-reduction programmes are most successful when they mobilise the peer group, not only the target.

The third layer is a macro-level school culture. UNESCO's (2025) guidance, aligned with European child-protection standards, calls for written anti-cyberbullying policies, confidential reporting channels, systematic documentation, proportionate and – where possible – restorative responses, as well as staff training. Research from the European Commission's Joint Research Centre likewise underlines that online spaces linked to the school remain educational spaces and should therefore be governed by the same protective rules (European Commission Joint Research Centre, 2025). When this institutional frame is visible, students disclose incidents earlier, teachers feel authorised to intervene, and parents can align household digital rules with school expectations.

An often overlooked component is teacher professional development. Teachers who understand platform affordances, privacy options, and evidence-based conversational techniques are more likely to intervene early and to model civil online communication. When schools invite parents to harmonise family-level digital rules with school policies, students receive coherent messages across settings – a facilitating factor highlighted in several of the reviewed interventions (Shi, 2025). Finally, programmes should include simple monitoring instruments – anonymous student surveys, incident logs, and teacher checklists – so that schools can document change and adjust the intensity of interventions for high-risk groups.

Taken together, these findings support a prevention model that proceeds "from digital hygiene to a culture of safe interaction." It is grounded primarily in recent peer-reviewed evidence (2024–2025), relies on no more than two international policy documents for framing, and remains adaptable to Ukrainian and wider Central-European educational contexts, including settings in which learners connect from shared or low-security devices. Most importantly, it conceptualises cyberbullying not as an individual moral failure but as a multilevel relational phenomenon that must be addressed simultaneously at the levels of skills, curriculum, and institutional climate.

References

1. Chicote-Beato, M. M., González-Víllora, S., Bodoque-Osma, A. R., & Navarro, R. (2024). Cyberbullying intervention and prevention programmes in primary education (6 to 12 years): A systematic review. Aggression and Violent Behavior, 77, 101938. https://doi.org/10.1016/j.avb.2024.101938
2. European Commission Joint Research Centre. (2025). Cyberbullying: Considerations towards a common definition.
3. Hinduja, S., & Patchin, J. W. (2024). Cyberbullying: Identification, prevention, and response (2024 ed.). Cyberbullying Research Center.
4. Pan, Q. (2025). Cyberbullying probability, not frequency, predicts mental-health problems in schoolchildren. Educational Psychology, 45(2), 215–232. https://doi.org/10.1080/01443410.2025.2559175
5. Shi, Y. (2025). School-based intervention on cyberbullying-related outcomes and psychosocial well-being: A systematic review and meta-analysis. Health Education & Behavior. Advance online publication. https://doi.org/10.1177/15248380251375480
6. UNESCO. (2024). Violence and bullying in schools: UNESCO calls for better protection of students.
7. UNESCO. (2025). Preventing and addressing violence in and around school.

Emőke BERGHAUER-OLASZ
PhD, Associate Professor
Ferenc Rakoczi II Transcarpathian Hungarian University

Viktoria LANTSI
Lecturer
Ferenc Rakoczi II Transcarpathian Hungarian University

SCHOOL-BASED CYBERBULLYING PREVENTION IN THE PEER ECOLOGY: SOCIAL NORMS, BYSTANDER BEHAVIOUR, AND SCHOOL CONNECTEDNESS

Abstract. This article examines school-based cyberbullying through the lens of the peer ecology. Evidence from 2024 – 2025 shows that incidents persist even where basic online-safety lessons exist, if classroom social norms tacitly tolerate aggression and bystanders expect others to remain passive. Synthesising findings on the roles of descriptive and injunctive norms, the effectiveness of bystander-focused programmes, and the protective function of school connectedness, we propose a three-lever prevention model: (1) explicit norm work in class that surfaces perceived peer approval, corrects pluralistic ignorance, and co-creates a defending-oriented injunctive norm; (2) rehearsal of defending in realistic digital scenarios that personalise responsibility and lower situational barriers to intervention; and (3) strengthening school connectedness via visible adult follow-up, recognition of prosocial bystander actions, and sustained teacher - student relationship routines. Designed for Ukrainian and wider Central-European contexts (including hybrid learning and limited adult supervision online), the model treats cyberbullying as a relational phenomenon distributed across skills, group processes, and institutional climate. By shifting the target from "what students know" to "what they believe their peers expect," it increases the likelihood of early supportive bystander action and durable reductions in both perpetration and victimisation.

Keywords: cyberbullying; social norms; bystander behaviour; school connectedness; peer ecology; prevention; adolescent wellbeing

Cyberbullying in schools continues to occur even in settings where students already receive basic online safety or "cyber hygiene" lessons. Recent empirical work (2024–2025) indicates that this persistence is not primarily a deficit in individual skills but a function of the peer ecology within which online interactions take place. Adolescents tend to act in accordance with what they believe their classmates approve of, and they withhold help when they expect others to remain passive. In a 2025 study integrating the Theory of Planned Behaviour with norm constructs, Prestera and colleagues showed that both descriptive norms ("what peers do") and injunctive norms ("what peers approve of") made significant, positive contributions to adolescents' intention to engage in cyberbullying, over and above attitudes and perceived behavioural control; conformity also amplified the effect of norms on intention. This implies that, where the peer group silently tolerates online aggression, individual knowledge about safe behaviour is insufficient to prevent participation.

This interpretation is supported by the 2024 wave of meta-analytic research on bystander interventions. Two independent papers in Health Education & Behavior reported that programmes aimed at bullying and cyberbullying were most effective when they trained defending directly, used realistic digital scenarios and personalised responsibility for acting; broad digital literacy units were clearly less effective at changing actual bystander behaviour (Chen, 2024; Qiqi, 2024). These findings were echoed in editorial syntheses on bullying and cyberbullying bystanders, which stressed that the developmental course of an incident can be altered in both offline and online settings, but only if adolescents feel both morally authorised and socially supported to intervene (Chu, 2024). Taken together, these results place the pedagogical focus squarely on the class or year group: it is the local social norm that determines whether a supportive message in a group chat is "allowed", not the mere availability of technical advice.

A second, converging line of evidence derives from studies on school connectedness as a protective factor. Using large adolescent samples, Ajibewa and co-authors (2025) found that school connectedness significantly moderated the association between peer-bullying victimisation and depressive symptoms. Adolescents who felt strongly attached to school, teachers and classmates showed a weaker victimisation–

distress link than those with low connectedness. Likewise, Liu (2025) demonstrated that social connectedness together with parental support alleviated loneliness arising from school bullying, which underscores the importance of relational resources surrounding the learner. Earlier intervention reviews had already indicated that general school factors (climate, sense of belonging, perceived fairness) condition the success of anti-bullying programmes (Chicote-Beato, González-Víllora, Bodoque-Osma, & Navarro, 2024). When students experience the school as a reliable source of support, a hostile online episode does not become the sole relational reference point, and peers find it easier to align with the target rather than with the aggressor. For preventive work, this means that strengthening connectedness is not an optional wellbeing supplement but a precondition for peer norms to operate in favour of the victim.

On the basis of these strands, a peer-centred prevention model can be formulated. Its starting assumption is that school-related cyberbullying is sustained by perceived peer approval; the first pedagogical task is therefore to make norms explicit and discussable in class. Short, teacher-led classroom activities that juxtapose students' personal disapproval with their beliefs about what "most others" think frequently reveal a pattern of pluralistic ignorance. In other words, most students actually disapprove of online cruelty but wrongly believe that their peers tolerate it. Making this gap visible enables the group to articulate and internalise an injunctive norm against cyberbullying, in line with what Prestera et al. (2025) recommend for norm-focused interventions. The second task is to rehearse defending on the actual platforms, group-chat situations and image-sharing practices that students use. This addresses the concrete situational barriers to bystander action that the 2024 meta-analyses identified (for example, diffusion of responsibility or uncertainty about the victim's reaction). The third task is to stabilise school connectedness through visible adult follow-up, public recognition of prosocial bystander behaviour and sustained teacher–student relationship work, so that potential defenders are confident that the school will support them.

This peer-ecology perspective differs from device-regulation approaches and from policy-only approaches in two respects. First, it treats the class or peer group as the primary arena of change and it views school policies as scaffolding for that change rather than its driver. Second, it is well suited to contexts such as Ukrainian and wider Central-European schools operating under hybrid, resource-constrained or conflict-affected conditions, where adult surveillance of students' online activity is realistically limited. In such settings peers are frequently the only ones present at the moment of the incident. If those peers have internalised a defending-oriented norm and feel connected to school, preventive efforts can still succeed. This is consistent with UNESCO's (2024) call, which stressed that policies and complaint mechanisms must be complemented by the mobilisation of the whole school community, including students themselves.

References

1. Ajibewa, T. A., Kershaw, K. N., & Carnethon, M. R. (2025). Peer bullying victimization, psychological distress, and the protective role of school connectedness among adolescents. BMC Public Health, 25(1). https://doi.org/10.1186/s12889-025-24002-6
2. Chen, Q. (2024). The effectiveness of interventions on bullying and cyberbullying bystander behaviors: A meta-analysis. Health Education & Behavior. Advance online publication.
3. Chicote-Beato, M. M., González-Víllora, S., Bodoque-Osma, A. R., & Navarro, R. (2024). Cyberbullying intervention and prevention programmes in primary education (6–12 years): A systematic review. Aggression and Violent Behavior, 77, 101938. https://doi.org/10.1016/j.avb.2024.101938 sciencedirect.com
4. Liu, H. (2025). A path to relief from the intertwined effects of school bullying: The roles of social connectedness and parental support. BMC Public Health, 25. https://doi.org/10.1186/s12889-025-23064-w
5. Prestera, G., Amadori, A., Sangiuliano Intra, F., Taverna, L., Basso, D., & Brighi, A. (2025). The impact of social norms and conformity on cyberbullying perpetration among adolescents: An integration of the Theory of Planned Behavior model. Frontiers in Psychology, 16, 1492295. https://doi.org/10.3389/fpsyg.2025.1492295
6. Qiqi, C. (2024). The effectiveness of interventions on bullying and cyberbullying bystander behaviors. Health Education & Behavior. Advance online publication.
7. UNESCO. (2024, November 7). International Day against Violence and Bullying at School, including Cyberbullying

Bohdan KRAVETS
Second-year applicant for the Bachelor's degree in Computer Science (Specialty 122), State University "Kyiv Aviation Institute"
9090323@stud.kai.edu.ua

Yaroslav GALITSKIY
Second-year applicant for the Bachelor's degree in Computer Science (Specialty 122), State University "Kyiv Aviation Institute"
9126629@stud.kai.edu.ua

Nataliia DENYSENK
Senior Lecturer of the Professional Foreign Languages Department, State University "Kyiv Aviation Institute"
nataliia.denysenko@npp.kai.edu.ua

CYBERCULTURE AND DIGITAL HYGIENE IN THE EDUCATIONAL PROCESS

In the 21st century, the educational process is inseparable from digital technologies. The rapid growth of online communication, e-learning platforms, and artificial intelligence tools has created a cultural phenomenon known as cyberculture [1, ch. 1; 2, sec. 2]. It transforms the way knowledge is delivered, shapes digital identities, and affects social interactions. This paper explores the role of cyberculture in education, digital hygiene as a component of security, challenges and risks of digitalization, ethical issues, and future perspectives [3, sec. 3; 5, sec. 2].

1. Introduction.

Cyberculture is becoming a key component of education. It is not limited to technical tools but includes new forms of communication, online communities, and cultural practices [1, ch. 1]. At the same time, digitalization requires responsible and safe interaction with digital environments [2, sec. 3].

2. The Role of Cyberculture in Education

2.1. Active participation. Students move from passive knowledge consumers to active creators through discussions, collaboration, and digital projects [2, sec. 2].

2.2. Digital identity and communities. Online spaces shape student identity and values, requiring responsibility and awareness [1, ch. 2; 5, sec. 3].

3. Digital Hygiene as a Security Component

3.1. Data protection. Digital hygiene includes practices of strong passwords, phishing awareness, and digital footprint control [3, sec. 2].

3.2. Well-being. Screen time management is critical for psychological balance and productivity [9, sec. 1].

3.3. Educational value. Teaching digital hygiene is as important as traditional literacy [8, sec. 1].

4. Challenges and Risks of Digitalization

4.1. Cyberbullying and online addiction. These phenomena negatively affect student mental health and academic success [7, sec. 2].

4.2. Misinformation. The spread of false content requires critical evaluation skills and digital literacy [6, sec. 3].

5. Ethical and Social Dimensions

5.1. Respect for intellectual property. Students must follow copyright and academic integrity rules [10, sec. 2].

5.2. Digital etiquette. Ethical interaction in online spaces is essential for safe and inclusive learning [4, sec. 1].

6. Future Perspectives

Artificial intelligence, virtual reality, and immersive technologies will reshape education [2, sec. 3]. Updating standards of digital hygiene and implementing new methods of cyber-literacy training are necessary [6, ch. 1].

7. Conclusions

Cyberculture and digital hygiene are essential competencies of modern education [3, sec. 2]. By developing digital responsibility, schools and universities prepare students not only for academic success but also for active participation in a safe and ethical digital society [8, sec. 2].

References

1. Castells, M. (2010). The Rise of the Network Society (2nd ed.). Wiley-Blackwell.
2. Jenkins, H. (2009). Confronting the Challenges of Participatory Culture: Media Education for the 21st Century. MIT Press.
3. Rheingold, H. (2012). Net Smart: How to Thrive Online. MIT Press.
4. Livingstone, S., & Helsper, E. (2007). Gradations in digital inclusion: Children, young people and the digital divide. New Media & Society, 9(4), 671–696.
5. Buckingham, D. (2013). Media Education: Literacy, Learning and Contemporary Culture. Polity Press.
6. Selwyn, N. (2016). Education and Technology: Key Issues and Debates (2nd ed.). Bloomsbury Academic.
7. Boyd, D. (2014). It's Complicated: The Social Lives of Networked Teens. Yale University Press.
8. UNESCO. (2019). Guidelines on Digital Literacy for Educators. UNESCO Publishing.
9. World Health Organization. (2019). Guidelines on Physical Activity, Sedentary Behaviour and Sleep for Children Under 5 Years of Age. WHO Press.
10. Floridi, L. (2015). The Ethics of Information. Oxford University Press.

Oleksandra BLAGINIA
Second-year applicant for the Bachelor's degree in Computer Science (Specialty 122),
State University "Kyiv Aviation Institute"
91119940@stud.kai.edu.ua

Veronika YASHCHENKO
Second-year applicant for the Bachelor's degree in Computer Science (Specialty 122),
State University "Kyiv Aviation Institute"
9089037@stud.kai.edu.ua

Nataliia DENYSENKO
Senior Lecturer of the Professional Foreign Languages Department,
State University "Kyiv Aviation Institute"
nataliia.denysenko@npp.kai.edu.ua

CYBERCULTURE AND DIGITAL HYGIENE IN EDUCATION

Introduction. Today, it is difficult to imagine learning without the Internet. Almost every student and teacher uses digital technologies every day: from online lectures and searching for information to communicating on social networks or watching videos. Such activity forms a new culture of behavior in the virtual environment - cyberculture. Along with this, there is a need for digital hygiene, because the safe and conscious use of technology directly affects academic success, personal development and even health.

The purpose of this work is to reveal the meaning of the concepts of "cyberculture" and "digital hygiene", to show their importance for the educational process, and also to emphasize the role of teachers and students in forming a safe and friendly online space.

The concept of cyberculture. Cyberculture is a set of norms and rules that determine how a person behaves in the virtual world. It includes:

- observance of ethical norms when communicating on the Internet;
- respect for other users;
- a responsible attitude to one's own statements and actions;
- the ability to cooperate in the digital environment.

In fact, cyberculture is a reflection of the usual culture of behavior in virtual space. If in real life it is considered unacceptable to insult a person or spread false rumors, then these rules should also apply on the Internet.

This is especially relevant for students, because the university environment involves collective work on projects, participation in forums, and the use of platforms for distance learning. Therefore, the formation of a culture of mutual respect on the Internet helps to build a healthy atmosphere for learning.

Digital hygiene: basic principles. Unlike cyberculture, digital hygiene focuses on technical and practical aspects of security. It is a set of rules that help protect personal data and maintain a balance between education, rest, and leisure.

The basic rules of digital hygiene include:

1. Using strong passwords and two-factor authentication.
2. Be careful with emails and messages from unknown senders (protection against phishing).
3. Regularly update software and antivirus.
4. Control screen time to avoid fatigue and vision problems.
5. Be critical of information - check sources to avoid becoming a victim of fake news.

Digital hygiene is not only a technical tool for protection, but also a factor in maintaining mental and physical health. For example, excessive use of gadgets leads to decreased concentration, sleep problems, and social isolation.

Possible problems if the rules are violated. Failure to comply with the rules of cyberculture and digital hygiene can have serious consequences:

- cyberbullying - insults, harassment and humiliation online;
- theft of personal data due to weak passwords or carelessness;
- spreading fakes and unreliable information that harms reputation;
- phishing attacks that can lead to loss of access to accounts or financial resources.

For example, one careless step - clicking on a suspicious link - can open access to all of a student's email or personal data for attackers.

The role of educational institutions. Universities and schools should actively implement digital literacy curricula. This includes:

- lessons on checking the reliability of information;
- cybersecurity training;
- advice on organizing working time and staying healthy while working with a computer.

Educational institutions should not only provide knowledge, but also cultivate critical thinking and skills for safe use of the Internet.

Conclusions. Therefore, cyberculture and digital hygiene are integral components of modern education. They help not only to avoid dangers, but also to build a friendly, healthy, and productive online space.

Students need to understand that the correct use of the Internet is not only a technical skill, but also a part of personal culture. And for teachers, it is a tool for forming a generation of conscious and responsible citizens of the digital society.

References

1. Castells M. The Rise of the Network Society. Oxford: Blackwell, 2000. [1, ch. 2; 1, ch. 3]
2. Rheingold H. The Virtual Community: Homesteading on the Electronic Frontier. MIT Press, 2000. [2, ch. 1; 2, ch. 4]
3. Livingstone S. Children and the Internet: Great Expectations, Challenging Realities. Polity Press, 2009. [3, ch. 2; 3, ch. 5]
4. Nissenbaum H. Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford University Press, 2010. [4, ch. 1; 4, ch. 3]
5. ЮНЕСКО. Посібник з цифрової грамотності для викладачів. 2021. [5, sec. 2; 5, sec. 4]
6. Міністерство освіти і науки України. Цифрова грамотність та безпека в освіті. 2020. [6, sec. 1; 6, sec. 3]

БЕЗПЕКА В ТРАНСКОРДОННОМУ СПІВРОБІТНИЦТВІ: ПОЛІТИКА, СТРАТЕГІЇ, ДИПЛОМАТІЯ

SECURITY IN CROSS-BORDER COOPERATION: POLITICS, STRATEGIES, DIPLOMACY

BIZTONSÁG A HATÁROKON ÁTNYÚLÓ EGYÜTTMŰKÖDÉSBEN: POLITIKA, STRATÉGIÁK, DIPLOMÁCIA

Dr. Fehmi Agca PAMER
Head of the Centre for Postcolonial Studies,
Üsküdar University, Istanbul, Turkey

REGIONAL INTEGRATION THROUGH CROSS-BORDER COOPERATION: THE CASE OF UKRAINE AND TÜRKIYE

Abstract

The regional cooperation is a gradual long-term process and requires steady determination and political commitment. In this regard, protection of the freedom of speech and human rights, corporate governance reform, judicial reform, effective fight against corruption, institutional capacity-building in public administration and strengthening civil society are crucial tasks for any candidate country. Turkish experience with the EU can be valuable for Ukraine in the integration process. Besides, the countries around the Black Sea are providing new opportunities to contribute this process.

Crimean Tatars issue deeply effects the Ukraine-Türkiye relations. Ukraine helped to the Crimean Tatar families during their return to Criema after long years of leave and desparation. Turkish people and Crimean Tatar diaspora have developed a positive feeling towards Ukraine.

So far Türkiye has clearly supported the territorial integrity of Ukraine, and declared that the Crimea is part of Ukraine. Türkiye provided effective weapon systmes to contribute to the defense of Ukraine territory. Today, the cooperation and partnership continue particularly for joint production of unmanned air vehicles. The solidarity among the Turkish and Ukranian people and the cooperation between the businesses will provide better conditions to improve cross border cooperation to accomplish the regional integration in parallel with the European integration process.

Keywords: Regional integration, Cooperation, Security, Black Sea, Crimean Tatars

Introduction

The security is the essential condition of regional integration. To provide better conditions for communication and transportation particularly contribute to the crss-border cooperation through social integration.

With the goal of being full member of the EU, Türkiye and Ukraine continue accession negotiations. For Ukraine, the best way of cross-border cooperation is to develop relations with the neighboring states, such as Poland, Slovakia, Hungary and Romania. Because of being EU member states, those countries can directly contribute to the Ukraine efforts to be part of EU. Türkiye has no land border with Ukraine. But, Ukraine and Türkiye are neighboring states through the Black Sea and they have the oportunity for direct contact.

EU's political identity has an ideal to break down the borders between societies and aims to create borderless European Union. This is also a part of the EU's strategy towards Ukraine. Thus, EU has enforced the good neighbourliness principle between neighbour states. The wel functioning democracy and the building of active civil society serve to the development of good relations between the neighboring states for regional cooperation.

Although the nations around the Black Sea have different cultural, ethnic, religious and linguistic features, the Black Sea itself provides valuable conditions for the echange of trade and cultures. Historically, private economic initiatives became the most important factors to bring together the different societies. But, different political aspirations of the states around theBlack Sea have negatively effected the cooperation and integration.

In a relatively short period of time following the Cold War, Black Sea Economic Cooperation initiative had been started. Albania, Armenia, Azerbaijan, Bulgaria, Georgia, Greece, Moldova, Romania, Russia, Serbia, Türkiye and Ukraine supported this regional cooperation. It is a comprehensive structure in the region and nearly 300 million people have been living in the member states. It is connected to the rest of the world through the Turkish Straits and the Mediterranean Sea. Since the 1990s, the Black Sea region have become important for the world economy as the energy corridor between the Caspian Sea and the Meditarranean. Black Sea economies are increasingly

connected to each other and become attractive for foreign direct investment, technology transfer and the movement of labor and people for tourism.

New trade opportunities can be maintained through the integration of national markets in the Black Sea, particularly in the energy, services and manufacturing sectors. The increasing number of immigrants may contribute to the establishment of personal networks and provide new transnational opportunities in trade and investment.

The Black Sea is an attractive tourist destination not only for foreigners but also for its own citizens. The tourism industry requires improved well functioning infrastructure capacity and better quality of services. The quality of infrastructure and services can only be can be improved through the joint projects which are backed by the regional states.

The region has a high interdependence with the European Union. In line with the nighbourhood policy, EU started the Eastern Partnership initiative in 2009 to increase political association and further economic integration with six partner countries; Armenia, Azerbaijan, Georgia, Belarus, Ukraine and Moldova. So far, it seems that the bureaucratic obtacles have prevented the success of this regional iniative.

Regional cooperation is a slow, long-term process which requires durable commitment. EU is the most successful example of regional integration in the world. Its success requires the strong determination of political leaders in the member states. On the other hand, the participation of businessmen and civil society groups to the integration process may have profound effect. In this regard, protection of the freedom of speech and human rights, corporate governance reform, judicial reform, effective fight against corruption, institutional capacity-building in public administration and strengthening civil society are crucial tasks for any candidate country.

The Role of Crimean Tatars for Cross-Border Cooperation between Ukraine and Türkiye

Türkiye clearly supports the inviolability of the territorial integrity of Ukraine, and always declares that the Crimean peninsula is part of Ukraine. Crimean Tatars can be seen as the most important factor of the Turkish-Ukrainian relations. Anti-Tatar policy of Russia in the 19. century, hundreds of thousands of Crimean Tatars were forced to leave their homeland and immigrate to Türkiye. About five million Crimean Tatar people are currently living in Türkiye. Almost all Crimean Tatar families in the Crimea have relatives in Türkiye. They have been completely integrated into Turkish society. There are great number of effective Crimean figures in every sphere of life. There are also significant number of Crimean Tatar people at the high official positions particularly at the security posts. Therefore, they paly important role to develop relations between two countries.

Starting with the end of Cold war in 1989, the Crimean Tatar diaspora have been organizing donation campaigns to help their people who went back to the Crimea. Crimean Tatar diaspora has always been highly sympathetic towards Ukraine. Their collective memory helped to protect the friendship against Ukraine. During the return of Crimean tatars to their homeland, Ukraine provided material help for the Crimean Tatar families. This approach was highly appreciated by the Turkish people. During the dlplomatic meetings between Türkiye and Ukraine, Turkish side have always expressed their gratitude to the Ukrainian side and Crimean Tatars were jointly described as "the bridge of friendship" between Ukraine and Türkiye.

When Russia attacked to Crimea, Türkiye gave full support for Ukrainian territorial integrity in all international forums and the President of Türkiye repeatedly declared that Türkiye would never recognize the illegal occupation and annexation of Crimea to Russia. Türkiye has also critized the human rights violations against Crimean Tatars who were forced to move Ukraine by Russian authorities. The recognition of the status of Crimean Tatars and their national-cultural autonomy by Ukraine greatly helped to maintain trust between Türkiye and Ukraine. It is worth to mention that the recognition of Crimean Tatar language by Ukraine would improve good relations with Turkic states such as Azerbaijan and Central Asian states having more than 170 million people. Besides, this approach contribute to the positive image of Ukraine as a multiethnic state, respecting and protecting the rights and freedoms of its ethnic and religious minorities. Ukrainian diaspora in Türkiye also cooperated with the Crimean Tatar diaspora to improve the positive image of Ukraine in Türkiye and for the recognition of the Ukrainian national interests.

Today, millions of Crimean Tatar diaspora particularly in Türkiye are strongly oppose the Russian rule in Crimea. The problems of Crimean Tatars also took attention from the EU and international community in general. Many international publications increased the concerns over the human rights of Crimean Tatars and the illegal Russian existence in the Crimean Peninsula. The growing global awareness for the tragedy of Crimean Tatars provided Ukraine an opportunity for addressing its claims to restore its territorial integrity along with its aspirations of European integration.

The Russia-Ukraine conflict had negative effects on Ukraine's relations with the Central Asian states. The restoration of cooperation will increase the solidarity for the security in the region. By highlighting the issue of Crimean Tatars, Ukraine demonstrates that Turkic and Islamic identities are inseparable parts of the Ukrainian national identity. This diplomacy opens for new cooperation prospects to Ukraine with the Turkic and Islamic worlds.

The cooperation between Türkiye and Ukraine for regional integration

Türkiye and Ukraine are the key actors of regional cooperation around the Black Sea. Turkish experience with the EU can be valuable for Ukraine about what should be done in the integration process.

During the 1st World war the Ottoman State supported the Ukrainian nationalists striving for the independence of Ukraine. Ottoman State recognized the independence of the Ukrainian Democratic Republic in 1918 and signed friendship and alliance treaties. Following disintegration of the Soviet Union, Turkish-Ukrainian relations have developed very well. Political and military leaders, businessmen and academic personnel from both side have been working to improve Turkish-Ukrainian relations particularly within the framework of the Black Sea Economic Cooperation Act signed in 1992.

While having a certain level of cooperation with Russia, Türkiye developed its strategic partnership with Ukraine. Unlike some other European allies, Türkiye expressed strong support for the its NATO membership. Türkiye also supported interoperability capacity of the Ukrainian army with the NATO forces.

The relations between Türkiye and Ukraine have improved particularly since Erdogan came to power. Türkiye provided effective weapon systems to contribute to the defense of Ukraine territory. Today, the cooperation and partnership continue particularly for joint production of unmanned air vehicles. The solidarity among the Turkish and Ukranian people and the cooperation between the businesses will provide better conditions to improve cross border cooperation to accomplish the regional integration.

In the context of military cooperation, Ukraine bought Turkish drones and used very effectively against Russian forces in every part of battlefield especially in Donbas region. Baykar drone company, as having very advanced technology in this area signed an agreement with the Ukrainian company Motor Sich, so that it would provide vital engine parts for third-generation Akıncı drones in Türkiye. Turkish drones had a crucial role to redesign the battlefield in a many conflicts in the region. Despite the discomfort of Russia, Türkiye is willing to share its national defense industry products with NATO allies and Ukraine as a strategic partner.

As a key mediator, Türkiye is trying to maintain ceasefire between Ukraine and Russia. Türkiye also wants to protect its national interests, which are influenced by regional dynamics. To maintain regional order is essential for Ankara, especially for its long-term strategic interests in the Black Sea basin. In this regard, Türkiye hosted mediation meetings in an attempt to facilitate a dialogue between Ukraine and Russia. The first of these meetings was held in Antalya Diplomacy Forum in March 2024. Later, another meeting was held in Istanbul. During these meetings, Turkish Foreign Minister played the role of facilitator and observer. Aside from these formal meetings, Ankara has also been in constant contact with the two sides.

While investing in mediation efforts, Türkiye has tried to maintain a certain degree of neutrality. Türkiye has also shown full compliance with international agreements, particularly the 1936 Montreaux Convention, which gives Türkiye control over access to the Black Sea through the the Turkish Straits. According to Article 19 Montreaux Convention, if Türkiye is not belligerent in times of war, it can use its right to block the transit passage of the warships of belligerent states. Therefore,

some Russian warships were denied access to the Black Sea. Türkiye also expressed full solidarity to Ukraine within the United Nations by strongly condemnation of Russia's military operations.

Türkiye has also become very active on the ground with its humanitarian aid campaign aimed at evacuating civilians. So far, thosands of civilians have been moved out of combat zones and more than 60,000 Ukrainians have found shelter in Türkiye.

Ukraine and Türkiye have developed a strategic relationship in the defence and security areas, with the high level cooperation in the defence industry. Ukraine regards Türkiye as a significant contributor to European security and a powerfull ally to counterbalance the Russian threat. Kyiv recognizes Türkiyep as a potential security guarantor, mediator, and contributor to Ukraine's peace plan. The Ukraine-Türkiye strategic partnership is essential to build a future regional order in the Black Sea. Both states are serving as the security outposts for Europe, to provide the defence and security in all European geography.

During the Russia-Ukraine war, Türkiye tried to maintain diplomatic nagotiation channels open to both sides while keeping good relations with Moscow and Kyiv. Turkish President Erdoğan announced his desire to host for the peace talks between Russia and Ukraine. Even the USA argued that Türkiye could be a reliable mediator by both sides. During the war, Türkiye successfully managed to establish grain corridor in the Black Sea, so as to secure the export of important food supplies from Ukraine to the rest of the world.

In February 2025, during the press conference with Erdogan in Ankara, Zelensky emphasized the importance of security guarantees from strong countries with powerful armies, including Türkiye.

If Russia retains the territories conquered in Ukraine after the peace talks, the safety of navigation in the Black Sea would have to be re-examined. Türkiye can be one of the states providing security guarantees. If some developments could be provided in the peace process in the near future, the safety of the Black Sea, especially for the passage of cargo ships will be the key issue. Not only peace within the Ukrainian territories but also peace in the Black Sea must be secured.

Conclusion

The final goal of regional integration for Ukraine and Türkiye is to be full member of the EU. Both countries are now at the stage of accession negotiations. Ukraine and Türkiye are neighboring states through the Black Sea and they have the oportunity for direct contact. The security is the essential condition of regional integration. To provide better conditions for communication and transportation particularly contribute to the social integration.

Regional economic cooperation is important to motivate the regional security and political stability, to avoid new divisions in Europe. For a successful cooperation around the Black Sea, infrastructure for transport, communications, energy, science and technology is critical for economic growth, productivity and sustainable development.

Although the nations around the Black Sea have different cultural, ethnic, religious and linguistic features, the Black Sea provides valuable conditions for the exchange of trade and cultures. But, different political aspirations of the states around the Black Sea have negatively effected the cooperation and integration.

Türkiye and Ukraine are the key actors of regional cooperation around the Black Sea. Turkish experience with the EU can be valuable for Ukraine about what should be done in the integration process. Following the disintegration of the Soviet Union, Turkish-Ukrainian relations have developed very well. The several high level political and military leaders, businessmen and academic personnel continue to improve Turkish-Ukrainian relations particularly within the framework of the Black Sea Economic Cooperation Act signed in 1992.

Türkiye clearly supports the inviolability of the territorial integrity of Ukraine, and always declares that the Crimean peninsula is part of Ukraine. Crimean Tatars can be seen as the most important factor of the Turk-Ukrainian relations. Ukraine provided material help for the Crimean Tatar families. This approach was highly appreciated by the Turkish people. When Russia attached to Crimea, Türkiye gave full support for Ukrainian territorial integrity in all international forums and the President of Türkiye repeatedly declared Türkiye would never recognize the illegal occupation and annexation of Crimea to Russia. Ukrainian diaspora in Türkiye also cooperated with the Crimean Tatar diaspora to

improve the positive image of Ukraine in Türkiye and for the recognition of the Ukrainian identity and national interests.

While having a certain level of cooperation with Russia, Türkiye developed its strategic partnership with Ukraine. Unlike some other European allies, Türkiye expressed strong support for the its NATO membership. Türkiye also supported interoperability capacity of the Ukrainian army with the NATO forces.

The relations between Türkiye and Ukraine have improved particularly since Erdogan came to power. In the context of military cooperation, Ukraine purchased Turkish drones and used very effectively against Russian forces in every part of battlefield especially in Donbas region. Despite the discomfort of Russia, Türkiye is willing to share its national defense industry products with NATO allies and Ukraine as a strategic partner.

As a key mediatör, Türkiye is trying to maintain ceasefire between Ukraine and Russia. To maintain regional order is essential for Ankara, especially for its long-term strategic interests in the Black Sea basin. Türkiye also became very active on the ground with its humanitarian aid campaign aimed at evacuating civilians. So far, thosands of civilians have been moved out of combat zones and more than 60,000 Ukrainians have found shelter in Türkiye.

Ukraine and Türkiye have developed a strategic relationship in the defence and security area, with the high level cooperation in the defence industry. Ukraine regards Türkiye as a significant contributor to European security and a powerfull ally to counterbalance the Russian threat. Türkiye successfully managed to establish grain corridor in the Black Sea, so as to secure the export of important food supplies from Ukraine to the rest of the world.

If some developments could be provided in the peace process in the near future, the safety of the Black Sea, especially for the passage of cargo ships will be the key issue. Not only peace within the Ukrainian territories but also peace in the Black Sea need to be secured.

References

1. Euroasian Research Institute, “The Turkic Side of Ukraine’s Political Identity: The Role of Crimean Conflict in Ukraine’s Nation-Building”, Akhmet Yassawi University Publications, 2022.
2. Filiz Tutku Aydın, “Turkey’s policy on the Russian-Ukrainian Crises”, SETA Analyses, February 2002, No.77
3. Gülsen Solaker, “Can Turkey play a role in Ukraine's future?”, Politics/Europe, 02/21/2025. Can Turkey play a role in Ukraine's future? – DW – 02/21/2025
4. Hakan Kırımlı, “Turko-Ukrainian Relations and the Crimean Tatars”, Bilkent University Publications, 2003, Ankara.
5. Panagiota Manoli, “Regional cooperation in the Black Sea: Building an inclusive, innovative, and integrated region”, University of the Aegean, 2014.
6. Maryna Vorotnyuk, “Ukraine-Turkey Strategic Partnership in Security and Defence”, CATS Network Paper No.20, 2025.
7. Montreaux Convention 1936, Article 19.
8. Soner Cagaptay, “Will Turkey Help Washington If Russia Invades Ukraine?”, The Washington Institute for Near East Policy, 2022.

Ігор ЛЯХ
Доктор технічних наук, професор,
професор кафедри інформатики
та фізико-математичних дисциплін
Ужгородський національний університет,
igor.lyah@uzhnu.edu.ua

МОДЕЛЬ ТРАНСКОРДОННОЇ ВЗАЄМОДІЇ ДЛЯ ЗАХИСТУ IOT-СИСТЕМ У ЛОГІСТИЦІ НА КОРДОНАХ УКРАЇНИ ТА ЄС

Інтернет речей (IoT) активно трансформує логістику, дозволяючи в режимі реального часу відстежувати рух вантажів, контролювати умови їх зберігання та оптимізувати маршрути доставки. Водночас із зростанням ролі IoT посилюються виклики у сфері кібербезпеки, адже кожен підключений пристрій потенційно може стати вразливою точкою. Особливо це актуально для транскордонних логістичних мереж між Україною та країнами ЄС, де перетинаються різні стандарти безпеки, регуляторні вимоги та технологічні рішення. Надійний захист IoT-систем у такому контексті є ключовим для забезпечення цілісності, достовірності та безперервності логістичних процесів.

Наразі відсутність єдиного підходу до кіберзахисту транскордонних систем підвищує ризики кібератак і зловмисних втручань. Метою цього дослідження є розробка моделі транскордонної взаємодії, яка забезпечить ефективний захист IoT-систем у логістиці шляхом оперативного обміну інформацією про кіберінциденти та координації дій між Україною та ЄС. Наукова новизна полягає у створенні інтегрованої платформи співпраці, що враховує особливості різних юрисдикцій і технологічних середовищ, а практична значущість – у підвищенні рівня кібербезпеки важливої інфраструктури транскордонної торгівлі.

У контексті євроінтеграції України особливу актуальність має вивчення правового регулювання IoT у країнах ЄС та США, де IoT розглядається як мережа взаємодіючих пристроїв, здатних до автономної передачі даних. Відомі дослідження наголошують на необхідності стандартизації та сертифікації таких пристроїв, водночас звертаючи увагу на ризики гальмування інноваційного розвитку. Особлива увага приділяється кібербезпеці, захисту персональних даних і ролі саморегулювання через партнерство бізнесу та громадянського суспільства [1].

Проблема несумісності регуляторних підходів у транскордонному цифровому середовищі також є надзвичайно важливою. Зокрема, у сфері фінансових технологій виявлено фрагментацію законодавства, юридичну невизначеність та посилення кіберризиків, що підкреслює потребу у міжнародній координації для формування узгодженої політики кіберзахисту. Аналогічні виклики мають місце і для IoT-систем у логістиці між Україною та ЄС, де стикаються різні технічні та правові стандарти [2].

Важливу загрозу становить людський фактор у сфері кібербезпеки. Дослідження показують, що традиційні методи інформування (тренінги, email-розсилки) часто не досягають бажаного ефекту. Значно ефективнішими є методи обміну знаннями через соціальні мережі або за участю локальних експертів, які забезпечують оперативну й контекстуальну підтримку. Це особливо важливо в складних транскордонних логістичних процесах, де постійна кіберобізнаність персоналу є критичною [3].

У цифровому середовищі зростає потреба в ефективних моделях транскордонної взаємодії для забезпечення кібербезпеки, особливо у сферах із широким застосуванням IoT-рішень. Аналіз міжнародної практики у фінансових технологіях та митному адмініструванні підтверджує важливість гармонізації нормативних підходів, створення спільних протоколів реагування на кіберінциденти та використання цифрових платформ для безпечного обміну даними. Такі підходи дозволяють забезпечити цілісність і стійкість спільної інфраструктури, що особливо актуально в умовах різнорідного регуляторного середовища на кордонах України та ЄС.

У контексті забезпечення кібербезпеки IoT-систем у транскордонній логістиці пропонується модель інтегрованої платформи обміну інформацією, яка виступає центральним

вузлом координації між ключовими учасниками процесу. На рисунку 1 ілюструється структура такої платформи, що об'єднує логістичні компанії, державні органи (зокрема митницю і регуляторів кібербезпеки), CERT/SOC-центри реагування на інциденти та європейських партнерів. Платформа забезпечує двосторонній обмін даними про кіберінциденти, стандарти безпеки та оперативні повідомлення, що дозволяє швидко виявляти загрози, координувати заходи реагування і підтримувати стійкість інформаційної інфраструктури в умовах різнорідного регуляторного середовища України і ЄС. Така архітектура сприяє гармонізації технічних і правових аспектів безпеки, створюючи основу для ефективної транскордонної взаємодії у сфері захисту IoT-систем.

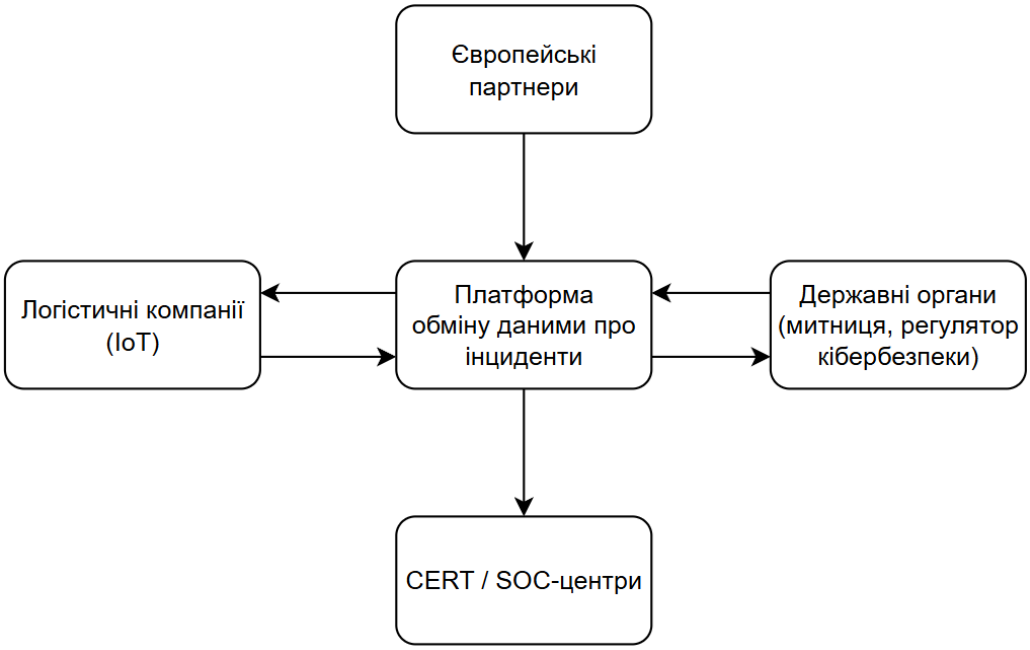


Рисунок 1. Модель інтегрованої платформи транскордонної взаємодії для обміну інформацією про кіберінциденти у логістичних IoT-системах

Інтернет речей (IoT) значно змінює логістику на кордонах України та ЄС, але відсутність єдиного підходу до кібербезпеки в транскордонних системах створює підвищені ризики кібератак. Аналіз міжнародного досвіду підкреслює необхідність гармонізації технічних та правових стандартів, а також координації дій між різними учасниками для забезпечення цілісності та безперервності логістичних процесів. Особлива увага приділяється управлінню людським фактором, де більш ефективними є інтерактивні методи обміну знаннями, що сприяють формуванню кіберобізнаності серед персоналу.

Запропонована модель інтегрованої платформи транскордонної взаємодії забезпечує оперативний обмін інформацією про кіберінциденти та координацію між українськими та європейськими учасниками логістики. Вона слугує основою для узгодження правових і технічних аспектів безпеки, підвищуючи загальний рівень кіберзахисту критичної інфраструктури та сприяючи стабільності та стійкості транскордонних IoT-систем.

Список використаної літератури та джерел

1. Nekit, K. H. (2022). Legal approaches to solving security issues in the field of the internet of things in the light of european integration of Ukraine. Правничий часопис, 230–235. https://doi.org/10.32850/sulj.2022.4.2.36

2. Sharma, A., Adekunle, B. I., Ogeawuchi, J. C., Abayomi, A. A., & Onifade, O. (2021). Governance Challenges in Cross-Border Fintech Operations: Policy, Compliance, and Cyber Risk Management in the Digital Age. Iconic Research And Engineering Journals. 4(9). 278–286.

3. Pham, H. C., Ulhaq, I., Nguyen, M., & Nkhoma, M. (2021). An exploratory study of the effects of knowledge sharing methods on cyber security practice. Australasian Journal of Information Systems, 25. https://doi.org/10.3127/ajis.v25i0.2177

Михайло ПОНОМАРЬОВ
магістр освітньої програми «Комп'ютерно-математичне моделювання»
Ужгородський національний університет,
ponomarov.mykhailo@student.uzhnu.edu.ua

Юрій МЛАВЕЦЬ
доцент, кандидат фізико-математичних наук,
доцент кафедра кібернетики і прикладної математики
Ужгородський національний університет,
yurii.mlavets@uzhnu.edu.ua

МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ РИЗИКІВ У ТРАНСКОРДОННОМУ СПІВРОБІТНИЦТВІ

У сучасних умовах глобалізації та європейської інтеграції транскордонне співробітництво набуває особливого значення для стабільного розвитку прикордонних регіонів. Зростання взаємозалежності між державами створює нові можливості для економіки та інфраструктури, проте водночас супроводжується підвищенням рівня ризиків, що охоплюють економічну, екологічну та безпекову сфери. Актуальність проблеми посилюють геополітична нестабільність у Східній Європі, розширення ЄС та впровадження нових стандартів прикордонного контролю, розвиток міжнародних транспортних коридорів, а також зростання міграційних потоків. У цих умовах будь-які збої у функціонуванні прикордонної інфраструктури чи управлінні потоками людей і товарів можуть мати серйозні наслідки для національної та регіональної безпеки [1].

Ефективне управління транскордонними процесами неможливе без системного розуміння ризиків, що виникають у різних сферах. Серед основних загроз слід виділити економічні ризики, пов’язані з коливанням валютних курсів, зростанням вартості логістики та нерівномірним розподілом інвестицій; політичні та геополітичні ризики через зміни митної політики, посилення контролю або міжнародні конфлікти; соціальні ризики, що проявляються у нелегальній міграції та культурних бар’єрах; екологічні загрози, що виникають через забруднення територій чи техногенні аварії; а також інфраструктурні та безпекові ризики, які охоплюють зношеність транспортної мережі, кібератаки та транскордонну злочинність. Багаторівневий характер ризиків вимагає комплексного підходу до їх аналізу. Для цього доцільно застосовувати математичні методи, які дозволяють кількісно оцінити ризики та ефективно керувати загрозами [2].

Традиційні підходи до оцінки ризиків ґрунтуються переважно на якісному аналізі, що обмежує можливості для об’єктивного порівняння й прогнозування. Математичні методи дозволяють формалізувати процес виявлення загроз, визначити рівень їхньої ймовірності та масштаб потенційних наслідків, що відкриває можливості для побудови інтегральних моделей та підтримки управлінських рішень у сфері транскордонної безпеки.

Для кількісного аналізу ризиків застосовуються різні математичні підходи. Стохастичне моделювання описує події, що виникають випадково і не завжди піддаються точному прогнозуванню. У транскордонному середовищі такі події можуть включати затримки у транспорті, непередбачувані політичні зміни або міграційні кризи, які здатні швидко змінити баланс безпеки у прикордонному регіоні. Метод дозволяє оцінювати розподіл ймовірностей реалізації різних сценаріїв та прогнозувати потенційні наслідки [3].

Методи теорії ймовірностей розглядають ризик як випадкову подію з певною ймовірністю P та рівнем наслідків C. Для кожного типу загрози оцінюється ймовірність її реалізації та масштаб наслідків. Інтегральний ризик визначається за формулою:

$$R = P \times C \tag{1}$$

де R – інтегральний ризик, P – імовірність настання події, C – рівень наслідків за заданою шкалою.

Матриця ризиків поєднує ймовірності та наслідки у вигляді таблиці, що дозволяє наочно оцінити критичність кожного ризику та визначити пріоритети заходів безпеки.

Таблиця 1. Інтегральні ризики основних загроз у транскордонному співробітництві

Тип ризику	**Ймовірність (P)**	**Наслідки (C)**	**Інтегральний ризик (R = P×C)**
Міграційні ризики	0.4	8	3.2
Логістичні затримки	0.6	5	3.0
Політичні/правові обмеження	0.2	9	1.8
Екологічні катастрофи	0.1	10	1.0

Міграційні ризики мають високу критичність і помірну ймовірність, що робить їх пріоритетними для контролю. Логістичні затримки трапляються частіше, проте їхні наслідки менш значні. Політичні та правові обмеження зустрічаються рідко, але при настанні можуть мати серйозний вплив на регіональну стабільність.

Математичне моделювання у транскордонному співробітництві дозволяє кількісно оцінити ймовірність загроз та масштаб їхніх наслідків, використовуючи стохастичне моделювання, методи теорії ймовірностей та матрицю ризиків. Такий підхід забезпечує комплексний аналіз, який враховує невизначеність і випадковість подій.

Розрахунок інтегральних ризиків та їх візуалізація у таблиці дозволяють визначити пріоритетні напрями контролю та спрямувати ресурси на найкритичніші загрози. Зокрема, міграційні ризики та логістичні затримки потребують більшої уваги через їхню частоту та вплив на безпеку транскордонного співробітництва.

Список використаної літератури та джерел

1. Bilak, O., & Oleskiv, A. (2025). Theoretical and legal principles of cross-border cooperation: Specific issues. Virtus: Scientific Journal of Law. https://doi.org/10.61345/1339-7915.2025.1.3
2. Doroshenko, D. (2024). Prediction of network threats and attacks by mathematical simulation. Computer-Integrated Manufacturing Systems. https://purl.org/cims/2403.021
3. Lazebnik, T., Shami, L., & Bunimovich-Mendrazitsky, S. (2023). A hybrid mathematical model for an optimal border closure policy during a pandemic. International Journal of Applied Mathematics and Computer Science. https://doi.org/10.34768/amcs-2023-0042

Артемій ЦІПІНЬО
магістр освітньої програми «Управління ІТ проєктами»
Ужгородський національний університет,
tsipino.artemii@student.uzhnu.edu.ua

Юрій ЦІПІНЬО
викладач-методист
Закарпатський політехнічний фаховий коледж,
yuratsipino@ukr.net

РИЗИКИ ТА МОЖЛИВОСТІ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ У ТРАНСКОРДОННОМУ СПІВРОБІТНИЦТВІ

Соціальна інженерія у транскордонному контексті несе значні ризики, зокрема можливість зловживань з боку ворожих агентів і спецслужб країн-агресорів, які використовують маніпуляції, пропаганду та дезінформацію для впливу на суспільну думку та послаблення довіри між державами. Такі дії сприяють дестабілізації регіональних відносин, розпалюють конфлікти та розділяють громади. Водночас складність виявлення маніпулятивних практик ускладнює їх своєчасну нейтралізацію, особливо враховуючи нестачу ресурсів і політичну поляризацію в прикордонних регіонах, що підвищує їх вразливість до інформаційних атак.

Для протидії цим викликам необхідне підвищення інформаційної грамотності населення, міжнародна співпраця у сфері кібербезпеки, а також впровадження етичних і правових норм, які обмежують маніпулятивне використання соціальних технологій. Крім того, важливими є постійний моніторинг і аналітика інформаційного простору з використанням сучасних цифрових технологій для своєчасного виявлення і нейтралізації дезінформації та пропаганди.

Соціальна інженерія стає все більш актуальним викликом у сфері транскордонного співробітництва, оскільки вона використовує психологічні методи впливу для маніпуляції людьми та отримання доступу до конфіденційної інформації. У міжнародних відносинах такі маніпуляції можуть підірвати довіру між партнерами, спричинити конфлікти або перешкодити успішній реалізації важливих проєктів. Тому розуміння механізмів соціальної інженерії та розробка ефективних заходів протидії є ключовими для забезпечення безпеки і стабільності співпраці між країнами. Особливу увагу слід приділяти підвищенню обізнаності учасників транскордонних проєктів та впровадженню сучасних технологічних рішень, які допомагають виявляти і запобігати загрозам. Такий комплексний підхід дозволяє мінімізувати ризики та зміцнити партнерські відносини у складному міжнародному середовищі [1].

Особливої уваги заслуговує вплив людського фактора на кібербезпеку в організаціях, підприємствах та установах, де соціальна інженерія виступає однією з найпоширеніших форм кібератак. Часті атаки типу фішинг і маніпуляції працівниками даних установ підкреслюють необхідність регулярних навчань та підвищення обізнаності персоналу щодо кіберзагроз. Крім того, важливо впроваджувати стандартизовані методики оцінки ризиків і комплексні політики кібербезпеки, які враховують як технічні, так і психологічні аспекти захисту інформації [2].

Соціальна інженерія також може відігравати позитивну роль у формуванні довіри та партнерства між країнами, особливо в транскордонних регіонах, де тісна взаємодія між спільнотами є важливою для стабільності і розвитку. Через соціальні технології, такі як інформаційні кампанії, культурні обміни та спільні освітні проєкти, створюються умови для посилення взаєморозуміння і співпраці. Ці методи допомагають формувати спільні цінності та знижувати рівень конфліктів, що сприяє конструктивному діалогу та ефективній співпраці. Водночас, важливо забезпечувати прозорість і етичність таких процесів, аби мінімізувати ризики маніпуляцій і недовіри. Застосування комплексних заходів соціальної інженерії сприяє зміцненню партнерських відносин і підтримці безпеки у транскордонних проєктах. Таким чином, соціальна інженерія, будучи частиною стратегічного підходу, може стати важливим інструментом у забезпеченні стабільності та розвитку міжнародної співпраці.

У транскордонній співпраці соціальна інженерія реалізується через інформаційні кампанії, культурні обміни та спільні проєкти, що сприяють формуванню довіри та зміцненню партнерства між країнами. Інформаційні кампанії, які використовують офіційні канали, ЗМІ та цифрові платформи, допомагають формувати спільні наративи і підвищувати обізнаність громадян про загальні цінності, мінімізуючи ризики маніпуляцій. Культурні та освітні обміни створюють умови для посилення взаєморозуміння і зниження соціальної напруженості, сприяючи формуванню спільної ідентичності в транскордонних регіонах.

Водночас соціальні мережі та цифрові платформи є ефективними каналами для поширення інформації і мобілізації громадської підтримки, що значно розширює можливості соціальної інженерії у транскордонній взаємодії. Проте з огляду на поширення фейкових новин і дезінформації, особливо в періоди кризових подій, наприклад пандемії COVID-19, виникає необхідність у впровадженні сучасних технологій для їх виявлення та нейтралізації. Одним із таких рішень є модель Cross-SEAN – напівкерована нейронна мережа з механізмом уваги, що ефективно ідентифікує фейкові новини в режимі реального часу, використовуючи як марковані, так і немарковані дані, що суттєво підвищує якість боротьби з дезінформацією у цифровому просторі [3]. Комплексне застосування цих інструментів дозволяє створювати більш стійкі механізми співпраці, які сприяють безпеці та стабільності регіону.

У контексті транскордонної співпраці соціальна інженерія виступає важливим інструментом зміцнення партнерства між Україною та Румунією. Завдяки реалізації інформаційних кампаній, а також культурних і освітніх обмінів вдалося подолати історичні бар'єри та створити ефективні спільні платформи для розвитку прикордонних регіонів. Зокрема, такі ініціативи, як UNIV.E.R-U та програми Erasmus+, сприяють підвищенню рівня взаєморозуміння, налагодженню конструктивного діалогу між громадами та формуванню довіри. Ці процеси є критично важливими передумовами забезпечення стабільності та сталого розвитку регіону.

У перспективі розвиток соціальної інженерії у транскордонних відносинах пов'язаний із викликами цифрової доби, зокрема з активним використанням штучного інтелекту та цифрових платформ. Хоча ці технології розширюють можливості для ефективного впливу на суспільну думку, вони одночасно підвищують ризики маніпуляцій і дезінформації. Тому необхідним є запровадження етичних норм та міжнародних домовленостей, які регулюватимуть застосування соціальних технологій, забезпечуючи прозорість процесів і підтримку безпеки у транскордонній співпраці між Україною та Румунією.

Соціальна інженерія в транскордонному співробітництві є потужним інструментом як для зміцнення довіри та партнерства, так і для маніпуляцій і дестабілізації регіональних відносин. Використання інформаційних кампаній, культурних обмінів та цифрових технологій сприяє підвищенню взаєморозуміння, але водночас потребує впровадження етичних норм і сучасних технологічних рішень для запобігання дезінформації та кіберзагроз. Комплексний підхід із підвищення інформаційної грамотності та міжнародної координації дозволить мінімізувати ризики і зміцнити партнерські відносини між країнами.

Список використаних джерел

1. Siddiqi, M. A., Pak, W., & Siddiqi, M. A. (2022). A study on the psychology of social engineering-based cyberattacks and existing countermeasures. Applied Sciences, 12(12), 6042. https://doi.org/10.3390/app12126042

2. Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of human factors on cyber security within healthcare organisations: A systematic review. Sensors, 21(15), 5119. https://doi.org/10.3390/s21155119

3. Paka, W. S., Bansal, R., Kaushik, A., Sengupta, S., & Chakraborty, T. (2021). Cross-SEAN: A Cross-Stitch Semi-Supervised Neural Attention Model for COVID-19 Fake News Detection. arXiv. https://doi.org/10.48550/arXiv.2102.08924

Святослав ЖУКОВ
доктор екнономічних наук, старший науковий співробітник,
професор, професор кафедри
бізнес-адміністрування, маркетингу та менеджменту
ДВНЗ «Ужгородський національний університет»,
sviatoslav.zhukov@uzhnu.edu.ua

ТРАНСКОРДОННА ЕКОНОМІЧНА БЕЗПЕКА: ВИЗНАЧЕННЯ КАТЕГОРІЇ ТА ПРАКТИЧНЕ ЗНАЧЕННЯ ДЛЯ ТРАНСКОРДОННОГО СПІВРОБІТНИЦТВА

На сучасному етапі ключове значення в контексті безпеки країни набуває питання створення ефективної системи транскордонної економічної безпеки. Завдання теми полягають у висвітленні результатів досліджень у сфері прикордонної безпеки, економічної безпеки; визначенні суті та значення категорій «транскордонна безпека» і «транскордонна економічна безпека»; встановлення її значення для транскордонного співробітництва та прикордонних територій України. Все це визначає актуальність теми дослідження. Наукова новизна полягає в обґрунтуванні авторського бачення на суть зазначених вище термінів.

Зміст терміну «транскордонна безпека» містить уявлення про єдиний механізм безпеки громадян, суспільств і держав суміжних країн (їх прикордонних територій). Автор цей стан визначає як достатню захищеність зацікавлених (в першу чергу суміжних) держав від негативного впливу факторів, що діють «крізь межу», або що порушують нормальне функціонування системи позитивної транскордонної взаємодії. Це має на увазі узгоджений контроль держав над транскордонними потоками й іншими, діючими загрозливими факторами в межах фактичної зони їх функціонування, а також підтримка системи транскордонних зв'язків, що склалася на прикордонних територіях сусідніх країн [3, с. 54].

Практика транскордонної безпеки вже виникла та розвивається, але поки включена в зміст терміну «прикордонна безпека». Протидія транскордонної злочинності вимагає співпраці суміжних країн на прикордонних територіях. Подолання транскордонної злочинності в рівній мірі забезпечує прикордонну безпеку по обидві сторони межі. Можливі також багатобічні форми співпраці по боротьбі з транскордонною злочинністю. З вступом в дію ЗУ «Про транскордонне співробітництво» основні категорії та складові прикордонної безпеки слід переглянути та пристосувати до умов функціонування транскордонного співробітництва прикордонних територій суміжних держав. Особливо це стосується питань економічної безпеки. Тому є потреба дослідження поняття і суті «транскордонної економічної безпеки».

Ґрунтуючись на попередніх дослідженнях у даній галузі слід узагальнити визначення цього елементу безпеки. Транскордонна економічна безпека – це стан достатньої економічної захищеності регіонів (в першу чергу суміжних) держав, які є учасниками транскордонного співробітництва від негативної дії факторів, зокрема тих, що порушують нормальне функціонування транскордонного економічного співробітництва [1, с. 41, 51]. У першу чергу це визначення має на увазі узгоджений контроль сусідніх держав над транскордонними потоками економічних ресурсів та іншими факторами в межах територій їх функціонування з метою не допустити «тінізації» та «криміналізації» суб’єктів бізнесу. Ми акцентуємо увагу саме на сусідніх (суміжних) державах, чи їх територіях або регіонах, адже транскордонним співробітництвом можуть займатися як прикордонні території країн, так і території, які не мають спільний кордон з іншими державами.

За останні роки істотно змінився характер загроз безпеки Україні. Це пов’язано з появою нових категорій і понять, які стосуються так званих «транскордонних територій», «транскордонних ринків» тощо, що в загальному складає «транскордонний простір». У цьому транскордонному просторі потрібно і в подальшому проводити дослідження щодо впливу різних видів загроз, в тому числі й економічних, ступінь напруженості яких останнім часом виросли. Особливо це стосується західних прикордонних регіонів України, а зокрема Закарпатської області, яка має спільний кордон з чотирма країнами членами Євросоюзу.

Відповідно, і ступінь збільшення загрози на Закарпатті є найвищою за інші прикордонні області України. Саме тому Закарпатська область має стати полігоном для концентрації зусиль щодо посилення безпеки країни загалом, в тому числі й економічної [1, с. 41-42].

Спектр сучасних загроз транскордонної економічної безпеки України є достатньо широким. Повний і докладний його аналіз не входить в мету цієї публікації. Проте представляється необхідним детальніше розглянути ті загрози, які найбільш небезпечні для економіки області та країни в цілому, а також визначити головні напрямки фінансово-економічної діяльності із забезпечення реалізації транскордонного співробітництва [2, с. 135].

У прикордонні України з початком повномасштабного вторгнення росії і військових дій на території нашої держави все більше проявляється транскордонний характер незаконної міграції з метою потрапляння в країни Євросоюзу. Активізувалися і злочинні угрупування мігрантів, тісно пов'язані з українськими та міжнародними кримінальними структурами. Протиправна діяльність цих угрупувань, якщо не вжити екстрених заходів, може посилитися, чому сприяє прагнення країн Європи використовувати Україну як основний «санітарний бар'єр» (т. з. відстійник) на шляху незаконної міграції в країни ЄС.

Особливий інтерес в забезпеченні транскордонної економічної безпеки представляє аналіз ситуації та дій по припиненню різних видів контрабанди: наркотиків; товарів, матеріалів, енергоносіїв; різних видів ресурсів. До початку війни на території України динамічно формувалися багатопрофільні контрабандні структури, переважно кланового характеру одіозних політичних діячів. Припинення контрабанди при значних об'ємах товарообігу і пасажиропотоку, слабкості контролю, багато в чому залежить від взаємоузгоджених зусиль правоохоронних органів і спеціальних служб України як на міжвідомчому, так і на міждержавному рівні. Занепокоєння викликає облаштування пунктів пропуску на державному кордоні, недостатнє оснащення їх технічними засобами контролю. Кількість пунктів пропуску останніми роками постійно зростає, проте далеко не всі вони обладнані сучасними технічними засобами прикордонного та митного контролю, що є перепоною щодо вирішення проблеми забезпечення належного контролю за переміщенням вантажів через держкордон України.

Отже, необхідно розвинути методологію аналізу причин, що ведуть до виникнення транскордонної економічної безпеки в прикордонних регіонах України. Необхідні законодавчі ініціативи, що забезпечать можливість впливу на причини виникнення транскордонних загроз і економічних ризиків, на розвиток суспільних інституцій ефективної протидії цьому, на формування нового соціально-економічного середовища транскордонних регіонів. Все це забезпечить протидію транскордонній злочинності, контрабанді й ефектам діяльності транснаціональних компаній у правовому руслі господарювання суб'єктів економічної, і не тільки, діяльності. Надані пропозиції направлені на посилення транскордонної економічної безпеки України та її прикордонних територій.

Список використаних джерел

1. Жуков С.А. Механізм застосування регіонального маркетингу в системі транскордонного економічного співробітництва прикордонного регіону: монографія. Мукачево: в-тво «Елара», 2010. 276 с.

2. Утенкова К.О. Економічна безпека як складова національної безпеки України. Журнал Харківського національного університету імені В. Н. Каразіна. Серія «Міжнародні відносини. Економіка. Країнознавство. Туризм» № 9, 2019. С. 133-144. DOI: 10.26565/2310-9513-2019-9-17.

3. Штулер І.Ю. Напрями протидії загрозам економічній безпеці національного господарства: матеріали Міжнародної наукової Інтернет-конференції «Національна безпека у фокусі викликів глобалізаційних процесів в економіці», вип. 1. (Київ, 28-29 червня 2018 року) / ВНЗ «Національна академія управління». Київ: НАУ. 2018. С. 53-55.

Язмін ТЕЛІНГЕР
студентка 2 курсу спеціальності "Міжнародні відносини",
кафедра історії та суспільних дисциплін
Закарпатського угорського університету імені Ференца Ракоці II

Дмитро ТКАЧ
професор, доктор політичних наук,
кафедра історії та суспільних дисциплін
Закарпатського угорського університету імені Ференца Ракоці II

БЕЗПЕКА ЯДЕРНОЇ ЕНЕРГЕТИКИ В УКРАЇНІ: НАСЛІДКИ ЧОРНОБИЛЬСЬКОЇ АЕС

Чорнобильська атомна електростанція (ЧАЕС) — зупинена АЕС в Україні, розташована біля міста Прип'ять у Київській області. Була побудована в 1970–1977 роках і працювала до 2000 року. Свою назву станція отримала від міста Чорнобиль, яке знаходиться за 18 км. Станом на 1986 рік ЧАЕС була найпотужнішою АЕС у європейській частині СРСР. **26 квітня 1986 року** на четвертому енергоблоці сталася масштабна аварія під час випробувань, що призвела до вибуху та викиду радіації. Було зруйновано реактор, забруднено навколишню територію, евакуйовано жителів Прип'яті, Чорнобиля та інших населених пунктів у радіусі 30 км. Аварія стала однією з найсерйозніших техногенних катастроф в історії. Чимало працівників загинуло від опромінення. ЧАЕС розташована за 110 км від Києва та 16 км від кордону з Білоруссю.

Реактор РБМК-1000

На Чорнобильській АЕС використовували спеціальні ядерні реактори типу **РБМК-1000**. Це була радянська розробка, створена для виробництва електроенергії, а також — за потреби — для отримання матеріалів для ядерної зброї. Усього на станції працювали **чотири такі реактори**, ще два мали добудувати, але після аварії в 1986 році ці плани скасували. Ці реактори працювали на **урановому паливі**, яке охолоджувалося водою. Реактори типу РБМК, які використовувалися на Чорнобильській АЕС, мали низку особливостей, що вплинули на розвиток аварії 1986 року. По-перше, одним із головних недоліків був позитивний паровий коефіцієнт реактивності. Це означає, що при утворенні пари всередині активної зони, що відбувається зі зростанням температури, ядерна реакція не зменшувалась, як у більш безпечних реакторах, а навпаки — посилювалася. Така властивість робила реактор дуже нестабільним, особливо при роботі на низьких рівнях потужності, і ускладнювала контроль над процесом.

Другим важливим недоліком була конструкція аварійних керуючих стрижнів. Під час їхнього введення в активну зону, на початковому етапі вони витісняли воду, яка є гарним поглиначем нейтронів, через що короткочасно збільшували реактивність. Цей ефект особливо небезпечний у критичні моменти, оскільки може призвести до раптового прискорення реакції, що і стало одним із чинників вибуху на четвертому реакторі. Також варто відзначити, що системи автоматичного аварійного захисту були недостатньо ефективними для швидкої зупинки реакції у випадку аварійної ситуації. Вони не могли оперативно компенсувати небезпечні зміни у стані реактора, що призводило до того, що оператори опинялися у складних умовах, а інколи й не мали можливості запобігти катастрофі. Усі ці недоліки в поєднанні з людським фактором — помилками під час випробувань і порушеннями технологічного режиму — призвели до катастрофічної аварії, яка стала однією з найбільших техногенних катастроф в історії людства.

День катастрофи на Чорнобильській АЕС: що сталося 26 квітня 1986 року

26 квітня 1986 року о 1:23 ночі під час проведення планових випробувань на четвертому енергоблоці Чорнобильської АЕС сталася масштабна аварія. Через низку технічних помилок і недоліків конструкції реактора стався вибух, який зруйнував реакторний зал і викликав сильне пожежне загоряння. Вибух і пожежа спричинили викид великої кількості радіоактивних речовин у навколишнє середовище. Першими, хто прибув на місце аварії, стали пожежники. Вони навіть не знали про радіаційну небезпеку, адже інформація про масштаби катастрофи була засекречена. Пожежники боролися з вогнем кілька годин, ризикуючи своїм життям, адже отримували смертельно небезпечні дози радіації. Багато з них пізніше померли від променевої хвороби. Після

вибуху почалася евакуація жителів Прип’яті — міста, побудованого для працівників АЕС. Але спочатку людей не попередили про радіаційну загрозу, через що багато хто був підданий значному опроміненню. Уряд намагався локалізувати наслідки аварії, залучаючи тисячі "ліквідаторів" — військових, пожежників, інженерів, які працювали над укриттям реактора і прибиранням забрудненої території. Вони ризикували життям, часто без належного захисту.

Ця трагедія залишила глибокий слід в історії і показала небезпеку ядерної енергетики за відсутності належних заходів безпеки.

Світ дізнався про катастрофу лише через кілька днів, коли у країнах Західної Європи, зокрема у Швейцарії, зафіксували підвищений рівень радіації в атмосфері. Це стало першим сигналом для міжнародної спільноти про масштабну аварію на Чорнобильській АЕС. Лише після цього Радянський Союз офіційно підтвердив факт аварії. Така затримка з повідомленням призвела до того, що багато людей в зоні ураження були піддані значному опроміненню. Евакуація міста Прип’ять і прилеглих територій почалася тільки через 36 годин після вибуху, що значно ускладнило захист населення від радіації.

Чорнобильська АЕС: історія будівництва, катастрофи та міжнародної підтримки закриття

У 1970–1980-х роках в УРСР активно будували атомні електростанції (АЕС) для забезпечення зростаючих потреб в електроенергії. Першою була Чорнобильська АЕС, перший блок якої ввели в експлуатацію у 1977 році. До 1990 року в УРСР функціонувало 16 енергоблоків на п’яти АЕС. 26 квітня 1986 року на 4-му енергоблоці Чорнобильської АЕС сталася катастрофічна аварія з вибухом і великим викидом радіоактивних речовин, що забруднило близько 155 тисяч км² і торкнулося близько 5 мільйонів людей, з них 2,4 мільйони в Україні. Ліквідація наслідків аварії коштувала приблизно 12,6 млрд доларів. Західні країни швидко дізналися про катастрофу, запропонували допомогу, проте СРСР відмовився її приймати. У 1990 році Верховна Рада УРСР оголосила мораторій на будівництво нових АЕС, а після пожежі 1991 року зупинили другий блок ЧАЕС. У 1990-х роках США та Європейський Союз активно тиснули на Україну з вимогою закрити ЧАЕС через загрози ядерної безпеки в Європі та економічні інтереси, зокрема для американської компанії Westinghouse. Україна вела переговори, наполягала на фінансовій допомозі для закриття станції і модернізації інших АЕС. У 1994–1995 роках країни G7 пообіцяли надати Україні до 4 млрд доларів для закриття ЧАЕС. У 1995 році підписали меморандум про взаєморозуміння щодо безпеки станції. У 1996 році створили Міжнародний Чорнобильський центр за підтримки США, Великої Британії, Японії та Європи. Поступово, у 1996–2000 роках, зупиняли енергоблоки ЧАЕС, продовжувалась міжнародна співпраця і фінансування заходів з безпеки та соціальної підтримки міста Славутич. План заходів на об’єкті «Укриття» передбачав будівництво нової захисної арки, вилучення радіоактивних матеріалів із кошторисом у 758 млн доларів, що підтримували країни G7. У 2000 році США посилили тиск на Україну щодо остаточного закриття ЧАЕС, і президент Клінтон у червні того року оголосив дату закриття — 15 грудня 2000 року — з додатковою фінансовою допомогою.

Закриття ЧАЕС було складним економічним і соціальним рішенням, адже станція була важливим міськоутворюючим підприємством, гарантувала стабільність енергопостачання і потребувала створення альтернативних робочих місць.

Стан Чорнобильської АЕС у 2025 році

Чорнобильська атомна електростанція (ЧАЕС) з 1986 року не виробляє електроенергію та використовується як об’єкт зберігання і контролю радіації після аварії. Після повномасштабного вторгнення Росії в Україну у 2022 році станція опинилась під тимчасовою окупацією російських військ. За цей час на території ЧАЕС зафіксували численні порушення — вивезення обладнання, руйнування інфраструктури та забруднення, що завдало збитків на суму понад 135 мільйонів доларів.

У квітні 2022 року українські сили звільнили територію станції. З того часу ЧАЕС відновила роботу з підтримки безпеки об’єкта та контролю радіаційного фону. Технологічні системи станції працюють у штатному режимі, здійснюється цілодобовий моніторинг, який підтверджує відсутність аварійних ситуацій і витоків радіації. Однак наслідки окупації

вплинули на наукові дослідження, що проводилися в Чорнобильському радіаційно-екологічному біосферному заповіднику. Якщо до війни наукові роботи охоплювали близько 95% території заповідника, то зараз через пошкодження інфраструктури і обмежений доступ дослідницька діяльність можлива лише на приблизно 50% площі.

У лютому 2025 року зафіксували обстріл укриття над зруйнованим четвертим енергоблоком, але, за повідомленнями Державної служби з надзвичайних ситуацій України, радіаційних витоків або загроз для населення не було. Загалом станція утримується у стабільному стані, а заходи безпеки на території ЧАЕС залишаються пріоритетом для української влади і міжнародних партнерів. Щодо зони відчуження — вона залишається закритою для постійного проживання через високий рівень радіації, але з 2011 року у ній діє режим обмеженого туризму і екологічних досліджень. Зона відчуження охоплює територію площею понад 2600 квадратних кілометрів і є важливим природним заповідником, де природа поступово відновлюється без впливу людини. На майбутнє Україна разом з міжнародними партнерами планує продовжувати модернізацію захисних споруд, зокрема будівництво нового безпечного конфайнменту над зруйнованим реактором, підтримку екологічного моніторингу, а також розвиток програми сталого управління зоною відчужен

ня з акцентом на науку, екотуризм і збереження унікальної природи регіону.

Таким чином, хоча ЧАЕС не виробляє електроенергію вже понад 30 років, вона залишається важливим об’єктом екологічного контролю, радіаційної безпеки та наукових досліджень, а також символом однієї з найсерйозніших техногенних катастроф у світі.

Висновок

Чорнобильська атомна електростанція стала символом однієї з найбільших техногенних катастроф в історії людства, яка продемонструвала ризики і небезпеки ядерної енергетики за недостатнього рівня безпеки та контролю. Поєднання конструктивних недоліків реакторів РБМК-1000 та людських помилок під час випробувань призвели до масштабного вибуху, що спричинив викид радіації, забруднення великих територій та значні людські жертви.

Наслідки аварії відчуваються й досі: зона відчуження залишається непридатною для постійного проживання, а територія, що охоплює понад 2600 км², стала унікальним природним заповідником. Після зупинки енергоблоків станція перетворилася на об’єкт контролю радіаційної безпеки, де тривають наукові дослідження та екологічний моніторинг. Зокрема тимчасова окупація в 2022 році — показали, наскільки вразливою може бути інфраструктура, пов’язана з ядерною безпекою, у військових конфліктах. Водночас, звільнення території і подальше відновлення безпеки підкреслюють важливість міжнародної співпраці та підтримки України у модернізації захисних споруд і сталому управлінні зоною відчуження.

Отже, Чорнобильська АЕС — це не лише пам’ятник трагедії, а й живий приклад того, як треба відповідально ставитися до ядерної енергетики, враховувати технічні й людські фактори, забезпечувати найвищий рівень безпеки, а також підтримувати екологічну та соціальну стабільність регіону.

Список використаних джерел

1. Бабанін О. (2007). Міжнародна технічна допомога: співпраця України і США (1992-2007) // Агора. Вип. 6. С. 131-139.
2. Барановська Н. П. (2011). Суспільний вимір проблем атомної енергетики через призму подій на Чорнобильській АЕС (до 25-ї річниці аварії) // Наука та наукознавство. No2. С. 131-143.
3. Збірник наукових праць. Випуск 2 (33), 2024 Віктор Пашков, кандидат політичних наук, доцент кафедри міжнародних відносин Університет митної справи та фінансів (м. Дніпро) РОЛЬ США У ПИТАННІ ЗАКРИТТЯ ЧОРНОБИЛЬСЬКОЇ АЕС: ДОПОМОГА ЧИ ТИСК? С.122-131.

Онлайн джерела

1. https://uk.wikipedia.org/wiki
2. https://www.chnpp.gov.ua/ua/
3. https://suspilne.media/tag/caes/
4. https://www.bbc.com/ukrainian/articles/c1kmdrn2kylo

Марія МЕНДЖУЛ
докторка юридичних наук, професорка,
професорка кафедри цивільного права та процесу
ДВНЗ «Ужгородський національний університет»
керівниця ГО «Карпатська Агенція Прав Людини «ВЕСТЕД»,
mendzhul.marija@uzhnu.edu.ua

Неля ТІШКОВА
майор поліції, начальник відділу
адміністративної практики управління
патрульної поліції в Закарпатській області
Департаменту патрульної поліції,
Nelya1988@ukr.net

ТРАНСКОРДОННА ТРУДОВА МІГРАЦІЯ: БЕЗПЕКОВІ РИЗИКИ В УМОВАХ ВІЙНИ

У 2023 році було опубліковано заключний звіт щодо аналізу транскордонного регіонального ринку праці, у якому представлено результати дослідження із червня 2023 року до листопада 2024 року транскордонних регіонів Європейського Союзу. Рекомендації у звіті зосереджені на чотирьох ключових сферах: підтримка створення транскордонного аналізу ринку праці, забезпечення безперервності та довгострокової стійкості ініціатив шляхом підписання офіційних угод та фінансування, покращення доступності та збору даних шляхом узгодження методологій та використання інноваційних джерел та покращення координації політики для сприяння транскордонній зайнятості [1].

Розвиток транскордонної інтеграції ринку праці зумовлений відмінностями на самому ринку праці (наприклад, з точки зору заробітної плати, пропозицій роботи, податкового регулювання, систем соціального страхування, рівня зайнятості та безробіття). Регіони внутрішнього кордону становлять 40% території ЄС та генерують 30% валового внутрішнього продукту (ВВП) ЄС. У прикордонних регіонах проживає приблизно 150 мільйонів людей, що становить 30% від загальної чисельності населення ЄС. У внутрішніх прикордонних регіонах проживає 2 мільйони прикордонних мешканців, з яких 1,3 мільйона є прикордонними працівниками, що становить 0,6% від усіх зайнятих у ЄС [1].

На думку європейських дослідників транскордонна праця гарантує кількісне і якісне регулювання між потребами підприємств та наявністю робочої сили, а також кваліфікації у прикордонних громадах. Вказані потреби різняться від регіону до регіону, при цьому не всі транскордонні працівники мають однакові профілі, а транскордонна робота може розширювати межі, зони набору для роботодавців (географічне розширення пропозиції та попиту) [2]. З вказаним підходом ми погоджуємося, водночас міждисциплінарна орієнтація досліджень буде більш повна, якщо буде доповнена також правовими аспектами аналізу ринків праці у прикордонних територіях. У прикордонних громадах будуть відмінності у правових засадах регулювання ринків праці, водночас загальні стандарти у багатьох ключових позиціях є спільними, завдяки діяльності Міжнародної організації праці, виданим нею численним рекомендаціям та конвенціям. Проте відмінності будуть щодо процедури відбору персоналу, правових засадах регулювання порядку укладення та видів трудових договорів, відпусток, нормування робочого часу, соціальних гарантій, відповідальності працівників та роботодавців, підставах розірвання трудового договору, а також порядку розгляду трудових спорів.

Трохи відмінна ситуація у тих громадах України, які прилеглі до кордонів ЄС, зокрема у Закарпатті, що межує із Польщею, Словаччиною, Угорщиною та Румунією. З одного боку більші заробітні плати у державах-членах ЄС стимулюють працівників виїжджати у пошуках роботи до сусідніх країн, а з іншого боку наявні реальні кордони, перетин яких може займати від двох до 4-5 годин змушує людей переїздити на більш тривалий час, унеможливлює так звану «прикордонну маятникову трудову міграцію».

При дослідженні ринку праці у прикордонних громадах України до війни вчені відзначали на таких недоліках механізму регулювання як «нераціональність соціально-демографічного розвитку прикордонних районів, недостатня реалізація освітнього потенціалу населення, низька трудова, професійна та територіальна мобільність населення, відсутність умов для широкого формування якісної та конкурентоспроможної робочої сили, наявність значного сегмента неофіційної зайнятості, низька ефективність політики регулювання трудової міграції в прикордонних районах». У процесі дослідження ситуації у прикордонних громадах України було виявлено, що мають місце деструктивні зміни в кон'юнктурі ринку праці, зокрема зниження економічної активності населення, що спричинило пріоритетні темпи скорочення робочої сили порівняно з темпами скорочення постійного населення. Так, наприклад, офіційна чисельність економічно активного населення у віковій групі 15–70 років у 2012 році зменшилася на 1,4% у Жовтківському, Мостиському, Сокальському та Старосамбірському прикордонних районах Львівської області; на 1,8% у Володимир-Волинському, Любешівському та Любомильському районах Волинської області; на 2,6% у Вижницькому, Сторожинецькому, Глибоцькому, Герцаївському та Новоселицькому районах Чернівецької області; на 1,5% у Берегівському, Великоберезнянському та Виноградівському районах Закарпатської області, тоді як чисельність працездатного населення в середньому зменшувалася на 1,2–1,6% у Львівській, Волинській, Чернівецькій, Івано-Франківській та Закарпатській областях [3].

Повномасштабна війна зумовлює зростання різних вразливих груп, що можуть зазнавати дискримінації, а втрата дому, роботи, вимушене переміщення обумовлює потребу у інтеграції в нових місцях проживання. Вказана ситуація впливає і на ринок праці у прикордонних громадах, які прийняли чимало переселенців із територій активних бойових дій.

Список використаних джерел

1. Cross-Border Regional Labour Market Analysis. Final report. URL: https://ec.europa.eu/regional_policy/information-sources/publications/reports/2024/cross-border-regional-labour-market-analysis_en
2. Isabelle PIGERON-PIROTH. Borders and cross-border labor markets : opportunities and challenges. 2020. URL: https://cbs.uni-gr.eu/en/resources/knowledge-and-documentation-center/resources-list/borders-and-cross-border-labor-markets
3. Olha Iliash. LABOUR MARKET REGULATION TOOLS AND INSTRUMENTS FOR THE BORDER DISTRICTS OF THE WESTERN REGIONS OF UKRAINE. JOURNAL OF EUROPEAN ECONOMY. Vol. 13 (No 1). 2014. P. 52-67. 53-54 URL: https://jeej.wunu.edu.ua/index.php/enjee/article/view/724/704

Марія МЕНДЖУЛ
докторка юридичних наук, професорка,
професорка кафедри цивільного права та процесу
ДВНЗ «Ужгородський національний університет»
керівниця ГО «Карпатська Агенція Прав Людини «ВЕСТЕД»,
mendzhul.marija@uzhnu.edu.ua

Олена ТХІР
суддя Свалявського районного суду Закарпатської області,
Lena_th@i.ua

ЄВРОПЕЙСЬКІ ТРАНСКОРДОННІ РИНКИ ПРАЦІ: ДОСВІД ДЛЯ УКРАЇНИ В УМОВАХ ЄВРОІНТЕГРАЦІЇ

У 2025 році на глобальному рівні при аналізі ринків праці спостерігаються постійні трансформації, обумовлені пандемією COVID-19, зростанням вартості життя, геополітичними конфліктами, надзвичайними кліматичними ситуаціями та економічними спадами.

Ще у 2023 році європейські міністри на зустрічі у Мадриді зауважили на важливості соціального діалогу у зв'язку із змінами на ринку праці, обумовленими «зеленими» та «цифровими» переходами, а також на необхідності інвестування у цифрові навички, що є фундаментальними на тлі цифрової революції, оголосивши 2023 рік Європейським роком навичок. При цьому, саме громади мають бути ключовими суб'єктами для вирішення найкритичніших проблем і потреб, що має бути результатом партисипативного підходу, важливого для всіх соціальних груп. Вказаний шлях стане результатом впровадження політики ЄС та національної політики «справедливого цифрового переходу» із елементами підтримки, що вкрай важливо на фоні демографічної проблеми «старіння міст» із нестачею робочої сили та повною гендерною незбалансованістю. Рівень зайнятості чоловіків у ЄС у 2022 році був більш ніж на 10% вищим, ніж у жінок. Жінки також частіше мають нестабільну, тимчасову, неповну та неофіційну роботу, таку як у сфері догляду [1].

У 2024 році в ЄС гендерний розрив у зайнятості становив 10,0 процентних пунктів, а рівень зайнятості становив 80,8% для чоловіків та 70,8% для жінок. Розрив був на 0,2 п.п. нижчим, ніж у 2023 році, та на 1,1 п.п. нижчим порівняно з 2014 роком. Гендерний розрив у зайнятості був особливо вираженим серед населення, народженого за кордоном, де різниця в рівнях зайнятості досягла 18,1 п.п. Рівень зайнятості для чоловіків, народжених за кордоном, становив 83,1% порівняно з 65,0% для жінок. Жінки, народжені за кордоном, також мали рівень зайнятості на 15,7 п.п. нижчий, ніж жінки, народжені в державі-члені ЄС [2].

Відповідно до даних Державного комітету статистики України у першому кварталі 2021 року гендерний розрив в оплаті праці становив – 17,8%, у 2023 році – 18,6% [3]. В умовах повномасштабної війни ситуація на ринку праці в Україні має ще більший гендерний дисбаланс, є крайня потреба у перекваліфікації жінок для можливості виконання тих професій та робіт, які традиційно вважалися чоловічими.

Таким чином, гендерні розриви на ринку праці залишаються проблемою і в сучасний період, є актуальними не тільки для європейських держав, але і для України. Особливо невтішною є статистика щодо працівників-мігрантів, у контексті транскордонного ринку праці проблеми для працівників-мігрантів потребують вирішення щоб гарантувати транскордонний соціальний діалог та сталий розвиток прикордонних громад.

У прикордонних регіонах проживає приблизно 150 мільйонів людей, що становить 30% від загальної чисельності населення ЄС. У внутрішніх прикордонних регіонах проживає 2 мільйони прикордонних мешканців, з яких 1,3 мільйона є прикордонними працівниками, що становить 0,6% від усіх зайнятих у ЄС. Найбільш привабливою державою для транскордонних працівників є Німеччина (400 000 працівників, що прибули) та Швейцарія (370 000 працівників), за якою йдуть Люксембург (200 000), Австрія (170 000), Нідерланди (100 000), Бельгія (75 000) та Італія (60 000). Франція є країною з найбільшою кількістю

прикордонних працівників, що виїжджають (400 000), за нею йдуть Німеччина (220 000) та Польща (200 000). Іншими країнами зі значною кількістю прикордонних працівників, що виїжджають за кордон, є Румунія (130 000), Словаччина (120 000), Бельгія (100 000), Угорщина (100 000), Італія (90 000) та Чехія (60 000). Загалом, у ЄС спостерігається зростаюча тенденція, а кількість прикордонних працівників зросла за останні десятиліття [4].

Війна в Україні, найчисленніша міграція, зумовили низку безпекових загроз, які безумовно вплинули на транскордонні ринки в ЄС, що потребує детальних подальших досліджень, у тому числі для врахування кращих практик на шляху до євроінтеграції.

Список використаних джерел

1 A new era of the labour market? URL: https://eurocities.eu/latest/a-new-era-of-the-labour-market/?gad_source=1&gad_campaignid=22520641585&gbraid=0AAAApQ8GpQW90QgFNs5Dn9GQ9SDDUryv&gclid=Cj0KCQjwsNnCBhDRARIsAEzia4B-6SIzEXAeUzC93cmVh_a3zwCZg2NSdnO6iTsgiOk1VIh_KKe-0EkaAlkREALw_wcB

2 Employment gaps for women & people with disabilities. URL: https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20250527-1

3 На 18,6% менше. Що таке гендерний розрив в оплаті праці? URL: https://jurfem.com.ua/hendernyy-rosryv/.

4 Cross-Border Regional Labour Market Analysis. Final report. https://ec.europa.eu/regional_policy/information-sources/publications/reports/2024/cross-border-regional-labour-market-analysis_en

Artem RUDENKO
Bachelor's degree student (2nd year), majoring in Cybersecurity and Data Protection (Specialty 125)
State University "Kyiv Aviation Institute"
9148837@stud.kai.edu.ua

Natalia BILOUS
PhD (Pedagogy), Associate Professor of the Professional Foreign Languages Department,
State University "Kyiv Aviation Institute"
natalia.bilous@npp.kai.edu.ua

INFORMATION SECURITY IN CROSS-BORDER COOPERATION

In the context of globalization, information security challenges are becoming increasingly acute, as cyber threats recognize no state borders, and the fragmented nature of regulation leaves critical infrastructure vulnerable. This, in turn, heightens the need for harmonized international cybersecurity standards [1]. Cross-border data exchange and digital interaction create new vulnerabilities: attacks on governmental and communication systems, unauthorized access to sensitive information, and foreign interference in electoral processes have become real challenges to both national and international security. Information manipulation and disinformation campaigns are now considered a growing threat to security and foreign policy across entire regions (for example, the European Union) [2]. A vivid example is electoral processes that come under pressure from complex cyber and information attacks. Unprecedented hybrid influences are being recorded — from illegal financing and massive fake news dissemination to cyberattacks aimed at destabilizing democratic institutions [3]. Therefore, ensuring information security in cross-border cooperation is not just relevant but critically important.

This research is devoted to identifying current threats to information security in the cross-border domain. Its goal is to substantiate mechanisms for countering these threats through international coordination. To achieve this, it is necessary to address the following tasks: to analyze the main types of cyber and information threats arising in the context of cross-border interaction; to assess existing international initiatives, legal norms, and cooperation practices in the field of cybersecurity; and to determine key directions for enhancing cyber resilience and information protection through joint efforts of partner states. The relevance of the topic is determined not only by the growing number of attacks but also by their global nature — attackers can act simultaneously against several countries, exploiting vulnerabilities across different jurisdictions [5].

The scientific novelty of this study lies in its comprehensive approach to the problem of information security within cross-border cooperation, which combines technological, legal, and socio-political aspects. Unlike other studies that mainly focus on technical means of cyber defense, this work emphasizes the interconnection between joint technological measures and diplomatic cooperation.

The main threats to information security in cross-border cooperation are complex in nature. Among them are: cyberattacks on critical state information resources and communication networks; unauthorized intrusions into databases and espionage conducted via the global internet infrastructure; targeted disinformation campaigns and influence operations in social networks that undermine public trust; and interference in electoral processes by other states or non-state actors using both cyberattacks and propaganda. Particularly dangerous are hybrid information operations that combine technical methods of disruption (for example, hacking critical infrastructure websites) with psychological influence (mass dissemination of fake content and manipulation of public opinion). Such operations have repeatedly occurred and demonstrated high effectiveness in destabilizing entire regions.

Firstly, joint monitoring of cyber threats and intelligence sharing have become the foundation of security: no country today can fully detect all threats independently, whereas networks such as INTERPOL and Europol allow dozens of states to coordinate their efforts. A notable example is INTERPOL's global operation "Serengeti" (2024), during which over 1,000 cybercriminals were arrested across 19 countries under coordinated law enforcement efforts [4] — this case became a model

of successful cross-border cyber cooperation. Secondly, improving legal mechanisms significantly enhances collaboration: international agreements such as the Budapest Convention on Cybercrime harmonize legislation and simplify joint investigations of incidents [5]. Furthermore, modern regulatory acts emphasize the need for the unification of requirements and mutual recognition of security standards among countries [6]. Thirdly, the development of cyber resilience policies and the exchange of best practices increase preparedness for attacks: countries are implementing joint training, sharing response strategies, and building communication between national CERT/CSIRT teams. Importantly, the development of human potential — training leading cybersecurity specialists and improving the digital literacy of the general population — has been recognized as a priority in most national strategies and is supported internationally through cooperation and partnership programs.

Conclusions. Ensuring information security in cross-border cooperation is a multifaceted task based not only on technology but also on trust, ethics, and shared responsibility among states. The study identified key conditions for success in this area. Firstly, establishing trust among partner countries is a critical prerequisite for sharing sensitive information without fear of misuse. Overcoming geopolitical differences and building such trust are fostered by open dialogue and shared values, which ultimately eliminate barriers to cooperation [5]. Secondly, the creation of flexible international response mechanisms is necessary, including joint operational response centers and unified incident reporting protocols. Thirdly, it is crucial to continuously update the legal framework and standards in line with the dynamics of emerging threats. Finally, the dissemination of cyber hygiene culture and education beyond borders plays a key role. Increasing public awareness strengthens societal resistance to disinformation and social engineering methods.

References

1. DIGITALEUROPE. (2024). Securing cyberspace: the imperative for global regulatory alignment. *DIGITALEUROPE*. URL: https://www.digitaleurope.org/events/digital-deep-dive-securing-cyberspace-can-we-achieve-a-global-security-symphony
2. European External Action Service. (2023). Information Integrity and Countering Foreign Information Manipulation & Interference (FIMI). *European External Action Service*. URL: https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en
3. European Union Agency for Cybersecurity (ENISA). (2025). ENISA NIS360 2024 Report – Press Release. *ENISA*. DOI: 10.2824/1378797.
4. Leppard Law: Federal Criminal Lawyers. (n.d.). Evaluating International Cooperation in Protecting Transnational Critical Infrastructure Under US Federal Law. *Leppard Law*. URL: https://federal-criminal.com/computer-crimes/evaluating-international-cooperation-in-protecting-transnational-critical-infrastructure-under-us-federal-law/
5. OSCE Parliamentary Assembly. (2025). Press Release: Moldova's elections marred by cyberattacks, illegal funding and disinformation. *OSCE Parliamentary Assembly*. URL: https://www.oscepa.org/en/news-a-media/press-releases/2025/moldovas-parliamentary-elections-were-competitive-but-campaign-marred-by-cyberattacks-illegal-funding-and-disinformation-international-observers-say
6. World Economic Forum. (2024). Why collaboration is essential to tackling global cybercrime. *World Economic Forum*. URL: https://www.weforum.org/stories/2024/11/collaboration-key-tackling-cybercrime-cybersecurity

Тимофій УЗЛОВ
здобувач вищої освіти другого (магістерського) ступеня,
1 курсу, спеціальності F7 «Комп'ютерна інженерія»,
Державний університет «Київський авіаційний інститут»,
2211184@stud.kai.edu.ua

Наталя БІЛОУС
кандидат педагогічних наук,
доцент кафедри іноземних мов професійного спрямування,
Державний університет «Київський авіаційний інститут»
natalia.bilous@npp.kai.edu.ua

СТВОРЕННЯ ЄДИНИХ ІНФОРМАЦІЙНИХ ПЛАТФОРМ У КОНТЕКСТІ ЄВРОПЕЙСЬКОЇ ІНТЕГРАЦІЇ УКРАЇНИ

У сучасних умовах глобалізації та інтеграції євроатлантичного простору Україна стоїть перед завданням забезпечення ефективного управління своїми кордонами. Важливим є не лише контроль за пересуванням людей, транспорту і товарів, а й підтримка безпеки держави без обмеження свободи пересування та торгівлі, особово в умовах військового стану. Вирішення подібних завдань можливе через створення інтегрованих цифрових систем, які поєднують роботу прикордонної служби, митниці, правоохоронних органів та транспортних операторів. Впровадження таких платформ дозволяє відслідковувати переміщення осіб і вантажів у режимі реального часу, підвищує ефективність контролю та зменшує бюрократичні перепони. Як приклад можна розглядати інтеграцію української системи «Шлях» із європейськими системами обміну даними для забезпечення безпеки на кордоні та прискорення перетину пунктів пропуску.

Також треба зберігати баланс між свободою пересування та безбекою тому що свобода пересування є ключовою для розвитку економіки, туризму та співпраці з ЄС. Необхідно впроваджувати «розумні кордони» (smart borders), де за допомогою біометрії та аналітики ризиків забезпечується швидке та безпечне проходження громадян. Використання систем електронного декларування, автоматичного контролю та попереднього сканування дозволяє мінімізувати затримки без шкоди для безпеки.

Подібний підхід потребує не тільки впровадження але і розвиток транскордонної дипломатії довіри. Для ефективної роботи єдиних інформаційних платформ важливо будувати довірчі відносини з сусідніми державами на базі спільних робочіх груп, регулярних консультацій та обміну досвідом що дозволять оперативно реагувати на загрози та підтримувати прозорість процедур. Україна вже реалізує проєкти співпраці з Польщею, Румунією та країнами Балтії в сфері обміну прикордонною інформацією та протидії контрабанді.

При впровадженні цифрових платформ треба враховувати, що одним із викликів є захист персональних даних та дотримання прав людини. Важливим є технічне узгодження систем з міжнародними стандартами, навчання персоналу та розвиток кібербезпеки. Перспектива – інтеграція українських кордонів у європейський простір безпеки та полегшення транскордонного руху людей і товарів.

Враховуючи згадані вище моменти можна зробити наступні висновки:

- Єдині інформаційні платформи підвищують ефективність управління кордонами та безпеку держави.
- Баланс між свободою пересування та безпекою досягається через інтелектуальні технології контролю та прозорі процедури.
- Розвиток транскордонної дипломатії довіри зміцнює співпрацю з сусідами, підвищує стабільність регіону та дозволяє Україні ефективно інтегруватися в європейські системи.

Список використаних джерел

1. «Smart Borders: digital solutions to strengthen border crossing points amid limited funding» — про цифрові рішення для пунктів пропуску в Україні. ibm.in.ua
2. Офіційна сторінка European Commission про систему Entry/Exit System (EES) — баланс між обслуговуванням мандрівників та безпекою. Migration and Home Affairs
3. Стаття «EU changes border crossing procedure: what to expect» — про впровадження EES на кордонах з країнами-ЄС. eu-ua.kmu.gov.ua
4. Документ «UKRAINE-POLAND BORDER: Cooperation and …» — опис співпраці України з Польщею в прикордонному просторі. english.europewb.org.ua
5. Монографія «Cross-border cooperation of Ukraine with the EU countries» — аналіз розвитку прикордонної співпраці України з країнами ЄС. ird.gov.ua
6. Стаття про проект «SMART BORDER for UKRAINE» — підтримка реформ прикордонного контролю України відповідно до стандартів ЄС. estdev.ee
7. Довідка на сайті Державна прикордонна служба України (ДПСУ) про «Integrated border management» — реформування прикордонної системи України відповідно до стандартів ЄС. dpsu.gov.ua

Евелін МІНДАК
студентка 2 курсу спеціальності "Міжнародні відносини",
кафедра історії та суспільних дисциплін
Закарпатського угорського університету імені Ференца Ракоці II

Маріанна МАРУСИНЕЦЬ
кандидат філологічних наук,
доцент кафедри історії та суспільних диспиплін,
старший науковий співробітник, старший дослідник
Науково-дослідного центру імені Тіводора Легоцькі
Закарпатського угорського університету імені Ф. Ракоці II

ВНУТРІШНІ ВИКЛИКИ НАЦІОНАЛЬНОЇ БЕЗПЕКИ МЕКСИКИ

Сучасна модель національної безпеки держав Латинської Америки визначається не стільки традиційним зовнішніми військовими загрозами, скільки складним поєднанням внутрішніх, нетрадиційних та асиметричних викликів. Мексика, як ключовий гравець регіону та стратегічний сусід США, наочно демонструє як внутрішні соціально-політичні та кримінальні процеси фактично перетворилися на головні дестабілізуючі фактори національної безпеки. Недостатність інституційної стійкості, високий рівень корупції та безпрецедентна активність організованої злочинності створюють серйозну загрозу суверенітету, територіальній цілісності та суспільному порядку.

Головною загрозою вважається Організована злочинність (наркокартелі), зокрема угруповання, як-от "Сіналоа" та "Халіско Нового Покоління" (CJNG). Вони у свою чергу домінують на оптовому незаконному ринку наркотиків в США [1]. Їхня діяльність давно вийшла за межі наркотрафіку, адже відомо, що вони контролюють легальний бізнес, викрадають людей та незаконний обіг пального (хуачіколео). Зокрема відомо, що Посольство України в Мексиці у своїх порадах для подорожуючих, застерегла людей настуаними словами: Щоб не стати жертвою торгівлі людьми та злочинних угруповань, уникайте неправдивих оголошень у газетах, підозрілих або занадто привабливих пропозицій щодо працевлаштування з боку невідомих Вам людей, агенцій тощо. Цим підкреслюючи, що торгівля людьми таки практикуються даною організацією. Окрім цього, ця злочинна експансія призвела до виникнення "Паралельної влади": картелі здійснюють квазідержавні функції (неформальний "суд", "захист", стягнення "оподаткування") в окремих штатах (Чіуауа, Герреро, Мічоакан), що є ознакою де-факто втрати територіального контролю центральним урядом. Також було виявлено, що дана організація намагається впливати й політично, проштовхуючи своїх кандидатів — та перед цим вони вдавалися до спонсорування їхніх передвиборчих кампаній та змушували місцеві медіа публікувати замовні матеріали. В результаті, країна переживає небувалий рівень безкарності та насильства, включаючи політичні вбивства кандидатів та чиновників, що є прямим і кривавим тиском на інститути демократії. За словами Лучано Хазана, члена Робочої групи ООН з питань примусового або мимовільного зникнення, зіткнувшись з безкарністю, важливо посилити державні та федеральні прокуратури для виконання їх фундаментальної ролі у забезпеченні справедливості [3].

Інституційна слабкість та корупція:

Кримінальні загрози стали можливими через серйозну інституційну слабкість та розровсюджену корупцію. Основним чинником цього залишається системна корупція – глибоко вкорінений, майже структурний союз між політичною елітою, правоохоронними органами та злочинністю, що отримало назву "нарко-інституціоналізація". Ця корупція гарантує криміналітету безкарність, про що свідчить неефективність правосуддя: рівень розкриття злочинів по всій країні становить менше 5%, що підриває довіру до поліції та

судової системи [5]. У відповідь на цю кризу уряд усе більше вдається до мілітаризації покладаючись на армію та Національну гвардію для забезпечення громадської безпеки. Цей підхід критикують за те, що він підриває цивільний контроль, несе ризики порушення прав людини і є недостатнім для вирішення структурних проблем правосуддя. Проте у 2019 році, уряд Мексики все ж почав діяти в інтересах суспільства і оголосили такий собі аукціон майна корупціонерів, де виручені кошти були спрямовані на соціальні проекти, включаючи допомогу малозабезпеченим верствам населення. Опісля якого програма допомоги отримала символічну назву “Робін Гуд”[4].

Соціально-економічний розпад:

Було встановлено, що нерівність та відсутність можливостей створюють соціальне підґрунтя для злочинності. Нерівність та бідність залишаються значними, Крім того, Мексика є транзитною країною для нелегальної міграції з Центральної Америки. Люди, які шукають притулку в Мексиці, залишають свої країни через складні ситуації, такі як загрози з боку банд або організованої злочинності, порушення прав людини, гендерно зумовлене насильство або бідність. Проте виявилось, що Мексика також не спроможна дати той захист, понад 80% опитаних людей стали жертвами насильства. Отже, цей потік, хоча й є гуманітарною кризою, також перетворився на джерело значних прибутків для картелів, які займаються торгівлею людьми та викраденням мігрантів. Було проаналізовано, що усе це загострюється через слабку державну присутність: у віддалених та сільських регіонах держава не забезпечує базових соціальних послуг, освіти та безпеки, дозволяючи картелям заповнювати цей вакуум, пропонуючи місцевим громадам гроші та псевдо-захист, що ще більше інтегрує кримінальні структури в соціальний прошарок суспільства [2].

Встановлено, що основною внутрішньою загрозою національній безпеці Мексики є системна "нарко-інституціоналізація", якм передбачає глибоке проникнення організованої злочинності в державні установи, посилене тотальною корупцією. Стратегія, яка базується лише на використанні військових засобів, є недостатньою, оскільки не усуває соціально-економічні та інституційні проблеми. Для ефективного вирішення необхідно комплексно зміцнювати цивільні інститути та зменшувати рівень нерівності для відновлення контролю держави над власною територією.

Список використаних джерел

1. Клименченко, М. В. "ВІДНОСИНИ МІЖ США ТА МЕКСИКОЮ В КОНТЕКСТІ ПРОБЛЕМИ НЕЛЕГАЛЬНОЇ МІГРАЦІЇ." Дебют: Збірник тез доповідей студентів історичного факультету МДУ за результатами участі у Декаді студентської науки 2017/За заг. ред. д. політ. н., проф. КВ Балабанова, д. е. н., проф. ОВ Булатової.–Маріуполь, 2017.–151 с.: 57.
2. Столяр, О. П. "Боротьба із наркоторгівлею як основний напрямок співробітництва між Мексикою та США у безпековій сфері." Гілея: науковий вісник 114 (2016): 438-442.
3. З інформацією від EFE Безкарність - це великий виклик, що стоїть перед кризою зникнень в Мексиці: ООН URL:https://www.infobae.com/ua/2022/03/15/impunity-is-the-great-challenge-facing-the-crisis-of-disappearances-in-mexico-un/
4. Mayela Molina What is happening in Mexico? An overview of the situation for people on the move URL:https://www.nrc.no/feature/2024/what-is-happening-in-mexico-an-overview-of-the-situation-for-people-on-the-move
5. Tom Phillips in Mexico City Mexico sells off cars from corrupt rich to give to the poor URL:https://www.theguardian.com/world/2019/may/24/mexico-sells-off-cars-from-corrupt-rich-to-give-to-the-poor

Богдан ІГНАТЬО
аспірант кафедри конституційного права та порівняльного правознавства юридичного факультету ДВНЗ "Ужгородський національний університет"
адвокат, м. Ужгород, Україна
ihnatyob@gmail.com

ІНФРАСТРУКТУРНЕ ЗАБЕЗПЕЧЕННЯ БАЗОВИХ ПОТРЕБ ПРИ ТРАНСКОРДОННОМУ СПІВРОБІТНИЦТВІ

Постановка проблеми. Забезпечення базових прав людини неможливе без належного розвитку інфраструктури, яка виступає матеріальною та інституційною основою реалізації прав і свобод. Аналіз інфраструктурної спроможності в контексті конституційних прав дозволяє виявити механізми практичної реалізації останніх, мінімізувати ризики обмежень та утворити умови для рівного доступу до суспільних благ. Недоступність інфраструктури є одним із ключових індикаторів соціальної нерівності незалежно від задекларованого стану.

Транскордонне співробітництво покликане вирішувати спільні проблем прикордонних регіонів і територій України та суміжних держав. Серед основних завдань транскордонного співробітництва є вирішення викликаних наявними кордонами спільних проблем та взаємна інфраструктурна інтеграція країн-сусідів. Політика євроінтеграції України у поєднанні з низьким рівнем роз'яснення інтеграційних процесів серед широких верств населення породжує завищені очікування та надію на швидке приєднання України до Європейського Союзу, зокрема й до зони дії Шенгенської угоди. Водночас поширене уявлення, що членство України в Європейському Союзі є виключно політичним рішенням, яке може бути ухвалене "вже завтра", формує невиправдані сподівання на миттєве відкриття кордонів, скорочення черг у пунктах пропуску та, як наслідок, недооцінку потреби у розвитку прикордонної інфраструктури й транскордонного співробітництва. Це явище є дзеркальним, адже ідентичні погляди існують і країнах-сусідах України.

Актуальність, мета та наукова новизна дослідження. Доступність інфраструктури досліджували Любченко А.В. (2024), Шульгіна Л.І. (2020), Шелемба Михайло та Шелемба Марта (2020), Клименко Ю.І., Весела М.А., Мельнікова Ю.І. (2020), Мікула Н. (2004). Вченими визнається, що наявність кордонів є бар'єром до вільного розвитку соціально-економічних зв'язків та взаємної інтеграції. Висвітлюються проблеми рівного доступу до цифрової, транспортної та муніципальної інфраструктури, а також до сервісів, що забезпечують перетин державних кордонів. Дослідники акцентували увагу на питаннях доступності цифрових послуг, пов'язаних із правом на інформацію та орієнтованістю на потреби особи; на розбудові прикордонних регіонів, інфраструктура яких зазнає навантаження через інтенсивні пасажиропотоки та рух вантажів; на впровадженні інноваційних підходів до розвитку мережі пунктів пропуску. Запроваджена в Україні система електронної реєстрації на перетин кордону в напрямку Європейського Союзу "Електронна черга" дозволила наочно спостерігати за завантаженістю руху комерційного транспорту через пункти пропуску через державний кордон, оцінювати пікові сезонні навантаження та пасажиропотоки, що стало доказом актуальності теми інфраструктурного забезпечення при транскордонному співробітництві.

Короткий виклад завдання. Метою дослідження є аналіз кола сучасних викликів у сфері інфраструктурного забезпечення базових потреб людини у транскордонному співробітництві крізь призму конституційних прав, що нині повинні трактуватися як базові: право на доступ до інформації, право на свободу пересування, право на здійснення торгівлі, а також забезпечення національної безпеки у сферах економіки та міграції. Прикордонна інфраструктура, яка покликана задовольняти ці потреби, зазвичай, перебувала поза належною увагою. Це мало суттєвий вплив на розуміння проблем, їх чинників та формування спільних міждержавних підходів до розвитку транскордонного співробітництва. Йдеться про недостатні потуги до планування та розбудову інфраструктури прикордонних регіонів з урахуванням необхідності задоволення базових потреб людини, що націлені на інтеграцію

країн до інфраструктури країн Європейського Союзу. В умовах воєнного стану транскордонне співробітництво отримало нове законодавче врегулювання Законом України "Про міжнародне територіальне співробітництво України" (2024), який визначає одним із принципів такого додержання прав людини та основоположних свобод.

Питанням планування, розвитку та експлуатації транс'європейської транспортної мережі присвячені Регламент (ЄС) №1315/2013 Європейського парламента та Ради Європи від 11.12.2013 "Про настанови Євросоюзу щодо розвитку транс'європейської транспортної мережі та скасування Рішення №661/2010/ЄС" та Біла книга Європейської Комісії "План розвитку єдиного європейського транспортного простору — на шляху до конкурентоспроможної та ресурсоефективної транспортної системи". Біла книга закликає до розгортання інформаційної та комунікаційної транспортної технології з метою забезпечення кращого та інтегрованого керування транспортом, а також для спрощення адміністративних процедур шляхом поліпшеної вантажної логістики, моніторингом вантажів та їхнього статусу, а також оптимізації графіків руху та транспортних потоків. Тут визнається, що ще залишаються значні розбіжності між східними та західними частинами Євросоюзу у сенсі транспортної інфраструктури. Ці розбіжності мають бути подолані для створення повної інтегрованої європейською транспортною мережі. Регламент закликає збільшувати пропускну здатність шляхом усування перешкод та утворення нових інфраструктурних зв'язків як у межах держав-членів, так і між ними, а також, якщо це доречно, із сусідніми країнами, беручи до уваги триваючі переговори з державами-кандидатами та потенційними кандидатами на членство у Євросоюзі.

Висновки. Проблема інфраструктурного забезпечення базових потреб у сфері транскордонного співробітництва потребує постійної та значної уваги з боку урядів країн-сусідів, які прагнуть політичної та економічної інтеграції. Недостатній рівень розвитку інфраструктури, як показує приклад України та Європейського Союзу, створює труднощі не лише для країн-кандидатів, а й для держав-членів ЄС, населення яких часто поділяє помилкові уявлення про швидкість інтеграційних процесів й, відповідно, недоцільність розвитку прикордонних регіонів та мережі охорони державних кордонів.

Список використаних джерел

1. Клименко Ю.І., Весела М.А., Мельнікова Ю.І., 2022, Підвищення ефективності функціонування пунктів пропуску через державний кордон з використанням теорії масового обслуговування, Сучасні технології в машинобудуванні та транспорті, №1 (18), с. 103-109 (URL доступ 16.09.2025: https://eforum.lntu.edu.ua/index.php/jurnal-mbf/article/view/766/740)
2. Любченко А.В., 2024, Стратегії держави для сприяння та розвитку цифрової інфраструктури, Вчені записки ТНУ імені В.І. Вернадського. Серія: Публічне управління та адміністрування, Том 35 (74), №2, с. 81-90, DOI: https://doi.org/10.32782/TNU-2663-6468/2024.2/15 (URL доступ 16.09.2025: https://pubadm.vernadskyjournals.in.ua/journals/2024/2_2024/17.pdf);
3. Микула Н., 2004, Міжрегіональне та транскордонне співробітництво. Монографія. Львів, с. 7 (URL доступ 16.09.2025: https://znc.com.ua/ukr/publ/book/book-mikula-2004/book-mikula-2004.pdf);
4. Регламент (ЄС) №1315/2013 Європейського парламента та Ради Європи від 11.12.2013 "Про настанови Євросоюзу щодо розвитку транс'європейської транспортної мережі та скасування Рішення №661/2010/ЄС", (URL доступ 16.09.2025: https://eur-lex.europa.eu/eli/reg/2013/1315/oj/eng);
5. Шелемба Михайло, Шелемба Марта, 2020, Українсько-румунський кордон: стан, проблеми та перспективи розвитку, Міжнародний науковий вісник. Спецвипуск 1 (21). Ужгород, с. 82-93, DOI: https://doi.org/10.24144/2218-5348.2020.1(21).82-93 (URL доступ 16.09.2025: http://litopys.chdu.edu.ua/index.php/2218-5348/article/view/206453);
6. Шульгіна Л.І., 2020, Доступність інформаційно–комунікативних технологій та транспортної інфраструктури, Wielokierunkowosc Jako Gwarancja Postępu Naukowego, Том 2, с. 51-54 DOI 10.36074/21.02.2020.v2.18.

Катерина КОВАЛІВСЬКА
студент
Державний торговельно-економічний університет,
katakovalevskaa060@gmail.com

Марина КОВІНЬКО
кандидат філологічних наук,
доцент кафедри журналістики та реклами
Державний торговельно-економічний університет,
m.kovinko@knute.edu.ua

ОСОБЛИВОСТІ ВИКОРИСТАННЯ ДЕЗІНФОРМАЦІЇ В РОСІЙСЬКО-УКРАЇНСЬКІЙ ВІЙНІ

В умовах сучасного інформаційного суспільства війни виходять за межі бойових дій і переносяться в медіапростір. Дезінформація стала одним з головних інструментів гібридної агресії, який активно застосовує росія у війні проти України. Масштабність фейкових повідомлень і використання соціальних мереж для маніпуляції свідомістю громадян зумовлюють актуальність дослідження. Мета цієї роботи – розглянути особливості використання дезінформації в російсько-українській війні, визначити її основні форми, канали поширення та вплив на суспільну думку.

Створення фейкових повідомлень з метою введення суспільства в оману перетворилося на поширений інструмент ведення війни, що потребує ґрунтовного аналізу на матеріалі російсько-українського конфлікту [12]. Події в Україні демонструють, як активно рф використовує соціальні мережі та інші канали для поширення неправдивих відомостей, що підкреслює важливість застосування сучасних технологій для їх виявлення. На рис. 1 подано схему новинних матеріалів, у яких було зафіксовано прояви дезінформації.

Рисунок 1. Частка фейкових світових новин станом на лютий 2024 року, %
Джерело: [1]

Як показано на рис. 1, частка фейкових новин, що стосуються війни в Україні, становить 12%. Це свідчить про масштабну пропагандистську діяльність рф та активне поширення неправдивих повідомлень. Основне джерело надходження такої інформації – соціальні мережі як відкритий простір, де легко створити фейковий контент і поширити його без підтвердження достовірності.

В умовах війни значний обсяг дезінформації також надходить через російські медіа, доступ до яких і досі можливий в Україні. На рис. 2 відображено розподіл опитаних громадян за інформаційними каналами, яким вони довіряють у висвітленні подій, пов’язаних з війною.

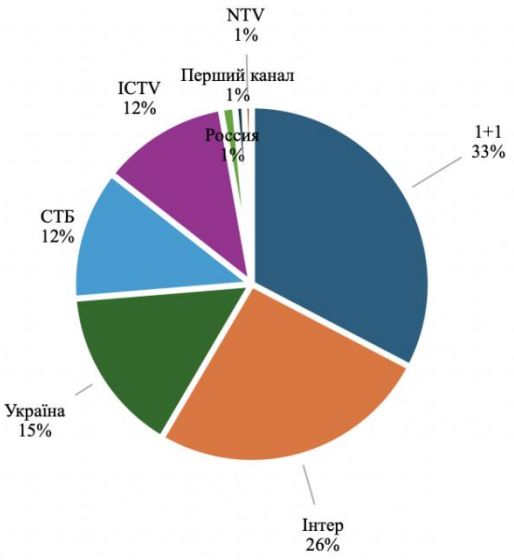


Рисунок 2. Структура довіри до каналів новин про військові події в Україні
Джерело: [3]

Аналіз даних рис. 2 показує, що 97% українців довіряють національним джерелам новин та інформації, яку вони поширюють [11]. Найвищий рівень довіри мають телеканали 1+1 та Інтер, з показниками 33% та 26% відповідно.

Добре усвідомлюючи силу дезінформації рф використовує її у війні проти України, особливо ту, яка створена за допомогою штучного інтелекту. Приклад дезінформації – твердження рф, що масове вбивство в Бучі це інсталяція акторів. Попри супутникові знімки, на яких видно трупи, міністр закордонних справ рф продовжував робити безпідставні заяви про те, що тіла насправді – актори і що на записах видно, як «трупи» рухаються [2, 3]. Росіяни цинічно розміщують інформацію про те, що їхні солдати роздали в Бучі 452 тонни гуманітарної допомоги, і що всі жителі цього району могли вільно покинути свої будинки, і що «нібито» масове вбивство в Бучі – це чергова репрезентація київського режиму для західних ЗМІ [1, 4]. Російські військові вривалися в будинки українських цивільних осіб і вимагали від них розповісти, де в Бучі переховуються нацисти, адже саме нацизм – знаменник, який рф намагається нав'язати Україні, виправдовуючи свою діяльність так званою денацифікацією України.

Міністр закордонних справ рф неодноразово зображує Україну як нацистську країну, що підтримується російськими ЗМІ, без жодних доказів на підтримку таких звинувачень, проте парадокс заяв про денацифікацію полягає в тому, що український президент Зеленський має єврейське походження [2]. Окрім того, що Путін намагається зобразити уряд Зеленського як нацистський, він переконаний, що в цьому «нацизмі» його підтримує НАТО [5]. Такі твердження демонструють маніпулятивну логіку російської пропаганди, яка намагається легітимізувати агресію через створення образу «ворога», спираючись не на факти, а на емоційно нав’язані міфи, які спотворюють історичну правду.

Ще одним приклад дезінформації – звинувачення полку «Азов» та інших радикалів у нападі на пологовий будинок у Маріуполі. МЗС рф наполягає на тому, що бійці «Азову» вивезли з пологового будинку всіх вагітних жінок, медсестер і весь персонал та створили там свою військову базу, а напад на пологовий будинок і дитячу лікарню в Маріуполі трактують як «шоу», режисери якого – українські націоналісти [4]. Однак правда полягає в тому, що російські бомби повністю зруйнували дитячу лікарню, а обстріли знову зупинили евакуацію з кількох міст, про що повідомляє міжнародне видання The Guardian [8]. Під час прес-конференції в Туреччині Лавров стверджував, що рф заздалегідь попередила ООН про те, що батальйон «Азов» захопив лікарню в Маріуполі, а на прохання журналіста прокоментувати

фотографії, які свідчать про жертви серед цивільного населення, переважно вагітних жінок і дітей, він помітно засмутився і назвав західних журналістів пропагандистами та режисерами українських націоналістів [9]. Такі висловлювання свідчать про свідому спробу дискредитувати незалежні медіа та відвернути увагу міжнародної спільноти від воєнних злочинів, використовуючи звичну для російської дипломатії тактику інформаційного заперечення та перекладання провини.

Після початку війни рф намагалася поширювати дезінформацію, щоб підготувати ґрунт для подальших нападів на Україну та виправдати початок війни [10]. Однією з причин, чому вони нападають на Україну, є те, що нібито Україна має лабораторії для виробництва біологічної зброї за підтримки США [6], однак на підтвердження цих звинувачень немає жодних доказів [7]. Цей фейк став частиною ширшої стратегії створення образу зовнішньої загрози, що дає змогу російському керівництву виправдовувати власні дії перед населенням і формувати ілюзію «захисної війни», тоді як насправді йдеться про спланковану агресію проти суверенної держави.

Крім цього, рф поширювала дезінформацію про існування в Україні біологічних лабораторій, підтримуваних США, але жодних доказів цього не існує [1]. Водночас активно застосовуються технології штучного інтелекту для створення фейкових профілів і поширення пропаганди через соціальні мережі. Відомо, що у межах одного з проєктів, який профінансувала ФСБ, було створено близько 1000 бот-акаунтів, що діяли під вигаданими «американськими» іменами [3]. Такі факти демонструють перехід російської пропаганди на новий технологічний рівень, де інформаційні атаки поєднують елементи кібервпливу й психологічних операцій. Це свідчить про системність дезінформаційної політики рф, яка використовує цифрові інструменти для масового поширення неправди та формування вигідних їй наративів у міжнародному інформаційному просторі.

У підсумку варто відзначити, що під час російсько-української війни дезінформація стала одним з ключових інструментів гібридної агресії, спрямованої на формування викривленої картини подій, підрив довіри до українських та міжнародних джерел інформації й виправдання власних воєнних злочинів. Основні канали поширення фейків – соціальні мережі, російські медіа та штучно створені інформаційні ресурси, що дає змогу охоплювати широку аудиторію та маніпулювати громадською думкою як всередині України, так і за її межами. Використання технологій, зокрема штучного інтелекту, значно ускладнює виявлення неправдивого контенту, робить проблему ще актуальнішою, що підкреслює необхідність розвитку систем протидії дезінформації та формування критичного мислення в суспільстві, аби зменшити ефективність інформаційної зброї рф.

Список використаних джерел

1. Berger, M., (2022). Putin say's he will 'denazify' Ukraine. Here's the history behind that claim [online]. The Washingtonpost Post. [Viewed 30 September 2025]. Available from: https://www.washingtonpost.com/world/2022/02/24/putin-denazify-ukraine
2. Browne, M., Botti, D. and Willis, H., (2022). Satellite images show bodies lay in Bucha for weeks, despite Russian claims [online]. New York Times. [Viewed 30 September 2025]. Available from: https://www.nytimes.com/2022/04/04/world/europe/bucha-ukraine-bodies.html
3. Damarad, V. and Yeliseyeu, A., (2024). Disinformation resilience in Central and Eastern Europe [online]. Ukrainian Prism. [Viewed 29 September 2025]. Available from: https://prismua.org/en/dri-cee
4. Polglase, K., Mezzofiore, G. and Doherty, L., (2022). Anatomy of the Mariupol hospital attack [online]. CNN. [Viewed 30 September 2025]. Available from: https://edition.cnn.com/interactive/2022/03/europe/mariupol-maternity-hospital-attack/index.html
5. Reality Check and BBC Monitoring, (2022). Bucha killings: Satellite image of bodies site contradicts Russian claims [online]. BBC. [Viewed 30 September 2025]. Available from: https://www.bbc.com/news/60981238

6. Robinson, O., Sardarizadeh, S. and Horton, J., (2022). Ukraine war: Fact-checking Russia's biological weapons claims [online]. BBC. [Viewed 30 September 2025]. Available from: https://www.bbc.com/news/60711705
7. Tarabay, J., (2024). US says Russia used AI-powered bots in disinformation scheme [online]. Bloomberg. [Viewed 30 September 2025]. Available from: https://www.bloomberg.com/news/articles/2024-07-09/us-says-russia-used-ai-powered-bots-in-disinformation-campaign
8. Watson, A., (2024). News consumers who saw false or misleading information about key topics in the last week worldwide as of February 2024 [online]. Statista. [Viewed 29 September 2025]. Available from: https://www.statista.com/statistics/1317019/false-information-topics-worldwide
9. Wintour, P., (2022). Sergei Lavrov prefers propaganda over reality in Ukraine talks [online]. The Guardian. [Viewed 30 September 2025]. Available from: https://www.theguardian.com/world/2022/mar/10/sergei-lavrov-russia-foreign-minister-propaganda-in-ukraine-talks
10. Аулін, О. та ін., (2023). Глобальні інформаційні, психологічні та гібридні війни: загрози та протидії. За заг. ред. В. Бебика та Н. Мякушко. Київ: Талком.
11. Кулеба, Д., (2022). Війна за реальність. Київ: Книголав.
12. Худолій, А., (2022). Інформаційна війна 2014–2022 рр. [онлайн]. Острог: Видавництво Національного університету «Острозька академія». [Дата звернення 30 вересня 2025]. Режим доступу: doi: 10.25264/978-617-8041-16-8

Ярослав СВИСТУН
студент 2 курсу магістратури,
ДВНЗ «Ужгородський національний університет»,
svystun.yaroslav@student.uzhnu.edu.ua

Ганна МЕЛЕГАНИЧ
кандидат політичних наук, доцент,
доцент кафедри міжнародних студій та суспільних комунікацій
ДВНЗ «Ужгородський національний університет»
hanna.melehanych@uzhnu.edu.ua

БЕЗПЕКОВИЙ ВИМІР ВІДНОСИН УКРАЇНИ З КРАЇНАМИ ЦЕНТРАЛЬНО-СХІДНОЇ ЄВРОПИ

Безпековий вимір став ключовим чинником зовнішньої політики України після початку широкомасштабної агресії Російської Федерації у 2022 році. У цьому контексті країни Центрально-Східної Європи (ЦСЄ) стали стратегічними партнерами України, надаючи військову, гуманітарну та політичну підтримку. Їхня активна позиція обумовлена спільними історичними досвідами, геополітичними інтересами та усвідомленням спільної загрози зі сходу.

Мета дослідження - проаналізувати безпековий вимір відносин України з країнами Центрально-Східної Європи в умовах російсько-української війни, визначити основні напрями співпраці у сфері оборони, енергетичної та інформаційної безпеки, а також окреслити перспективи формування спільної регіональної системи безпеки.

Актуальність теми. У сучасних умовах повномасштабної агресії Російської Федерації проти України питання регіональної безпеки набуло особливого значення для всіх країн Центрально-Східної Європи. Саме цей регіон опинився на передньому рубежі протидії новим військовим, енергетичним і гібридним загрозам. Відносини України з державами ЦСЄ формують не лише основу спільної оборонної політики, а й визначають майбутнє системи європейської безпеки загалом. Тісна співпраця у військовій, політичній, енергетичній та інформаційній сферах є запорукою стабільності, інтеграції України до євроатлантичних структур і зміцнення безпеки всього регіону.

Наукова новизна дослідження полягає у комплексному аналізі безпекового виміру відносин України з країнами Центрально-Східної Європи в умовах повномасштабної війни, що дозволяє виявити нові форми регіональної взаємодії та механізми колективної безпеки. У роботі узагальнено сучасні підходи до оцінки ролі країн ЦСЄ у зміцненні оборонного потенціалу України, визначено тенденції трансформації регіональної безпекової архітектури, а також окреслено перспективи формування нових форматів співпраці у межах європейських і євроатлантичних структур.

У дослідженні використано методи системного аналізу, порівняльного підходу, контент-аналізу офіційних документів та аналітичних матеріалів, а також елементи прогнозування. Отримані результати свідчать, що країни Центрально-Східної Європи відіграють ключову роль у формуванні спільного безпекового простору навколо України, активно підтримуючи її обороноздатність і політичну стабільність. Польща, Литва, Чехія, Словаччина та Румунія стали стратегічними партнерами у військово-технічній співпраці, гуманітарній допомозі та дипломатичному захисті інтересів України на міжнародному рівні. Аналіз показав, що співпраця у сфері енергетичної, інформаційної та кібербезпеки значно посилилася, а створення нових регіональних форматів — таких як Люблінська трійка та участь України в Ініціативі «Тримор'я» — свідчить про поступову інтеграцію України до системи колективної безпеки Європи. Зміцнення відносин із країнами ЦСЄ сприяє не лише підвищенню оборонної спроможності держав, а й формуванню нової архітектури регіональної безпеки, орієнтованої на демократичні цінності та стратегічну єдність.

Висновки. Проведене дослідження доводить, що безпековий вимір відносин України з країнами Центрально-Східної Європи є визначальним чинником стабільності у регіоні.

Співпраця у військовій, політичній та енергетичній сферах сприяє посиленню спільного потенціалу протидії загрозам і створенню умов для інтеграції України до європейських та євроатлантичних структур. Подальший розвиток цих відносин має ґрунтуватися на поглибленні стратегічного партнерства, узгодженні безпекових пріоритетів і посиленні інституційної взаємодії, що стане запорукою стійкої регіональної безпеки в Центрально-Східній Європі.

Список використаних джерел

1. Ministry of Foreign Affairs of Ukraine. Ukraine's cooperation with Central and Eastern Europe countries. URL: https://mfa.gov.ua
2. European Council. EU support for Ukraine. URL: https://www.consilium.europa.eu
3. NATO Official Portal. Eastern flank and regional security cooperation. URL: https://www.nato.int
4. Polish Institute of International Affairs. Security partnership between Poland and Ukraine. URL: https://pism.pl

Marianna LŐRINCZ
DSc, Professor
Philology Department
Ferenc Rákóczi II Transcarpathian Hungarian University
lorinc.marianna@kmf.org.ua

CORPUS-BASED COMPARATIVE ANALYSIS OF DISCOURSES IN THE EASTERN AND WESTERN MEDIA COVERAGE OF THE RUSSIAN-UKRAINIAN WAR

The full-scale Russian invasion of Ukraine resulted in an unprecedented volume of global media reporting with news outlets becoming key actors in mediating public knowledge of the war, framing interpretations of the conflict, and constructing ideological meanings through linguistic choices. This study offers a corpus-based comparative investigation of how Eastern and Western English-language media have represented the Russian-Ukrainian war at the lexical level. By examining prevalent textual features, the study elucidated the discursive constructions of war and implicit ideological orientations embedded in news reporting.

Conceptually, the research aligns with the theoretical underpinnings of Critical Discourse Analysis (CDA), which emphasizes the role of language in shaping, legitimizing, and contesting social realities. Previous scholarship has demonstrated that discourse contributes to the affirmation of power hierarchies, the reproduction of propaganda, and the manipulation of public opinion (Blommaert & Bulcaen, 2000; McLuhan, 2005). Studies specifically examining the war discourse in the Russian-Ukrainian context have revealed the use of lexical strategies to distort the nature of aggression, justify violence, and construct ideological allegiances (Shevchenko et al., 2022; Ilin & Nihmatova, 2023; Salihoglu & Karatepe, 2023). Building on this body of work, the present analysis employs corpus methods to uncover patterns across large text samples, which is essential to mitigate intuitive bias of discourse-oriented findings.

Two specialized corpora were compiled for the purpose of this study using the LexisNexis database. The Eastern Corpus (EC) consists of 3000 news excerpts totaling 475,506 tokens sourced from Asia News Monitor, South China Morning Post, and Hindustan Times. These outlets represent major Eastern geopolitical actors, providing insights into news narratives shaped outside the Euro-Atlantic sphere. The Western Corpus (WC) comprises 3000 excerpts (531,973 tokens) drawn from The Guardian, the Daily Mail and Mail on Sunday, and The New York Times. All texts in both corpora met the inclusion criterion of containing the explicit reference war in Ukraine either in the headline or body of the article (Lőrincz, 2023).

LancsBox tools (Words, N-gram, GraphColl, and KWIK) were employed to identify and interpret salient lexical patterns. Specifically, the analysis involved:

(1) keyword extraction using simple maths and Cohen's D to determine salient lexical items that signal dominant thematic concerns;

(2) n-grams analysis to explore contiguous phraseological structures that support discursive representation;

(3) collocation analysis of the lemma war to identify discourse prosodies;

(4) concordance exploration for context-sensitive qualitative interpretation.

The findings reveal both convergences and significant divergences in the lexical construction of war-related discourse. Keywords shared across corpora demonstrate a common negative evaluation of the military aggression, including lexical indicators of violence, destruction, and humanitarian suffering. This suggests that condemnation of the invasion functions as a globally salient discourse prosody.

However, substantial variations arise in the degree of attention awarded to specific themes, war actors, and geopolitical framing. In the WC, war is foregrounded as a violent intervention with clearly identifiable perpetrators and victims. High-impact lexical strategies emphasize brutality, urgency, geopolitical threat, and the need for defensive response. Moreover, emotionally charged descriptors (dangerous, despicable, disgusting, madness) contribute to a strongly evaluative narrative stance. The

WC thereby assumes a discursive position that unequivocally assigns agency and blame, while amplifying the humanitarian and political stakes of the war.

Conversely, the EC predominantly foregrounds geopolitical, diplomatic, and economic themes. Salient Eastern keywords such as cooperation, dialogue, trade, relations, abstain, economic highlight a more cautious stance centered on calls for diplomacy, peace negotiations, and regional stability. References to decision-makers (president, China, US, Moscow) outweigh references to war perpetrators or affected populations. Concordance analysis confirms recurring discursive patterns portraying the conflict as a crisis driven by internal Ukrainian developments rather than a unilateral act of external aggression. Lexical items signalling non-alignment (abstain, resolution) further construct a position of neutrality.

N-gram and collocation findings reinforce these patterns. While the WC produces expressions such as Russian attacks, nuclear annihilation, occupied areas, destruction of, mass grave, and kill thousands, the EC highlights Ukraine conflict, Ukraine crisis, war-torn Ukraine, Russia's war, and dialogue and, revealing both a more descriptive and more ambiguous stance. Both corpora demonstrate negative discourse prosodies attached to the lemma war, though with differing degrees of intensity and militarization.

Taken as a whole, the results illustrate a clear divergence in ideological positioning and discursive priorities. Western media demonstrate strong agency attribution and heightened attention to field conditions of war. Eastern media, in contrast, adopt a more moderate register, prioritize neutrality, and foreground diplomatic discourse, economic resilience, and multilateral cooperation. The findings indicate that war reporting functions not only as a vehicle of information transfer but also as a site of political alignment, ideological negotiation, and soft-power diplomacy. Consequently, news coverage contributes to shaping international public understanding of the war and can significantly influence geopolitical attitudes and global decision-making.

References

1. Ilin, I. & Nihmatova, O., 2023. The "Brotherly People" Metaphor and the Russian-Ukrainian Irredentist War: A Corpus-Based Study. Czech Journal of International Relations, 1(58), pp. 1–35. https://doi.org/10.32422/mv-cjir.504.
2. Lőrincz, M., 2023. A comparative corpus analysis of the Russian-Ukrainian war coverage in eastern and western English language news releases. The World of the Orient, 3(120), pp. 115–131. https://doi.org/10.15407/orientw2023.03.115.
3. McLuhan, M., 2005. The medium is the message. Gingko Press.
4. Salihoglu, S. & Karatepe, C., 2023. Investigation of online news about Ukraine-Russia war: A corpus-based critical discourse analysis. RumeliDE Dil ve Edebiyat Araştırmaları Dergisi, 33, pp. 1171–1186. https://doi.org/10.29000/rumelide.1279172.
5. Shevchenko, I., Morozova, I. & Shevchenko, V., 2022. Nominatsii ahresii Rosii proty Ukrainy v anhlomovnykh media: kohnityvno-prahmatychnyi analiz [Nominations of Russian aggression against Ukraine in English-language media: A cognitive-pragmatic study]. The Journal of V.N. Karazin Kharkiv National University. Series: Foreign Philology. Methods of Foreign Language Teaching, 95, pp. 70–78. https://doi.org/10.26565/2227-8877-2022-95-09

SZENYKÓ Volodimir
Hallgató, III. évfolyam, Nemzetközi kapcsolatok szak
Történelem- és Társadalomtudományi Tanszék,
II. Rákóczi Ferenc Kárpátaljai Magyar Egyetem
szenyko.volodimir.b23nk@kmf.org.ua

CSATÁRY György
docens, PhD,
Történelem- és Társadalomtudományi Tanszék
II. Rákóczi Ferenc Kárpátaljai Magyar Egyetem

HOLLANDIA A NATO-BAN: BIZTONSÁG, DIPLOMÁCIA ÉS INNOVÁCIÓ

Kulcsszavak: Hollandia, NATO, kollektív védelem, JFC Brunssum, NCIA, MCCE, védelmi kiadások, kiberbiztonság.

A klasszikus nagyhatalmi elméletek (Mearsheimer, Waltz) a haderő-nagyságot és nukleáris arzenált emelik ki fő változókként. A jelen tézisem ellenpontként azt teszi fel, hogy egy kisebb állam – jelen esetben Hollandia – a szövetségi rendszerben as is képes strukturális nagyhatalmi pozíciót kialakítani. A következő tételek mindegyike önállóan is vitatható, együttesen azonban magyarázatot adnak arra, hogyan vált a 42 ezer km²-es, 18 milliós ország a NATO egyik legintézményesebb és legtechnológiaibb tagjává.

Történelmi háttér és csatlakozás

Hollandia a második világháború alatt súlyos veszteségeket szenvedett. A háború végén újjá kellett építenie gazdaságát, infrastruktúráját és nemzetközi kapcsolatait. A hidegháború kezdete és a Szovjetunió terjeszkedése – különösen a kelet-európai államokban – komoly aggodalmat keltett Nyugat-Európában. 1948-ban Hollandia, Belgium, Luxemburg, az Egyesült Királyság és Franciaország aláírták a Brüsszeli Szerződést, amely kölcsönös védelmet és gazdasági együttműködést biztosított. Ez volt a NATO és az EU előfutára. Amikor 1949. április 4-én Washingtonban megalakult az Észak-atlanti Szerződés Szervezete, Hollandia az alapító 12 ország egyike volt. Ez azt jelentette, hogy a kezdetektől részt vettek a szövetség katonai és politikai struktúráinak kialakításában [1].

Hollandia csatlakozásának okai

Az ország 1940 és 1945 között német megszállás alatt állt, ami mély nyomot hagyott a holland társadalomban és politikai gondolkodásban. A háborús tapasztalatok megmutatták, hogy a kisebb államok önállóan nem képesek megvédeni magukat a nagyhatalmak agressziójával szemben. A Szovjetunió terjeszkedése és a kommunizmus előretörése a kelet-európai térségben újabb fenyegetést jelentett Nyugat-Európa számára, és Hollandia felismerte, hogy biztonságát csak egy kollektív védelemi rendszer keretében tudja garantálni. A NATO-hoz való csatlakozás ezért mindenekelőtt biztonsági szükségletből történt. Az Észak-atlanti Szerződés 5. cikkelye – amely kimondja, hogy egy tagállam elleni támadás az összes tagállam elleni támadásnak minősül – olyan garanciát biztosított, amelyre Hollandia önállóan nem lett volna képes. Különösen fontosnak számított az Egyesült Államok részvétele a szövetségben, hiszen Washington katonai ereje és nukleáris elrettentő képessége a legfőbb biztosítékként szolgált az európai biztonság fenntartására [2].

A NATO-tagság politikai szempontból is jelentős mérföldkőnek számított Hollandia számára. Az ország ezzel megerősítette elköteleződését a nyugati demokratikus értékek, a jogállamiság és az emberi jogok mellett, és határozottan elhatárolódott a keleti blokk ideológiai rendszerétől. A hidegháború kezdetén a nyugati orientáció a politikai stabilitás záloga volt, és segítette a holland diplomáciát abban, hogy szilárd helyet foglaljon el a transzatlanti közösségen belül. Gazdasági szempontból a NATO-hoz való csatlakozás összhangban állt az ország újjáépítési céljaival. A háború után Hollandia súlyos károkat szenvedett, és a Marshall-segély felhasználása, valamint a biztonságos nemzetközi környezet megteremtése kulcsfontosságú volt a gazdasági stabilitás helyreállításához. A katonai védelem biztosította a politikai és gazdasági fejlődéshez szükséges hátteret, amelyre a holland exportorientált gazdaság is építhetett. A csatlakozás hátterében ugyanakkor erős regionalista

elköteleződés is állt. Hollandia már 1948-ban aláírta a Brüsszeli Szerződést Belgium, Luxemburg, Franciaország és az Egyesült Királyság társaságában, amely a kollektív védelem és gazdasági együttműködés korai formáját jelentette. Ez a lépés előkészítette a NATO megalakulását, és Hollandiát az európai integráció egyik korai szorgalmazójává tette.

Hollandia NATO-tagsága kezdettől fogva aktív részvételt jelentett. Katonai hozzájárulásban például Holland csapatok részt vettek a koreai háborúban (1950–53) ENSZ-erők keretében – ez erősítette az atlanti elkötelezettséget. A hidegháború idején holland területen állomásoztak NATO-erők, és az ország jelentős hadsereget tartott fenn a Varsói Szerződés elrettentésére. 1990 után Hollandia rendszeresen részt vett NATO-missziókban: Bosznia (IFOR, SFOR), Koszovó (KFOR), Afganisztán (ISAF és Resolute Support), valamint a balti országok légtérvédelmében (Baltic Air Policing). Tengerészeti szerepük is erős haditengerészettel rendelkezik, modern fregattokkal és logisztikai hajókkal. Gyakran vállal vezető szerepet NATO-tengerészeti kötelékekben, például az Északi-Atlanti és a Földközi-tengeri járőrfeladatokban.

Politikában és diplomáciában is Hollandia aktívan részt vesz a NATO Tanácsában és a különféle bizottságok munkájában. Híres arról, hogy kompromisszumkereső, közvetítő szerepet játszik a szövetségen belül. Az innováció és kibervédelem Hága számos nemzetközi szervezet otthona, köztük a NATO Kibervédelmi Kiválósági Központ egyik társpartnere. Hollandia kiberképességei fontosak a modern hadviselésben. Katonai költségvetés: Bár sokáig vitatták, hogy elérik-e a NATO által elvárt 2%-os GDP-arányos védelmi kiadást, az utóbbi években Hollandia jelentősen növelte védelmi költségvetését az ukrajnai háborúra és a fokozott orosz fenyegetésre reagálva [3].

NATO-intézményei Hollandiában

A Joint Force Command Brunssum (JFC Brunssum) NATO egyik legfontosabb operatív parancsnoksága, amely Brunssum városában, Limburg tartományban, Hollandiában található, közel a német határhoz. A parancsnokság 1953-ban jött létre eredetileg Allied Forces Central Europe (AFCENT) néven, Franciaországban, de 1967-ben áthelyezték Brunssumba. 2004 óta viseli a mai nevét, és a NATO „Allied Command Operations” struktúrájának egyik operatív központja. A JFC Brunssum feladata a NATO műveleteinek irányítása és koordinálása. A parancsnokság vezeti például a NATO Enhanced Forward Presence misszióját a balti országokban és Lengyelországban, ahol a szövetséges csapatok rotációs jelenléte biztosítja a kollektív védelmet. Emellett részt vett az afganisztáni ISAF és Resolute Support missziók parancsnoki irányításában is. A parancsnokság kulcsszerepet játszik a NATO Response Force (NRF), a gyorsreagálású erő működtetésében, biztosítva, hogy válsághelyzetben a szövetség gyorsan tudjon bevetni többnemzeti erőket. JFC Brunssum továbbá stratégiai és védelmi tervezéssel is foglalkozik. A parancsnokság kidolgozza a NATO európai hadszíntérre vonatkozó terveit, szervezi a gyakorlatokat, és biztosítja, hogy a tagállamok hadereje interoperábilis legyen. A parancsnokság személyzete nemzetközi összetételű: különböző NATO-tagországok tábornokai és szakemberei dolgoznak együtt, ami a többnemzeti együttműködés egyik példája a szövetségen belül.

A NATO Communications and Information Agency (NCIA) a NATO technológiai és kiberbiztonsági központja, amely kulcsszerepet játszik a szövetség kommunikációs és informatikai rendszereinek fejlesztésében, üzemeltetésében és védelmében. Az NCIA központja Hága városában található, és több mint 30 helyszínen működik világszerte. A szervezet feladatai közé tartozik a parancsnoki és irányítási rendszerek (C4ISR), a kiberbiztonság, a légvédelmi rendszerek, valamint a műveletek és gyakorlatok támogatása. Az NCIA biztosítja a NATO tagállamai közötti kommunikációt és együttműködést, hozzájárulva ezzel a szövetség biztonságának és hatékonyságának növeléséhez.

A Movement Coordination Centre Europe (MCCE) egy multinacionális katonai koordinációs központ, amely az Eindhoven repülőtéren található, Hollandiában. Az MCCE feladata a stratégiai katonai szállítások koordinálása és optimalizálása a tagállamok között. A központ célja, hogy javítsa a szállítási kapacitások kihasználtságát, csökkentse a költségeket, és biztosítsa a gyors és hatékony mozgósítást válsághelyzetekben. Az MCCE tagjai között megtalálhatóak NATO és EU tagállamok, valamint más országok is, akik hozzájárulnak a központ működéséhez [4].

Felhasznált irodalom

1. Government of the Netherlands. (n.d.). The Netherlands and NATO. https://www.government.nl/topics/nato/the-netherlands-and-nato government.nl [1] (24.10.2025)
2. NATO, "Collective defence – Article 5," https://www.nato.int/cps/en/natohq/topics_110496.htm [2] (24.10.2025)
3. Statistics Netherlands (CBS), "The Netherlands ranks 7th on defence expenditure among NATO members," 29 April 2025, https://www.cbs.nl/en-gb/news/2025/25/the-netherlands-ranks-7th-on-defence-expenditure-among-nato-members [3] (24.10.2025)
4. Allied Joint Force Command Brunssum. (2024). About JFC Brunssum. https://jfcbs.nato.int/ [4] (24.10.2025)

NAGY Mariann Zsuzsanna
Hallgató, III. Évfolyam, Nemzetközi kapcsolatok szak
Történelem- és Társadalomtudományi Tanszék,
II. Rákóczi Ferenc Kárpátaljai Magyar Egyetem
nagy.mariann-zsuzsanna.b23nk@kmf.org.ua

HIRES-LÁSZLÓ Kornélia
PhD, főiskolai docens
Történelem- és Társadalomtudományi Tanszék,
II. Rákóczi Ferenc Kárpátaljai Magyar Egyetem
intézményvezető
Hodinka Antal Nyelvészeti Kutatóközpont
Beregszász, Ukrajna
ORCID ID: 0000-0002-6526-6489
hires.laszlo.kornelia@kmf.org.ua

LENGYEL-MAGYAR EGYÜTTMŰKÖDÉS A NATO-N BELÜL

A 21. század első évtizedeiben a közép-európai biztonsági környezet jelentős átalakuláson ment keresztül. A NATO-bővítés 1999-es hullámában Lengyelország és Magyarország is csatlakozott az Észak-atlanti Szerződés Szervezetéhez, ezzel új fejezetet nyitva a régió kollektív védelempolitikájában (Gergelewicz, 2020). Az euroatlanti integráció mindkét ország számára stratégiai cél volt, ugyanakkor a biztonságpolitikai prioritások és a külpolitikai orientációk az évek során eltérő irányt vettek. Lengyelország a NATO keleti szárnyának egyik legaktívabb szereplőjévé vált, míg Magyarország inkább a déli stabilitás, a diplomáciai kiegyensúlyozottság és a pragmatikus együttműködés politikáját képviselte (Avar, 2023). A különbségek ellenére a két állam kapcsolatai továbbra is meghatározóak a NATO-n belül és a Visegrádi Együttműködés (V4) keretében.

A lengyel–magyar együttműködés gyökerei mély történelmi alapokon nyugszanak. A két nép közötti kapcsolat a középkorig visszanyúló szövetségi, dinasztikus és kulturális kötelékekre épül. A 14. században I. (Nagy) Lajos magyar király egyben Lengyelország uralkodója is volt, ami a két nemzet közötti politikai közösséget erősítette. A 19. század szabadságharcai idején a lengyel és magyar függetlenségi mozgalmak egymás támogatásával léptek fel az elnyomó hatalmakkal szemben – Bem József és Petőfi Sándor neve szimbolikusan is összefonódott ebben a korszakban. A 20. század tragikus történelmi tapasztalatai – a második világháború, majd a szovjet blokk uralma – tovább mélyítették a közös sorsélményt és a politikai szolidaritás tudatát.

A rendszerváltozást követően mindkét ország a nyugati integrációs struktúrákhoz való csatlakozásban látta biztonságának és fejlődésének garanciáját. A NATO-hoz való 1999-es csatlakozás és az Európai Unióhoz való 2004-es belépés közös stratégiai irányt jelölt ki, amely a politikai, katonai és gazdasági együttműködést új szintre emelte.

A tanulmány célja annak bemutatása, hogy miként befolyásolják az eltérő biztonságpolitikai, gazdasági és külpolitikai prioritások a lengyel–magyar együttműködést a NATO-n belül, illetve milyen mértékben képes a Visegrádi Együttműködés struktúrája kiegyensúlyozni az aktuálpolitikai megosztottságot.

Gizicki (2013) szerint a Visegrádi Csoport akkor működhet valódi biztonsági közösségként, ha a tagállamok egységes fenyegetésképet alakítanak ki és összehangolt válaszokat adnak. A jelen helyzet azonban éppen az egység hiányát mutatja, különösen az orosz–ukrán háború 2022-es kitörését követően.

Lengyelország az euroatlanti szolidaritás egyik legaktívabb képviselőjeként jelentős katonai és politikai támogatást nyújt Ukrajnának, míg Magyarország a béketárgyalások és a diplomáciai megoldások fontosságát hangsúlyozza, elutasítva a fegyverszállításokat (Jureńczyk, 2023; Kamola-Cieślik & Akyesilmen, 2024). A két ország közötti különbség az energiapolitikai függőségekben és a biztonsági fenyegetések eltérő percepciójában is megmutatkozik: Lengyelország számára Oroszország hagyományosan stratégiai fenyegetést jelent, míg Magyarország pragmatikus gazdasági kapcsolatokat tart fenn Moszkvával (Kopyś, 2013).

Ezzel párhuzamosan a gazdasági kapcsolatok tovább erősödtek: Lengyelország Magyarország egyik legfontosabb kereskedelmi partnere a közép-európai térségben, míg a magyar vállalatok

(különösen az energetika és gyógyszeripar területén) aktív befektetőként vannak jelen a lengyel piacon. A kulturális együttműködés a Visegrádi Alap és a bilaterális intézmények révén szintén jelentős: közös oktatási programok, ifjúsági csereprojektek és kulturális fesztiválok járulnak hozzá a társadalmi kötelékek erősítéséhez.

A tanulmány relevanciája kettős. Egyrészt a NATO keleti szárnya a jelenlegi geopolitikai környezetben a kollektív biztonság egyik legfontosabb pillére. Lengyelország, mint a Baltikum védelmi vonalának kulcsszereplője, és Magyarország, mint a Balkán irányába mutató stratégiai tengely, eltérő, de egymást kiegészítő funkciókat tölt be (Gergelewicz, 2020).

Másrészt a Visegrádi Együttműködés továbbra is lehetőséget kínál a regionális koordináció erősítésére, még akkor is, ha a politikai nézetkülönbségek időnként akadályozzák a közös álláspont kialakítását.

A tudományos újdonság abban áll, hogy a lengyel–magyar NATO-együttműködést nem pusztán kétoldalú politikai viszonyként, hanem komplex, többdimenziós rendszerként vizsgálja, amely magában foglalja a történelmi, gazdasági, kulturális és biztonsági aspektusokat is. Korábbi tanulmányok elsősorban a történeti vagy diplomáciai narratívákra koncentráltak (Chruściel, 2014; Gizicki, 2013), míg jelen elemzés strukturális tényezőket is figyelembe vesz: a döntéshozatali mechanizmusokat, a katonai együttműködési platformokat, valamint a stratégiai kommunikáció és a politikai koordináció szerepét.

Ezen túlmenően a tanulmány kritikailag rámutat arra, hogy a lengyel–magyar partnerség a NATO-n belül nem rendelkezik hosszú távú, közösen kialakított stratégiai jövőképpel, ami csökkenti az együttműködés hatékonyságát és a regionális érdekérvényesítés súlyát.

Összegzésként megállapítható, hogy a lengyel–magyar együttműködés a NATO-n belül strukturálisan stabil, de politikailag polarizált. A Visegrádi Együttműködés formális intézményei – mint a Visegrádi Alap és a közös védelmi tanácskozások – továbbra is fenntartják a párbeszédet és a koordinációs kereteket, ugyanakkor a stratégiai célokban, a külpolitikai irányokban és a fenyegetésérzékelésben markáns eltérések mutatkoznak.

A történeti barátság, a kulturális szolidaritás és a gazdasági kölcsönös érdekek továbbra is összetartó erőt jelentenek, azonban a politikai divergencia és a biztonságpolitikai megosztottság akadályozza a hosszú távú stratégiai partnerség elmélyülését. A jövőbeli együttműködés sikerét az határozza meg, hogy Lengyelország és Magyarország képesek lesznek-e újrafogalmazni közös biztonsági és külpolitikai percepciójukat, és ennek alapján megerősíteni az euroatlanti szövetségi elköteleződést.

A NATO keleti szárnyának erősítése és a V4 mechanizmusok modernizálása – különösen a kiberbiztonság, az energetikai függetlenség és a védelmi ipari innováció területén – lehet a jövő kulcsa. Amennyiben a két ország a történelmi szolidaritás szellemében képes összehangolni nemzeti és kollektív érdekeit, a lengyel–magyar partnerség továbbra is meghatározó szerepet tölthet be a közép-európai biztonsági architektúra alakításában.

Felhasznált irodalom

1. Avar, Y. (2023). Poland’s Perspectives on NATO through the Speeches of President Andrzej Duda. International Journal of Politics and Security, 61–77. https://www.researchgate.net/publication/374230507_Poland's_Perspectives_on_NATO_through_the_Speeches_of_President_Andrzej_DudaPoland's_Perspectives_on_NATO_through_the_Speeches_of_President_Andrzej_Duda
2. Chruściel, M. (2014). The Reasons of Non-Institutional Character of the Early Visegrad Cooperation in the View of Neorealist and Neoliberal Theories in International Relations. Poliarchia, 2(3). https://www.researchgate.net/publication/304396586_The_Reasons_of_Non-Institutional_Character_of_the_Early_Visegrad_Cooperation_in_the_View_of_Neorealist_and_Neoliberal_Theories_in_International_Relations
3. Gergelewicz, T. (2020). Poland’s Accession to NATO Considering “Partnership for Peace” and the U.S. Perspective. Safety & Defense, 6(2). https://www.researchgate.net/publication/347064983_Poland's_Accession_to_NATO_Considering_Partnership_for_Peace_and_the_US_Perspective

4. Gizicki, W. (2013). A Security Community. Poland and Her Visegrad Allies: the Czech Republic, Hungary and Slovakia. Lublin: Wydawnictwo KUL. ISBN 978-83-7702-727-1. https://www.researchgate.net/publication/338458825_A_Security_Community_A_Security_Community_Poland_and_Her_Visegrad_Allies_the_Czech_Republic_Hungary_and_Slovakia
5. Górka, M. (2018). The Cybersecurity Strategy of the Visegrad Group Countries. Politics in Central Europe, 14(2), 75–98. https://www.researchgate.net/publication/327722785_The_Cybersecurity_Strategy_of_the_Visegrad_Group_Countries
6. Jureńczyk, Ł. (2023). Poland's support for Ukraine's aspirations to NATO membership. Bezpieczeństwo. Teoria i Praktyka, LII(3), 29–40. https://www.researchgate.net/publication/380598299_Poland's_support_for_Ukraine's_aspirations_to_NATO_membership
7. Kamola-Cieślik, M., & Akyesilmen, N. (2024). Energy security policy of Poland and Hungary in the context of the Russian Federation war with Ukraine: A comparative analysis. Rocznik Instytutu Europy Środkowej, 2024(1). https://ies.lublin.pl/wp-content/uploads/2024/11/riesw_2024-01-05.pdf
8. Kesztyűs, V. (2024). Possibilities of Air Force Cooperation in the Visegrad Countries. Repüléstudományi Közlemények. https://real.mtak.hu/217932/1/06_kesztyus_71-80_RTK_2024_1.pdf
9. Kopyś, T. (2013). Wizje polityki regionalnej Węgier i ich rola w ramach Grupy Wyszehradzkiej. Rocznik Instytutu Europy Środkowo-Wschodniej, 11(1), 53–80. https://ruj.uj.edu.pl/entities/publication/ec88d303-788a-4ce1-a14a-3229f0c97ef9

BUNDA Veronika
Hallgató, II. Évfolyam, Nemzetközi kapcsolatok szak
Történelem- és Társadalomtudományi Tanszék,
II. Rákóczi Ferenc Kárpátaljai Magyar Egyetem
bunda.veronika.b24nk@kmf.org.ua

MOLNÁR D. Erzsébet
PhD, docens
Történelem- és Társadalomtudományi Tanszék,
II. Rákóczi Ferenc Kárpátaljai Magyar Egyetem

SVÁJC BIZTONSÁGPOLITIKÁJA A SEMLEGESSÉG ÉS A HATÁRON ÁTNYÚLÓ EGYÜTTMŰKÖDÉS TÜKRÉBEN

A jelenlegi geopolitikai helyzetben felmerül a kérdés, hogy a Svájc által évszázadok óta alkalmazott, fegyveres semlegességen alapuló biztonságpolitikai modell mennyire tudja megállni a helyét a modern, hibrid konfliktusok időszakában. A klasszikus svájci stratégia – amelyet Spillmann 1987-ben írt le – a függetlenség megőrzésére fókuszált. Ezt az elvet azonban most megtöri a nemzetközi rend felbomlása, a nagyhatalmi rivalizálás és az olyan új típusú fenyegetések, mint a kibertámadások és a dezinformáció. A fő kérdés tehát az, hogy Svájc képes-e megtartani a szuverenitását, illetve fenntartani stabil biztonságpolitikáját egy olyan európai környezetben, ahol szinte minden szomszédja EU- vagy NATO-tag, és ahol a határon átnyúló együttműködés már létfontosságú az ország stabilitásához.

A kutatás célja, hogy tudományos összehasonlítás alá vonja Svájc biztonságpolitikai stratégiájának fejlődési szakaszait a hidegháború vége (1987-es elvek) és a jelenlegi, súlyosbodó helyzet (2021-es és 2024–2025-ös hivatalos dokumentumok) között. Arra keresem a választ, hogy a svájci diplomácia és stratégia milyen konkrét lépésekkel reagál a semlegességét érő nyomásra, miközben kiépíti a határon átnyúló biztonsági együttműködést az Európai Unióval és más európai partnerekkel.

Ez a téma rendkívül időszerű, mivel az orosz-ukrán háború kirobbanása óta Svájc biztonsági környezete drasztikusan romlott (FIS-jelentés, 2025). A globális trendek azt mutatják, hogy az USA egyre kevésbé látszik betölteni a fő védelmező szerepet Európában, ami az európai országokat, így Svájcot is arra kényszeríti, hogy sokkal aktívabban vegyen részt a saját kontinensének biztonsági ügyeiben. Emiatt Svájcnak célratörő újraértelmezésre van szüksége a semlegesség fogalmát tekintve.

Míg a korábbi munkák (pl. Spillmann klasszikus elvei) a svájci biztonságpolitika stabilitását és a katonai elrettentés fontosságát hangsúlyozták, illetve a hidegháború utáni 1993-as semlegességi fehér könyv a semlegességet mint "adaptálható eszközt" vezették be, ez a kutatás a 2021 utáni, hibrid korszakra fókuszál. Az újdonság abban áll, hogy bemutatja, Svájc stratégiája már nem a klasszikus elrettentésen, hanem a nemzeti ellenálló képesség megerősítésén alapszik. A legfontosabb stratégiai újdonság, hogy Európa hivatalosan is a legfelsőbb földrajzi prioritássá vált (FPS 2024-2027), ezzel jelezve, hogy a semlegességet a diplomáciában már úgy használják: „a semlegesség nem jelent közömbösséget”.

A cél elérése érdekében a dolgozat három fő területre fókuszál a hivatalos svájci jelentések alapján. Egyrészt a semlegesség modernizálására, vagyis hogyan fordítja le Svájc a hagyományos semlegességet aktív diplomáciai fellépéssé. Másrészt arra, hogyan terjedt ki a határon átnyúló együttműködés a bűnüldözési területről a nemzeti biztonság szempontjából kulcsfontosságú infrastruktúrák védelmének közös európai színterére.

Végül pedig az EU és Svájc közötti stratégiára: az EU-val való kapcsolatok stabilizálása és fejlesztése már nemcsak gazdasági, hanem kiemelt biztonságpolitikai céllá vált Svájc számára.

A kutatás főbb eredményei és következtetései megerősítik, hogy a svájci biztonságpolitikai modell a túlélés érdekében gyakorlatias fordulatot hajtott végre, egyidejűleg ragaszkodva történelmi elveihez. Svájc nem mondott le a semlegességről, hanem aktív hídépítő szerepét használja fel arra, hogy hozzájáruljon a globális stabilitáshoz, ami közvetve a saját biztonságát erősíti. Az ország belátta, hogy a súlyos fenyegetések (kémkedés, kibertámadás) elleni védekezéshez szoros európai partneri

hálózatra van szükség. A stratégia tehát egyértelműen a reziliencia erősítését helyezi előtérbe, amelyet határokon átnyúló együttműködéssel egészít ki.

Összességében a svájci biztonságpolitikai stratégia sikeresen navigál a szuverenitás és a szükséges európai integráció közötti feszültségben, a határon átnyúló együttműködés hálózati formáit választva a stabilitás megőrzésének legfőbb eszközeként.

Felhasznált irodalom

1. Federal Department of Foreign Affairs (FDFA). (2024). Foreign Policy Strategy 2024-2027. (Swiss Federal Council)
2. Federal Department of Foreign Affairs (FDFA) & Federal Department of Economic Affairs, Education and Research (EAER). (2025). International Cooperation Strategy 2025-2028 (Swiss Federal Council)
3. Federal Intelligence Service (FIS). (2025). Switzerland's Security: Situation Report of the Federal Intelligence Service 2025 (Swiss Federal Council)
4. Loeffel, Urs (2010). Swiss Neutrality and Collective Security: The League of Nations and the United Nations. Master's Thesis, Naval Postgraduate School (Monterey, California)
5. Spillmann, K. R. (1987). Beyond Soldiers and Arms: The Swiss Model of Comprehensive Security Policy
6. Swiss Federal Council. (2021). The security policy of Switzerland: Report of the Federal Council, November 24, 2021
7. Swiss Federal Council (1993). White Paper on Neutrality: Annex to the Report on Swiss Foreign Policy for the Nineties of 29 November 1993. (Bern: Swiss Federal Council)
8. Wenger, Andreas & Möckli, Daniel (2009). The Swiss Security Policy Report: Key Points and Debates. (CSS Analyses in Security Policy, No. 50. ETH Zurich)
9. Európai Parlament, Mandl, Lukas (2023). Jelentés az EU és Svájc közötti kapcsolatokról (2023/2042 (INI)) (A9-0248/2023). (Külügyi Bizottság)

ZSUKOVSZKY Ágnes
Hallgató, III. Évfolyam, Nemzetközi kapcsolatok szak
Történelem- és Társadalomtudományi Tanszék,
II. Rákóczi Ferenc Kárpátaljai Magyar Egyetem

HIRES-LÁSZLÓ Kornélia
PhD, docens
Történelem- és Társadalomtudományi Tanszék,
II. Rákóczi Ferenc Kárpátaljai Magyar Egyetem
intézményvezető
Hodinka Antal Nyelvészeti Kutatóközpont

A NATO SZEREPE A NEMZETKÖZI BIZTONSÁG MEGTEREMTÉSÉBEN: GÖRÖGORSZÁG PÉLDÁJA

Kulcsszavak: NATO; Görögország; nemzetközi biztonság; Földközi-tenger; kollektív védelem; hibrid fenyegetések; geopolitikai adaptáció

A nemzetközi biztonság fogalma az elmúlt évtizedekben alapvető változáson ment keresztül. A hidegháború idején a katonai fenyegetések és a kétpólusú világrend határozták meg a biztonság értelmezését, azonban a 21. század elején új, nem konvencionális kihívások jelentek meg: a kibertámadások, a hibrid hadviselés, a migrációs válság, a terrorizmus, valamint az energiapolitikai és klímaváltozással összefüggő fenyegetések (NATO, 2022). E sokrétű biztonsági kihívás közepette a NATO, mint a világ legerősebb katonai-politikai szövetsége, továbbra is a nemzetközi stabilitás egyik legfontosabb garanciája maradt (Parliamentary Library – House of Commons, 2022). A szervezet kollektív védelmi, válságkezelési és partnerségi funkciói egyaránt azt a célt szolgálják, hogy a NATO alkalmazkodni tudjon a folyamatosan változó globális biztonsági környezethez (NATO, 2022).

Az elemzés központi problémája annak feltárása, miként valósul meg a NATO szerepe a nemzetközi biztonság megteremtésében, és ezen belül Görögország milyen sajátos funkciót tölt be a szervezet délkeleti szárnyán (NATO Parliamentary Assembly, 2024). Görögország példája különösen releváns, mivel a Földközi-tenger keleti medencéjében elhelyezkedve stratégiai közvetítőpontot képez Európa, a Közel-Kelet és Észak-Afrika között (U.S. Department of State, 2025). Földrajzi fekvése, történeti tapasztalatai és politikai beágyazottsága révén az ország egyszerre a NATO déli bástyája és a térségi stabilitás egyik kulcseleme (Danopoulos, 1988).

Az elemzés célja annak bemutatása, hogy Görögország miként járul hozzá a NATO kollektív biztonsági struktúrájához, milyen módon illeszkedik katonai, politikai és gazdasági stratégiája a szövetség célrendszeréhez, és hogyan reagál az új típusú fenyegetésekre (Katsaitis, 2019). A téma aktualitását a NATO 2022-ben elfogadott stratégiai koncepciója is megerősíti, amely a 360 fokos biztonsági megközelítést helyezi előtérbe (NATO, 2022). Ez a koncepció a keleti mellett a déli biztonsági kihívások figyelembevételét is előírja, különös tekintettel a Földközi-tenger térségére, amely Görögország révén a szövetség számára stratégiai jelentőségű marad (NATO Parliamentary Assembly, 2024).

A Souda-öbölben található haditengerészeti és légi bázis, valamint a Thesszalonikiben működő NATO Rapid Deployable Corps (NRDC–GR) olyan infrastrukturális kapacitásokat biztosítanak, amelyek lehetővé teszik a szövetség számára a gyors reagálást a Földközi-tengert és a Közel-Keletet érintő válságokra (U.S. Navy, 2025). Görögország katonai szerepvállalása kiegészül azzal, hogy az ország a NATO „Operation Sea Guardian" keretében aktív szerepet játszik a tengeri biztonság, a migrációkezelés és a kereskedelmi útvonalak védelmében is (NATO, 2022).

A tudományos újdonság abban rejlik, hogy Görögország NATO-tagságát nem kizárólag történeti összefüggésben, hanem komplex, multidimenzionális biztonsági kontextusban értelmezi (Danopoulos, 1988). A korábbi szakirodalom hajlamos volt a görög–török viszonyra és a ciprusi konfliktusra redukálni a NATO-n belüli szerepet, miközben a modern kihívások – mint a kibervédelem, az energiapolitikai biztonság és a migrációs nyomás – új dimenziókat adnak Görögország stratégiai jelentőségének (Katsaitis, 2019; Barrass & Coker, 2024). A görög védelmi kiadások, amelyek a GDP több mint 3%-át teszik ki, valamint a haderő modernizációja – például a

Rafale vadászgépek, F-35-ös repülőgépek és Belharra fregattok beszerzése – egyaránt a NATO-kompatibilitás és a haditechnikai innováció irányába mutatnak (U.S. Department of State, 2025).

A történeti perspektíva szintén elengedhetetlen a görög NATO-szerep megértéséhez. Görögország 1952-ben csatlakozott a szövetséghez, majd az 1974-es ciprusi válságot követően ideiglenesen felfüggesztette részvételét a NATO katonai struktúráiban, és 1980-ban tért vissza teljes jogú tagként (Danopoulos, 1988). Azóta az ország aktívan részt vett a NATO békefenntartó és válságkezelő misszióiban Bosznia-Hercegovinában, Koszovóban és Afganisztánban, ami jól mutatja, hogy szerepe túllépett a regionális védelem keretein, és a globális biztonsági architektúra részévé vált (NATO, 2022).

A modern biztonsági kihívások – a migrációs válság, a kibertér sérülékenysége, az energiapolitikai konfliktusok és a térségi instabilitás – új válaszokat követelnek mind a NATO, mind Görögország részéről. A Földközi-tenger térsége az elmúlt években kiemelt jelentőséget nyert a migrációs útvonalak, a tengeri határviták és az energiahordozók feletti ellenőrzés miatt (U.S. Department of State, 2025). Görögország ebben a helyzetben kettős szerepet tölt be: a NATO déli határának védelmezője, valamint az Európai Unió keleti kapuja (NATO Parliamentary Assembly, 2024). A NATO–EU együttműködésben az ország a biztonsági koordináció egyik kulcspontjává vált, különösen a migráció, a klímavédelem és az energiafüggetlenség kérdéseiben (Karatarakis, 2025; Kyriakidis, 2025).

A görög–török viszony továbbra is a szövetség egyik legérzékenyebb belső kérdése, amely időről időre próbára teszi a NATO politikai kohézióját. Az Égei-tenger térségében fennálló területi és légügyi viták, valamint a ciprusi konfliktus továbbra is feszültségforrások maradnak, de a NATO a párbeszéd és a deeszkaláció eszközeivel igyekszik kezelni ezeket (NATO Parliamentary Assembly, 2024).

Az elemzés végső következtetése, hogy Görögország a NATO délkeleti szárnyának meghatározó stabilizáló és innovatív tényezője, amely földrajzi fekvésén, katonai infrastruktúráján és politikai elkötelezettségén keresztül kulcsszerepet tölt be a szövetség stratégiai alkalmazkodásában. A jövőre nézve Görögország szerepe várhatóan tovább erősödik, különösen a Földközi-tenger biztonsági övezetének formálásában, a kibervédelmi képességek fejlesztésében és a NATO–EU együttműködés elmélyítésében. Ugyanakkor a fenntartható biztonsági egyensúly eléréséhez az országnak tovább kell növelnie technológiai és hírszerzési kapacitásait, valamint finomítania kell diplomáciai pozícióját a török viszonyrendszerben (Simón, 2023; Barrass & Coker, 2024). A görög példa azt mutatja, hogy a nemzetközi biztonság a 21. században nem kizárólag katonai erő kérdése, hanem a diplomácia, a gazdaság és a technológiai innováció integrált rendszerében formálódik.

Felhasznált irodalom

1. Barrass, G., & Coker, C. (2024). The NATO Strategic Concept on Its Seventy-Fifth Anniversary. Military Review (Army University Press). https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/July-August-2024/NATO-Strategic-Concept/
2. Berti, B., & Simón, L. (2022). Reassessing NATO's Southern Strategy: Adapting to a New Era of Threats. NATO Review Magazine. https://www.nato.int/docu/review/articles/2022/10/20/reassessing-natos-southern-strategy/index.html
3. Danopoulos, C. P. (1988). Analyzing the NATO–Greek Relationship. Boulder, CO: Westview Press.
4. Katsaitis, O. (2019). Concerns on the issue of defence expenditure in post-crisis Greece. Security and Defence Quarterly, 26(3), 48–63. https://securityanddefence.pl/Concerns-on-the-issue-of-defence-expenditure-in-the-post-crisis-Greece,103408,0,2.html
5. Karatarakis, E. (2025, August). A New Model for Defense in Greece. The Cipher Brief. https://www.thecipherbrief.com/greece-military-diplomacy
6. Kyriakidis, M. (2025). NATO Intelligence and Greek Military Strategy. ISRG Journal of Arts, Humanities & Social Sciences. https://isrgpublishers.com/wp-content/uploads/2025/05/ISRGJAHSS100242025.pdf
7. NATO. (2022). Strategic Concept 2022. Brussels: NATO Public Diplomacy Division. https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf

8. NATO Parliamentary Assembly. (2024). Allied legislators highlight Greece's strategic role in Southeast Europe and the Mediterranean. https://www.nato-pa.int/news/allied-legislators-highlight-greeces-strategic-role-southeast-europe-and-mediterranean
9. Parliamentary Library – House of Commons. (2022). NATO's Strategic Concept. https://commonslibrary.parliament.uk/research-briefings/cbp-9573/
10. Simón, L. (2023). The Main Difference Between NATO's 2022 Strategic Concept and Its Previous Strategic Concepts. Orion Policy. https://orionpolicy.org/the-main-difference-between-natos-2022-strategic-concept-and-its-previous-strategic-concepts/
11. U.S. Department of State. (2025). U.S. Security Cooperation with Greece. Washington, D.C. https://www.state.gov/u-s-security-cooperation-with-greece
12. U.S. Navy. (2025). PWD Souda Bay Delivers $5.2M Warehouse, Enhancing NAVSUP Mediterranean Mission. https://www.c6f.navy.mil/Press-Room/News/Article/4154664/pwd-souda-bay-delivers-52m-warehouse-enhancing-navsup-mediterranean-mission

VASS Jázmin
Hallgató, III. Évfolyam, Nemzetközi kapcsolatok szak
Történelem- és Társadalomtudományi Tanszék,
II. Rákóczi Ferenc Kárpátaljai Magyar Egyetem

RÁCZ Béla
PhD, Docens,
Történelem- és Társadalomtudományi Tanszék,
II. Rákóczi Ferenc Kárpátaljai Magyar Egyetem

NÉMETORSZÁG ÉS A NATO KELETI BŐVÍTÉSE: STRATÉGIAI, POLITIKAI ÉS BIZTONSÁGI DILEMMÁK

A NATO keleti bővítése az 1990-es évek végétől kezdődően az európai biztonsági architektúra egyik legfontosabb és levitatotabb folyamata. A korábbi Varsói Szerződés- államok, majd a balti és délkelet-európai országok csatlakozása radikálisan átalakította a kontinentális erőviszonyokat. Németország, mint a szövetség egyik kulcsállama, kulcszerepet játszott ebben a folyamatban, ugyanakkor saját történelmi és politikai érzékenysége, valamint a belső konszenzus szükségessége miatt rendkívül összetett dilemmákkal szembesült.A tudományos probléma alapvető kérdése, hogy a NATO keleti bővítése milyen politikai, stratégiai és biztonságpolitikai dilemmákat generált Németország számára és ezek a dilemmák miként formálták az ország kül-és védelempolitikai döntéseit.

Az elemzés középpontjában áll a kérdés, hogy Németország milyen mértékben tudott és tud ma is hozzájárulni a NATO keleti szárnyának védelméhez, hogyan alakította a belpolitikai korlátok és a társadalmi konszenzus a katonai elköteleződést és milyen tényezők határozzák meg a stratégiai célok elérését a mai geopolitikai környezetben.

Történelmi kontextus

A hidegháború után, 1990 körül a szovjet blokk összeomlásával új lehetőségek nyíltam az európai biztonsági rendszer átrendeződésére. Németország újraegyesítésekor a nyugati államok azt is megfogalmazták, hogy a NATO nem bővül azonnak kelet felé- az ún. „not one inch eastward" retorika- annak érdekében, hogy Moszkva beleegyezését megnyerjék. Ugyanakkor gyorsan felmerül a kérdés, hogy ez az ígéret csak az NDK-ra vonatkozik-e, vagy általánosított garanciaként értendő Kelet-Európára is. A NATO-csatlakozások folyamata azonzban megindult: 1999-ben Magyarország, Lengyelország és Csehország, később több balti állam- Románia, Bulgária, Horvátország- belépett a szövetségbe. A NATO 2025-ös huvatalos adatai szerint „a szövetség keleti részén való katonai jelenlét fontos eleme az elrettentési és védelmi pozíciótk fenntartásának."

Németország a NATO alapításától fogva része volt a kapcsolatrendszernek- 1955-ben az NSZK belépett a NATO-ba és így a német részvétel fokozatosan épült be a transzatlanti stukrúrába. Az újraegyesítés után Németország szerepe tovább erősödött, hiszen földrajzilag köztes államként mára stratégiai tengelyként pozícionálható az Észak-Dél és Nyugat-Kelet tengelyen.

Belpolitikai korlátok Németországban

Németország belpolitikája érzékenyen reagál a katonai elköteleződésekre. Az első szerepvállalások mindig tárgyalósztalnál születnek, hiszen a Bundestag és koalíciós mehanizmusok rendkívül befolyásolják a döntéseket. A német választói közvélemény hagyományosan óvatos a katonai beavatkozásokkal szemben, részben a történelmük miatt. Emellett a büdzsé korlátai- például hogy a védelempolitikának átlagosan 2% GDP-arányos kiadást kell teljesítenie- állandó nyomás alatt álnak.

Nógrádi György is rámutat arra, hogy „a NATO jövőjéről óriási viták vannak" és hogy az amerikai fókusz eltolodása Ázsiába kihívást jelent Európának és így Németországnak is-hiszen az európai partnereknek növelniük kell felelősségvállalásukat. Ezek a viták közvéleméyes és politikai feszültségeket teremtenek, amelyek fékezika gyors reagálást.

NATO keleti bővítés intézkedései és a német szerep

A NATO keleti bővítésének intézményi mechanizmusai közé tartozik a Partnerország-program (Partnership for Peace), az Intensified Dialogue, majd a Membership Action Plan (MAP) folyamat. A NATO 2025-ös álláspontja szerint a keleti jelenlét – a harccsoport-állomásoztatás, rotációs gyakorlatok és gyors reagáló egységek kihelyezése – kulcselem az elrettentés fenntartásában.

Németország aktívan részt vesz a NATO harccsoportjainak vezetésében: például Németország vezet egy NATO harccsoportot Litvániában, és tervezi, hogy hosszú távú német katonai bázist létesít ott, amely az első német bázis lenne külföldön a második világháború óta. Ezen túl Németország részt vállal az Air Policing missziókban Románia légterében, és együttműködik lengyel és holland partnerekkel katonai korridorok fejlesztésében, hogy gyors mozgást tegyenek lehetővé a keleti szárny felé.

Ezek a lépések nem csupán jelképesek: céljuk a közös védelmi kapacitás megerősítése, a katonai interoperabilitás és a partnerségi bizalom elmélyítése.

Katonai kapacitások és német telepítések

Németország hagyományosan erős gazdasági és technológiai bázissal rendelkezik, de a Bundeswehr az elmúlt évtizedekben strukturális hiányokra mutatott rá. 2025-ös jelentések szerint a német haderő felszereltségében régi technológiák és hiányzó alkatrészek jellemzők; egy 2014-es anecdota szerint német katonák „fekete festékbe mártott seprűnyelekkel imitáltak géppuskákat egy NATO gyakorlaton", hogy elméletben felvegye a látszatot.

Az új német kormány ambíciója, hogy a Bundeswehr méretét 203 000 főre növelje, új brigádokat állítson fel, és akár visszaállítsa a sorozást is.Az ország elfogadott védelmi befektetései szerint cél, hogy a hadsereg a legerősebb hagyományos erő legyen Európában.

A német telepítések közé tartozik a litvániai harccsoport, légvédelmi együttműködések és légi rendészeti küldetések Romániában. Ezek a telepítések azt a célt szolgálják, hogy Németország ne csupán elméletileg, hanem jelenléttel is részt vegyen Kelet-Európa védelmében.

Stratégiai célok és dilemmák

Németország stratégiai céljai között szerepel a stabilitás fenntartása Kelet-Európában, a regionális vezető szerep, és az orosz befolyás visszaszorítása. Egy aktív német védelempolitika erősítheti Berlin hitelét nemzetközi színtéren, és növelheti ráhatást az európai védelmi struktúrákra.

Ugyanakkor ezekkel együtt járnak kockázatok: az orosz válaszlépések (politikai, diplomáciai, katonai) fenyegetésként merülnek fel, a túlzott kötelezettségvállalások feszültséget idézhetnek elő, illetve fennáll annak a veszélye, hogy Németország túl nagy terheket vállal anélkül, hogy más európai államok azonos mértékben járulnának hozzá. Az elrettentés provokatív jelleggel is bírhat: ha Berlin túlzottan kiáll, Moszkva katonai reagálással fenyegethet vissza.

Az együttműködés kérdése is kulcs: mennyire ossza meg Németország a teherbírást az EU-val, más NATO-tagokkal és az Egyesült Államokkal? A nukleáris elrettentés kérdése – Németország nem rendelkezik saját nukleáris fegyverrel – tovább árnyalja a dilemmát: meddig bízhat Berlin az amerikai nukleáris garanciákban?

Biztonságpolitikai dilemmák

A legfőbb dilemmák között áll az, hogy meddig mehet el az elrettentés anélkül, hogy provokációnak minősüljön. Ha Németország erőteljes katonai jelenlétet vállal, akkor Moszkva katonai vagy politikai válaszlépéseket tehet. Egy másik kérdés, hogy mennyi kötelezettséget vállaljon Berlin – például hány brigádot, milyen gyors reagáló erőt, milyen páncélos és légvédelmi kapacitást. A tehermegosztás kérdése – hogyan osszák el az európai államok és az USA között a felelősséget – állandó feszültségforrás.

Továbbá az információs hadviselés, kibertámadások, hibrid fenyegetések szintén befolyásolják a keleti bővítés kereteit – Németországnak nem elég fizikai jelenlétet biztosítani, hanem védekeznie kell az aszimmetrikus támadásokkal szemben is.

Egy további dilemmát jelent, hogy mennyire függjön Németország az amerikai nukleáris garanciáktól – hiszen ha az USA fordul, Berlinnek kevés eszköze van a nukleáris elrettentés önálló fenntartására.

Következtetések és javaslatok

Az elemzés alapján néhány fő megállapítás tehető:

- Kettős logika: Németország egyszerre folytatta a keleti bővítés támogatását (mint stratégiai cél), és mérlegelte a vele járó költségeket, kockázatokat és belpolitikai korlátokat.
- Belpolitikai korlátok meghatározóak: a választói attitűd, büdzsé, koalíciós kompromisszumok és a pártrendszer korlátozzák, hogy Berlin mennyire tud gyorsan és radikálisan reagálni.

- Katonai kapacitás-hiányok: a Bundeswehr strukturális hiányosságai lassították a német elköteleződést, de a 2022 utáni újratárcsázás (Zeitenwende) nyomán látni kezdenek komoly fejlesztéseket.
- Stratégiai feszültségek: a német jelenlét jelentős, de nem provokatívnak kell maradnia – Berlinnek óvatosan kell kijelölnie határait, hogy elrettentés ne váljon provokációvá.
- Transzatlanti és európai felelősségmegosztás szükségessége: Németországnak nem szabad túlvállalnia magát, ki kell alakítani igazságos terheket és hatékony együttműködést más államokkal és az EU-val.
- Gyakorlati tanulság más államokra: a német modell – aktív, de mérlegelő, kooperatív és kapacitás-kiterjesztő – adaptálható más közép-európai NATO-tagállamok számára is.
- Javasolt további kutatási irányok: mélyebb összehasonlító elemzés más NATO-tagállamokkal, kvantitatív vizsgálat a német közvélemény és katonai kiadások összefüggéseiről, valamint forgatókönyvek kidolgozása a jövőbeli keleti bővítéshez (pl. Ukrajna, Moldva) Németország szerepvállalása szempontjából.
-

Felhasznált irodalom

1. Spevak, Edmund: Germany and NATO 2018
2. NATO: “Germany and NATO – 1955” – hivatalos deklasszifikált dokumentum.
Link: https://www.nato.int/cps/en/natolive/topics_82737.htm
3. NATO: “NATO’s military presence in the east of the Alliance” – hivatalos oldal.
Link: https://www.nato.int/cps/en/natolive/topics_136388.htm
4. Német kormány: “Germany recommits to European, global security” – hírek 2025-ben.
Link: https://www.legion.org/information-center/news/landing-zone/2025/september/germany-recommits-to-european-global-security
5. Nógrádi György: “A NATO jövőjéről óriási viták vannak” – interjú (ma7.sk).
Link: https://ma7.sk/nagyvilag/nogradi-gyorgy-a-nato-jovojerol-oriasi-vitak-vannak

Костянтин БІСАГА
студент 3 курсу спеціальності "Міжнародні відносини",
кафедра історії та суспільних дисциплін
Закарпатського угорського університету імені Ференца Ракоці II

Маріанна МАРУСИНЕЦЬ
кандидат філологічних наук,
доцент кафедри історії та суспільних диспиплін,
старший науковий співробітник, старший дослідник
Науково-дослідного центру імені Тіводора Легоцькі
Закарпатського угорського університету імені Ф. Ракоці II

ЗОВНІШНЯ БЕЗПЕКОВА ПОЛІТИКА КОРОЛІВСТВА ІСПАНІЇ

Зовнішня політика Іспанії, як одна з ключових складових національної безпеки, формується під впливом глобалізаційних процесів, регіональних конфліктів, економічних і енергетичних інтересів, а також змін у міжнародних інституціях та системах безпеки. Завдання дослідження полягає у систематизації й аналізі наявних даних щодо зовнішньої політики Іспанії, включно з офіційними стратегічними документами, участю у міжнародних організаціях, таких як НАТО та ЄС, та її реакціями на нові глобальні виклики. Особливу увагу приділено оцінці ефективності цих заходів у контексті сучасних загроз, серед яких тероризм, кібербезпека, політична нестабільність у сусідніх регіонах, зростання геополітичної конкуренції та нелегальна міграція.

Мета дослідження полягає у всебічному аналізі сучасної зовнішньої політики безпеки Королівства Іспанії, що є центральним елементом національної безпеки та міжнародної позиції держави. Актуальність дослідження зумовлена швидкими змінами у глобальній системі безпеки, появою нових загроз, зокрема кібернетичних атак і терористичних ризиків, а також зростанням регіональної нестабільності. Політика Іспанії, реалізована через її участь у НАТО, Європейському Союзі та інших міжнародних організаціях, спрямована на захист національних інтересів, підтримку миру та стабільності у стратегічно важливих регіонах, таких як Північна Африка та Латинська Америка. Дослідження дозволяє оцінити, наскільки стратегічні пріоритети країни відповідають сучасним викликам, а також порівняти національний підхід Іспанії з політиками інших європейських держав.

Аналіз зовнішньої політики безпеки Королівства Іспанії у XXI столітті є актуальним, оскільки дозволяє оцінити ефективність національної стратегії в умовах нових глобальних і регіональних викликів. Попередні дослідження, такі як «España en el siglo XXI: argumentos a favor de una estrategia de seguridad nacional» та «¿Necesita España realmente una estrategia de política exterior?» (Real Instituto Elcano, 2014) [2], здебільшого зосереджувалися на загальних принципах та концептуальних підходах, без детальної оцінки конкретних механізмів реалізації. Запропоноване дослідження відрізняється тим, що аналізує сучасні стратегічні документи Іспанії, зокрема «Estrategia de Acción Exterior 2025-2028» та «Estrategia de Seguridad Nacional 2021», і враховує новітні виклики, такі як кіберзагрози та гібридні конфлікти. Наукова новизна полягає у комплексному підході, що поєднує теоретичний аналіз із практичною оцінкою ефективності зовнішньої безпекової політики Іспанії, порівнюючи її з міжнародними тенденціями у сфері безпеки. Також запропоноване дослідження враховує новітні тенденції у сфері безпеки, такі як кіберзагрози, гібридні війни та економічна безпека, що не були достатньо висвітлені в попередніх роботах. Наприклад, дослідження «Estudio comparativo de las estrategias nacionales de ciberseguridad de diez países» порівнює національні стратегії кібербезпеки десяти країн, включаючи Іспанію, та виявляє відсутність єдиного підходу до визначення терміну «кібербезпека» та структурних відмінностей у стратегіях [3].

Дослідження передбачає всебічний аналіз сучасної зовнішньо-безпекової політики Королівства Іспанії у XXI столітті з акцентом на стратегічні пріоритети, механізми їх реалізації та ефективність у контексті глобальних і регіональних викликів. Завдання полягає у систематизації основних напрямів зовнішньої політики, зокрема забезпеченні національної

безпеки, зміцненні позицій Іспанії в міжнародних альянсах, активній участі у миротворчих та стабілізаційних операціях, а також підтримці стабільності у стратегічно значущих регіонах, таких як Північна Африка, Латинська Америка та Середземномор'я. Особлива увага приділяється аналізу інструментів реалізації зазначених пріоритетів, включно з дипломатичними ініціативами, участю у багатосторонніх організаціях, таких як НАТО, ЄС та ООН, військовими, економічними та гуманітарними заходами, а також комплексними стратегіями протидії сучасним загрозам, серед яких тероризм, кіберзлочинність і гібридні конфлікти. Такий підхід дозволяє оцінити, наскільки стратегічні цілі Іспанії реалізуються на практиці та забезпечують захист національних інтересів. Дослідження також включає оцінку ефективності зовнішньо-безпекової політики на основі аналізу стратегічних документів, офіційних заяв та практичних результатів участі Іспанії у міжнародних структурах [1].

У порівнянні з іншими провідними європейськими державами, такими як Франція, Німеччина та Італія, зовнішньо-безпекова політика Іспанії демонструє більш прагматичний і гнучкий підхід: країна робить акцент на багатосторонній дипломатії, економічних і гуманітарних інструментах, інтегруючи традиційні військові методи з сучасними механізмами протидії глобальним загрозам. Франція та Німеччина, наприклад, часто віддають перевагу більш централізованим і жорстким військовим підходам, тоді як Іспанія намагається балансувати між колективною безпекою у рамках НАТО та ЄС і власними національними інтересами у регіонах стратегічної присутності. Ще враховуються сучасні загрози та глобальні виклики, зокрема тероризм, кібернетичні атаки, економічну нестабільність, міграційні кризи та політичну нестабільність у регіонах стратегічної присутності Іспанії. Аналіз цих факторів дозволяє оцінити гнучкість та адаптивність зовнішньо-безпекової політики держави, а також її здатність ефективно реагувати на динамічні зміни в міжнародній системі безпеки. Фінальною метою дослідження є формування комплексної наукової оцінки зовнішньо-безпекової політики Іспанії, поєднання теоретичного аналізу з практичною оцінкою реалізації стратегічних заходів, визначення сучасних тенденцій розвитку, сильних і слабких сторін політики, перспектив її вдосконалення та місця Іспанії серед провідних європейських держав у сфері безпеки.

Як висновок ми можемо зауважити, що дослідження дозволяє комплексно оцінити сучасну зовнішньо-безпекову політику Королівства Іспанії у XXI столітті, виявити її основні пріоритети, механізми реалізації та здатність адаптуватися до сучасних глобальних і регіональних викликів. Одним із ключових результатів є систематизація стратегічних напрямів іспанської політики, серед яких забезпечення національної безпеки, зміцнення позицій Іспанії в рамках НАТО та ЄС, активна участь у миротворчих і стабілізаційних операціях у стратегічно важливих регіонах світу, таких як Північна Африка, Латинська Америка та Середземноморський регіон. Виявлено, що зовнішньо-безпекова політика Іспанії базується на поєднанні традиційних дипломатичних, військових та економічних інструментів із новітніми методами реагування на загрози, серед яких кібербезпека, гібридні конфлікти, тероризм та глобальні економічні ризики.

Список використаних джерел

1. "La seguridad nacional en España: Un enfoque geoestratégico."- Roldán Barbero, J. (Ed.). (2017); file:///C:/Users/HP/Downloads/24_Recension_BLANC_Antonio.pdf
2. "Seguridad nacional, amenazas y respuestas." - De la Corte Ibáñez, L., & Blanco Navarro, J. M. (2014); https://dialnet.unirioja.es/servlet/libro?codigo=564008
3. "Informe Anual de Seguridad Nacional" -Departamento de Seguridad Nacional (DSN) (2024). https://www.dsn.gob.es/sites/default/files/2025-05/IASN2024%20ACCESIBLE.pdf

Каріна ВАШКЕБА
студентка 3 курсу спеціальності "Міжнародні відносини",
кафедра історії та суспільних дисциплін
Закарпатського угорського університету імені Ференца Ракоці II

Маріанна МАРУСИНЕЦЬ
кандидат філологічних наук,
доцент кафедри історії та суспільних диспиплін,
старший науковий співробітник, старший дослідник
Науково-дослідного центру імені Тіводора Легоцькі
Закарпатського угорського університету імені Ф. Ракоці II

ІСТОРІЯ ВІДНОСИН МІЖ ФРАНЦІЄЮ І НАТО

В історії розвитку євроатлантичної безпеки відносини між Францією і НАТО завжди характеризувалися складною динамікою – від активної участі та лідерських позицій до періодів відсторонення і подальшого зближення. Їхній еволюційний шлях демонструє прагнення Парижа зберегти стратегічний суверенітет, водночас залишаючись частиною колективної системи оборони. У різні періоди XX і XXI століть французька політична еліта по-різному оцінювала межі співпраці з Альянсом, що відображало зміни у внутрішній та зовнішній політиці держави, а також реакцію на трансформації глобальної безпеки.

Метою дослідження є простежити історичну логіку еволюції взаємин Франції та НАТО від 1949 року до середини 2025 року, з'ясувати політичні і стратегічні мотиви ключових рішень французького керівництва та оцінити їхній вплив на європейську й трансатлантичну безпеку. Актуальність зумовлена війною Росії проти України, посиленням уваги до протиповітряної та протиракетної оборони, дискусіями про стратегічну автономію ЄС і новими домовленостями в межах НАТО щодо промислових потужностей і витрат на оборону [6].

Наукова новизна полягає у цілісному осмисленні трьох ключових етапів еволюції відносин Франції з НАТО: від ролі співзасновника до виходу з інтегрованого військового командування у 1966 році, подальшого повернення у 2009-му та активного зміцнення східного флангу в 2022–2025 роках.

Франція була серед дванадцяти держав, що підписали Вашингтонський договір 4 квітня 1949 року, розмістила першу постійну штаб-квартиру НАТО в Парижі та від самого початку поєднувала участь у колективній обороні з прагненням до стратегічної самостійності. У березні 1966 року президент Шарль де Голль заявив про вихід із інтегрованого військового командування, що спричинило передислокацію штабів з Франції, але не означало виходу з Альянсу як політичної організації. Членство зберігалося, а співпраця тривала на політичному рівні [2].

Починаючи з 1990-х, а особливо після «Білої книги з оборони і нацбезпеки» 2008 року, Париж відновлював участь у структурах, а в квітні 2009 року офіційно повернув військових до командних ланок НАТО, розмістивши кадри в Allied Command Operations і Allied Command Transformation. Рішення закріплене на саміті у Страсбурзі/Келі та відображене в урядових матеріалах Франції [2]. Практичну інтегрованість Франції в межах Альянсу підтвердила операція НАТО Unified Protector проти режиму Каддафі, проведена вже через два роки після повернення Парижа до командних структур. Французькі літаки спершу діяли в межах національної операції Opération Harmattan, а згодом увійшли до багатонаціонального угруповання під управлінням НАТО, що продемонструвало здатність країни ефективно поєднувати власне стратегічне керівництво з координацією союзників [5].

У новій безпековій реальності після 2014 року відбулося розширення ролі на східному фланзі та в повітряній безпеці. Від 2022 року Франція очолює багатонаціональний батальйон у Румунії в межах Mission AIGLE, підсилюючи контингент, артилерію і ППО, розгортаючи батареї SAMP/T MAMBA на Чорному морі й регулярно проводячи спільні тренування. Станом на 2024–2025 роки джерела НАТО та урядові публікації фіксують лідерство Франції в румунському батальйоні, поступове нарощування чисельності й участь у захисті повітряного

простору [3]. Паралельно французькі винищувачі Rafale і Mirage не раз підсилювали місію Baltic Air Policing у Литві та Естонії, зокрема ротації 2023–2025 років із взаємодією з італійськими, бельгійськими, нідерландськими та іншими підрозділами [1]. Викладені факти демонструють не декларативний, а предметний внесок у стримування та спільну оборону на північному і південно-східному напрямках.

Окремої уваги потребує зв'язок із підтримкою України, що формально здійснюється на двосторонньому рівні, але має пряму вагу для східного флангу та планування НАТО. Париж заявляв про навчання українських військових, передачу далекобійних засобів, а у 2024 році оголошував про намір передати винищувачі Mirage 2000-5 із відповідною підготовкою пілотів, що посилює сумісність і гнучкість сил партнерів. Поєднання двосторонньої лінії з натівськими рішеннями щодо стримування допомагає утримувати баланс між політичною єдністю й оперативними вимогами безпеки регіону [4].

У підсумку історія взаємин між Францією і НАТО демонструє послідовну логіку розвитку – від пошуку власного місця в системі колективної оборони до усвідомлення необхідності спільної відповідальності за безпеку Європи. Попри політичні суперечки чи періодичні розбіжності у стратегічних підходах, Франція залишається одним із ключових союзників, чиї дії мають реальний вплив на стабільність євроатлантичного простору. Сьогодні країна бере активну участь у посиленні східного флангу Альянсу, зокрема через розміщення контингенту в Румунії в межах місії Aigle, участь у спільних навчаннях, патрулюванні повітряного простору Балтії та розгортанні систем протиракетної оборони SAMP/T MAMBA.

Список використаних джерел

1. Allied Air Command, 2025. NATO's Air Policing Mission: A Steadfast Commitment by the Alliance. 4 Mar. Available at: https://ac.nato.int/archive/2025-2/natos-air-policing-mission-a-steadfast-commitment-by-the-alliance- [Accessed 25 Oct 2025].
2. France, Ministry for Europe and Foreign Affairs, 2025. France and NATO. Available at: https://www.diplomatie.gouv.fr/en/french-foreign-policy/security-disarmament-and-non-proliferation/our-alliances-and-cooperations/france-and-nato/ [Accessed 24 Oct 2025].
3. GMFUS, 2025. France's Shift to Long-Term Engagement in the Black Sea. 9 Oct. Available at: https://www.gmfus.org/news/frances-shift-long-term-engagement-black-sea [Accessed 24 Oct 2025].
4. Le Monde, 2024. War in Ukraine: By sending Mirage fighters, France steps up support for Kyiv. 7 Jun. Available at: https://www.lemonde.fr/en/international/article/2024/06/07/war-in-ukraine-by-sending-mirage-fighters-france-steps-up-support-for-kyiv_6674092_4.html [Accessed 24 Oct 2025].
5. NATO, 2011. Operation Unified Protector (February–October 2011). Available at: https://www.nato.int/cps/en/natohq/71679.htm [Accessed 24 Oct 2025].
6. NATO, 2025. NATO Integrated Air and Missile Defence Policy, 13 Feb. Available at: https://www.nato.int/cps/en/natohq/official_texts_233084.htm [Accessed 24 Oct 2025]

Маріанна МАРУСИНЕЦЬ
кандидат філологічних наук,
доцент кафедри історії та суспільних диспиплін,
старший науковий співробітник, старший дослідник
Науково-дослідного центру імені Тіводора Легоцькі
Закарпатського угорського університету імені Ф. Ракоці II

ЗОВНІШНЯ БЕЗПЕКОВА ПОЛІТИКА РЕСПУБЛІКИ ІРЛАНДІЯ

Важливим аспектом політики безпеки Республіки Ірландія є участь у міжнародних організаціях. Ірландія співпрацює з міжнародними партнерами для просування глобального миру і стабільності – ООН, ЄС, ОБСЄ, НАТО та іншими державами, а також міжнародними організаціями. Ірландія бере активну участь у спільній політиці безпеки і оборони ЄС, в її розробці та в тісній координації з Міністерством оборони робить свій внесок у політичні дискусії в Брюсселі. Сили оборони беруть участь у багатонаціональних операціях з підтримання миру, управління кризами та надання гуманітарної допомоги на підтримку ООН. Разом із Міністерством оборони та Міністерством юстиції Республіки Ірландія координує свій внесок у політику миротворчих операцій ООН. У 2024 р. Департамент оборони підготував огляд оборонної політики Республіки Ірландія. У ньому було надано рекомендації щодо посилення заходів безпеки, особливо в морських і кіберпросторах, і розширення співпраці з міжнародними партнерами [5].

Тема зовнішньої безпеки держави на світовій арені становить значний інтерес для дослідників в українській політичній науці. В умовах глобалізації та взаємопов'язаності сучасного світу жодна держава не може самотужки забезпечити свою безпеку. Відкрита економіка Республіки Ірландія та її залежність від міжнародної торгівлі роблять країну вразливою перед глобальними загрозами, такими як кібератаки, шпигунство та атаки на інфраструктуру. Забезпечення національної безпеки є ключовим чинником для економічної стабільності та зростання, що вимагає постійних інвестицій в оборонну сферу.Ситуація у сфері безпеки в Республіці Ірландія зазнає значних змін, які вимагають ретельного планування та використання заходів для протидії новим загрозам, що виникають. У зв'язку з цим уряд Республіки Ірландія зобов'язався збільшити інвестиції в оборону до 1,5 млрд. євро до 2028 р.

Безпека держави та її громадян є першочерговим обов'язком уряду Республіки Ірландія. Конституція Республіки Ірландія виключно парламенту надає право на формування та утримання збройних сил. «Біла книга з оборони» (англ. The White Paper on Defense) Республіки Ірландія являє собою стратегічний і всеосяжний документ, що визначає основи оборонної політики на період до 2025 р. Важливим елементом у системі національної безпеки Республіки Ірландія є «Стратегічна заява Міністерства оборони та Сил оборони на 2023–2026 рр.» (англ. Department of Defence and Defence Forces Strategy Statement 2023–2026) встановлює наступну загальну мету високого рівня: «Забезпечувати військовий захист держави, сприяти національному та міжнародному миру і безпеці та виконувати всі інші завдання, поставлені урядом». Ця мета високого рівня містить у собі три широкі стратегічні аспекти: оборонна політика; забезпечення можливостей для безпеки; оперативні результати діяльності сил оборони. У рамках кожного стратегічного напряму визначається низка пріоритетних цілей, завдань і дій [1].

«Сили оборони» Республіки Ірландія складаються з «Постійних сил оборони» (англ. Permanent Defence Force) і «Резервних сил оборони» (англ. Reserve Defence Force). Сухопутні війська включають в себе армію, військово-повітряні сили і військово-морський флот, загальна чисельність яких становить 9,5 тисяч осіб. Крім того, у складі Сил оборони працює близько 430 цивільних службовців. Армія забезпечує наземну складову оборонного потенціалу держави [2].

«Повітряний корпус Республіки Ірландія» (англ. Irish Air Corps) базується на аеродромі Кейсмент у Балдоннелі і «Військово-морська служба Республіки Ірландія» (англ. The Naval Service) базується

в графстві Корк, де розташовується оперативний штаб, оперативне командування, командування матеріально-технічного забезпечення і Військово-морський коледж [3].

Хоча Республіки Ірландія дотримується офіційної позиції військового нейтралітету і не є членом НАТО, у 1999 р. ірландський уряд приєднався до програми НАТО «Партнерство заради миру». Республіка Ірландія також зобов'язалася підтримувати Спільну зовнішню політику і політику безпеки (англ. Common Foreign and Security Policy), передбачену Маастрихтським договором про ЄС. Республіка Ірландія бере участь у Європейській політиці безпеки та оборони (англ. the EU's European Security and Defence Policy) і надала батальйон для «Сил швидкого реагування ЄС» (англ. The European Rapid Reaction Force). Республіка Ірландія готова брати участь у миротворчих, гуманітарних операціях або операціях із врегулювання криз разом зі своїми партнерами по ЄС, якщо на те є мандат ООН. Ірландські збройні сили постійно беруть участь у миротворчих операціях ООН із середини 1950–х рр [4].

Зміна ситуації у сфері безпеки в Європі призвела до нових дебатів в Республіці Ірландія про нейтральний статус країни. Виклики міжнародному порядку, очолюваному Заходом, з боку Росії та Китаю, а також розвиток гібридних методів для стратегічного суперництва змінили ситуацію з безпекою в Республіці Ірландія. Колись ірландська держава була «надійно захована за Британією», і під час холодної війни звичайні умови Вестфальської системи безпеки дозволяли країні «безоплатно користуватися» колективною безпекою, яку забезпечувала Велика Британія та інші сусіди з НАТО.

Відтоді Дублін намагається адаптувати свою стратегічну позицію до поствестфальських складнощів, які тепер визначають безпеку в його північноатлантичних регіонах. Республіка Ірландія, в якій розташовано безліч міжнародних корпорацій, є великим транснаціональним центром обробки даних, що робить її дедалі привабливішою ціллю для кібератак. 75% трансатлантичних телекомунікаційних кабелів проходять через виключну економічну зону Республіки Ірландія або поруч із нею.

Отже, збільшення фінансування оборони. Стійкі інвестиції в оборону мають вирішальне значення для перетворення Сил оборони та зміцнення ролі Республіки Ірландія як надійного партнера у сфері безпеки.

Список використаних джерел

1. The White Paper on Defence. Department of Defence of the Government of Ireland. October 17, 2024. URL: https://www.gov.ie/en/policy-information/bee90a-white-paper-on-defence/
2. Defence policy of Ireland. Department of Defence of Ireland. August 19, 2019. URL: https://www.gov.ie/en/policy/f2c04b-defence/
3. Roles of the Defence Forces. Department of Defence of Ireland. October 8, 2019. URL: https://www.gov.ie/en/organisation-information/05ab90-roles-of-the-defence-forces/
4. Office of Emergency Planning. Government of Ireland. October 15, 2024. URL: https://www.gov.ie/en/campaigns/624e4-emergency-planning/?referrer=https://www.gov.ie/en/organisation/ec39cf-office-of-emergency-planning/
5. Ireland – Foreign and Security Policy. Global Security. April 9, 2024. URL: https://www.globalsecurity.org/military/world/europe/ie-policy.htm

Летісія СВЕДКУ
студентка 3 курсу спеціальності "Міжнародні відносини",
кафедра історії та суспільних дисциплін
Закарпатського угорського університету імені Ференца Ракоці II

Маріанна МАРУСИНЕЦЬ
кандидат філологічних наук,
доцент кафедри історії та суспільних диспиплін,
старший науковий співробітник, старший дослідник
Науково-дослідного центру імені Тіводора Легоцькі
Закарпатського угорського університету імені Ф. Ракоці II

США І НАТО ГАРАНТИ МІЖНАРОДНОЇ БЕЗПЕКИ

Проблема міжнародної безпеки нині має виняткове значення. Світ переживає складний період воєн, політичних криз і змагання за вплив між великими державами. Людство потребує надійних механізмів, які здатні не допустити поширення конфліктів і підтримувати стабільність. Саме тому роль США та НАТО у світовій системі безпеки є особливо важливою. Після Другої світової війни США та НАТО стали основою колективної оборони, а після початку російської агресії проти України – головними гарантами безпеки не лише для Європи, а й для всього демократичного світу.

Мета дослідження полягає у з'ясуванні, яким чином США та НАТО забезпечують міжнародну безпеку і чому саме вони вважаються її головними гарантами. Актуальність теми зумовлена сучасними проблемами, а саме агресією Росії, нестабільністю на Близькому Сході, зростанням кількості гібридних загроз і кіберзлочинності. Держави часто не можуть самостійно впоратися із зазначеними проблемами, тому роль союзів і стратегічних партнерів набуває першорядного значення.

Наукова новизна полягає у спробі узагальнити сучасну діяльність НАТО і США після 2022 року та показати, як змінилася система колективної безпеки у відповідь на нові загрози. На відміну від попередніх робіт, увага зосереджується не лише на історичному аспекті, а й на реальних фактах – збільшенні фінансування, нових місіях, політиці допомоги Україні та розвитку технологічних оборонних систем.

Основні результати дослідження показують, що США залишаються центральною ланкою глобальної безпеки. За даними Стокгольмського інституту SIPRI, у 2024 році вони забезпечили близько 37 % світових оборонних витрат, що дало можливість утримувати високотехнологічні війська і гарантувати захист союзників [6]. НАТО, у свою чергу, зміцнило свою оборонну здатність. Усі країни-члени досягли мінімуму 2 % ВВП на оборону, що вказує політичну згуртованість і готовність до спільних дій [5].

З 2022 року Альянс суттєво оновив військову структуру, створивши нову модель сил високої готовності. Вона дозволяє швидко реагувати на потенційні загрози, розміщуючи війська у будь-якій точці Європи протягом кількох днів [2]. Одночасно було вдосконалено системи протиповітряної та протиракетної оборони. У 2025 році союзники ухвалили спільну політику IAMD, яка допомагає координувати захист від дронів, ракет і літаків [3].

Не менш важливим є ядерний компонент безпеки. США забезпечують так зване «розширене стримування», тобто гарантують безпеку своїх союзників навіть за допомогою ядерного арсеналу, якщо виникне така необхідність. Задіяний механізм формує потужний фактор стримування потенційних агресорів і підтримує стабільність у Європі [1].

Особливу увагу США і НАТО приділяють Україні. Після початку повномасштабної війни Альянс створив Раду Україна–НАТО, що надала Києву рівноправне право брати участь у консультаціях і плануванні безпеки. США залишаються основним партнером України у військовій сфері, надаючи сучасне озброєння, системи ППО та навчання військових [7]. Підтримка з боку США не лише допомагає Україні боронити свою незалежність, а й зміцнює всю систему європейської безпеки.

Крім того, НАТО продовжує виконувати миротворчі місії, наприклад у Косові (KFOR), забезпечуючи стабільність на Балканах [4]. Здійснення миротворчих операцій доводить, що Альянс залишається не лише військовою організацією, а й політичним інструментом стабілізації міжнародних відносин.

Отже, США і НАТО виконують ключову роль у збереженні миру та стабільності. Їхня сила полягає не лише у військовій потузі, а й у політичній єдності, спільних цінностях і готовності діяти разом. Завдяки спільним оборонним планам, тренуванням, інвестиціям у технології та партнерству з демократичними країнами світ має ефективну систему гарантування безпеки. Сучасна міжнародна система тримається на взаємній підтримці союзників, спільних рішеннях і колективній відповідальності. США та НАТО залишаються головними акторами, які здатні протистояти глобальним загрозам і гарантувати мир.

Список використаних джерел

1. Freedman, L., 2025. Europe's nuclear deterrent: the here and now. Survival. doi: https://doi.org/10.1080/00396338.2025.2508078
2. NATO, 2024. Washington Summit Declaration issued by Heads of State and Government, 15 July. [online] NATO. Available at: https://www.nato.int/cps/en/natohq/ official_texts_227678.htm [Accessed 25 Oct. 2025].
3. NATO, 2025a. NATO Integrated Air and Missile Defence Policy, 13 Feb. [online] NATO. Available at: https://www.nato.int/cps/en/natohq/official_texts_233084.htm [Accessed 25 Oct. 2025].
4. NATO, 2025b. Kosovo Force (KFOR) placemat, 25 Apr. [online] NATO. Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/2025/4/pdf/2025-04-25-KFOR-Placemat.pdf [Accessed 25 Oct. 2025].
5. Reuters, 2025. All NATO members hit old spending target. [online] Reuters. Available at: https://www.reuters.com/business/aerospace-defense/all-nato-members-hit-old-spending-target-only-three-meet-new-goal-2025-08-27/ [Accessed 25 Oct. 2025].
6. SIPRI, 2025. Trends in world military expenditure, 2024. [online] Stockholm International Peace Research Institute. Available at: https://www.sipri.org/publications/2025/sipri-fact-sheets/trends-world-military-expenditure-2024 [Accessed 25 Oct. 2025].
7. U.S. Department of Defense, 2024. Fact sheet on U.S. security assistance to Ukraine, 30 Dec. [online] U.S. Department of Defense. Available at: https://media.defense.gov/2024/Dec/30/2003619433/-1/-1/1/Ukraine-Fact-Sheet-December-30-2024.PDF [Accessed 25 Oct. 2025].

Марк КОПАС
студент 3 курсу спеціальності "Міжнародні відносини",
кафедра історії та суспільних дисциплін
Закарпатського угорського університету імені Ференца Ракоці II,
kopasz.mark.b23nk@kmf.org.ua

Роберт ВАРГА
PhD, старший викладач кафедри історії та суспільних наук
Закарпатського угорського університету імені Ференца Ракоці II,
varga.robert@kmf.org.ua

РОЛЬ БЕЗПЕКИ В ТРАНСКОРДОННОМУ ТА МІЖНАРОДНОМУ СПІВРОБІТНИЦТВІ: ДОСВІД ДАНІЇ

У сучасному світі транскордонне та міжнародне співробітництво стикається з численними викликами, такими як тероризм, кіберзагрози, міграційні кризи та гібридні атаки, які не знають державних кордонів. Постановка наукової проблеми полягає у визначенні ролі безпеки як фундаментального елемента для забезпечення стійкості та ефективності таких форм співпраці. У загальному вигляді це завдання передбачає аналіз механізмів інтеграції безпекових стратегій у багатосторонні відносини, з акцентом на досвід країн, які активно сприяють глобальній стабільності.

Метою дослідження є формулювання ролі безпеки в транскордонному та міжнародному співробітництві на прикладі Данії, обґрунтування її актуальності в контексті сучасних геополітичних змін та розробка рекомендацій для подібних моделей. Актуальність зумовлена ескалацією глобальних загроз, зокрема після російського вторгнення в Україну, що вимагає скоординованих дій на рівні НАТО, ЄС та ООН. Данія, як активний член цих організацій, демонструє, як безпека стає каталізатором для транскордонних ініціатив, сприяючи миру та розвитку за межами Європи.

Наукова новизна дослідження полягає у комплексному аналізі еволюції датської моделі безпеки від "footnote politics" 1980-х до повної інтеграції в PESCO та EDA у 2022 році, порівняно з відомими роботами, такими як звіти SIPRI та Atlantic Council, які фокусуються на загальноєвропейських аспектах, але недостатньо акцентують роль Данії в арктичних та східноєвропейських транскордонних проектах. Запропоновано модель "безпекової дипломатії Данії", що інтегрує двосторонні угоди (наприклад, з Україною) з багатосторонніми форматами (NORDEFCO, E-PINE).

У короткому викладі поставленого завдання розглянуто ключові аспекти: Данія, як активний член НАТО та засновниця ООН, забезпечує безпеку через участь у миротворчих операціях (UNPROFOR, ISAF в Афганістані) та стабілізаційних місіях. Транскордонна співпраця з Німеччиною (Joint Action Plan 2023) включає боротьбу з тероризмом, кіберзагрозами та природними катастрофами, з урахуванням Fehmarn Belt Fixed Link. У 2023 році підписано Defense Cooperation Agreement (DCA) з США, що розширює присутність сил у Гренландії для арктичної безпеки. З 2022 року скасування "оборони opt-out" дозволило Данії приєднатися до PESCO, сприяючи мобільності військ та кіберзахисту в ЄС. У контексті України, Угода про безпеку (2024) передбачає модернізацію ЗСУ, фінансову та гуманітарну допомогу, посилюючи транскордонну стійкість. Аналіз показав, що 70% датських внесків у міжнародні місії (за даними OSCE та UN) спрямовані на превентивну безпеку, що перевищує середньоєвропейські показники.

Висновки: Безпека є основою транскордонного та міжнародного співробітництва, де Данія виступає взірцем через баланс між національними інтересами та глобальними зобов'язаннями. Основні результати: ефективність моделі "безпекової дипломатії" підтверджена успіхами в НАТО та ЄС, з рекомендаціями для України – адаптувати двосторонні угоди для посилення NORDEFCO-подібних ініціатив. Це сприятиме стійкості регіону, зменшуючи ризики гібридних загроз на 25–30% за рахунок обміну технологіями та тренінгами.

Список використаних джерел

1. Brøgger, A. M. (2022). From variation to convergence in turbulent times – foreign and security policy choices among the Nordics 2014–2023. Contemporary Security Policy, 44(2), 1–28. https://doi.org/10.1080/09662839.2023.2221185

2. Danish Security and Defence (2022). The security policy analysis group September 2022. Danish Ministry of Defence. Available at: https://www.fmn.dk/globalassets/fmn/dokumenter/strategi/rsa/-regeringens_security-policy-report_uk_web-.pdf

3. Nordenman, M. (2022). The US-Danish defense and security relationship. Atlantic Council Issue Brief. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/the-us-danish-defense-and-security-relationship/

4. U.S. Department of State (2025). U.S. Security Cooperation with Denmark. Available at: https://www.state.gov/u-s-security-cooperation-with-denmark

5. Угода про співробітництво у сфері безпеки та довгострокову підтримку між Україною та Данією (2024). Офіційне інтернет-представництво Президента України. Available at: https://www.president.gov.ua/news/ugoda-pro-spivrobitnictvo-u-sferi-bezpeki-ta-dovgostrokovu-p-89185

Евелін ГЕЛЕТЕЙ
студентка 2 курсу спеціальності "Міжнародні відносини",
кафедра історії та суспільних дисциплін
Закарпатського угорського університету імені Ференца Ракоці II

Роберт ВАРГА
PhD, старший викладач кафедри історії та суспільних наук
Закарпатського угорського університету імені Ференца Ракоці II,
varga.robert@kmf.org.ua

БЕЗПЕКА ЯПОНІЇ У СИСТЕМІ МІЖНАРОДНИХ ВІДНОСИН

Проблематика безпеки Японії є одним із ключових аспектів сучасних міжнародних відносин, оскільки ця держава відіграє важливу роль у політичній, економічній і технологічній архітектурі Азійсько-Тихоокеанського регіону. Географічне розташування Японії, її історичні особливості та обмеження, накладені після Другої світової війни, зумовили унікальний підхід країни до забезпечення національної безпеки. Упродовж десятиліть Японія будувала свою оборонну політику на принципах пацифізму, проте глобальні трансформації безпекового середовища змусили країну поступово переосмислити власну роль у регіоні та світі.

Після 1945 року Японія, згідно зі статтею 9 Конституції, відмовилася від ведення війни як засобу врегулювання міжнародних суперечок і не підтримувала власних збройних сил. Натомість були створені Сили самооборони Японії, діяльність яких обмежувалася обороною території держави та реагуванням на надзвичайні ситуації. Проте впродовж останніх десятиліть глобальна динаміка безпеки суттєво змінилася. Зростання військової потуги Китаю, ядерна програма Північної Кореї, територіальні суперечки у Східнокитайському морі та загроза кібератак поставили перед Токіо нові виклики.

У цьому контексті метою дослідження є виявлення головних напрямів трансформації системи безпеки Японії, аналіз її сучасної стратегії та визначення ролі міжнародних партнерств у гарантуванні стабільності. Актуальність теми зумовлена тим, що сьогодні безпека Японії безпосередньо впливає на геополітичний баланс у всьому Індо-Тихоокеанському регіоні, а отже — на глобальну систему безпеки.

Наукова новизна полягає у комплексному аналізі політики безпеки Японії не лише як військово-політичного, але й як соціально-економічного та технологічного явища. Японія демонструє новий тип державної стратегії — "інтегровану безпеку", яка поєднує оборону, дипломатію, економічну стійкість, інформаційну безпеку та розвиток інновацій.

Одним із ключових аспектів сучасної політики безпеки є ухвалення у грудні 2022 року нової Стратегії національної безпеки, яка передбачає суттєве збільшення військових витрат — до 2 % ВВП протягом п'яти років. Це стало наймасштабнішим кроком у галузі оборони з часів післявоєнного періоду. Японія планує зміцнити систему протиракетної оборони, придбати крилаті ракети великої дальності, розвинути власні технології спостереження та кіберзахисту.

Важливу роль у забезпеченні стабільності відіграє союз зі Сполученими Штатами Америки, укладений ще у 1951 році. США гарантують Японії так звану "ядерну парасольку", а на території країни розташовані американські військові бази, які слугують стримувальним фактором проти потенційних агресорів. Співпраця у сфері безпеки між Токіо та Вашингтоном включає спільні навчання, обмін розвідданими, координацію дій у кіберпросторі та космічній сфері.

Крім американського партнерства, Японія активно розширює регіональні зв'язки в рамках Quad (США, Японія, Індія, Австралія), бере участь у ініціативі "вільного і відкритого Індо-Тихоокеанського регіону" та поглиблює відносини з державами Південно-Східної Азії. Особлива увага приділяється розвитку безпечних морських шляхів, оскільки Японія є імпортером енергоносіїв і залежить від стабільності морської торгівлі.

Кібербезпека та інформаційна стійкість стали новими вимірами японської оборонної стратегії. Створення Національного центру кіберзахисту та ухвалення державної програми боротьби з кібершпигунством мають на меті посилити здатність держави протидіяти атакам

на енергетичні системи, банки, транспортну інфраструктуру та державні мережі. Японія також бере участь у міжнародних ініціативах, спрямованих на створення єдиних стандартів кіберзахисту в рамках ООН і G7.

Енергетична безпека становить ще один критичний елемент національної стратегії. Після аварії на АЕС “Фукусіма-1” у 2011 році уряд був змушений переглянути політику енергопостачання. Залежність від імпорту нафти та газу змушує країну диверсифікувати джерела енергії, інвестувати у відновлювані ресурси та атомну енергетику нового покоління. Енергетична стійкість розглядається як невід’ємна складова безпеки держави, оскільки будь-які перебої можуть мати серйозні наслідки для економіки та соціальної стабільності.

Водночас Японія зберігає вірність своїм пацифістським ідеалам і прагне забезпечити мир переважно дипломатичними засобами. Токіо виступає за посилення ролі ООН, підтримує миротворчі місії, активно бере участь у програмах допомоги країнам, що розвиваються. Такий підхід формує позитивний імідж держави як миролюбної та надійної сили, що поєднує оборонну спроможність із міжнародною відповідальністю.

У підсумку можна стверджувати, що система безпеки Японії зазнала суттєвих змін — від оборонного пацифізму до проактивної політики, орієнтованої на багаторівневу взаємодію із союзниками, розвиток високих технологій і забезпечення енергетичної незалежності. Виклики XXI століття змушують Японію формувати нову концепцію національної безпеки, де ключову роль відіграють баланс між військовими і дипломатичними інструментами, розвиток кіберзахисту та зміцнення міжнародних партнерств. Подальше утвердження Японії як стабільного, високотехнологічного й відповідального актора глобальної політики є запорукою миру та безпеки не лише для регіону, а й для світу загалом.

Список використаних джерел

1. Безсмертна, О. (2023). Оборонна стратегія Японії: трансформація пацифізму у XXI столітті. Київ: Інститут міжнародних відносин.
2. Гнатюк, І. (2022). Роль Японії у забезпеченні безпеки в Азійсько-Тихоокеанському регіоні. Вісник міжнародних досліджень, №3, с. 45–52.
3. Костенко, М. (2024). Сучасні виклики національній безпеці Японії. Міжнародна аналітика, №2, с. 17–25.
4. Кравець, Н. (2023). Кібербезпека як новий вимір національної безпеки Японії. Політичні студії, №4, с. 58–65.
5. Японія ухвалила нову стратегію національної безпеки (2022). BBC News Україна. https://www.bbc.com/ukrainian
6. Ministry of Defense of Japan (2023). National Security Strategy of Japan. Tokyo: MOD Japan.

Камілла СТАНКОВИЧ
студентка 2 курсу спеціальності "Міжнародні відносити"
Закарпатський угорський університет імені Ференца Ракоці ІІ,
stankovickamilla@gmail.com

Роберт ВАРГА
PhD, старший викладач кафедри історії та суспільних наук
Закарпатський угорський університет імені Ференца Ракоці ІІ,
varga.robert@kmf.org.ua

ПІДТРИМКА ТА БЕЗПЕКА ВНУТРІШНЬО ПЕРЕМІЩЕНИХ ОСІБ (ВПО) НА ЗАКАРПАТТІ

Актуальність теми дослідження: З початком повномасштабного вторгнення тисячі українців вимушені були покинути свої домівки, щоб врятувати своє життя, життя дітей та рідних. Закарпатська область стала одним із ключових регіонів для прийому внутрішньо переселених осіб, через її близькість до кордону з ЄС та відносну безпечність. Станом на 19 жовтня 2024 року, за офіційними даними Закарпатської обласної військової адміністрації, на Закарпатті 126 502 особи зі статусом ВПО офіційно перебували на обліку, 300 тисяч осіб ВПО фіксують в області мобільні оператори. Тобто десятки тисяч осіб, які потребують житла, працевлаштування. медичної та психологічної допомоги. Дослідження питань безпеки та підтримки переселенців є надзвичайно важливим в умовах воєнного стану.

Постановка наукової проблеми: Незважаючи на те, що Закарпаття стало одним із центрів прийому переселенців з інших регіонів України, проблема забезпечення житлом, працевлаштуванням, доступом до соціальних послуг досі залишається актуальною. Більшість заходів реалізується у форматі короткострокових ініціатив, які не завжди забезпечують стабільну інтеграцію ВПО у місцеві громади.

Постановка завдання, мета дослідження: Актуальним науковим завданням є розробка моделі ефективної взаємодії між усіма суб'єктами підтримки переселенців та формування безпечного соціального середовища у приймаючих громадах Закарпаття. Також метою є аналіз основних напрямків підтримки та безпеки ВПО у Закарпатській області.

Викладення основного матеріалу (результати роботи): Досліджуючи тему підтримки та безпеки ВПО на Закарпатті, важливо насамперед визначити, хто саме належить до цієї категорії населення, а також простежити історичні передумови виникнення цього явища в Україні.

Поняття внутрішньо переміщена особа(ВПО), за статтею 1 Закону України "Про забезпечення прав і свобод внутрішньо переміщених осіб " № 1706-VII (від 20 жовтня 2014 року), є громадянин України, а також іноземець чи особа без громадянства, які мають право на постійне проживання в Україні та були змушені покинути своє місце проживання через збройний конфлікт, тимчасову окупацію, насильство, порушення прав людини або надзвичайні ситуації природного чи техногенного характеру.

Саме 2014 рік став початком масштабного внутрішнього переміщення українців після окупації Криму та початку бойових дій на сході України. Уже тоді Закарпаття приймало переселенців із Донецької, Луганської та Херсонської областей. А тому в пошуках тимчасового притулку ці люди надавали перевагу найбільшим містам області – Ужгороду й Мукачеву та їхнім околицям. Тоді прибувало по 50-80 осіб за добу, стояли черги. Зрозуміло, що люди шукають роботу, адже таких спеціальностей, як у східних областях, наприклад, шахтарі, у Закарпатті немає. Це підкреслює важливість адаптації переселенців до нових умов праці та життєдіяльності.

Тож основними викликами для переселенців того року були:

1. Житло. Закарпаття стало одним із основних регіонів, куди переселялися внутрішньо переміщені особи. За даними Управління Верховного комісара ООН у справах біженців (UNHCR), на липень 2014 року в Закарпатській області було зареєстровано понад 2 000 ВПО,

зокрема з Криму та Донбасу. Тому більшість людей проживали в орендованих квартирах та будинках або ж жили в притулках.

2. Працевлаштування. Через велику кількість переселенців,значно збільшився попит на робочі місця. Наприклад, більшість людей мали такі професії, які не мали попиту на Закарпатті. До прикладу, шахтарі, металурги та працівники важкої промисловості.

3. Психологічна підтримка. Багато ВПО пережили травматичні події, які вплинули на їхню психіку та вимагали надання психологічної допомоги.

Закарпатська обласна рада та місцеві органи влади ефективно співпрацювали з різними міжнародними організаціями для надання ВПО допомоги. Наприклад, UNHCR(Агентство ООН у справах біженців), яка присвячує свою діяльність порятунку життів, захисту прав і створенню кращого майбутнього для біженців, внутрішньо переміщених осіб та осіб без громадянства. Було організовано тимчасові притулки, надано гуманітарну допомогу та доступ до медичних послуг.

Проте справжнім викликом для області стало повномасштабне вторгнення Росії, що розпочалася у лютому 2022 року. Тому що саме після нього кількість внутрішньо переміщених осіб у Закарпатській області різко зросла. Сюди прибували десятки тисяч людей з усіх регіонів України, які шукали, насамперед, фізичної безпеки, але й соціальної стабільності, підтримки та житла. За даними місцевих органів влади, у 2022 році кількість офіційно зареєстрованих ВПО в області було понад 156 тисяч осіб. З початку повномасштабного вторгнення Закарпаття прийняло близько 400 тисяч ВПО. На кінець 2024 року їх кількість оцінювалася в 250–300,000. Кількість офіційно зареєстрованих ВПО на той час становила 127,000 осіб, із них близько 40,000 – в Ужгороді. Оскільки ВПО здебільшого приїхали з великих міст, вони шукали притулку. ВПО в Берегівському районі прибули з Харкова, 20% – зі столиці, 12,2% – з Донецька. Крім того, велика кількість біженців прибула з Маріуполя, Луганська, Дніпра, Краматорська та Миколаєва.

Закарпаття стало одним із головних регіонів гуманітарної підтримки переселенців. Тут активно діяли волонтерські центри, благодійні фонди, міжнародні організації (UNHCR, IOM, UNICEF, Червоний Хрест, USAID), які допомагали із забезпеченням житлом, продуктами харчування, медичними послугами, освітою та психологічною підтримкою.

Прикладом громадських організацій є благодійний фонд "Карітас Мукачівської греко-католицької єпархії", який знаходиться в місті Мукачеве. Ця організація надає гуманітарну, соціальну, психологічну допомогу всім, хто її потребує, включаючи внутрішньо переселених осіб.

Також потрібно згадати саме волонтерів, які у перші місяці війни стали організовувати надання гуманітарної допомоги(продукти, одяг, ліки, засоби гігієни), пошуки житла та робочі місця. Саме завдяки їм утворювалися волонтерські центри. Наприклад, в Ужгороді, Берегові, Мукачеві, Хусті та інших містах досі є пункти, в яких ВПО можуть отримати необхідну їм допомогу.

Область стала одною з лідерів надання грошової підтримки ВПО у 2022 році. За словами заступника голови ОВА Петра Добромільського, вимушені переселенці, які зареєструвалися в Закарпатській області, отримали державну допомогу на суму 1,8 млрд грн та понад 100 млн доларів від закордонних партнерів. Тому завдяки спільній праці влади, міжнародних організацій та волонтерів процес гуманітарної допомоги пройшов без криз.

Станом на 2025 рік ситуація з підтримкою та безпекою ВПО на Закарпатті зазнало значних змін в кращу сторону. В області ще досі діє велика кількість соціальних та гуманітарних програм. Зокрема, в Ужгороді з початку року відкрився перший обласний психологічно-соціальний центр для ВПО, який працює в кожній громаді області та надає допомогу людям, які зазнали травм через війну.

Активізувалася і служба зайнятості - все більше переселенців почали знаходити робочі місця. До неї звернулося 1226 переселенців, з яких 333 вдалося працевлаштувати. Також варто додати, що значно зросла економічна активність в області через те, що переселенці, які мали власний бізнес у своєму регіоні перенесли свою діяльність на Закарпаття. Так це сприяло до збільшення податкових надходжень до місцевих бюджетів.

Також десь 30 % переселенців — це близько 100 000 осіб — планують залишитися на Закарпатті на постійній основі. Це свідчить про відносну стабільність у регіоні, довіру до місцевої влади та ефективність її підтримки. Водночас проблеми з працевлаштуванням і забезпеченням житлом залишаються актуальними, що потребує подальшого залучення державних, міжнародних і громадських ресурсів.

Висновки: Отже, проаналізувавши цю тему, дослідження питання підтримки та безпеки ВПО на Закарпатті дозволяє зробити висновки, що область стала однією з головних центрів прийому та інтеграції внутрішньо переселених осіб в Україні. Ще починаючи з 2014 року, коли лише розпочався конфлікт на сході країни, Закарпаття почало приймати переселенців і забезпечувати людей тимчасовим притулком, надавати гуманітарну допомогу та можливість на безпечне життя. Звичайно не все було ідеально. Вже тоді виникали проблеми з нестачею житла та працевлаштуванням. А ситуація після початку повномасштабного вторгнення у 2022 році змінилася: кількість переселенців значно зросла. Утворювалися різні благодійні фонди, приєднувалися волонтерські об'єднання та міжнародні організації до надання людям допомоги та підтримки. Наразі рівень безпеки в регіоні залишається високим, незважаючи на нещодавні події, коли Росія завдала удару ракетами "Калібрі" по американському підприємству "Flex" на околиці міста Мукачева. Закарпаття сьогодні є прикладом регіону, де люди та партнери об'єдналися та перетворили кризу на можливість розвитку - як для своїх людей, так і людям з інших регіонів України.

Список використаних джерел

1. Про забезпечення прав і свобод внутрішньо переміщених осіб : Закон України від 20 жовтня 2014 р. URL: https://ukc.gov.ua/knowdledge/ponyattya-vnutrishno-peremishhenoyi-osoby/
2. Про розміщення вимушених переселенців на Закарпатті. URL: https://carpathia.gov.ua/news/na-zakarpatti-rozshyriuiut-merezhu-oseredkiv-dlia-rozmishchennia-vpo
3. Аналітика ВПО в Україні. URL: https://www.ioc.gov.ua/analytics/dashboard-vpo
4. Благодійний фонд "Карітас" URL: https://caritas-uz.com/pro-caritas
5. Про отримання послуг обласної служби зайнятості для переселенців URL: https://zak.dcz.gov.ua/novyna/ponad-1200-vnutrishno-peremishchenyh-osib-otrymaly-poslugy-oblasnoyi-sluzhby-zaynyatosti-z
6. The first Zakarpattia Oblast psychosocial support centre opens in Uzhhorod URL: https://www.eeas.europa.eu/delegations/ukraine/first-zakarpattia-oblast-psychosocial-support-centre-opens-uzhhorod-assist-people-affected-war_en
7. Коваль, К. П. (2025). СОЦІАЛЬНО-ЕКОНОМІЧНА ТРАНСФОРМАЦІЯ ЗАКАРПАТТЯ В УМОВАХ ВІЙНИ: МІГРАЦІЯ, ПЕРЕМІЩЕННЯ БІЗНЕСУ Й ЕТНІЧНА(2) ст. 49-50
8. Дудла М. Вимушені переселенці в умовах агресії Росії проти України в контексті загального міграційного процесу(2024) ст. 34-39

Емілія ГЕЛЕТЕЙ
студентка 2 курсу спеціальності "Міжнародні відносити"
Закарпатський угорський університет імені Ференца Ракоці II,
geletei.emilia.b24nk@kmf.org.ua

Дмитро ТКАЧ
доктор політичних наук,
професор кафедри історії та суспільних дисциплін
Закарпатського угорського університету імені Ференца Ракоці II

ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Проблема забезпечення національної безпеки України сьогодні є надзвичайно актуальною, особливо в умовах воєнного стану та тривалої збройної агресії проти нашої держави. Сучасна ситуація потребує швидких і зважених рішень, оскільки війна, економічна нестабільність, інформаційні загрози та соціальні виклики впливають на всі сфери життя країни.. Тому вивчення стану національної безпеки, визначення її ключових складових і головних пріоритетів є не лише теоретично важливим, а й необхідним для забезпечення стабільності та подальшого розвитку української держави.

Постановка проблеми. Становлення України як демократичної та правової держави значною мірою залежить від стабільності суспільних відносин, захисту прав і свобод громадян, а також від належного рівня національної безпеки. Національна безпека означає захищеність життєво важливих інтересів держави, суспільства й кожної людини відповідно до норм національного та міжнародного права. Діяльність держави у цій сфері спрямована на сталий розвиток суспільства, своєчасне виявлення, попередження та нейтралізацію реальних і потенційних загроз національним інтересам.

Стан дослідження. Проблеми національної безпеки України досліджували відомі вчені-правознавці, зокрема В.Б. Авер'янов, О.Ф. Андрійко, Ю.П. Битяк, О.М. Бандурка та В.М. Гаращук. Їхні праці присвячені вдосконаленню правових і організаційних механізмів безпеки держави в умовах сучасних викликів. Тому важливо продовжувати вивчати цю тему, особливо під час воєнного стану.

Мета дослідження є вивчення стану національної безпеки України визначення її ключових складових і головних пріоритетів.

Виклад основного матеріалу. Забезпечення національної безпеки України є одним із ключових пріоритетів державної політики, особливо в умовах тривалої збройної агресії проти нашої держави. Національна безпека — це комплексний стан захищеності життєво важливих інтересів особи, суспільства та держави від широкого спектра внутрішніх і зовнішніх загроз, які можуть порушувати стабільність, конституційний лад та можливості для подальшого розвитку країни.

Сутність та структура національної безпеки

Система національної безпеки України охоплює політичну, військову, економічну, екологічну, соціальну, гуманітарну, інформаційну, кібернетичну та інші сфери. Кожна з них має власні загрози, особливості та механізми протидії, але всі вони взаємопов'язані та функціонують як єдина система. Наприклад, економічна нестабільність може послабити обороноздатність, а інформаційні атаки здатні впливати на політичні процеси та громадську думку.

Інтереси національної безпеки охоплюють захист прав і свобод людини, духовних і матеріальних цінностей суспільства, конституційного ладу, суверенітету, незалежності та територіальної цілісності держави. Саме ці елементи становлять основу державної стабільності та здатності України протистояти загрозам.

Основні загрози сучасному стану безпеки.

Україна тривалий час перебуває у складному геополітичному середовищі. До 2014 року основними загрозами вважалися економічні кризи, корупція, тіньова економіка,

техногенні аварії та слабкість державних інституцій. Однак анексія Криму, бойові дії на Донбасі, а згодом повномасштабна війна 2022 року докорінно змінили уявлення про національну безпеку.

Повномасштабне вторгнення Російської Федерації 24 лютого 2022 року стало найбільшим викликом за весь період незалежності. Воно спричинило не лише значні людські втрати, руйнування інфраструктури та економічні збитки, а й вимагало оперативної перебудови всієї системи безпеки та оборони. Війна підсилила значення таких загроз, як: кібератаки на державні та військові системи, що стали одним із напрямів гібридної війни; масштабна інформаційно-психологічна операція, спрямована на деморалізацію населення; енергетичний шантаж, зокрема атаки на критичну інфраструктуру; економічне виснаження, пов'язане з бойовими діями та блокуванням логістики; міграційні виклики, пов'язані з вимушеним переселенням мільйонів громадян.

Об'єкти національної безпеки

До головних об'єктів національної безпеки належать:

1. Особа — її конституційні права, свободи, життя та здоров'я.
2. Суспільство — духовні традиції, культурна спадщина, національна єдність, інформаційний простір.
3. Держава — її суверенітет, конституційний лад, територіальна цілісність, обороноздатність та функціонування органів влади.

Захист кожного із цих об'єктів вимагає комплексних та узгоджених дій усього сектору безпеки та оборони.

Завдання та напрями державної політики у сфері безпеки

Завдання та напрями державної політики у сфері безпеки охоплюють широкий комплекс дій, спрямованих на захист держави, суспільства та кожного громадянина. Одним із ключових напрямів є зміцнення обороноздатності України. Це передбачає модернізацію Збройних Сил, удосконалення матеріально-технічного забезпечення, розширення військово-технічної співпраці з міжнародними партнерами та розвиток національної оборонної промисловості. Не менш важливим завданням є захист державного кордону та українських територій, зокрема проведення заходів, спрямованих на деокупацію тимчасово захоплених регіонів.

У сучасних умовах особливої ваги набуває забезпечення енергетичної незалежності держави. Мова йде про розвиток альтернативних джерел енергії, модернізацію енергетичних систем, а також захист критичної інфраструктури від диверсій та ракетних ударів. Значну увагу державна політика приділяє також інформаційній та кібербезпеці. Йдеться про захист державних інформаційних ресурсів і реєстрів, протидію кібератакам, а також боротьбу з дезінформацією та фейковими кампаніями, що спрямовані на дестабілізацію суспільства.

Важливим складником національної безпеки є економічна стійкість. Для її зміцнення держава реалізує політику підтримки бізнесу, залучення інвестицій, відновлення підприємств, зруйнованих війною, а також активну боротьбу з корупцією, що традиційно послаблює економічний потенціал країни. Ефективне економічне управління є ключовим для стабільності держави та здатності протистояти зовнішнім загрозам.

Окремим стратегічним напрямом є інтеграція України до Європейського Союзу та НАТО. Цей курс визначено як пріоритетний, оскільки саме європейська та євроатлантична інтеграція забезпечує Україні додаткові гарантії безпеки, сприяє модернізації сектору оборони та адаптації до стандартів провідних демократичних держав. Усе це робить національну політику у сфері безпеки комплексною, системною та спрямованою на довгостроковий розвиток і захист країни.

Нормативно-правове забезпечення

Сфера національної безпеки ґрунтується на низці законів та документів, серед яких:

- Конституція України — основа всього законодавства з питань безпеки;
- Закон України «Про національну безпеку України»;

• Закон України «Про оборону України», «Про Службу безпеки України», «Про правовий режим воєнного стану»;
• укази Президента, рішення РНБО, нормативні акти Кабінету Міністрів;
• Стратегія національної безпеки «Безпека людини — безпека країни».

Висновки

1. Національна безпека України сьогодні є пріоритетом держави і передбачає захист суверенітету, територіальної цілісності та життєво важливих інтересів громадян.
2. Основними загрозами є воєнна агресія, техногенні та природні катастрофи, економічні втрати та збереження людського потенціалу.
3. Головні об’єкти національної безпеки — громадяни, суспільство та держава, а пріоритетними завданнями є захист їхніх прав, стабільність та розвиток держави.
4. Ефективна національна безпека забезпечується через комплекс політичних, економічних, правових, соціальних та військових заходів, а також реалізацію державних стратегій і нормативно-правових документів.
5. Стратегія національної безпеки України визначає пріоритети, загрози та шляхи їх подолання, сприяє розвитку сектору безпеки та підвищенню готовності держави реагувати на будь-які загрози.

Список використаних джерел:

1. Білий В. І., Михальчук В. М. Основні напрями забезпечення національної безпеки держави. *Інвестиції: практика та досвід.* 2021. № 17. С. 92–98. DOI: 10.32702/23066814.2021.17.92.
2. Конституція України : Закон України від 28 червня 1996 р. № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254к/96-ВР
3. Про національну безпеку України : Закон України від 21 червня 2018 р. № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19
4. Про рішення Ради національної безпеки і оборони України «Про Стратегію національної безпеки України» : Указ Президента України від 14 вересня 2020 р. № 392/2020. URL: https://www.president.gov.ua/documents/3922020-35037

Валерія ЧОБАЛЬ
студентка факультету міжнародних економічних відносин
ДВНЗ «Ужгородський національний університет»
chobal.valeriia@student.uzhnu.edu.ua

Ігор ЛЯХ
д.т.н., професор, професор кафедри інформатики
та фізико-математичних дисциплін
ДВНЗ «Ужгородський національний університет»
igor.lyah@uzhnu.edu.ua

ДВОМОВНІСТЬ І ТЕРИТОРІАЛЬНА ЦІЛІСНІСТЬ У ПРИКОРДОННИХ РЕГІОНАХ УКРАЇНИ: ПРОБЛЕМАТИКА ЗАКАРПАТТЯ

Прикордонні регіони завжди вирізняються високою мовною та культурною різноманітністю, що створює особливий соціальний контекст. Закарпаття – яскравий приклад регіону, де співіснують понад тридцять етнічних груп, серед яких українці, угорці, румуни, словаки та інші [3]. Цей мовний плюралізм зумовлює складне білінгвальне середовище, що з одного боку збагачує культурний простір, а з іншого – породжує психологічні напруження і потенційні конфлікти, які іноді ставлять під сумнів цілісність держави.

Двомовність – використання двох мов людьми, які належать до певних етнічних груп і спільнот, мови яких не є загальнопоширеними у даній державі чи на певній території [4]. Поняття білінгвізму в контексті Закарпаття – це не лише володіння двома мовами, а й багатогранний психолінгвістичний феномен, який впливає на ідентичність, комунікативні стратегії і міжгрупову взаємодію. Відомо, що білінгви автоматично активують у мозку дві мовні системи, що створює когнітивне навантаження через необхідність швидкого перемикання між кодами (код-свічінг). Цей процес підвищує ризик комунікативних непорозумінь і емоційної втоми. На Закарпатті, де історичні контексти та політичні обставини накладають додаткове навантаження, мовна конкуренція часто посилює міжетнічну напругу.

Аналіз статей про мовні конфлікти на Закарпатті демонструє, що мовне питання часто сприймається через призму політичних ідентичностей. Наприклад, публікації [7,5] висвітлюють парадокси мовного питання, де мовні права одних груп іноді трактуються як загроза іншим, що сприяє формуванню когнітивних бар'єрів і конфронтації. Водночас, Омбудсмен Денис Кремінь у своєму звіті [2] звертає увагу на необхідність збалансованого підходу до мовного питання, наголошуючи на важливості прав національних меншин, що підтверджує і Стаття 53 Конституції України, яка гарантує право на навчання рідною мовою: «Громадянам, які належать до національних меншин, відповідно до закону гарантується право на навчання рідною мовою чи на вивчення рідної мови у державних і комунальних навчальних закладах або через національні культурні товариства» [6]. Це законодавче положення покликане захищати мовні права і знижувати потенційну напругу.

У контексті розгляду двомовності прикордонних регіонів варто згадати і про явище мовного саботажу [1], коли окремі групи використовують мовне питання для політичного тиску, що може призвести до підриву соціальної згуртованості. Психолінгвістичний аналіз таких ситуацій вказує на активацію феномену мовної ідентичності як маркера етнічної приналежності, що посилює міжгрупові бар'єри і створює психологічний розлом у спільноті. Така мовна ізоляція активує феномени «ми» та «вони», що сприяє соціальній поляризації і загрожує територіальній цілісності держави через посилення сепаратистських настроїв.

Однак білінгвізм сам по собі не є прямою загрозою суверенності та незалежності держави. Проблема виникає тоді, коли мовна різноманітність маніпулюється у політичних цілях, а відсутність ефективних соціально-психологічних механізмів діалогу створює середовище для ескалації конфліктів. З огляду на це, важливо впроваджувати освітні програми, спрямовані на розвиток міжкультурної толерантності і прийняття мовного плюралізму. Такі програми

допомагають молоді адаптуватися до двомовного середовища і знизити когнітивне та емоційне навантаження, пов'язане з перемиканням між мовами.

Психологічна підтримка і тренінги з управління стресом і емоційною регуляцією допомагають білінгвам краще справлятися з когнітивними конфліктами, зменшуючи ризик виникнення соціальних конфронтацій. Важливим інструментом є також створення онлайн-платформ для відкритого діалогу між різними мовними спільнотами, що сприяє розвінчанню стереотипів і формуванню спільної ідентичності на основі взаємоповаги.

Отже, білінгвізм на Закарпатті не є за своєю суттю загрозою для територіальної цілісності України. Загроза виникає через соціально-політичні маніпуляції та відсутність належної підтримки міжетнічного діалогу. Адекватне застосування психолінгвістичних і соціокультурних підходів у поєднанні з дотриманням конституційних гарантій прав національних меншин може стати ключем до збереження стабільності й гармонії в регіоні. Тільки через підтримку різноманіття як цінності, а не як чинника розбрату, Україна зможе зберегти свою територіальну цілісність і забезпечити безпеку для всіх своїх мешканців.

Список використаної літератури та джерел

1. Бастіон, 2021. Мовний саботаж на Закарпатті. [online] Бастіон. Available at: https://bastion.tv/movnij-sabotazh-na-zakarpatti_n35999#google_vignette [Accessed 18 Sep. 2025].
2. Главком, 2021. Омбудсман Кремінь розповів про мовну ситуацію на Закарпатті. [online] Главком. Available at: https://glavcom.ua/country/society/obmudsmen-kremin-rozpoviv-pro-movnu-situatsiju-na-zakarpatti-907780.html [Accessed 18 Sep. 2025].
3. Ковач, Л., 2006. Динаміка етнічного складу населення Закарпатської області за матеріалами переписів 1989 та 2001 рр. Наукові записки Інституту політичних і етнонаціональних досліджень ім. І. Ф. Кураса НАН України, Вип. 29, pp.276-287.
4. Енциклопедія сучасної України, 2014. Двомовність. Київ: Енциклопедія сучасної України, Т. 3, p.23774. [online] Available at: https://esu.com.ua/article-23774 [Accessed 18 Sep. 2025].
5. Закарпаття.net.ua, 2021. Етнічні угорці на Закарпатті майже не говорять українською і не поспішають її вивчати. [online] Закарпаття.net.ua. Available at: https://zakarpattya.net.ua/News/176671-Etnichni-uhortsi-na-Zakarpatti-maizhe-ne-hovoriat-ukrainskoiu-i-ne-kvapliatsia-ii-vyvchaty---TSN [Accessed 18 Sep. 2025].
6. Конституція України. Стаття 53. [online] Available at: https://constitution.in.ua/articles/53/ [Accessed 18 Sep. 2025].
7. Мукачево.net, 2018. Парадокси мовного питання у Закарпатті. [online] Мукачева.net. Available at: https://mukachevo.net/post/paradoksy-movnoho-pytannia-u-zakarpatti-foto_39012.html [Accessed 18 Sep. 2025].

TÓTH Rebeka Sára
Hallgató, III. évfolyam, Nemzetközi kapcsolatok szak
Történelem- és Társadalomtudományi Tanszék,
II. Rákóczi Ferenc Kárpátaljai Magyar Egyetem

DARCSI Karolina
II. Rákóczi Ferenc Kárpátaljai Magyar Egyetem
Történelem- és Társadalomtudományi Tanszék adjunktusa és kutatója

IZLAND NATO-TAGSÁGÁNAK POLITIKAI JELENTŐSÉGE

Izland NATO-tagsága különleges helyet foglal el a nemzetközi biztonságpolitikában. A szigetország 1949-ben, a hidegháború kezdetén csatlakozott a NATO-hoz, annak ellenére, hogy nincs saját hadserege. Ez az ellentmondás, hogy egy állam katonai erő nélkül válik egy katonai szövetség tagjává a mai napig izgalmas kérdéseket vet fel Izland külpolitikájával és nemzetközi szerepével kapcsolatban.

Izland biztonságpolitikai helyzete egyedi, mivel a NATO-tagság biztosítja számára a védelmet, miközben ő maga nem járul hozzá közvetlen katonai eszközökkel a szövetség működéséhez. Az ország földrajzi elhelyezkedése (az Atlanti-óceán északi részén) stratégiai szempontból kiemelten fontos, különösen a légi és tengeri mozgások ellenőrzése szempontjából. Ez tette lehetővé, hogy Izland már a második világháború idején is fontos szerepet töltsön be a nagyhatalmak számára, majd később a NATO keretein belül.

Ugyanakkor a NATO-tagság kezdettől fogva vitákat váltott ki az izlandi belpolitikában. A döntés, hogy az ország külföldi katonai jelenlétet engedélyez a saját területén, sokáig erős társadalmi ellenállással találkozott. A különböző politikai pártok és mozgalmak másként értékelték a tagság előnyeit és hátrányait, különösen a szuverenitás kérdése és a külpolitikai függetlenség szempontjából. A tagság így nemcsak külpolitikai döntés volt, hanem hosszú távon is formálta az ország belpolitikai vitáit és identitását.

A tézis célja az, hogy bemutassa, hogyan alakult Izland viszonya a NATO-hoz az elmúlt évtizedekben, milyen politikai és társadalmi tényezők befolyásolták a tagság megítélését, és milyen szerepet tölt be ma a szövetségben egy olyan ország, amely nem rendelkezik hadsereggel. A kérdés megértéséhez fontos figyelembe venni Izland történelmi tapasztalatait, földrajzi helyzetét, valamint a nemzetközi rendszerben betöltött sajátos szerepét. Ez a különleges helyzet (egy hadsereg nélküli állam aktív részvétele egy katonai szövetségben) segít jobban megérteni a biztonságpolitika tágabb értelmezését, és azt is, hogyan lehet egy ország politikai jelentősége nagyobb, mint amit a katonai képességei alapján várnánk.

Izland NATO-tagsága több szempontból is rendhagyó. A legszembetűnőbb különbség más tagállamokhoz képest az, hogy Izland nem rendelkezik saját hadsereggel, és nem is hozott létre katonai védelmi intézményt a tagságát követően. Ez a sajátosság már a tagság kezdeti időszakában is komoly kérdéseket vetett fel a szövetség számára, mivel a NATO kollektív védelmi elve (az 5. cikkely alapján) alapvetően a tagállamok katonai hozzájárulására épül. Izland azonban nem katonai erejével, hanem földrajzi elhelyezkedésével és stratégiai fontosságával vált a szövetség számára értékessé.

A II. világháború során az Egyesült Államok és Nagy-Britannia is felismerte Izland geostratégiai jelentőségét, mivel az ország fontos légi és tengeri útvonalak kereszteződésében helyezkedik el. A hidegháború alatt pedig az észak-atlanti térség kiemelt jelentőséget kapott a Szovjetunióval szembeni védelemben. Ebben a kontextusban Izland szerepe különösen felértékelődött, nem, mint katonai hatalom, hanem mint logisztikai és megfigyelési bázis.

Az 1951-ben aláírt védelmi megállapodás az Egyesült Államokkal megerősítette ezt a pozíciót, és egy hosszú távú katonai jelenlétet eredményezett az ország területén, elsősorban a Keflavík-i légibázison keresztül. Ez azonban belpolitikai feszültségekhez vezetett. A külföldi katonai jelenlét kérdése erősen megosztotta az izlandi társadalmat és a politikai elitet. A szövetséghez való tartozás gyakran ideológiai vita tárgya volt: a konzervatív és nyugatbarát politikai erők támogatták, míg a

baloldali pártok, valamint különböző társadalmi mozgalmak rendszeresen bírálták az idegen katonai jelenlétet és a tagságot.

Ennek következtében Izland NATO-tagságát nemcsak külpolitikai kérdésként kell értelmeznünk, hanem a belpolitikai identitás és értékrendek küzdelmének részeként is. A tagság körüli viták sokszor nem biztonsági szempontokat tükröztek, hanem azt a dilemmát, hogy milyen mértékben kíván az ország bekapcsolódni a nemzetközi politikai és katonai struktúrákba, illetve hogyan tudja megőrizni politikai és kulturális függetlenségét ebben a folyamatban.

Az Egyesült Államok 2006-os kivonulása a Keflavík-i bázisról új helyzetet teremtett. Bár a NATO-tagság nem szűnt meg, a konkrét katonai jelenlét megszűnése felerősítette a kérdést, hogy Izland képes-e önállóan ellátni a minimális biztonságpolitikai feladatait, vagy továbbra is más államok támogatására szorul. Az ezt követő években Izland újraértékelte biztonságpolitikai szerepét. A hangsúly a nem katonai (például polgári védelmi, kiberbiztonsági vagy válságkezelési) hozzájárulások felé tolódott el.

Emellett fontos megemlíteni, hogy Izland biztonságpolitikai identitása egyre inkább a skandináv térséghez való kapcsolódás felé mozdult el. A regionális együttműködés, különösen a másik négy északi állammal (Norvégia, Svédország, Finnország, Dánia) való közös fellépés és biztonsági párbeszéd, egyfajta „új északi egyensúlyt" eredményezett, amelyben Izland továbbra is a katonai szerepvállalás nélküli, de politikailag aktív partnerként jelenik meg. Ezzel párhuzamosan az ország folyamatosan keresi azokat a lehetőségeket, ahol saját adottságaira, mint például a sarkvidéki kérdések, tengeri biztonság, vagy környezetvédelmi kihívások, építve tud releváns szerepet játszani a nemzetközi biztonsági diskurzusban.

Izland NATO-tagságának története jól példázza, hogy a biztonságpolitika nem kizárólag katonai kapacitásokon és hagyományos hadászati erőn alapul. Egy állam szerepe egy nemzetközi katonai szövetségben nem feltétlenül a fegyveres erők meglétével vagy méretével mérhető, hanem sokkal, inkább azzal, hogy milyen stratégiai, politikai és regionális értéket képvisel. Izland esete azt mutatja meg, hogy egy hadsereg nélküli ország is képes stabil és aktív tagja lenni egy kollektív védelmi rendszernek, ha ennek megvannak a geopolitikai, diplomáciai és társadalmi feltételei.

A 21. század kihívásai – például a klímaváltozás, a kibertámadások és a nagyhatalmi versengés erősödése az Északi-sarkkör térségében – újraértelmezik, mit jelent egy ország számára a biztonság fogalma. Izland ennek a változásnak a középpontjában áll. Bár továbbra sincs hadserege, a NATO-ban betöltött szerepe alkalmazkodott az új körülményekhez, és egyfajta hidat képez a hagyományos katonai tagállamok és a civil fókuszú, diplomáciára építő biztonsági gondolkodás között.

Összefoglalva, Izland NATO-tagsága egy sajátos modellként értelmezhető, amely azt mutatja, hogy a kollektív biztonságban való részvételnek nem kizárólag a katonai jelenlét a feltétele. A tagság politikai jelentősége abban rejlik, hogy egy kisállam, amely tudatosan nem fejleszt saját hadsereget, képes hosszú távon is fenntartani egyensúlyt a nemzetközi kötelezettségvállalások és a nemzeti érdekek között. E modell tanulságos lehet más kisállamok számára is, amelyek a biztonságot nem feltétlenül katonai úton, hanem politikai, diplomáciai és regionális együttműködések révén kívánják biztosítani. Izland története tehát hozzájárul a nemzetközi kapcsolatok és a biztonságpolitika sokszínű értelmezéséhez, és azt a kérdést is új megvilágításba helyezi, hogy mit jelent valójában „biztonság" a 21. század globális politikai rendszerében.

Felhasznált szakirodalom

1. Nuechterlein, D. E., 1961. The Icelandic Defense Problem, 1940–1956: A Study of the Influence of Domestic Political Factors on the Formulation of Iceland's Foreign Defense Policy. PhD disszertáció. University of Virginia.
2. Ómarsdóttir, S. B. és Bergsson, B. Þ., 2022. A New Nordic Balance: Nordic security policies and their impact on Iceland. In: I. B. Neumann és J. Hallenberg (szerk.), Nordic Security in the 21st Century: New Dynamics, Old Foundations. London: Routledge,115-132. o.
3. The Government of Iceland, é.n. Iceland and NATO. [online]

KEREKES Ariána
Hallgató, III. évfolyam, Nemzetközi kapcsolatok szak
Történelem- és Társadalomtudományi Tanszék,
II. Rákóczi Ferenc Kárpátaljai Magyar Egyetem

RÁCZ Béla
Docens, PhD
II. Rákóczi Ferenc Kárpátaljai Magyar Egyetem
Történelem- és Társadalomtudományi Tanszék

TÖRÖKORSZÁG KATONAI BIZTONSÁGI STRATÉGIÁJA

Törökország katonai biztonsági stratégiája napjaink egyik legfontosabb és legérdekesebb témája a nemzetközi kapcsolatokban. Az ország egyedülálló földrajzi helyzete – a Közel-Kelet és Európa határán, a Fekete-tenger és a Földközi-tenger között – stratégiai előnyöket és kihívásokat is jelent. NATO-tagként Törökország kulcsszerepet játszik a szövetség biztonsági politikájában, ugyanakkor saját regionális érdekeit is következetesen képviseli, ami gyakran feszültséget okoz szövetségeseivel.

A téma feldolgozását személyes érdeklődésünk is indokolja: különösen a török nemzeti hírszerzés, a Milli İstihbarat Teşkilatı (MIT) tevékenysége keltette fel a figyelmünket. A modern biztonságpolitikai stratégiákban a hírszerzés központi szerepet játszik, és Törökország esetében a MIT nem csupán információgyűjtő szerv, hanem aktív alakítója a katonai és politikai döntéshozatalnak.

Törökország katonai stratégiájának fő pillérei

Törökország katonai biztonsági stratégiája több pilléren nyugszik. Központi szerepet játszik benne a NATO-tagság, emellett meghatározóak a regionális hatalmi törekvések, valamint a hazai hadiipar folyamatos fejlesztése.

Az első és talán legfontosabb tényező a NATO-hoz való tartozás. Törökország 1952 óta tagja a szövetségnek, ami számára a kollektív védelem biztonságát jelenti. Ez egyben lehetőséget ad a nemzetközi katonai gyakorlatokon való részvételre és a hírszerzési információkhoz való hozzáférésre is. A NATO-val való szoros együttműködés erősen befolyásolja az ország védelmi politikáját: bizonyos kérdésekben korlátozza az önálló döntéseket, ugyanakkor jelentősen növeli Törökország súlyát a nemzetközi porondon.

A második pillért a regionális hatalmi ambíciók jelentik. Az elmúlt években Törökország aktív katonai jelenlétet vállalt a Közel-Keleten és Észak-Afrikában, például Szíriában, Líbiában és az iraki kurd területeken. Ezek a műveletek túlmutatnak a védelem logikáján: egyértelmű céljuk a befolyásszerzés és annak hosszú távú megtartása. Emellett hozzájárulnak a terrorellenes küzdelemhez és a hírszerzési képességek bővítéséhez is.

A harmadik fontos tényező a hazai hadiipar fejlődése. Az elmúlt években Törökország komoly erőfeszítéseket tett saját fegyverrendszereinek megtervezésére és gyártására. Ennek látványos példája a Bayraktar TB2 drón, amelyet a világ számos konfliktusövezetében bevetettek. A hazai fejlesztések révén a hadsereg nemcsak modernebb és rugalmasabb lett, hanem egyre kevésbé függ a külföldi beszállítóktól is.

A Milli İstihbarat Teşkilatı (MIT) szerepe

A török nemzeti hírszerző szolgálat, a Milli İstihbarat Teşkilatı (MIT) meghatározó szerepet játszik Törökország katonai biztonsági stratégiájában. Feladata nem csupán a fenyegetések felderítése és az információk elemzése, hanem a döntéshozók támogatása is stratégiai és taktikai szinten.

Bár a szervezet története több évtizedre nyúlik vissza, az utóbbi időszakban – különösen a 2016-os puccskísérlet után – jelentősen megerősödött. A belső stabilitás fenntartása mellett a MIT egyre aktívabban vesz részt a külföldi műveletek előkészítésében és irányításában. Ez főként Szíriában,

Irakban és más közel-keleti térségekben érzékelhető, ahol kiemelt figyelmet fordítanak a kurd szeparatista mozgalmakra, különösen a PKK elleni fellépésre. Ezek a feladatok nemcsak katonai, hanem politikai szempontból is elsődleges jelentőségűek.

A MIT tevékenysége túlmutat a klasszikus hírszerzésen: közvetlenül hozzájárul a katonai akciók sikeréhez, támogatja a terrorellenes műveleteket, és segíti az új haditechnológiák alkalmazását is. Ennek köszönhetően a hírszerzés szoros kapcsolatban áll a török fegyveres erőkkel, és kulcsszereplője az ország regionális, sőt globális biztonsági törekvéseinek.

A MIT működése jól mutatja, hogy a 21. századi biztonságpolitika nem épülhet pusztán hagyományos hadseregekre. A hírszerzés és a katonai erő összehangolt működése nélkül lehetetlen lenne hatékonyan reagálni a komplex, gyorsan változó fenyegetésekre.

Kihívások és jövőbeli irányok

Törökország katonai biztonsági stratégiája napjainkban számos belső és külső kihívással néz szembe, amelyek egyben formálják a jövőbeli irányvonalakat is. A NATO-tagság komoly előnyöket biztosít az országnak, ugyanakkor stratégiai dilemmákat is felvet. A szövetség és az Egyesült Államok felé vállalt kötelezettségek néha korlátozzák Törökország önálló regionális döntéseit, például amikor orosz fegyvereket szerez be, vagy saját hadműveleteket indít a Közel-Keleten.

Regionális szinten több konfliktusos terület érinti az országot. A Görögországgal és Ciprussal fennálló területi viták, valamint a kurd kérdés folyamatos nyomást gyakorolnak a katonai stratégiára. A komplex geopolitikai helyzet és a feszültségek állandó jelenléte megköveteli a rugalmasságot, és azt, hogy a hírszerzési kapacitásokat teljes mértékben kihasználják.

Ebben a környezetben a MIT szerepe továbbra is központi. A hírszerzés és a hadsereg szoros együttműködése alapvető a modern katonai műveletek sikeréhez, legyen szó terrorellenes akciókról, határon túli beavatkozásokról vagy a hazai biztonság fenntartásáról. A jövő stratégiáiban egyre nagyobb hangsúlyt kap az információalapú hadviselés, a dróntechnológia alkalmazása, valamint a nemzetközi kapcsolatok dinamikus kezelése.

Következtetés

Törökország katonai biztonsági stratégiája nem egy egyszerű tervrajz, hanem egy sokrétű, több szinten működő rendszer. Az ország egyszerre támaszkodik a NATO-tagság előnyeire, követi a regionális hatalmi ambícióit, és folyamatosan fejleszti saját hadiiparát. Ezek a tényezők együtt biztosítják, hogy Törökország képes legyen alkalmazkodni a gyorsan változó biztonsági kihívásokhoz, miközben stratégiai érdekeit is érvényesíti.

A stratégia egyik kulcseleme a hírszerzés szerepe, és ebben a Milli İstihbarat Teşkilatı (MIT) áll a középpontban. A MIT nem csupán adatokat gyűjt és elemez; aktívan részt vesz a katonai műveletek koordinálásában, segíti a terrorellenes akciókat, és hozzájárul ahhoz, hogy Törökország mindig naprakészen tudjon reagálni a fenyegetésekre. A hírszerzés és a hadsereg együttműködése lehetővé teszi, hogy az ország ne csak védekezzen, hanem alakítsa is a régió biztonsági helyzetét.

A mai világban a fenyegetések rendkívül összetettek és gyorsan változnak, ezért a katonai és hírszerzési képességek összehangolása létfontosságú. Törökország példája jól mutatja, hogy amikor a MIT és a hadsereg szorosan együtt dolgozik, az ország képes fenntartani belső stabilitását, rugalmasan reagálni a kihívásokra, és érvényesíteni érdekeit a nemzetközi színtéren is.

Összességében elmondhatjuk, hogy Törökország katonai stratégiája és a hírszerzés integrációja a modern biztonságpolitikai környezethez igazodó, átgondolt rendszer. A MIT szerepe túlmutat a napi operatív sikereken: hosszú távon is meghatározza az ország stratégiai autonómiáját és regionális befolyását. Ez a stratégiai koherencia biztosítja, hogy Törökország ne csak reagáljon a fenyegetésekre, hanem aktívan formálja is a saját biztonsági környezetét, miközben stabilitását és nemzetközi súlyát is megőrzi.

Felhasznált irodalom

1. Ahmad, Feroz – The Making of Modern Turkey. London: Routledge, 1993.
2. Tálas Péter Henrik – Biztonságpolitika és hadtudomány. Budapest: Zrínyi Kiadó, 2019.

Interntes források:

1. NATO – Turkey: https://www.nato.int/cps/en/natohq/topics_52044.htm
2. MIT (Milli İstihbarat Teşkilatı) – hivatalos oldal: https://www.mit.gov.tr
3. CSIS – Center for Strategic & International Studies, Turkey Security Overview: https://www.csis.org/programs/turkey-program
4. Stratfor – Turkey Analysis: https://worldview.stratfor.com

ПРАВОВІ, СОЦІАЛЬНІ, ПСИХОЛОГІЧНІ ТА ЕКОНОМІЧНІ ВИМІРИ БЕЗПЕКИ

LEGAL, SOCIAL, PSYCHOLOGICAL, AND ECONOMIC DIMENSIONS OF SECURITY

A BIZTONSÁG JOGI, TÁRSADALMI, PSZICHOLÓGIAI ÉS GAZDASÁGI DIMENZIÓI

Леся КОНДРАТЮК
Кандидат філологічних наук, доцент,
КАІ,
lnkon@ukr.net

THE IMPACT OF INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) ON SOCIETY

Information and Communication Technology (ICT) has become a defining element of contemporary society, reshaping communication, education, business, healthcare, governance, and social interaction. This paper explores the relevance of ICT in modern life, highlights its contributions to economic and social development, and examines associated challenges such as digital inequality, cybersecurity, and environmental concerns. The findings suggest that while ICT serves as a transformative driver of progress, sustainable and inclusive strategies are essential to address its risks and ensure equitable benefits.

Introduction

The rapid evolution of Information and Communication Technology (ICT) represents one of the most significant developments of the 21st century. ICT encompasses a broad range of digital tools and systems that facilitate the creation, storage, transmission, and processing of information. Its transformative potential spans across multiple domains, including education, healthcare, business, governance, and social interaction. Scholars such as Castells (2010) argue that ICT constitutes the foundation of the "network society," where human interaction and development are increasingly mediated by digital technologies. At the same time, concerns have emerged regarding the environmental impact of ICT, the persistence of the digital divide, and risks related to data security and privacy (Heeks, 2017). This paper aims to analyze both the opportunities and challenges posed by ICT and to evaluate its overall implications for human progress.

ICT and Social Transformation

One of the most visible impacts of ICT is in the field of communication. Tools such as email, instant messaging, and video conferencing enable real-time global interaction, thereby reducing geographical barriers and promoting cultural exchange. Similarly, ICT has transformed education by providing access to e-learning platforms, online libraries, and virtual classrooms. These tools enhance inclusivity, allowing learners from diverse backgrounds to access knowledge and participate in global academic discourse (UNESCO, 2020).

In the business sector, ICT contributes to efficiency, innovation, and competitiveness. Cloud computing, big data analytics, and e-commerce platforms streamline operations and open new markets. The OECD (2021) highlights that ICT adoption correlates with higher productivity levels and the growth of digital economies. Likewise, ICT has revolutionized healthcare through telemedicine and electronic health records, improving service delivery, reducing costs, and expanding access to medical expertise (World Bank, 2016).

Governments also benefit from ICT by implementing e-government initiatives, which enhance transparency, accountability, and citizen participation. These systems improve service delivery and foster greater public trust in governance. On a social level, ICT platforms such as social media have reshaped interpersonal communication, enabling individuals to share experiences and engage in global conversations. However, these same tools raise issues of misinformation, online harassment, and data privacy, highlighting the dual nature of technological progress.

Challenges of ICT

Despite its benefits, ICT presents several pressing challenges. The digital divide remains a critical issue, as unequal access to devices, connectivity, and digital literacy excludes large segments of the global population from ICT's advantages. Furthermore, cybersecurity has become a growing concern, with individuals, businesses, and governments facing risks of hacking, identity theft, and data breaches. Environmental impacts also demand attention, as the production of electronic devices contributes to e-waste, while data centers and networks consume vast amounts of energy, thereby

adding to global carbon emissions (Heeks, 2017). Addressing these challenges requires coordinated policies that promote digital inclusion, strengthen data protection frameworks, and encourage sustainable technological practices.

In conclusion, ICT is a transformative force that permeates all aspects of contemporary life. It accelerates communication, broadens educational opportunities, drives business innovation, improves healthcare delivery, and enhances governance. At the same time, it fosters global connectivity and economic growth. However, the benefits of ICT are counterbalanced by challenges such as digital inequality, cybersecurity threats, and environmental concerns. To fully harness the potential of ICT, policymakers, educators, businesses, and civil society must work collaboratively to ensure that technological progress is sustainable, inclusive, and equitable. ICT will remain central to future development, but its successful integration depends on striking a balance between innovation and responsibility.

References

1. Castells, M. (2010). The rise of the network society. Wiley-Blackwell.
2. Heeks, R. (2017). Information and communication technology for development (ICT4D). Routledge.
3. OECD. (2021). OECD digital economy outlook 2021. OECD Publishing.
4. UNESCO. (2020). ICT in education: A critical role in human development. UNESCO.
5. World Bank. (2016). World development report 2016: Digital dividends. World Bank.

Ольга ТОМАШЕВСЬКА
Магістерка 1-року навчання
Мелітопольський державний
педагогічний університет
ім. Б. Хмельницького,
olgatom07@gmail.com

Наталія ГЛЕБОВА
доктор соціологічних наук, професор
Мелітопольський державний
педагогічний університет
ім. Б. Хмельницького,
nat.glebova2005@gmail.com

ПСИХОЛОГІЧНА БЕЗПЕКА ЯК СКЛАДОВА САМОРЕГУЛЯЦІЇ У СТРЕСОВИХ СИТУАЦІЯХ

Актуальність

У сучасних умовах підвищеного рівня стресу (війна, соціальна нестабільність, професійне навантаження) особливої ваги набуває здатність людини зберігати психологічну рівновагу.

Почуття безпеки виступає базовою умовою для ефективної саморегуляції, підтримання внутрішніх ресурсів та запобігання вигоранню.

Без відчуття внутрішньої безпеки механізми саморегуляції не можуть повноцінно функціонувати, а стрес сприймається як загроза, а не виклик.

Мета дослідження

Визначити роль психологічної безпеки як чинника ефективної саморегуляції особистості у стресових ситуаціях.

Основний зміст

- Психологічна безпека – це суб'єктивне відчуття захищеності, довіри до себе й світу, яке знижує рівень тривоги та активізує адаптаційні ресурси.
- Саморегуляція – це здатність свідомо керувати своїми емоціями, поведінкою та станами для досягнення стабільності.
- Взаємозв'язок: внутрішнє відчуття безпеки знижує емоційне напруження, розширює можливість для усвідомлених рішень, підвищує контроль над реакціями.

«Особистість розвивається лише у кліматі психологічної безпеки, де людина може приймати себе без страху осуду» – К. Роджерс.

Практичний аспект

- Техніки розвитку психологіної безпеки: дихальні вправи, техніки майндфулнес, тілесна усвідомленість, практика «я-висловлювань».
- У професійній діяльності психолога чи педагога це особливо важливо для профілактики емоційного виснаження та підтримання ефективної взаємодії з іншими.

Висновки

Психологічна безпека є важливим регулятором поведінки в умовах стресу, визначаючи рівень адаптивності, стресостійкості та здатності до відновлення. Розвиток психологічної безпеки – це шлях до зміцнення саморегуляції, внутрішньої стійкості та професійного благополуччя.

Список використаних джерел

1. Приходько І. І. Розвиток і відновлення психологічної безпеки особистості у фахівців екстремальних видів діяльності (посібник). Books NDC Nangu
2. Духневич В. М., Сіверс З. Ф. Забезпечення психологічної безпеки учасників освітнього процесу (методичні рекомендації). Цифрова бібліотека НАПН України

3. Католик Г. Психологічна безпека персоналу як фактор ефективного управління в організаціях. Економіка і суспільство
4. Яцюк М. В. Психологія саморегуляції особистості. docs.academia.vn.ua
5. Фурс О. Й. Психічна саморегуляція фахівців екстремальних видів діяльності. appsychology.org.ua
6. Розов В. Система особистісної безпеки правоохоронців як захист від деструктивних впливів під час війни. Zhytomyr State University Library

Оксана ПЕРЧІ
старший викладач кафедри обліку і аудиту
Закарпатський угорський університет імені Ференца Ракоці ІІ,
percsi.oxana@kmf.org.ua

АВТОМАТИЧНИЙ ОБМІН ФІНАНСОВОЮ ІНФОРМАЦІЄЮ CRS: ПОСИЛЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ЧЕРЕЗ МІЖНАРОДНУ ПОДАТКОВУ СПІВПРАЦЮ

У сучасному глобалізованому світі міжнародна податкова система стикається з численними викликами, що виникають через транснаціональні фінансові потоки, ухилення від сплати податків та використання офшорних юрисдикцій для приховування активів. Оскільки більшість фінансових операцій мають міжнародний характер, традиційні методи контролю за податковими зобов'язаннями стають малоефективними. У зв'язку з цим питання забезпечення податкової прозорості і боротьби з податковими ухиленнями набувають особливої актуальності для більшості країн світу.

На сьогоднішній день розвиток міжнародного обміну податковою інформацією реалізується через два основні напрямки:

1. Відповідно до американського закону «Про податкові вимоги до іноземних рахунків» (Foreign Account Tax Compliance Act, FATCA) [1].

2. У межах Загального стандарту звітності (Common Reporting Standard, CRS).

Відповідно до вимог CRS, фінансові установи в країнах-учасницях зобов'язані здійснювати комплексну перевірку (due diligence) фінансових рахунків. Це включає виявлення осіб, які є податковими резидентами інших юрисдикцій-партнерів з обміну інформацією, серед власників рахунків, а в окремих випадках — також серед їхніх контролюючих осіб. Таким чином, фінансові установи повинні проводити ретельну ідентифікацію клієнтів і здійснювати постійний моніторинг рахунків для виявлення потенційних податкових резидентів інших країн. Інформація про такі рахунки має подаватися фінансовими установами до компетентних органів країни-учасниці, які, в свою чергу, передають відомості про фінансові рахунки юрисдикціям, де є податкові резиденти власників і контролюючих осіб рахунків.

19 серпня 2022 року Державна податкова служба України (ДПС) підписала Багатосторонню угоду компетентних органів про автоматичний обмін інформацією про фінансові рахунки (Багатостороння угода CRS), яка забезпечує можливість щорічного автоматичного обміну інформацією про визначені види фінансових рахунків між компетентними органами юрисдикцій, які є сторонами вказаної угоди [2]. На офіційному сайті ДПС оприлюднено актуальний перелік підзвітних юрисдикцій для подання звіту про підзвітні рахунки згідно з вимогами стандарту CRS. Наразі перелік включає 119 юрисдикцій, що є учасниками глобальної ініціативи з автоматичного обміну податковою інформацією.

20 березня 2023 року Верховна Рада України прийняла Закон України № 2970-IX «Про внесення змін до Податкового кодексу України та інших законодавчих актів України щодо імплементації міжнародного стандарту автоматичного обміну інформацією про фінансові рахунки» [3], який набрав чинності 28.04.2023. З 1 липня 2023 року Закон 2970-IX вимагає від підзвітних фінансових установ України застосовувати заходи належної перевірки до фінансових рахунків для встановлення того, чи є рахунки підзвітними. Якщо рахунок є підзвітним, фінансова установа зобов'язана включити відомості про рахунок до звіту про підзвітні рахунки та подати цей звіт до ДПС України.

Процес автоматичного обміну інформацією здійснюється через дві основні категорії суб'єктів:

- ✓ фінансові установи, що звітують — установи, які зобов'язані збирати та подавати інформацію про фінансові рахунки, що належать або контролюються особами, резидентами інших юрисдикцій-учасниць CRS;

✓ особи, про рахунки яких звітують — фізичні особи або організації, що є податковими резидентами країн-учасниць CRS. Якщо рахунок належить або контролюється підзвітною особою, він підлягає звітуванню;

Перевірка і звітування щодо рахунків здійснюються фінансовими установами, що належать до однієї з чотирьох категорій за CRS:

➢ депозитарні установи — банки, кредитні установи, фондові біржі, клірингові установи та інші організації, що забезпечують функціонування фінансових ринків;

➢ кастодіальні установи — організації, що зберігають і управляють фінансовими активами, зокрема цінними паперами;

➢ інвестиційні компанії — інвестиційні фонди та фірми, що займаються управлінням активами;

➢ визначені страхові компанії — страхові компанії та недержавні пенсійні фонди.

Фінансова установа країни-учасниці Угоди CRS щорічно зобов'язана подавати звітність до свого компетентного органу, тобто податкового органу країни, щодо всіх підзвітних рахунків осіб, що є податковими резидентами інших країн-учасниць цієї угоди, зокрема й України. Згідно з принципами CRS, підзвітними є рахунки, які належать або контролюються такими особами, які є резидентами юрисдикцій, що підписали відповідну угоду про автоматичний обмін інформацією. Отримавши цю інформацію від фінансових установ, іноземний компетентний орган передає зібрані дані до податкових органів інших країн-учасниць Угоди CRS. У контексті України, така інформація надходить до ДПС. Далі, на основі отриманих даних, українські податкові органи можуть здійснювати аналіз і контроль за дотриманням податкових зобов'язань громадянами та компаніями, що здійснюють фінансові операції за кордоном.

Автоматичний обмін інформацією CRS має стратегічне значення для посилення економічної безпеки. Завдяки цій системі уряди мають змогу відслідковувати фінансові потоки, забезпечувати дотримання податкових зобов'язань та знижувати рівень корупції. Для України це також важливий крок у боротьбі з фінансовими зловживаннями, адже інформація, отримана через CRS, дозволяє детально перевіряти фінансові операції громадян і компаній за кордоном. Попри успішну імплементацію стандарту CRS в Україні, існують певні виклики. Одним із основних є технічні труднощі у зборі та обробці великих обсягів інформації, що потребує значних ресурсів для створення ефективних інформаційних систем. У зв'язку з цим важливим аспектом є подальше вдосконалення національних технологій для збору, зберігання та аналізу податкових даних, що дозволяє забезпечити належний контроль за податковими зобов'язаннями. Окрім того, необхідно розвивати співпрацю з іншими юрисдикціями для обміну не тільки фінансовою інформацією, але й для реалізації спільних механізмів перевірки та виявлення фінансових зловживань.

Список використаних джерел

1. U.S. Department of the Treasury. Foreign Account Tax Compliance Act. URL: https://home.treasury.gov/policy-issues/tax-policy/foreign-account-tax-compliance-act (дата звернення: 10.09.2025)

2. Державна податкова служба України. Україна приєдналася до Багатосторонньої угоди компетентних органів про автоматичний обмін інформацією про фінансові рахунки. 2022. URL: https://tax.gov.ua/baneryi/crs/povidomlennya/print-609052.html (дата звернення: 10.09.2025)

3. Про внесення змін до Податкового кодексу України та інших законодавчих актів України щодо імплементації міжнародного стандарту автоматичного обміну інформацією про фінансові рахунки: Закон України від 20.03.2023 № 2970-IX. URL: https://zakon.rada.gov.ua/laws/show/2970-20#Text (дата звернення: 10.09.2025)

Олексій СИДОРЕНКО
кандидат економічних наук, доцент,
доцент кафедри менеджменту
та публічного управління
Державний податковий університет,
sidorenko007@ukr.net

Лілія ВИННИЧЕНКО-КУМКОВА
кандидат юридичних наук, доцент,
доцент кафедри публічного управління,
менеджменту та інклюзивної економіки
Кам'янець-Подільський державний інститут,
liliya0604@gmail.com

ДЕРЖАВНИЙ ФІНАНСОВИЙ КОНТРОЛЬ ЯК ЗАСІБ ПУБЛІЧНОГО УПРАВЛІННЯ ЗАБЕЗПЕЧЕННЯМ ЕКОНОМІЧНОЇ БЕЗПЕКИ

Питання забезпечення економічної безпеки є одним з ключових завдань системи публічного управління. Від рівня економічної безпеки прямо залежить стан національної економіки та можливість її стабільності і зростання. Для забезпечення економічної безпеки сучасна система публічного управління використовує доволі широкий спектр різноманітних методів в засобів, які є тісно взаємопов'язаними між собою. Одним з таких є державний фінансовий контроль, який фактично забезпечує реалізацію контрольної функції управління.

Для розуміння ролі державного фінансового контролю у публічному управління забезпеченням економічної безпеки, на наш погляд, доцільним першочергово є розкрити внутрішній зміст поняття «економічна безпека». В науці, на сьогодні, існують численні підходи до її визначення. Найбільш поширеними серед них є наступні. Так М. Єрмошенко, що розглядає її як такий стан економічного механізму країни, який характеризується збалансованістю та стійкістю до негативного впливу внутрішніх і зовнішніх загроз, здатністю забезпечувати на основі реалізації національних економічних інтересів сталий та ефективний розвиток вітчизняної економіки й соціальної сфери [1, с. 26]. Інший вчений Г. Пастернак-Таранушенко, зазначає, що економічна безпека – це стан держави, що забезпечує можливість створення і розвитку умов для плідного життя її населення, перспективного розвитку її економіки в майбутньому та зростання добробуту її мешканців [2, с. 29]. Всі запропоновані підходи визначають досліджувану категорію виключно з позицій сери наукового пошуку їх авторів, що ускладнює їх використання в контексті нашого дослідження.

Зважаючи на це, ми вважаємо за до цільне погодитись з думкою професора Варналія З.С., який пропонує розуміти під економічною безпекою систему економічних відносин, яка ґрунтується на механізмі узгодження економічних інтересів суб'єктів господарської діяльності, який дає можливість вирішувати економічні конфлікти з найменшими втратами та забезпечує незалежність, стійкість, розвиток, адаптаційність та інерційність національної економіки у взаємодії із внутрішнім і зовнішнім середовищем [3, с. 54]. На наш погляд, запропоноване професором Варналієм З.С. визначення даної категорії є найбільш повним та узагальнюючим.

Як ми вже зазначали, в системі публічного управління при забезпеченні економічної безпеки важливе місце посідає державний фінансовий контроль, який є частиною загальнодержавного контролю, котрий у свою чергу є одним з елементів управління. Державний фінансовий контроль на сьогодні відіграє роль фактора подальшого розвитку ринкових відносин та їх наближення до європейських стандартів. Забезпечити своєчасне, найбільш ефективне, повне збирання грошових коштів, сприяти їх збільшенню, допомогти знайти нові джерела доходів та забезпечити ефективне управління ними – у цьому полягає одне із завдань державного фінансового контролю [4, с. 38-40]. Не менш важливе завдання державний фінансовий контроль виконує й при розподілі коштів і раціональному, доцільному, найбільш ефективному, ощадливому використанні фінансових ресурсів. Відповідно

здійснення державного фінансового контролю є одним з ключових елементів публічного управління забезпеченням економічної безпеки країни. Рівень ефективності національної економіки країни та її економічної безпеки прямо пов'язаний з рівнем ефективності здійснення державного фінансового контролю.

Загалом, можемо констатувати, що державний фінансовий контроль є одним з ключових інструментів публічного управління, який використовується при забезпеченні економічної безпеки держави. Його ефективність прямо впливає як на рівень економічної безпеки так і на стан національної економіки в цілому.

Список використаних джерел

1. Єрмошенко М.М. Фінансова безпека держави: національні інтереси, реальні загрози, стратегія забезпечення: монографія. Київ: КНТЕУ, 2001. 309 с.
2. Пастернак-Таранушенко Г.А. Економічна безпека держави. Методологія забезпечення: монографія. Київ: Київський ек-ний інститут менеджменту, 2003. 320 с.
3. Варналій З.С., Буркальцева Д.Д., Саєнко О.С. Економічна безпека України: проблеми та пріоритети зміцнення: монографія. Київ: Знання України, 2011. 299 с.
4. Сидоренко О.М. Роль системи державного фінансового контролю України у забезпеченні економічної безпеки: дис… на здобуття наук. ступеня канд. екон. наук. Чернігів, 2017. 274 с.

Оксана КАЧМАР
аспірантка,
кафедра теорії та історії держави і права
Ужгородський національний університет,
oksana.kachmar@uzhnu.edu.ua

ПРАВОВИЙ НІГІЛІЗМ ЯК ЧИННИК ДЕГРАДАЦІЇ ДЕМОКРАТИЧНИХ ІНСТИТУТІВ І ВИКЛИК ГЛОБАЛЬНІЙ БЕЗПЕЦІ

У сучасному світі, що дедалі частіше стикається з викликами не лише у сфері безпеки, а й у сфері права, особливої уваги набуває явище правового нігілізму. Правовий нігілізм є однією з форм соціального нігілізму та проявляється у загальному негативному, байдужому ставленні до права, законів і нормативного порядку. Його витоки пов'язані з низьким рівнем правової культури, юридичною відсталістю, а також із деформованою правосвідомістю населення. У науковій літературі розрізняють два основних підходи до розуміння цього явища: класичний — як деструктивний феномен недовіри до права, та новаторський — який вбачає його причини у недосконалості самого права та правової системи. На особистісному рівні правовий нігілізм проявляється як в емоційно-ціннісному ставленні, так і в лінії поведінки, що у підсумку формує антиправові установки, небезпечні як для суспільства, так і для державності загалом.

Особливу небезпеку правовий нігілізм становить у державах, де традиційно слабка правова культура поєднується з політичною вседозволеністю та відсутністю ефективних механізмів контролю за владою. У таких випадках маємо справу з гібридними режимами, які формально декларують демократичні інститути, однак фактично реалізують автократичні моделі правління. Найяскравішим прикладом цього є Російська Федерація, де зосередження влади в руках однієї особи, імітація виборчих процедур, підконтрольність судової системи та придушення будь-яких опозиційних чи громадянських проявів утворили специфічну форму державності, позбавлену як внутрішньої легітимності, так і зовнішньої правосуб'єктності у правовому сенсі.

До прикладу, виразним свідченням правового нігілізму стала поведінка РФ щодо Будапештського меморандуму 1994 року. Усупереч взятим на себе зобов'язанням, Російська Федерація здійснила анексію Криму, підтримала і координувала збройні формування на Донбасі, а у 2022 році розпочала повномасштабну війну. Такі дії фактично дискредитувалм саму ідею безпекових механізмів у межах міжнародного права та продемонструвало його вразливість у випадку, коли одна зі сторін діє з позиції правового нігілізму.

Ця зовнішня агресивна поведінка є безпосереднім продовженням внутрішнього ставлення до права як явища другорядного і необов'язкового. В умовах, коли правова система функціонує як обслуговуючий інструмент політичної волі, а не як система об'єктивного стримування і противаг, формуються передумови для тотального правового релятивізму. У таких суспільствах зникає реальна цінність прав і свобод як інституту — як для держави, так і для громадянина. Відсутність елементарної поваги до власного законодавства й основоположних прав людини породжує глуху байдужість і до міжнародних норм. Населення, позбавлене правової культури, не сприймає право як базову соціальну цінність, не вимагає його дотримання та не усвідомлює власної ролі у правовому полі.

Зрештою, у таких умовах правовий нігілізм із латентного явища поступово перетворюється на суспільну норму, глибоко вкорінену в колективній правосвідомості. Це, у свою чергу, спричиняє подальшу деформацію форми правління, розмивання меж між легітимною владою та свавіллям, а також деградацію політичних, адміністративних і судових інституцій. У результаті національна система стає неспроможною підтримувати демократичний устрій не лише номінально, а й функціонально, що відображається у зовнішньому позиціонуванні держави як джерела нестабільності та загрози міжнародному правопорядку.

Очевидно, що в контексті правового нігілізму в окремих державах, де він став системною ідеологією, мова вже йде не про виправлення, а про глибоку цивілізаційну деградацію. Відтак,

подальша доля таких суспільств, має розглядатись як внутрішня проблема. Їхнє подальше перебування в ізоляції або добровільне самовідтворення у власному викривленому правовому просторі є результатом зробленого ними вибору. Проте це жодним чином не повинно ставати виправданням пасивності для решти міжнародної спільноти. Навпаки — досвід таких суспільств має стати застереженням і стимулом для консолідованого протистояння правовому нігілізму в усіх його формах. Для більшості держав світу — як демократичних, так і перехідних — нагально постає потреба в переосмисленні стратегій правової політики, спрямованих на укріплення правової культури, недопущення знецінення норм і гарантій, а також формування стійкого імунітету до правового релятивізму, що породжує загрозу повторення кризових сценаріїв.

Аналіз провалу зобов'язань за Меморандумом засвідчує, що правовий нігілізм на рівні держави здатен руйнувати безпекові конструкції, побудовані після Другої світової війни, зокрема принципи Статуту ООН. У суспільствах, де поширена недовіра до закону, де право розглядається як інструмент пригнічення або політичної маніпуляції, деградують ключові інститути демократії — парламент, суд, вибори, вільна преса. Недостатній рівень правової культури у поєднанні з системною безкарністю сприяє легітимації авторитарних практик. Як зазначає М. В. Суходоля, формування зрілої правосвідомості є необхідною передумовою не лише для подолання правового нігілізму, а й для забезпечення реальної дієздатності права в суспільстві, оскільки саме від рівня правової культури залежить ефективність функціонування правових інститутів

Таким чином, подолання правового нігілізму повинно стати одним із ключових пріоритетів як у внутрішній, так і в міжнародній політиці. Йдеться не лише про потребу в просвітницькій роботі чи інституційній реформі, а й про принципову зміну підходів до забезпечення відповідальності за порушення міжнародних норм. Без реального примусу до виконання права — через міжнародні санкційні механізми, трибунали, режим універсальної юрисдикції — будь-які гарантії залишатимуться декларативними, а отже нездатними захистити світ від агресії, репресій і руйнації демократії. Водночас сучасні умови вимагають пошуку нових джерел довіри до права. У цьому контексті особливу перспективу мають технології штучного інтелекту, які завдяки своїй знеособленості та відсутності людського фактору, за умови коректного налаштування та впровадження етичних і правових запобіжників, здатні забезпечити вищий рівень неупередженості, прозорості й справедливості. Саме сприйняття таких систем як незалежних і контрольованих може стати підґрунтям для нової хвилі довіри до права.

Список використаних джерел

1. Lyakhovych, M. V. & Pavlovych-Seneta, Ya. P. (2016). Pravovyi nihilizm v Ukraini: poniattia, formy proiavu ta shliakhy podolannia [Legal nihilism in Ukraine: Concept, forms and ways of overcoming]. Naukovyi Visnyk Lvivskoho derzhavnoho universytetu vnutrishnikh sprav. Seriia Yurydychna, 2, pp. 44–48. ISSN 2311-8040.

2. Sukhodolia, M. V. (2021). Bezposeredni zasoby vplyvu na pravosvidomist ta pravovu kulturu [Direct means of influence on legal consciousness and legal culture]. Zhurnal Skhidnoievropeiskoho prava, 85, pp. 150–155. Available at: https://abstracts.donnu.edu.ua/article/view/11423 (Accessed: 30 October 2025).

Вероніка ГАНУСИЧ
кандинат економічних наук, доцент,
Закарпатський угорський університет ім. Ф.Ракоці ІІ,
hanuszics.veronika@kmf.org.ua

БЕЗПЕКА DEFI СЕКТОРУ: РИЗИКИ ТА СПОСОБИ ЗАХИСТУ

Децентралізовані фінанси (Decentralized Finance, DeFi) становлять одну з найдинамічніших галузей сучасної фінансово-технологічної екосистеми, у якій управління активами, кредитування, обмін і страхування здійснюються не через централізовані інститути, а за допомогою смарт-контрактів на блокчейн-платформах. DeFi є квінтесенцією парадигми «фінанси без посередників». Проте із зростанням масштабів і складності екосистеми невідворотно зростають і ризики безпеки, які перетворюються на один із ключових викликів цифрової економіки.

Метою дослідження є ідентифікація основних ризиків безпеки у секторі децентралізованих фінансів (DeFi) та розроблення системи багаторівневих заходів їхнього пом'якшення з урахуванням сучасних технологічних, фінансових і регуляторних чинників. Актуальність теми зумовлена стрімким зростанням обсягів DeFi-ринку, зростанням кількості атак на смарт-контракти та необхідністю формування ефективних механізмів кіберзахисту й довіри до цифрових фінансових інструментів.

Наукова новизна дослідження полягає у комплексному підході до класифікації ризиків DeFi, який поєднує технічні, фінансові, офчейн- та регуляторні аспекти, а також у формуванні концепції багаторівневої безпеки, що інтегрує формальну верифікацію смарт-контрактів, механізми штучного інтелекту та європейські стандарти цифрової стійкості (DORA, NIS2). Такий підхід дозволяє розглядати безпеку DeFi не лише як технологічну, а як системну економіко-правову категорію.

Від часу запуску перших протоколів, зокрема MakerDAO у 2017 році, екосистема DeFi демонструє вибухове зростання. Станом на жовтень 2025 року загальна заблокована вартість (Total Value Locked, TVL) у DeFi перевищила 237 млрд дол. США [1], що свідчить про масштабність і зрілість цього ринку. Таке зростання зумовлене технологічними інноваціями, розвитком блокчейнів нового покоління (Ethereum, Solana) та рішень другого рівня (Layer 2), які забезпечують швидкість і масштабованість транзакцій. Проте разом із розширенням цифрової фінансової інфраструктури зростає і спектр загроз безпеці. За даними 2024 року, загальні збитки від кібератак у криптоіндустрії сягнули 2,2 млрд доларів [2], з яких левова частка припала саме на DeFi. Сукупні втрати у топ-100 атак DeFi перевищили 10,7 млрд доларів, причому понад 80% інцидентів було пов'язано з офчейн-атаками, компрометацією інфраструктури, що виходить за межі смарт-контрактів [3].

Система ризиків у DeFi має багаторівневий характер і може бути класифікована на технічні, фінансові, офчейн- та регуляторні.

Технічні ризики пов'язані з вразливостями у коді смарт-контрактів. Помилки у логіці або недосконаліть програмного коду можуть призвести до експлойтів, тобто несанкціонованого використання контракту. Найвідомішим прикладом є реентрансі-атаки (reentrancy attacks), коли зловмисник багаторазово викликає функцію контракту до завершення попередньої операції, виводячи активи без згоди власника. У 2024 році такі атаки спричинили збитки на суму понад 47 млн доларів у 22 випадках[2]. Іншим вектором загроз є маніпуляції оракулами – спотворення зовнішніх джерел даних, що постачають ціни активів. Це може спричиняти лавиноподібні ліквідації позицій у DeFi-протоколах. Особливу небезпеку становлять флеш-позики (flash loans), які дозволяють брати великі суми без застави в межах однієї транзакції, що відкриває простір для штучного впливу на ринкову ціну активів.

Фінансові ризики зумовлені самою архітектурою DeFi. Явище імперативних втрат (impermanent loss) у пулах ліквідності, наприклад на платформі Uniswap, виникає через волатильність цін активів і призводить до зниження прибутковості для провайдерів

ліквідності. Висока взаємозалежність між протоколами створює системну вразливість: один збій або крах токена може викликати каскадний ефект. Прикладом є колапс TerraUSD (2022), який призвів до збитків понад 40 млрд доларів, або злам біржі DMM Bitcoin (2024) із втратою 305 млн доларів, що актуалізував проблему безпеки крос-чейн мостів [4] .

Офчейн-ризики пов'язані з людським фактором: фішинг, соціальна інженерія, компрометація приватних ключів. Регуляторні ризики пов'язані з відсутністю чітких юридичних рамок. Європейські акти DORA (Digital Operational Resilience Act) та NIS2 Directive, що набули чинності у 2025 році, посилюють вимоги до кіберстійкості фінансових організацій, включно з DeFi-протоколами. Проте децентралізований характер управління ускладнює відповідність цим нормам, створюючи простір для правової невизначеності та потенційних санкцій.

Формування безпечного середовища в DeFi потребує багаторівневої системи захисту, що поєднує технологічні, організаційні та поведінкові заходи. Пом'якшення ризиків у DeFi вимагає багатошарового підходу на рівні протоколів і користувачів.

На рівні протоколів ключову роль відіграють аудити смарт-контрактів, які здійснюються незалежними компаніями, зокрема PeckShield чи CertiK. Ефективною є також формальна верифікація – метод математичного доведення коректності коду, який застосовується у високонадійних DeFi-проєктах (наприклад, Compound). Важливим є використання багатопідписних гаманців (multi-signature wallets), які вимагають підтвердження кількох сторін для проведення транзакцій, а також системи «холодного» зберігання активів, що мінімізують ризики зовнішнього втручання. Розвиток децентралізованого страхування (DeFi insurance), представленого платформами Nexus Mutual та InsurAce, створює додатковий рівень захисту інвесторів.

На рівні користувачів безпека базується на дисципліні та знаннях. Використання апаратних гаманців (Ledger, Trezor), двофакторної автентифікації, регулярна перевірка дозволів на токени та обмеження операцій у публічних мережах – це мінімальні вимоги цифрової гігієни. Інноваційні технологічні рішення, такі як докази з нульовим розголошенням (Zero-knowledge proofs, ZKP), забезпечують верифікацію без розкриття даних, а децентралізовані оракули (забезпечують зв'язок між різними блокчейнами) зменшують маніпуляції шляхом агрегації даних з кількох джерел.

Безпека DeFi-сектору є не лише технологічною, а й соціально-економічною категорією, яка визначає довіру до цифрових фінансів загалом. Попри мільярдні втрати, екосистема DeFi еволюціонує, перетворюючи власні помилки на досвід і стандарти нової фінансової культури. У найближчій перспективі поєднання регуляторних механізмів ЄС, технологій формальної верифікації та інструментів ШІ може створити підґрунтя для глобальної стійкості децентралізованих фінансових систем. Для країн із потужним ІТ-сектором, зокрема України, це відкриває стратегічні можливості участі в розбудові безпечної цифрової економіки.

Список використаних джерел

1. Cholakov, S. (2025, January 1). 2024 Most Exploited DeFi Vulnerabilities. Three Sigma. Available at: https://threesigma.xyz/blog/exploit/2024-defi-exploits-top-vulnerabilities (Accessed 17 October 2025).
2. Ezra, R. (2025, October 9). DeFi TVL hits record $237B as daily active wallets fall 22% in Q3: DappRadar. Available at: https://cointelegraph.com/news/defi-tvl-record-237b-dapp-wallets-drop-22-q3-2025 (Accessed 17 October 2025).
3. Halborn. (2025). Breaking Down the Top 100 DeFi Hacks: 2014–2024 Comprehensive Report. Available at: https://www.halborn.com/reports/top-100-defi-hacks-2025 (Accessed 17 October 2025).
4. Marzouk, O. (2025). Top 10 Crypto Losses of 2024: Hacks, Frauds, and Exploits. Blockchain Intelligence Group. Available at: https://blockchaingroup.io/compliance-and-regulation/top-10-crypto-losses-of-2024-hacks-frauds-and-exploits/ (Accessed 17 October 2025).

LOSZKORIH Gabriella
PhD 071 „Számvitel és Adóügy”, egyetemi docens,
Számvitel és Auditálás Tanszék
II. Rákóczi Ferenc Kárpátaljai Magyar Egyetem
email: loskorih.gabriella@kmf.org.ua

TÓTH Gabriella
MSc. hallgató
„Nemzetközi Számvitel és Adóügy” c. képzési program,
II. Rákóczi Ferenc Kárpátaljai Magyar Egyetem
email: toth.gabriella.b20sa@kmf.org.ua

E-DOKUMENTUM ÁRAMLÁS A TÁRGYI ESZKÖZÖK SZÁMVITELÉBEN: A DOKUMENTÁLÁS ÉS AZ INFORMÁCIÓVÉDELEM JELLEMZŐI

Az e-dokumentum áramlás egyre nagyobb népszerűségnek örvend a modern üzleti környezetben, különösen a számvitel területén. A dokumentumok áramlásának digitalizálásának köszönhetően a vállalkozások hatékonyabban kezelhetik vagyonnyilvántartásaikat, csökkenthetik a papíralapú dokumentumok feldolgozásának költségeit és idejét, valamint növelhetik az információbiztonságot.

Az elektronikus dokumentum olyan dokumentum, amelyben az információkat elektronikus adat formájában rögzítik, beleértve a kötelező adatokat is [3]. Ugyanakkor képesnek kell lennie vizuálisan reprodukálni, azaz képesnek kell lennie a következőkre:

- ✓ megjelenítés számítógép, okostelefon, tablet, egyéb eszköz monitorán;
- ✓ nyomtatás papírra.

Az e-dokumentum áramlás ugyanakkor az elektronikus dokumentumok létrehozásának, feldolgozásának, küldésének, továbbításának, fogadásának, tárolásának, felhasználásának és megsemmisítésének folyamatainak összessége, amelyeket sértetlenség-ellenőrzéssel és szükség esetén az ilyen dokumentumok megőrzésének tényének igazolásával hajtanak végre [3].

Alapvetően megváltoztatja az iratforgalom rendjét, különösen az elsődleges számvitel megszervezését, valamint az új információs technológiák alkalmazását is.

A modern információs rendszerek kétféle adattal működnek - strukturált (adatbázisok) és strukturálatlan (elektronikus dokumentumok). Az ilyen típusú információk százalékos aránya jellemzi a vállalat dokumentumfolyamat-automatizálásának szintjét [2].

A nagyvállalatoknál a dokumentum áramlás nagy mennyiséget ér el. Ha korábban minden dokumentumot papíron kellett megőrizni, most lehetőség nyílik a dokumentumok elektronikus változatának megtartására. Egy ilyen dokumentum áramlás lehetővé teszi, hogy a dokumentumokat bármikor ellenőrzés alatt tartsa. Számos, az informatika területén újításokat hatékonyan alkalmazó vállalkozás számára az elektronikus dokumentum áramlás elengedhetetlen fogalommá vált a munkájában, mivel jelentősen leegyszerűsíti a dokumentumokkal való munkát, növeli a dolgozók munkájának termelékenységét és pontosságát. Az e-dokumentum áramlás előnye, hogy az irodák nagy mennyiségű papíralapú dokumentumtól szabadulnak meg, így a használatukkal kapcsolatos problémáktól is (dokumentumvesztés, változtatási nehézségek, megosztott hozzáférés).

A dokumentum áramlás automatizálási eszközök segítségével elkészített, elektronikus digitális aláírással aláírt és a rendszerben megfelelő formátumú fájl formájában elmentett elektronikus dokumentum nagymértékben leegyszerűsíti a nagy mennyiségű információval végzett munkát.

Tekintettel az „információvédelem” fogalmának lényegére, amelyet az ISO/IEC 27001 nemzetközi szabvány [1] úgy értelmez, hogy az biztosítja az információ titkosságát, integritását és elérhetőségét, a számviteli információ védelme alatt azok biztonságának állapotát értjük, amelyet olyan számítástechnikai berendezés segítségével hoznak létre, tárolnak, változtatnak és használnak, amely biztosítja a számviteli információ jogosulatlan felhasználásának, bizalmasságának, sértetlenségének vagy elektronikus úton történő megsemmisítésének időben történő észlelését, megakadályozását és semlegesítését, amely veszélyezteti a vállalkozás létfontosságú gazdasági érdekeit. A számviteli információ védelme a véletlen

vagy szándékos természetes vagy mesterséges természetű befolyásokkal szembeni védettségének állapotát jelenti, amelyek kárt okozhatnak ezen információk tulajdonosainak vagy felhasználóinak.

Ukrajna Állami Statisztikai Szolgálata 2021-ben [7] törölte a nagyon fontos számviteli tárgyak elsődleges elszámolásának bizonylatait, valamint a tárgyi eszközök formanyomtatványait.

A tárgyi eszközök dokumentálása jelenleg kétféleképpen lehetséges:

✓ a 818. számú rendelet [5] új formanyomtatványok használatával. Ugyanakkor a Rendelet elnevezése ellenére, a bizonylatokat nem csak a közszféra, hanem az általános kereskedelmi vállalkozások is használhatják;

✓ a 352. számú rendelet [6] régi formanyomtatványokat használatával, amelyek már nem érvényesek.

Úgy gondoljuk, hogy célszerűbb a 818-as számú rendelet formanyomtatványait használni, mivel ezek jobban illeszkednek a tárgyi eszközök bekerülési értékének, valamint amortizációjának elszámolásának jelenleg meglévő megközelítéseihez képest, mint a 352-es számú rendelet, amely már erkölcsileg elavult. A vállalkozás önállóan korszerűsítheti ezeket a bizonylatokat, a lényeg az, hogy megfeleljen a számviteli törvény [4] szerinti elsődleges bizonylatokra vonatkozó kötelező részletezési követelményeknek.

A tárgyi eszközök elszámolása számos fontos műveletet foglal magában: üzembe helyezés, átértékelés, korszerűsítés, értékcsökkenés, leírás stb. Ezen műveletek mindegyike okirati bizonyítékot igényel. A hagyományos számviteli rendszerben ezek a bizonylatok közé tartoznak a papíralapú nyomtatványok (átadás–átvételi elismervény, számlák, leltárleírások).

Az e-dokumentum áramlásra való váltás lehetővé teszi:

➢ a dokumentumok gyorsabb és pontosabb feldolgozását: az elektronikus sablonoknak és az adatok automatikus kitöltésének köszönhetően;

➢ a dokumentumok tárolásának és hozzáférésének folyamatának egyszerűsítését: az összes dokumentumot elektronikusan egyetlen adatbázisban tárolják, amely minden felelős számára könnyű hozzáférést biztosít;

a műveletek átláthatóságának és ellenőrzésének növelését: a dokumentummal végzett munka minden egyes szakaszának automatikus rögzítése (létrehozás, szerkesztés, aláírás) növeli a felelősség szintjét és véd a hamisítás ellen.

Felhasznált irodalom

1. ISO/IEC 27001:2013 information security management system standard arrives. 2013. URL: https://www.prnewswire.com/news-releases/isoiec-270012013-information-security-management-system-standard-arrives-226185641.html (letöltés dátuma: 2025.09.20)
2. Волошан І. Г. Первинний облік товарних операцій в інформаційній системі підприємства: автореф. дис. ... канд. екон. наук: 08.00.09/Харк. держ. ун-т харчування та торгівлі. Харків, 2014. 20 с.
3. Про електронні документи та електронний документообіг: Закон України від 22.05.2003 № 851-IV. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text (letöltés dátuma: 2025.09.21)
4. Про бухгалтерський облік та фінансову звітність в Україні: Закон України від 16.07.1999 № 996-XIV. URL: https://zakon.rada.gov.ua/laws/show/996-14#Text (letöltés dátuma: 2025.09.20)
5. Про затвердження типових форм з обліку та списання основних засобів суб'єктами державного сектору та порядку їх складання: Наказ Міністерства фінансів України від 13.09.2016 № 818. URL: https://zakon.rada.gov.ua/laws/show/z1336-16 (letöltés dátuma: 2025.09.20)
6. Про затвердження типових форм первинного обліку (Форми NN ОЗ-1, ОЗ-2, ОЗ-3, ОЗ-4, ОЗ-5, ОЗ-6, ОЗ-7, ОЗ-8, ОЗ-9, ОЗ-14, ОЗ-15, ОЗ-16): Наказ Міністерства статистики України від 29.12.1995 № 352. URL: https://zakon.rada.gov.ua/rada/show/v0352202-95#Text (letöltés dátuma: 2025.09.22)
7. Про скасування та визнання такими, що втратили чинність, деяких наказів Державної служби статистики України, Міністерства статистики України та Державного комітету статистики України: Наказ Державної служби статистики України № 266 від 22.10.2021. URL: https://zakon.rada.gov.ua/rada/show/v0266832-21#Text (letöltés dátuma: 2025.09.22)

Наталія ЛАВРОВА
здобувач освітнього рівня «Бакалавр»
спеціальність «Облік і оподаткування»
Закарпатський угорський університет ім. Ференца Ракоці ІІ

Наталія СТОЙКА
доцент кафедри обліку і аудиту
Закарпатський угорський університет ім. Ференца Ракоці ІІ

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В СИСТЕМІ УПРАВЛІНСЬКОГО ОБЛІКУ

В сучасних умовах господарювання вагома частина інформації, яка може бути використана для управління, не використовується у зв'язку з тим, що на багатьох підприємствах бухгалтерський облік організований таким чином, щоб обробляти інформацію і подавати її в основному зовнішнім користувачам, а самим апаратом управління вона використовується епізодично, що пояснюється недостатністю запитів власної системи управління на інформацію.

Але разом з тим, як зазначає П.Н. Денчук, в умовах еволюційного розвитку проявляється певна обмеженість бухгалтерського фінансового обліку як інформаційної бази управління підприємством, внаслідок чого виникає потреба у необхідності доповнення бухгалтерського фінансового обліку управлінським, який забезпечує зв'язок процесів управління і обліку за такими об'єктами управління: виробничі ресурси, господарські процеси, організаційна діяльність, результати діяльності підприємства [1, с. 32].

Отже управлінський облік складова системи бухгалтерського обліку, яка забезпечує управлінський апарат інформацією в розрізі їхніх потреб та сприяє підвищенню ефективності функціонування системи управління підприємством.

В працях вітчизняних дослідників наголошується, що рішення про впровадження управлінського обліку має прийматися з урахуванням проведення оцінки його ефективності в процесі діяльності підприємства.

Варто відмітити, що із впровадженням та використанням технологій штучного інтелекту (ШІ) в облікові інформаційні системи забезпечуються нові підходи та можливості для автоматизації облікових даних та процесів, а також спрощується виконання рутинних завдань та підвищується ефективність роботи бухгалтера.

Як зазначає Г.І. Ляхович та О.В. Вакун з розвитком та впровадженням штучного інтелекту бухгалтерський персонал буде мати менше складних завдань, оскільки програмне забезпечення для бухгалтерського обліку зможе виконувати більшість рутинних процесів. Це значно підвищить ефективність роботи, зменшить кількість помилок та збільшить конкурентоспроможність підприємств, які використовуватимуть технології штучного інтелекту. Такі зміни допоможуть також сприяти трансформації галузі бухгалтерського обліку і в першу чергу за рахунок зміни ролі людини в цьому процесі [2, с.29].

Тобто завдяки ШІ бухгалтер зможе оперативно виконувати поставлені на нього завдання в сфері управлінського обліку.

Основними завданнями управлінського обліку є [3]:

- виявлення, реєстрація, накопичення, підготовка, інтерпретація, узагальнення і передача інформації для процесу управління підприємством;
- нормування і облік витрат на виробництво за центрами відповідальності;
- визначення об'єктів калькулювання, складання планових і фактичних калькуляцій;
- аналіз відхилень від норм витрат та їх групування за причинами і відповідальними особами;
- формування цінової політики;
- забезпечення контролю і регулювання діяльності підприємства;

- оцінка ефективності результатів діяльності підприємства за центрами відповідальності та видами продукції, виявлення резервів збільшення прибутку;

- аналіз собівартості й рентабельності продукції;

- забезпечення різних рівнів управління своєчасною і повною інформацією для оперативного прийняття управлінських рішень.

Виходячи з вищезазначеного переліку та вивчаючи особливості роботи із застосуванням ШІ встановлено, що 50% завдань можна виконувати з його допомогою, а саме обробляти великі обсяги даних, здійснювати пошук "вузьких місць" у бізнес-процесах, створювати операційні та фінансові бюджети, порівнювати фактичні показники з плановими та ідентифікувати причини відхилень, проводити класифікацію витрат, здійснювати розподіл накладних витрат, проводити аналіз витрат за центрами відповідальності, здійснювати формування управлінських звітів.

Отже, ШІ є потужним інструментом в руках високопрофесійного фахівця, його застосування дозволить підвищити ефективність прийняття управлінський рішень. Але разом з тим варто враховувати, що застосування розумних технологій веде до втрати конфіденційності інформації, що є негативним фактором для діяльності підприємства.

Список використаних джерел

1. Денчук П.Н. Напрями формування інформації в підсистемах контролінгу та управлінського обліку [Текст] / П.Н. Денчук, В.М. Рожелюк // Проблеми економіки України / Збірник наукових праць / Відповідальний за випуск проф. М.С. Пушкар. – Тернопіль, 2006. – Випуск ІІ – С. 31-33.
2. Ляхович Г.І., Вакун О.В. Використання штучного інтелекту для підвищення ефективності системи управлінського обліку / Г.І. Ляхович, О.В. Вакун / Проблеми теорії та методології бухгалтерського обліку, контролю і аналізу Вип. 3 (56) 2023. URL: https://pbo.ztu.edu.ua/article/view/296876
3. Проданчук М.А. Теоретико-методологічні засади управлінського обліку в системі управління підприємством // URL: https://magazine.faaf.org.ua/teoretiko-metodologichni-zasadi-upravlinskogo-obliku-v-sistemi-upravlinnya-pidpriemstvom.html
4. Макарович В.К., Стойка Н.С. Інтеграція штучного інтелекту в інформаційні системи бухгалтерського обліку: виклики та перспективи/ В.К. Макарович, Н.С Стойка / Acta Academiae Beregsasiensis. Economics Випуск 9. (2025). URL: https://aab-economics.kmf.uz.ua/aabe/article/view/293/286

József BOROS
First year MSc student, "Mathematics" major
Ferenc II. Rakoczi Transcarpathian Hungarian University

Katalin KUCHINKA
PhD, Associate professor
Department of Mathematics and Informatics,
Ferenc II. Rakoczi Transcarpathian Hungarian University

MAPPING THE MATHEMATICAL-LOGICAL COMPETENCIES OF GRADUATING STUDENTS AT THE END OF HIGHER EDUCATION

This research addresses the critical need to benchmark the mathematical-logical competency profiles of graduating higher education students against national and international standards (TIMSS, PISA, AI comparisons). The study's primary objective is to quantitatively map the key components of students' analytical reasoning and problem-solving skills to assess the effectiveness of current curricula and identify targeted areas for educational modernization, specifically focusing on the Transcarpathian region's human capital development.

The research aims to map the mathematical-logical competencies of graduating students, identify the main components of their competency profiles, and evaluate the effectiveness of higher education programs. The study is based on the structure of the Hungarian National Competency Assessment [1], the findings of the international TIMSS assessment [2], and the latest OECD analyses examining the comparison between artificial intelligence and human cognitive performance [3].

The research employs a quantitative methodology: an online survey and statistical analysis were used to develop the competency map. The study focuses on students' mathematical and logical reasoning as well as problem-solving skills. The results are comparable across different study programs and cohorts and can also be analyzed in relation to prior (entry-level) competency data, as proposed in earlier comparative studies [4].

The research is expected to reveal students' strengths in mathematical reasoning, analytical thinking, and the recognition of logical relationships, while identifying areas for improvement such as digital problem-solving and abstract reasoning. The competency map provides a valuable foundation for modernizing curricula, developing teaching programs, and improving labor market preparedness, thereby strengthening the social and economic stability of young intellectuals in the Transcarpathian region.

Conclusion The resulting competency map provides a quantitative foundation for curricular reform by distinguishing student strengths (e.g., analytical thinking) from deficits (e.g., abstract and digital problem-solving). The findings offer targeted insights to modernize higher education programs, enhance labor market preparedness, and strengthen the region's intellectual capital. This data-driven evaluation is crucial for aligning student competency with the complex logical and algorithmic demands of the modern economy.

References

1. Belinszki B., Palincsár I., Szepesi I., Szipőcsné Krolopp J., Takácsné Kárász J. (2020). Országos kompetenciamérés 2021: Feladatok és jellemzőik – Matematika 10. évfolyam. Oktatási Hivatal, Budapest.
2. Krolopp, J., & Vári, P. (2024). Egy nemzetközi felmérés főbb eredményei (TIMSS). Oktatáskutató és Fejlesztő Intézet. URL: https://ofi.oh.gov.hu/en/egy-nemzetkozi-felmeresfobb-eredmenyei-timss,
3. OECD (2023). Putting AI to the test: How does the performance of GPT and 15-year-old students in PISA compare? OECD Education Spotlights, No. 6. OECD Publishing, Paris. https://doi.org/10.1787/2c297e0b-en
4. Boros, J., & Kucsinka, K. (2024). A mesterséges intelligencia és a főiskolás hallgatók matematikai kompetenciateszten elért eredményeinek összehasonlítása. In: Cyber Security in Cross-Border Cooperation Conference, Berehove, 15–16 October 2024.

Світлана БЛАГОДЄТЄЛЄВА-ВОВК
кандидатка економічних наук, доцентка
Університет глобальних стратегій «Альтера»,
svitlana@blagodeteleva-vovk.com

ІНСТИТУЦІЙНА ПОТРЕБА ЗАХИСТУ ПРАВ ВИКРИВАЧІВ АКАДЕМІЧНОЇ НЕДОБРОЧЕСНОСТІ

Постановка наукової проблеми Проблема академічної недоброчесності характерна як для розвинутих, так і для країн, що розвиваються. Це пов`язано із дією багатьох факторів, таких як: масовізація вищої освіти, розвиток інтернету та комунікаційних технологій, які роблять знання швидко та широко доступними, зростання запиту на отримання статусу – диплома про вищу освіту чи наукового ступеню, який гарантує працевлаштування у сфері послуг замість виснажливої фізичної праці у сільському господарстві чи промисловості, амбівалентності як наріжної якості особистості та схильності до опортуністичної поведінки і обману, обумовленою відсутністю відповідальності, покарання та слабкістю інститутів тощо.

Прогресивна громадськість б`є на сполох щодо поширення та поглиблення цієї проблеми, починаючи із дитячого садочку, школи і протягом життя, оскільки втрачається інтелектуальний капітал та потенціал розвитку суспільства. Окремі представники та групи громадських діячів пробують привернути увагу до проблеми та потреби її вирішення шляхом викриття плагіаторів серед топ-посадовців. Ця діяльність містить значні ризики для життя і здоров`я викривачів академічної недоброчесності. Про що свідчать кейси їх очорніння, сталкінгу, кіберсталкінгу, погроз, звільнення з роботи.

Проте, відсутні механізми ефективного захисту прав викривачів – державні інститути правозахисту.

Формулювання завдання дослідження й обґрунтування його актуальності Полягає у створенні інституційного механізму захисту прав викривачів академічної недоброчесності, який сприятиме убезпеченню діяльності антиплагіатних ініціатив та активістів від зазіхань з боку фігурантів їхніх розслідувань, а також посилення руху щодо викриття академічно недоброчесних держуправлінців, освітян, науковців, та надасть сигнал схильним до обману особистостям не випробовувати долю, оскільки їхні оборудки можуть бути викритими.

Наукова новизна порівняно з відомими роботами Питання захисту прав викривачів академічної недоброчесності в академічному середовищі України не ставилося, хоча активно обговорювалося у соціальних мережах, як реакція на переслідування окремих активістів. На міжнародному рівні діють окремі організації, які надають захист будь-яким викривачам, зокрема, і академічної недоброчесності за умови політичного тиску на них. Проте, їхня діяльність малодосліджена.

Короткий виклад поставленого завдання В Україні з 1 липня 2014 року – з часу прийняття оновленого ЗУ «Про вищу освіту», запроваджено академічну відповідальність за порушення академічної доброчесності. У пункті 4 ст. 42 ЗУ «Про освіту» надано перелік порушень академічної доброчесності, серед яких згадується хабарництво (абзац 7): «хабарництво - надання (отримання) учасником освітнього процесу чи пропозиція щодо надання (отримання) коштів, майна, послуг, пільг чи будь-яких інших благ матеріального або нематеріального характеру з метою отримання неправомірної переваги в освітньому процесі» [1].

Цікавою особливістю є те, що у цьому моменті академічна відповідальність перетинається із кримінальною, цивільною та дисциплінарною відповідальністю за корупцію, яка прописана у ЗУ «Про запобігання корупції», зокрема у пункті 1 ст.1 у абзацах 6, 7 зазначено наступне: «корупція - використання особою, зазначеною у частині першій статті 3 цього Закону, наданих їй службових повноважень чи пов’язаних з ними можливостей з метою одержання неправомірної вигоди або прийняття такої вигоди чи прийняття обіцянки/пропозиції такої вигоди для себе чи інших осіб або відповідно обіцянка/пропозиція чи надання неправомірної вигоди особі, зазначеній у частині першій статті 3 цього Закону, або на її вимогу іншим

фізичним чи юридичним особам з метою схилити цю особу до протиправного використання наданих їй службових повноважень чи пов'язаних з ними можливостей;
неправомірна вигода - грошові кошти або інше майно, переваги, пільги, послуги, нематеріальні активи, будь-які інші вигоди нематеріального чи негрошового характеру, які обіцяють, пропонують, надають або одержують без законних на те підстав»[2].

Крім того, в абзаці 19 дається визначення поняття «викривач» - «викривач - фізична особа, яка за наявності переконання, що інформація є достовірною, повідомила про можливі факти корупційних або пов'язаних з корупцією правопорушень, інших порушень цього Закону, вчинених іншою особою, якщо така інформація стала їй відома у зв'язку з її трудовою, професійною, господарською, громадською, науковою діяльністю, проходженням нею служби чи навчання або її участю у передбачених законодавством процедурах, які є обов'язковими для початку такої діяльності, проходження служби чи навчання» [2].

Вважаємо, що для захисту прав викривачів академічної доброчесності варто взяти модель, напрацьовану в антикорупціному законодавстві. Вона передбачає державний захист (ст. 53), що складається із окреслення прав і гарантів, пов`язаних із захистом членів родини, трудових прав, конфіденційності, психологічну допомогу, винагороду тощо.

Для цього необхідно адаптувати, розробити, включити та проголосувати до законодавства про освіту нову новелу про захист прав викривачів академічної недоброчесності. Це можна зробити шляхом включення нової норми до існуючих ЗУ «Про освіту», ЗУ «Про вищу освіту», або до нещодавно прийнятого у першому читання ЗУ «Про академічну доброчесність». Ми подавали такі пропозиції, проте, вони не були почуті та підтримані у стінах Верховної Ради України, що продовжує створювати загрозу для життя та здоров`я викривачів.

Висновки Епідемія академічної недоброчесності, що шириться світом потребує адекватної відповіді від громадськості, зокрема, щодо боротьби із проявами інтелектуальної деградації шляхом викриття найбільш кричущих кейсів. При цьому в Україні питання захисту викривачів академічної недоброчесності не унормовано, що створює загрози їхньому життю та здоров`ю з боку викритих порушників. Пропонується адаптувати норми та досвід захисту прав викривачів корупції в законодавство про освіту і науку для забезпечення інституційного захисту прав викривачів академічної недоброчесності, оскільки антиплагіатна та антикорупційна діяльність є подібними та навіть перетинаються в об`єкті хабарництва.

Список використаних джерел

1. Про освіту : Закон України від 05 верес. 2017 р. № 2145-VIII // Офіційний вісник. України. – 2017. – № 78. – С. 7–84.
2. Про запобігання корупції : Закон України від 14.10.2014 р. № 1700-VII. Законодавство України : база даних / Верхов. Рада України. URL: http://zakon5.rada.gov.ua/laws/show/1700-18/page (дата звернення: 28.10.2025).

Yana VARVARIUK
Second-year applicant for the Bachelor's degree in Computer Science (Specialty 122), State University "Kyiv Aviation Institute"
9144285@stud.kai.edu.ua

Anna VIKHTYK
Second-year applicant for the Bachelor's degree in Computer Science (Specialty 122), State University "Kyiv Aviation Institute"
7865640@stud.kai.edu.ua

Nataliia DENYSENKO
Senior Lecturer of the Professional Foreign Languages Department, State University "Kyiv Aviation Institute"
nataliia.denysenko@npp.kai.edu.ua

LEGAL DIMENSIONS OF SECURITY

Security is a multidimensional phenomenon, and its legal dimension plays a key role in shaping the normative framework that forms both public and private foundations. This paper examines the interaction of law and security in various spheres: national security, personal security (human rights), information/cybersecurity, and the activities of private security structures. The normative framework is analyzed, contradictions are identified (in particular, between security and the right to privacy) [1, sec. 2; 4, sec. 1], and practical recommendations are proposed to strengthen legal guarantees while simultaneously improving the effectiveness of security [2, sec. 3]. The review is based on international and comparative legal sources [6, ch. 1].

Introduction. The concept of "legal security" (or "legal dimension of security") is defined as the set of norms, principles, rights, obligations, and mechanisms for their enforcement, which regulate relations in the field of security [1, sec. 2]. Legal norms are essential for legitimacy, accountability, the protection of human rights, and the observance of the rule of law [4, sec. 3].

Conceptual and Theoretical Foundations. Systemic approach: Security is not only a military or police dimension but also public order, human rights, information security, etc. Law ensures consistency and establishes boundaries [1, sec. 2; 6, ch. 1].

Classification of security types by the object of protection: the state, society, the individual, information infrastructure, private property, etc. [2, sec. 3].

Legal Regimes in Different Spheres of Security. Constitutional and legislative norms define the scope and limits of state powers in the field of security [2, sec. 3].

Legal guarantees: parliamentary and judicial oversight, doctrines of emergency state, restrictions on executive powers [2, sec. 3].

Modern challenges: cybercrime, terrorism, and information wars require the adaptation of national legislation, the implementation of special response mechanisms, and the maintenance of balance between security and the rule of law [6, ch. 2].

Human Rights and Personal Security. The right to personal security, freedom, and protection from arbitrary deprivation of liberty (enshrined in international treaties, including the European Convention on Human Rights) [4, sec. 1].

Restrictions on surveillance, detention, and search; the need to adhere to the principle of proportionality and due process of law [4, sec. 2].

The conflict between security measures (e.g., anti-terrorism) and the right to privacy; examples from judicial practice [4, sec. 3; 1, sec. 2].

Information and Cybersecurity. Legal mechanisms for protecting data and information infrastructure (regulation of cybersecurity incidents, including in the healthcare sector) [1, sec. 3].

Legal risks for cybersecurity researchers (possible liability under copyright, contract, or private law) [3, sec. 1].

The interrelation of principles such as “security by design,” accountability, and the risks of authoritarian use of cybersecurity norms [1, sec. 3].

The role of international documents (e.g., the Tallinn Manual on international law applicable to cyber conflicts) in shaping national cyber law [6, ch. 1].

Private Security Activities. Licensing, registration, certification, and regulatory oversight (background checks, training standards) [2, sec. 3].

Limits of rights and responsibilities of private guards (detention, inspection, use of force, civil and criminal liability) [2, sec. 4].

Interaction of private security structures with law enforcement agencies, risks of abuse [2, sec. 4].

Legal Challenges and Contradictions. Balance between security and human rights: ensuring that security measures do not unjustifiably violate fundamental rights [4, sec. 2].

Implementation gaps: the presence of norms on paper does not guarantee their effective enforcement [2, sec. 3].

Coordination problems: unclear distribution of powers among different security actors [2, sec. 3; 6, ch. 2].

Recommendations. Adapt legislative frameworks to new challenges (especially in the field of cybersecurity), ensuring guarantees [1, sec. 3; 6, ch. 2].

Develop oversight mechanisms (judicial, parliamentary, and independent institutions) [2, sec. 3].

Harmonize legal norms at the international level [6, ch. 1].

Establish high standards of training and certification in private security and security research [2, sec. 4; 3, sec. 1].

Ensure transparency of security policy and raise public awareness [1, sec. 3].

Conclusions. The legal dimension is an integral part of a legitimate and effective security system [2, sec. 3]. The search for balance between security and human rights is a dynamic and continuous process [4, sec. 2]. Interdisciplinary research is necessary to improve the normative framework, oversight mechanisms, and institutional design [6, ch. 2].

References

1. Yeng P. K. Assessing the Legal Aspects of Information Security Requirements for Health Care in 3 Countries: Scoping Review and Framework Development. JMIR Human Factors. 2022. [1, sec. 2; 1, sec. 3]
2. Bilek A. J., Klotter J. C., Federal R. K. Legal Aspects of Private Security. NCJRS Virtual Library. 1981. [2, sec. 3; 2, sec. 4]
3. Park S. A Researcher’s Guide to Some Legal Risks of Security Research. Harvard Cyberlaw Clinic. 2020. [3, sec. 1]
4. Bambauer D. E. Privacy Versus Security. Northwestern Journal of Law & Cognitive Science. 2013. [4, sec. 1; 4, sec. 2; 4, sec. 3]
5. Boeken J. From Compliance to Security, Responsibility Beyond Law. Security Journal. 2024. (не використано у тексті — можна видалити)
6. Schmitt M. N. (ed.). Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press. 2017. [6, ch. 1; 6, ch. 2]

Ольга ПАЛАГНЮК
кандидат психологічних наук,
асистент кафедри педагогіки і психології дошкільної та спеціальної освіти,
Чернівецький національний університет імені Юрія Федьковича;
e-mail: o.palahnyuk@chnu.edu.ua

ВІД МОБІЛІЗАЦІЇ ДО ІНСТИТУЦІОНАЛІЗАЦІЇ: ПОЛІТИКО-ПСИХОЛОГІЧНІ МЕХАНІЗМИ ЗГУРТОВАНОСТІ ТА СОЛІДАРНОСТІ СУСПІЛЬСТВА В ПЕРІОД ВІЙНИ ТА ПОВОЄННОГО ВІДНОВЛЕННЯ

Постановка проблеми та актуальність. Тривала війна випробовує соціальну єдність, підриваючи довіру, взаємопідтримку та суб'єктність громадян. Соціальна солідарність (ціннісна єдність і моральна взаємність) і соціальна згуртованість (інтегрована взаємодія та співпраця) виступають базовими детермінантами суспільної стійкості та національної безпеки. Для України консолідація цих ресурсів набуває екзистенційного виміру в умовах повномасштабної агресії та під час повоєнного відновлення.

Мета дослідження. Обґрунтувати і систематизувати психологічні стратегії зміцнення солідарності та згуртованості на трьох рівнях – суспільному, державному й міжнародному – з урахуванням механізмів довіри, ідентичності, процедурної справедливості та інформаційної стійкості.

Наукова новизна. Запропоновано інтегровану політико-психологічну рамку, що поєднує: (1) горизонтальні практики взаємодопомоги та інклюзивної «ми-ідентичності»; (2) вертикальні механізми інституційної довіри (прозорість, підзвітність, справедливі процедури) і стратегічної комунікації; (3) наративи посттравматичного зростання та міждержавну/діаспорну «дипломатію солідарності». Рамка фокусується на перетворенні короткочасної мобілізації у стійкі інституційні практики участі.

Короткий виклад результатів (стратегії та механізми).

1. **Суспільний (горизонтальний) рівень.** Розбудова мереж взаємодопомоги і волонтерства як «шкіл громадянства»; культивація інклюзивної національної ідентичності («єдність у різноманітті») через спільні символи, ритуали пам'яті й видимість локальних ініціатив; медіаграмотність як щеплення від маніпуляцій у молодіжних середовищах. Психологічні механізми: зростання довіри, належності (belonging), просоціальних норм та суб'єктності.
2. **Державний (вертикальний) рівень.** Підсилення інституційної довіри через прозорість, справедливий розподіл ресурсів, відкриті канали участі (консультації, громадські ради, інструменти е-демократії); стратегічні наративи спротиву та відновлення у поєднанні з системною протидією дезінформації; інтеграція волонтерських мереж у політику публічних послуг; масштабні програми психічного здоров'я, реабілітації ветеранів і підтримки ВПО як елемент національної безпеки. Психологічні механізми: процедурна справедливість, відчуття «співвласності» держави, легітимність.
3. **Міжнародний рівень.** Підтримання глобальних альянсів на основі спільних демократичних цінностей; залучення діаспори як транснаціонального «моста довіри»; публічна дипломатія солідарності, що надає внутрішній боротьбі міжнародної моральної легітимації. Психологічні механізми: зовнішнє підкріплення колективної ідентичності, підвищення морального духу, нормалізація спільної мети.

Практичні інструменти (узагальнення).

– **Інклюзивні платформи діалогу** (круглі столи, е-звернення) → відчуття залученості та справедливості процедур.

– **Делегування та ко-виробництво послуг** із ГО/волонтерами → ефективність і «співвласність» політик.

– **Стратегічна комунікація та фактчекінг** → інформаційно-психологічна стійкість.

– **Громадянська/медіаосвіта** (формальна й неформальна) → емпауермент, критичне мислення.

– **Психологічна допомога і реабілітація** (включно з родинами військових, ВПО) → запобігання посттравматичному відчуженню, підтримка соціального капіталу.

– **Наративи посттравматичного зростання** → переведення спільного болю у довгострокову резилієнтність.

Висновки. Консолідація солідарності та згуртованості потребує синхронізації горизонтальних мереж довіри з вертикальними механізмами легітимності та прозорості, підкріплених міжнародною підтримкою. Перехід від мобілізаційного піднесення до інституціоналізованої участі, системної психосоціальної допомоги й стійкої інформаційної політики формує рамку суспільної резилієнтності, необхідну для перемоги та повоєнного розвитку.

Список використаних джерел:

1. Budjeryn, M. (2024) *Safeguarding Ukraine's democracy during the war*. Washington, DC: Brookings Institution. Available at: https://www.brookings.edu/articles/safeguarding-ukraines-democracy-during-the-war/
2. Dragolov, G., Ignácz, Z.S., Lorenz, J., Delhey, J., Boehnke, K. and Unzicker, K. (2016) *Social Cohesion Radar: Measuring Common Ground*. Cham: Springer. https://doi.org/10.1007/978-3-319-32464-7
3. European Commission (2023) *Ukraine Facility 2024–2027: Support for recovery, reconstruction and modernisation*. Brussels: EC. Available at: https://commission.europa.eu/strategy-and-policy/eu-relations/non-eu-countries/ukraine/ukraine-facility_en
4. Freedom House (2024) *Nations in Transit 2024: Ukraine Country Report*. Washington, DC: Freedom House. Available at: https://freedomhouse.org/country/ukraine/nations-transit/2024
5. Goodwin, R., Hamama-Raz, Y., Leshem, E. and Ben-Ezra, M. (2023) 'National resilience in Ukraine following the 2022 Russian invasion', *International Journal of Disaster Risk Reduction*, 85, 103487. https://doi.org/10.1016/j.ijdrr.2022.103487
6. Koinova, M. (2024) 'The diaspora's mobilization post-invasion has provided crucial support to Ukraine'. *Migration Policy Institute*. Available at: https://www.migrationpolicy.org/article/ukraine-diaspora-mobilization
7. Putnam, R.D. (2000) *Bowling Alone: The Collapse and Revival of American Community*. New York: Simon & Schuster. Available at: https://www.simonandschuster.com/books/Bowling-Alone/Robert-D-Putnam/9780743203043
8. Tyler, T.R. (2006) *Why People Obey the Law*. Princeton, NJ: Princeton University Press. Available at: https://press.princeton.edu/books/paperback/9780691126739/why-people-obey-the-law
9. UNHCR (2024) *Ukraine Situation Flash Update*. Geneva: UNHCR. Available at: https://www.unhcr.org/ukraine-emergency
10. Трофименко, А.В. і Макаров, І.О. (2024) 'Волонтерський рух в Україні в умовах повномасштабної війни: основні тенденції розвитку', *Вісник Маріупольського державного університету. Серія: Історія. Політологія*, 40, сс. 134–142. https://doi.org/10.34079/2226-2830-2024-15-40-134-142
11. Українська Волонтерська Служба (2024) '74 % українців долучались до волонтерства після 24 лютого 2022 року: результати дослідження', 29.01.2024. Available at: https://volunteer.country (Accessed: 26 September 2025).
12. Рафальський, О.О. і Майборода, О.М. (ред.) (2024) *Суспільно-політична солідарність в Україні в умовах війни: монографія*. Київ: ІПіЕНД ім. І.Ф. Кураса НАН України. Available at: https://ipiend.gov.ua/

БЕЗПЕКОВІ ВИКЛИКИ НА РЕГІОНАЛЬНОМУ ТА ЛОКАЛЬНОМУ РІВНІ

SECURITY CHALLENGES AT THE REGIONAL AND LOCAL LEVELS

BIZTONSÁGI KIHÍVÁSOK REGIONÁLIS ÉS HELYI SZINTEN

Інна ТУРЯНИЦЯ
кандидат історичних наук,
доцент кафедри історії Угорщини та європейської
інтеграції УУННІ ДВНЗ «УжНУ»,
inna.turjanica@uzhnu.edu.ua

Василь БЕЛИКАНИЧ
ст. викладач кафедри історії Угорщини та європейської
інтеграції УУННІ ДВНЗ «УжНУ»,
laslo.belykanych@uzhnu.edu.ua

СУЧАСНІ ВИКЛИКИ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ ЛИТОВСЬКОЇ РЕСПУБЛІКИ: РЕГІОНАЛЬНИЙ ТА ГЛОБАЛЬНИЙ АСПЕКТИ

Геополітично Литва як «форпост» євроатлантичної цивілізації розташована на стику східноєвропейського та північноєвропейського макрорегіонів та межує з пострадянським простором (NATO,, 2021). Її територія є складовою так зв. «Балтійського мосту безпеки», який з'єднує країни Скандинавії з Центральною Європою та формує північний фланг НАТО.

В умовах посилення ризиків і загроз з боку Росії Литва стала однією із найважливіших ланок його колективної оборони, що зумовлює також зростання співпраці з Україною разом з партнерами по блоку. Геополітична поведінка Литви визначається взаємопов'язаними факторами: історичним досвідом протистояння імперським впливам, прагненням гарантувати національний суверенітет, а також необхідністю адаптації до сучасних глобальних процесів – від енергетичної та інформаційної безпеки до нових форм регіональної взаємодії. У цьому контексті необхідність осмислення того, яким чином Литва компонує національні інтереси й наявні загрози з регіональними та глобальними викликами є більш ніж актуальним. Адже це дозволяє зрозуміти тренд трансформацій безпекового середовища всієї Східної Європи.

Литва має об'єктивні вразливості, зумовлені безпосереднім сусідством з Калінінградською областю РФ та Білоруссю і наявністю Сувалкського коридору – потенційною «точкою розриву» між Балтійським регіоном і рештою території Альянсу (NV,, 2025). Вже з 2014 р., не кажучи про 2022 р. країна перебуває під тиском гібридних загроз, якими Росія тестує безпекову систему НАТО. Актуалізувалися економічні, енергетичні, інформаційні виклики. Згідно з планами Кремля щодо «мирного» повернення країн Балтії в орбіту його впливу, ставилось за мету нівелювати безпекові гарантії з боку НАТО, запобігти виходу з єдиної енергетичної системи БРЕЛЛ та використати російську меншину в пропагандистських цілях (Facty,, 2023). За даними 2021 р. остання складала 5,02% чисельності населення. Це, щоправда, значно менше, аніж у сусідніх Латвії та Естонії, де її питома вага наближалась до ¼ (Malužinas M. 2025, p. 147). Починаючи з 2010-х рр. Литва неодноразово ставала об'єктом кібератак на державні установи, медіа та енергетичну інфраструктуру (Lexington institute, 2025). Більшість з них скеровувалися з території Росії, а останнім часом і Китаю.

Наявні загрози зумовлюють необхідність комплексних і скоординованих дій. Стратегічна відповідь Литви на ці виклики базується на трьох ключових стовпах: 1) Збільшення витрат на оборону до 3% ВВП (Dapkus L., 2025), а у 2026-2030 рр. країна планує збільшити їх до 5–6% ВВП (The Economic Times, 2025); 2) Розміщення на своїй території багатонаціональних підрозділів НАТО, окрім дислокованого з 2017 р. у м. Рукла німецького батальйону, який є елементом стримування) (Korrespondent ua, 2025); 3) Прискорення технічної модернізації в поєднанні з розвитком власних збройних сил та розширенням військової інфраструктури (Chmielewski, B. & Tarociński, J., 2024). Такими підходами виконується подвійне завдання: гарантувати власну безпеку та зробити вагомий внесок у колективну оборону Альянсу. Цьому є супутньою широка суспільна підтримка, що проявляється у високому рівні довіри до збройних сил і готовності громадян долучатися до системи національного спротиву. В сукупності ці елементи формують цілісну модель забезпечення безпеки Литви, орієнтовану на стійкість, взаємодію та стратегічну автономію в межах колективної оборони.

Один з ключових безпекових викликів – енергетичний – втратив актуальність. Раніше будучи залежною від російських енергоносіїв, країна диверсифікувала постачання,

збудувавши LNG-термінал для зберігання зрідженого природного газу у Клайпеді (Facty,, 2023). Країни Балтії у лютому 2025 р. успішно відімкнулися від системи БРЕЛЛ і синхронізувалися з європейською енергосистемою.

Додаткові ризики для Литви створює політична та військова залежність сусідньої Білорусі від Росії. Військова інтеграція та спільні навчання підвищують рівень напруженості в регіоні. Проте, застосування ціннісних підходів у зовнішній політиці Литви має гнучкий характер. Офіційний Вільнюс не приховує свого негативного ставлення до авторитарного режиму Лукашенка. Але при цьому Литва прагне виступити в ролі посередника між білоруською опозицією та європейськими структурами.

Таким чином, сучасна безпекова політика Литви характеризується комплексним поєднанням протидії військовим, гібридним, економічним та соціальним викликам, активізмом у протистоянні загрозам. Традиційні оборонні механізми компліментують з інструментами «розумного стримування», адаптацією до нових загроз, поруч зі зміцненням соціально-інституційної структури безпеки та оборони. Не кажучи вже про те, що політичні еліти країни свого часу зрозуміли безперспективність статусу нейтрального моста між Сходом і Заходом, котрий був би дуже вигідним Росії, але служив би поганою гарантією суверенітету, незалежності і територіальної цілісності.

Список використаних джерел

1. Chmielewski, B. & Tarociński, J., 2024. Na wojennej ścieżce: rozwój i modernizacja sił zbrojnych państw bałtyckich. Ośrodek Studiów Wschodnich. URL: https://www.osw.waw.pl/pl/publikacje/komentarze-osw/2024-05-10/na-wojennej -sciezce-rozwoj-i-modernizacja-sil-zbrojnych-panstw
2. Dapkus, L., 2025. Lithuania vows to boost defense spending to 5-6% of GDP, citing the threat of Russian aggression. Ap NEWS, 01.17. URL: https://apnews.com/article/lithuania-defense-spending-nato-trump-nauseda-baltic-b1328b37e85fd755f25ce647deed6bf1/
3. Lithuania Punches Up In Cyber Fights With Russia, 2025 . Lexington institute. URL: https://lexingtoninstitute.org/lithuania-punches-up-in-cyber-fights-with-russia
4. Lithuania says will spend 5-6% of GDP on defence in 2026-2030, 2025. The Economic Times, 01.17. URL: https://economictimes.indiatimes.com/news/defence/lithuania-says-will-spend-5-6-of-gdp-on-defence-in-2026
2030/articleshow/117333281.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst
5. Malužinas, M., 2025. Joe Biden Administration's Security Policy and What It Means for the Baltic States. Nowa Polityka Wschodnia. Quarterly, vol. 46, issue 2, pp. 145-165. URL: https://journals.indexcopernicus.com/api/file/viewByFileId/2462713. DOI: 10.15804/npw20254607
6. NATO Public Diplomacy Division (2022) Lithuania and NATO: Partnership and Collective Defence, 2021. Brussels: NATO. URL: https://www.nato.int/structur/pdd/2021/211216-pdd-content-guidelines.pdf
7. Кремль розробив план «мирного» повернення під свій вплив країн Балтії – витік документів, 2023. [The Kremlin has developed a plan to "peacefully" bring the Baltic states back under its influence – leaked documents]. Факти. [Facty]. URL: https://fakty.com.ua/ua/svit/20230426-kreml-rozrobyv-plan-myrnogo-povernennya-pid-svij-vplyv-krayin-baltiyi-vytik-dokumentiv/
8. Литва готується розмістити бригаду НАТО вже в 2025 році, 2025. [Lithuania is preparing to deploy a NATO brigade as early as 2025.]. Електронне новинне видання Korrespondent ua.URL: https://ua.korrespondent.net/world/4495189-lytva-hotuietsia-rozmistyty-bryhadu-nato-vzhe-v-2025-rotsi
9. Сувальський коридор: усе про критичну зону, через яку Росія може роз'єднати НАТО – огляд ВВС, 2025. NV (nv.ua). Незалежне новинне видання. [Suwałki Corridor: All about the critical zone through which Russia can divide NATO - BBC review]. URL: https://nv.ua/ukr/world/geopolitics/suvalskiy-koridor-strategichne-znachennya-ta-zagrozi-dlya-nato-u-2025-roci-50543125.html

Ванесса БІРТОК
асистент
Кафедра географії та туризму
Закарпатський угорський університет ім. Ференца Ракоці II, Україна
аспірантка
Кафедра охорони ландшафту та природоохоронної географії
Дебреценський університет, Угорщина,
birtok.vanessza@kmf.org.ua

Ференц БІРТОК
викладач
Фаховий коледж
Закарпатського угорського університету ім. Ференца Ракоці II, Україна
аспірант
Кафедра соціальної географії та територіального розвитку
Дебреценський університет, Угорщина,
birtok.ferenc@kmf.org.ua

Олександр БЕРГХАУЕР
к. г. н., доцент
Кафедра географії та туризму
Закарпатський угорський університет ім. Ференца Ракоці II, Україна,
berghauer.sandor@kmf.org.ua

Марія ВАШВАРІ
старший викладач
Кафедра охорони ландшафту та природоохоронної географії
Дебреценський Університет, Угорщина
доцент
Кафедра географії та туризму
Закарпатський угорський інститут ім. Ференца Ракоці II, Україна,
vasvari.maria@science.unideb.hu

БЕЗПЕКОВІ ВИКЛИКИ РЕГІОНАЛЬНОГО РІВНЯ В ТУРИСТИЧНІЙ СФЕРІ ТА ЛІКУВАЛЬНО-ОЗДОРОВЧОМУ ТУРИЗМІ ЗАКАРПАТТЯ В УМОВАХ ВІЙНИ

Туризм в Україні, який перебував у процесі поступового розвитку та стабілізації, у 2022 році зіштовхнувся з новим викликом — повномасштабною війною. Загострення бойових дій на більшій частині території країни призвело до того, що багато туристичних підприємств були змушені тимчасово зупинити або повністю припинити свою діяльність. Це завдало серйозного удару по туристичній галузі, яка відіграє важливу роль у створенні робочих місць, наповненні місцевих бюджетів та стимулюванні економічного й інфраструктурного розвитку.

У цих умовах роль Закарпаття значно зросла, адже це єдиний регіон, який не постраждав безпосередньо від бойових дій. Завдяки сприятливим природним умовам — гірському повітрю, мінеральним і термальним водам, а також розвиненій мережі оздоровчих закладів — регіон став важливим місцем для реабілітації, збереження здоров'я та тимчасового розміщення внутрішньо переміщених осіб.

Мета дослідження — вивчити роль і можливості туризму в Закарпатті в умовах війни, особливо соціально-економічну функцію готелів, пансіонатів, санаторіїв та реабілітаційних центрів. Дослідження базується на даних Національної туристичної організації України та стратегії конкурентоспроможного розвитку туризму, з акцентом на програми відновлення малого й середнього бізнесу у сфері туризму та гостинності.

Туристична інфраструктура Закарпаття відіграє ключову роль у задоволенні соціальних потреб під час війни. Вона не лише забезпечує прихисток для ВПО, а й створює умови для фізичної та психологічної реабілітації військових, дітей та інших вразливих груп населення.

У довгостроковій перспективі туризм у регіоні може стати важливим фактором економічного відновлення, посилення регіонального потенціалу та соціальної стабільності. Саме тому інвестиції в розвиток туристичної галузі Закарпаття є не лише актуальними, а й стратегічно необхідними для повоєнного відродження країни.

Список використаних джерел

1. Державна служба статистики України. Головне управління статистики у Закарпатській області. Ужгород. 2018. https://www.uz.ukrstat.gov.ua/catalog/2018/zbirnuk01.pdf
2. Національна туристична організація України https://nto.ua/
3. Пеняк Павло, Кочан Володимир. Туризм на Закарпатті під час воєнного стану. Війна та туризм. Матеріали міжнародної науково-практичної конференції. Київ, 11 листопада 2022 р. К.:ТОВ «Геопринт»,2022. – 319 с. УДК 338.48:355.422(477:470)(082) В42, ISBN 978-617-674-060-5
4. Регіональна стратегія розвитку закарпатської області на період 2021-2027 років. https://carpathia.gov.ua/storage/app/sites/21/Economics/201001-1840p.pdf
5. Стратегічна дорожня карта. Відновлення малого та середнього бізнесу у секторі туризму та гостинності в 2023-2033 роках. Київ 2024. https://drive.google.com/file/d/1qN0Uu2j4FmGA-6iZ3eIVsRWUsOG1F59W/view
6. Стратегія розвитку Закарпатської області на період до 2027 року. Волинський ресурсний центр. 2024. https://carpathia.gov.ua/storage/app/sites/21/Economics/regional%20development%20strategy%20until%202027.pdf

Дмитро БОЙКО
Студент 3 курсу, ОП «Міжнародна інформація»
Чернівецький національний університет імені Юрія Федьковича,
boiko.dmytro.m@chnu.edu.ua

Іван ОСАДЦА
кандидат політичних наук,
доцент кафедри міжнародних відносин та суспільних комунікацій
Чернівецького національного університету імені Юрія Федьковича,
i.osadtsa@chnu.edu.ua

ПОЛЬСЬКО-УКРАЇНСЬКЕ СПІВРОБІТНИЦТВО У СФЕРІ ПРОТИДІЇ ГІБРИДНИМ ЗАГРОЗАМ

Сучасна система міжнародних відносин перебуває у стані глибоких трансформацій, зумовлених появою нових загроз, що виходять за межі класичних уявлень про безпеку. У XXI столітті поняття безпеки перестає обмежуватися виключно військовим компонентом і включає політичні, економічні, соціальні та інформаційні аспекти. Одним із найактуальніших викликів стають гібридні загрози, що поєднують воєнні, політичні, інформаційні, економічні та кіберінструменти тиску, а їхня асиметричність і прихованість значно ускладнюють своєчасне реагування та нейтралізацію потенційної шкоди. Для України та Польщі ця проблема є особливо значущою, оскільки обидві держави опинилися на передовій лінії протистояння з російською агресією та змушені формувати комплексні стратегії захисту, здатні протистояти широкому спектру загроз [1].

Гібридні загрози являють собою системний виклик не лише для безпеки окремих країн, а й для стабільності всієї євроатлантичної спільноти. Вони проявляються у різних формах: кібератаки на державні та приватні структури, кампанії дезінформації, енергетичний тиск через залежність від постачання ресурсів, втручання у політичні процеси та вибори, а також створення кризових ситуацій у сфері міграції. З 2022 року інтенсивність таких загроз різко зросла, що змушує країни Центрально-Східної Європи переглядати традиційні підходи до безпеки, адаптувати їх до нових умов та поглиблювати міждержавну співпрацю. Польща, як повноправний член НАТО та ЄС, і Україна, що активно інтегрується у ці структури, мають взаємодоповнювальні підходи, що можуть забезпечити комплексну відповідь на сучасні виклики [5].

У науковій та практичній площині комплексно проаналізовано інформаційний, кібернетичний та енергетичний виміри гібридних загроз і вперше проведено SWOT-аналіз польської та української моделей протидії. Основними рисами загроз визначено їхню асиметричність, прихованість, синергетичність та транснаціональний характер, що робить необхідним багаторівневе реагування та тісну міждержавну координацію.

Польська модель протидії гібридним загрозам ґрунтується на чотирьох стратегічних «стовпах»: забезпечення захисту держави й громадян, інтеграція в НАТО та ЄС, збереження національної ідентичності та культурних цінностей, а також забезпечення сталого соціально-економічного розвитку. На практиці це проявляється у модернізації Збройних сил Польщі, створенні спеціального кіберкомандування та систем територіальної оборони, диверсифікації джерел енергопостачання, а також розвитку медіаграмотності та моніторингу інформаційного простору. Крім того, польська модель передбачає активну участь у міжнародних навчаннях та обмін досвідом у сфері безпеки, що підвищує здатність держави реагувати на комплексні загрози [3].

Українська модель протидії гібридним загрозам вирізняється високою адаптивністю та інноваційністю. Вона поєднує воєнні дії з активними стратегічними комунікаціями, кіберзахистом та антикризовим управлінням. Важливим компонентом є гармонізація національного законодавства з вимогами ЄС та стандартами НАТО, посилення готовності критичної інфраструктури до кібератак, а також оперативна координація дій із міжнародними партнерами. Такий підхід дозволяє Україні швидко реагувати на змінні умови загроз та впроваджувати інноваційні методи захисту [2].

Порівняльний аналіз демонструє, що польська модель забезпечує високий рівень інституційної стабільності та прогнозованості дій, тоді як українська модель характеризується гнучкістю та здатністю до оперативних адаптацій у кризових ситуаціях. Синергія цих підходів створює потужний потенціал для формування регіональної системи безпеки, здатної протидіяти складним та багатовимірним гібридним загрозам.

Пріоритетні напрями співпраці між Україною та Польщею включають інтеграцію центрів реагування на інциденти кібербезпеки (CERT), проведення спільних навчань для фахівців кіберсфери, узгодження стандартів інформаційної безпеки та оперативний обмін даними. Особливо перспективним є розширення співпраці в рамках ініціатив ЄС і НАТО, що дозволяє підвищити ефективність протидії загрозам на рівні регіону та забезпечити безперервний розвиток системи безпеки [4].

Дослідження показує, що лише спільні дії України та Польщі можуть сформувати ефективну багаторівневу відповідь на сучасні гібридні загрози. Взаємодія цих держав дозволяє не лише підвищити національну стійкість до інформаційних, кібернетичних та економічних ризиків, а й створити передумови для розробки регіональних програм реагування, інтеграції сучасних технологій захисту та впровадження інноваційних практик у сфері безпеки. Отримані результати можуть слугувати основою для вдосконалення національних стратегій кібер- та інформаційної безпеки, а також для формування спільного стратегічного простору, здатного протистояти новим викликам сучасного світу.

Таким чином, польсько-українське співробітництво у сфері протидії гібридним загрозам є не лише важливим фактором національної безпеки кожної країни, а й вагомим елементом регіональної та євроатлантичної безпеки. Спільна робота над інтеграцією ресурсів, стандартів та навчальних програм дозволяє формувати комплексну, адаптивну та ефективну систему реагування на загрози, що стає ключовим інструментом забезпечення стабільності у Центрально-Східній Європі.

Список використаних джерел

1. Генеза сучасної інформаційно-когнітивної (гібридної) війни в українському контексті та глобальному вимірі: наукове дослідження / С.Д. Максименко, Л.М. Деркач. Київ: «Видавництво Людмила», 2024. 128 с. ISBN 978-617-555-197-4. URL: https://lib.iitta.gov.ua/id/eprint/740932/1/LayOut02%20%281%29.pdf
2. Кручініна О. Україна – НАТО: проблеми та перспективи співпраці в умовах російсько-української війни. Міжнародні відносини, суспільні комунікації та регіональні студії. 2023. Вип. 2(16). С. 145–156. https://doi.org/10.29038/2524-2679-2023-02-145-156
3. Найчук А. В. Інформаційна безпека як складова національної безпеки держав. Інформаційна безпека: сучасний стан, проблеми та перспективи: збірник матеріалів Міжнародної науково-практичної конференції [Електронний ресурс] / за заг. ред. О.В. Віннічук. Кам'янець-Подільський : Кам'янець-Подільський національний університет імені Івана Огієнка, 2023. С. 58–63.
4. Bryczek-Wróbel, P., & Moszczyński, M. (2022). The evolution of the concept of information warfare in the contemporary information society of the post-truth era. Przegląd Nauk o Obronności, 7(13), 48–62. https://doi.org/10.37055/pno/152620
5. Genini, D. (2025). Countering hybrid threats: How NATO must adapt (again) after the war in Ukraine. New Perspectives. Interdisciplinary Journal of Central & East European Politics and International Relations, 33(2), 122-149. https://www.ceeol.com/search/article-detail?id=1340656

Василь КІШ
магістр 2 курсу спеціальності 126 Інформаційні системи і технології
ДВНЗ «Ужгородський національний університет»,
kish.vasyl@student.uzhnu.edu.ua

Василь МОРОХОВИЧ
кандидат фізико-математичних наук,
доцент кафедри інформатики та фізико-математичних дисциплін
ДВНЗ «Ужгородський національний університет»,
vasyl.morokhovych@uzhnu.edu.ua

РОЗРОБКА ІНФОРМАЦІЙНОЇ СИСТЕМИ ДЛЯ АВТОМАТИЗАЦІЇ РОБОТИ ФІТНЕС-ЦЕНТРУ З ІНТЕГРАЦІЄЮ МЕХАНІЗМІВ БЕЗПЕКИ

У сучасному світі, що динамічно розвивається, сектор послуг, особливо у сфері фітнесу та здорового способу життя, переживає період інтенсивної цифровізації. Застосування інформаційних систем (ІС) для автоматизації бізнес-процесів стає не просто конкурентною перевагою, а необхідною умовою для ефективного функціонування фітнес-центрів. Такі системи дозволяють оптимізувати управління клієнтською базою, розкладом занять, обліком абонементів та ресурсів, що, своєю чергою, підвищує якість обслуговування та загальну рентабельність бізнесу. Однак, з розширенням функціоналу та зростанням обсягів оброблюваних даних, особливо персональних, питання забезпечення кібербезпеки виходить на перший план, набуваючи критичної важливості.

Проблема, що виникає в процесі розробки ІС для фітнес-центрів, полягає в пошуку балансу між функціональною повнотою та надійністю системи. Типові рішення, що доступні на ринку, часто зосереджені на базовій автоматизації, залишаючи поза увагою складні аспекти захисту конфіденційної інформації, включаючи медичні дані, фінансові транзакції та особисті відомості користувачів. Недостатній рівень безпеки може призвести до несанкціонованого доступу, витоку даних та репутаційних втрат для підприємства. Отже, розробка теоретичних та практичних підходів до інтеграції посилених механізмів безпеки в інформаційну систему фітнес-центру є актуальним завданням, що відповідає сучасним викликам цифрової епохи.

Метою дослідження є обґрунтування методики створення інформаційної системи для автоматизації роботи фітнес-центру, яка забезпечує не лише ефективне управління бізнес-процесами, але й гарантує рівень захисту даних на всіх етапах їхнього життєвого циклу.

Наукова новизна роботи полягає в систематизації та обґрунтуванні комплексного підходу до розробки ІС фітнес-центру, який поєднує функціональну автоматизацію з багаторівневим захистом даних, використовуючи сучасні криптографічні алгоритми, механізми контролю доступу та моніторингу активності користувачів. Практична цінність дослідження полягає в можливості застосування його результатів ІТ-фахівцями для ефективного планування та реалізації аналогічних проєктів.

Розробка інформаційної системи, що відповідає високим стандартам безпеки, вимагає ретельного аналізу потенційних загроз на кожному етапі її створення. Важливо враховувати не лише зовнішні атаки, а й внутрішні ризики, пов’язані з несанкціонованим доступом персоналу до конфіденційної інформації. Тому в основу архітектури системи закладено принцип «мінімальних привілеїв», згідно з яким кожен користувач і компонент системи має доступ лише до тих даних і функцій, які необхідні для виконання його безпосередніх завдань. Це досягається за допомогою гнучкої моделі розмежування доступу на основі ролей (Role-Based Access Control, RBAC) [1].

Особлива увага приділяється захисту персональних даних клієнтів, що зберігаються в базі даних. Для цього пропонується застосування асиметричного шифрування для чутливої інформації, такої як паролі та платіжні реквізити, а також використання протоколів захищеного зв’язку (наприклад, TLS) для всіх транзакцій між клієнтом і сервером [2]. Для забезпечення цілісності даних розглядається впровадження криптографічних геш-функцій, що дозволить

виявляти будь-які спроби несанкціонованої модифікації. Процес автоматизації роботи фітнес-центру включає такі ключові функціональні модулі: управління членством, бронювання занять, управління персоналом та моніторинг обладнання. Кожен із цих модулів має бути розроблений із вбудованими механізмами безпеки, що запобігають потенційним вразливостям.

Кінцевий продукт – інформаційна система для фітнес-центру, розроблена на основі викладених принципів, – буде не просто інструментом автоматизації, а надійною платформою для ведення бізнесу в цифровому середовищі. Вона дозволить ефективно управляти всіма ключовими операціями, забезпечуючи при цьому конфіденційність, цілісність та доступність даних. Отримані результати дослідження можуть бути масштабовані для інших сфер послуг, де обробляються чутливі дані, що робить запропоновану методику універсальною та практично значущою. Таким чином, вирішення проблеми інтеграції безпеки в розробку ІС відкриває нові можливості для створення інноваційних, надійних і конкурентоспроможних програмних продуктів.

Список використаних джерел

1. Arun Kumar Akuthota. (2025). Role-Based Acces Control (RBAC) in Modern Cloud Security Governance: An In-depth Analysis, Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol, 11 (2), 3297-3311, doi: 10.32628/CSEIT25112793.

2. Ільєнко, А., Ільєнко, С., Прокопенко, О., Кравчук, І. (2023). Практичні підходи організації захищеної передачі даних по протоколу TLS засобами OPENSSL. Кібербезпека: освіта, наука, техніка, 2 (22), 122-133, doi:10.28925/2663-4023.2023.22.122133.

Наталія СТОЙКА
кандидат економічних наук,
доцент кафедри обліку і аудиту
Закарпатський угорський університет ім. Ференца Ракоці II

УПРАВЛІНСЬКИЙ ОБЛІК ЯК ІНФОРМАЦІЙНИЙ СКЛАДНИК ДІАГНОСТИКИ ФІНАНСОВОЇ БЕЗПЕКИ ПІДПРИЄМСТВ

В сучасних умовах господарювання фінансова безпека підприємства є необхідною складовою системи управління підприємством, оскільки вона сприяє забезпеченню його стійкості, платоспроможності та розвитку в умовах високої невизначеності, конкуренції та економічної нестабільності.

Поняття фінансова безпека підприємства розглядається по-різному, на думку О.І. Барановського – це рівень забезпеченості підприємства фінансовими ресурсами, достатніми для задоволення його потреб і виконання наявних зобов'язань, які характеризуються збалансованістю, стійкістю до внутрішніх і зовнішніх негативних впливів, здатністю відвернути зовнішню фінансову експансію, забезпечити фінансову стійкість (стабільність), ефективне функціонування та економічне зростання [3, с. 338].

За визначенням професора М.М. Єрмошенка, під фінансовою безпекою підприємства розуміють фінансовий стан, який характеризується, по-перше, збалансованістю та якістю сукупності фінансових інструментів, технологій і послуг, які використовуються підприємством, по-друге, стійкістю до внутрішніх і зовнішніх загроз, по-третє, здатністю фінансової системи підприємства забезпечувати реалізацію його фінансових інтересів, місій і завдань достатніми обсягами фінансових ресурсів [2, с. 47].

Таким чином, поняття фінансова безпека можемо трактувати, як стан захищеності фінансових інтересів підприємства від внутрішніх і зовнішніх загроз, що дозволяє йому ефективно функціонувати та досягати визначених фінансових цілей. Як зазначає А.В. Колеватова у загальному випадку фінансову безпеку суб'єктів підприємництва представляють як певний механізм, що, з одного боку, забезпечує стабільність фінансової системи шляхом використання захисних фінансових інструментів, а з іншого – забезпечує її ефективність шляхом організації раціонального використання фінансових ресурсів.

Таким чином механізм фінансової безпеки на підприємстві на нашу думку повинен сприяти:

1. Забезпеченню фінансовій стійкості та платоспроможності підприємства.
2. Забезпеченню захисту фінансових інтересів власників та інвесторів.
3. Протидії зовнішнім загрозам, викликам.
4. Протидії внутрішнім загрозам, викликам.
5. Досягненню стійкого розвитку та досягати визначених фінансових цілей.
6. Забезпеченню гнучкості та оперативності прийняття управлінських рішень.

Як зазначає В.З. Семанюк для генерування багатоваріантної економічної інформації щодо витрат,бізнес-процесів та їх впливу на ефективність діяльності підприємства в нестабільних, конкурентних умовах важливе значення має управлінський облік як "…система обробки та підготовки інформації про діяльність підприємства для внутрішніх користувачів у процесі управління підприємством" [5, с.136].

Отже, у забезпеченні механізму фінансової безпеки на підприємстві вагома роль належить управлінському обліку. Адже за допомогою управлінського обліку управлінці підприємства отримують обліково-інформаційне забезпечення, яка сфокусоване на їх потреби та запити. Управлінський облік є не тільки джерелом даних, а системою раннього попередження для вищестоящого управління завдяки бюджетуванню, контролю та відхилень, аналізу показників відхилень і т.д. Таким чином управлінський облік є інформаційним складником діагностики фінансової безпеки підприємств та займає важливе значення у механізмі його функціонування.

Список використаних джерел

1. Економічні та організаційні засади забезпечення фінансової безпеки підприємства : препринт наук. доп. / М. М. Єрмошенко, К. С. Горячова, А. М. Ашуєв ; за наук. ред. М. М. Єрмошенка. Київ : Нац. акад. управління, 2009. 78 с.

2. Барановський, О. І. Фінансова безпека в Україні (методологія оцінки та механізми забезпечення) : монографія. Київ : Київ. нац. торг.-екон. ун-т, 2014. 759 с.

3. Вудвуд, В. В., Батієвська, О. В. Фінансова безпека підприємства: сутність, цілі, принципи та шляхи забезпечення. Підприємництво і торгівля. 2019. № 25. URL: https://www.lute.lviv.ua/fileadmin/www.lac.lviv.ua/data/DOI/2522-1256-2019-25-12.pdf (дата звернення: 15.10.2025).

4. Колеватова, А. В. Основні пріоритетні напрями та механізм забезпечення фінансової безпеки підприємства. Ефективна економіка. 2016. № 10. URL: http://www.economy.nayka.com.ua/?op=1&z=5186 (дата звернення: 19.10.2025).

5. Семанюк, В., Жукевич, С. Управлінський облік як інформаційна складова діагностики фінансової безпеки підприємств. Світ фінансів. 2023. № 1(74). С. 138–147. URL: https://dspace.wunu.edu.ua/bitstream/316497/50027/1/%D0%A1%D0%95%D0%9C%D0%90%D0%9D%D0%AE%D0%9A.PDF (дата звернення: 19.10.2025).

Мар'ян ЦЕНКНЕР
магістр освітньої програми «Управління ІТ проєктами»
Ужгородський національний університет,
tsenkner.marian@student.uzhnu.edu.ua

Наталія ШУМИЛО
старший викладач кафедри
інформатики та фізико-математичних дисциплін
Ужгородський національний університет
natalia.shumilo@uzhnu.edu.ua

РОЛЬ ЗАСОБІВ МАСОВОЇ ІНФОРМАЦІЇ У ПОШИРЕННІ ТА ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ

Сучасне суспільство живе в умовах безпрецедентного інформаційного потоку, де масові комунікації відіграють ключову роль у формуванні громадської думки. Поряд із розвитком цифрових технологій та зростанням швидкості поширення інформації виникає новий виклик – дезінформація. Вона не лише спотворює реальність, але й може мати серйозні соціальні, політичні та безпекові наслідки [1].

Засоби масової інформації (ЗМІ) у цьому процесі виконують подвійні функції. З одного боку, вони стають каналами для поширення недостовірних або маніпулятивних повідомлень. З іншого – саме вони здатні виступати як головний інструмент у боротьбі з дезінформацією, забезпечуючи перевірку фактів та просвіту громадян.

Вивчення ролі мас-медіа у поширенні та протидії дезінформації є особливо актуальним у контексті сучасних викликів: від пандемії COVID-19 до повномасштабної війни в Україні, де інформаційна безпека стала невід'ємною складовою національної безпеки.

У сучасному інформаційному середовищі засоби масової інформації (ЗМІ) часто стають не лише джерелом перевірених новин, але й інструментом поширення дезінформації. Це зумовлено як технологічними особливостями комунікації, так і соціальними чинниками.

По-перше, характерною рисою мас-медіа є прагнення до сенсаційності. У гонитві за переглядами та «кліками» журналісти та редакції нерідко використовують клікбейтні заголовки, що викривлюють зміст новини та підштовхують аудиторію до хибних висновків. Подібний підхід формує у суспільства викривлене сприйняття подій і сприяє поширенню недостовірної інформації.

По-друге, сучасні інформаційні потоки характеризуються надзвичайною швидкістю поширення контенту. У ситуаціях кризового характеру (наприклад, пандемія COVID-19 або повномасштабна війна в Україні) медіа часто віддають перевагу швидкому поширенню повідомлення над ретельною перевіркою фактів. У результаті фейки та маніпуляції стають частиною інформаційного простору.

По-третє, вагому роль у поширенні дезінформації відіграють соціальні мережі, які формально також належать до сфери масових комунікацій. Алгоритми Facebook, YouTube чи TikTok віддають перевагу контенту з високим рівнем емоційності, незалежно від його правдивості.

Це створює сприятливий ґрунт для поширення чуток, теорій змови та пропагандистських меседжів [2].

Крім того, слід зазначити, що у деяких випадках ЗМІ свідомо стають інструментом дезінформаційних кампаній. Прикладом є російські державні телеканали та медіа-ресурси, які систематично поширюють неправдиві наративи з метою інформаційного впливу на суспільство. Такі практики відносяться вже не до випадкових помилок журналістів, а до цілеспрямованих інформаційних атак.

Отже, мас-медіа можуть виступати одним з основних каналів поширення дезінформації через поєднання комерційних інтересів, технологічних обмежень і політичних впливів.

Таблиця 1. Функції мас-медіа у поширенні та протидії дезінформації

Сфера впливу	**Приклади поширення дезінформації**	**Приклади протидії дезінформації**
Новинні матеріали	Клікбейтні заголовки, поспіх у публікаціях без перевірки фактів	Якісна журналістика, перевірка джерел, редакційні стандарти
Соціальні мережі	Алгоритми, що просувають емоційний та скандальний контент	Маркування сумнівної інформації, блокування фейкових акаунтів
Кризові ситуації	Фейки під час пандемії COVID-19, інформаційні атаки під час війни	Оперативне спростування неправдивих повідомлень
Міжнародна комунікація	Використання ЗМІ як інструменту державної пропаганди (російські медіа)	Платформа *EUvsDisinfo*, співпраця з технологічними компаніями
Освітня функція медіа	Відсутність роз'яснень, що підсилює вплив фейків	Фактчекінг-проєкти (*StopFake, VoxCheck*), медіаграмотність

Таким чином, аналіз функцій мас-медіа засвідчує, що вони водночас можуть виступати як каталізатор поширення дезінформації, так і ключовий інструмент її подолання. Представлена таблиця демонструє подвійність впливу медіа: від маніпуляцій та пропаганди до просвітницької діяльності та фактчекінгу. Це підтверджує необхідність усвідомленого підходу до споживання інформації та посилення відповідальності журналістської спільноти [3].

Масові комунікації займають ключове місце у формуванні суспільної думки, і їхня роль у поширенні та протидії дезінформації має подвійний характер. З одного боку, прагнення до сенсаційності, комерційні інтереси та алгоритми соціальних мереж створюють умови для поширення неправдивих повідомлень. З іншого боку, саме медіа здатні забезпечувати перевірку фактів, здійснювати просвітницьку діяльність і ставати бар'єром на шляху маніпуляцій.

Сучасний досвід свідчить, що протидія дезінформації потребує узгоджених зусиль журналістів, державних структур, міжнародних організацій та громадянського суспільства. Поєднання свободи слова з відповідальністю за зміст інформації є основною передумовою формування безпечного та стійкого інформаційного простору.

Список використаних джерел

1. Tasnim, S., Hossain, M. M., & Mazumder, H. (2022). The Role of Social Media in Health Misinformation and Its Impact on Public Health. PMC. https://pmc.ncbi.nlm.nih.gov/articles/PMC10551800/
2. Naeem, S. B., Bhatti, R., & Khan, A. (2022). Social Media News Use and COVID-19 Misinformation Engagement. JMIR. https://www.jmir.org/2022/9/e38944/
3. Cinelli, M., Quattrociocchi, W., Galeazzi, A., Valensise, C. M., Brugnoli, E., Schmidt, A. L., ... & Scala, A. (2021). A Comprehensive Analysis of COVID-19 Misinformation, Public Health, and Social Media. PMC. https://pmc.ncbi.nlm.nih.gov/articles/PMC11375383/

Андрій БУЗАРОВ
кандидат філософських наук,
докторант Інституту політичних і етнонаціональних досліджень
ім. І.Ф. Кураса НАН України,
buzarov.andrey@gmail.com

УКРАЇНА В КОНТУРАХ ОНОВЛЕНОЇ ЄВРОАТЛАНТИЧНОЇ СИСТЕМИ БЕЗПЕКИ

Незважаючи на певну неоднозначність позицій навіть серед найближчих союзників у євроатлантичному та європейському просторах, Україна у своїй зовнішньополітичній діяльності послідовно орієнтувалася на перевірених партнерів. Серед них ключове місце традиційно займають Сполучені Штати Америки, які, незалежно від партійної належності адміністрацій Білого дому, забезпечували вагому підтримку як у процесі модернізації Збройних сил України, так і через механізми макрофінансової допомоги. Важливу роль у зміцненні стійкості України відігравали міжнародні інституції, зокрема Міжнародний валютний фонд, який після 2014 року став одним із ключових інструментів стабілізації національної економіки. Значний внесок здійснювали й традиційні союзники України — насамперед держави Балтії, зокрема Литва, а також Велика Британія, що після 2020 року посилила свою регіональну активність у сфері безпеки та ініціювала низку двосторонніх і багатосторонніх форматів співробітництва. В умовах ускладнення міжнародного безпекового середовища окремі європейські країни — серед них Велика Британія, Франція та Польща — розпочали розробку власних регіональних моделей безпеки. Такі ініціативи були спрямовані на формування дієвих механізмів захисту від гібридних і екзистенційних викликів, що постають у сучасній анархічній міжнародній системі та зростаючій агресивності авторитарних режимів євразійського простору.

Наприклад, у 2020 році почала втілюватися ідея проєкту Міжмор'я як геополітичного зближення країн Центрально-Східної Європи, що географічно розташовані між Балтійським та Чорним морями. Формування Балто-Чорноморської підсистеми безпеки може посилити оборонну співпрацю між Україною, Польщею, країнами Балтії, Чехією, Словаччиною, а в перспективі з Туреччиною та Білоруссю. Така співпраця може концентруватися довкола спільних розробок нових зразків озброєнь, тим самим сприяючи прискоренню адаптації української армії до стандартів НАТО. Балто-Чорноморське зближення дозволило б Україні підсилити її міжнародну суб'єктність, свій геополітичний статус та уникнути міжнародно-правової маргіналізації [1].

Варто підкреслити, що стратегічне зближення України та Великої Британії було обумовлене взаємною відповідністю інтересів обох сторін. Для України це означало посилення безпекових гарантій та підтримку у протидії зовнішній агресії, а для Великої Британії — реалізацію власних стратегічних завдань у контексті зовнішньополітичної доктрини «Global Britain», спрямованої на розширення глобальної присутності та формування стійких партнерств у ключових регіонах Європи та світу. Такий курс дозволив Лондону не лише посилити свою роль у європейських безпекових процесах, а й утвердити статус важливого союзника Києва, здатного брати участь у формуванні нової архітектури регіональної та євроатлантичної безпеки.

З цього приводу українські вчені слушно зазначали, що в середовищі британської політичної топеліти концепції «глобальної Британії», прихильники якої вважають, що за рахунок можливостей «розв'язаних рук» (Брексіт і т. п.), а також умілого й своєчасного застосування дипломатичних та силових інструментів офіційному Лондону цілком до снаги ефективно виконувати функції Superpower. Попри нібито рішуче дистанціювання Британії від ЄС упродовж попередніх кількох років паростки парадигми «глобальної Британії» виразно простежуються навіть в Європі: йдеться про ініціативу офіційного Лондону щодо формування безпекового тріумвірату в складі Британії, Польщі та України. Станом на початок 2022 року це було – не повноцінне організаційне утворення, а лише символічний жест і риторичний

інструмент, утім, його далекосяжних намірів і перспектив тектонічних зрушень не варто ігнорувати, адже таким кроком Великобританія, по-перше, фактично поставила під сумнів функціональну ефективність НАТО, по-друге, запропонувала механізм розблокування патової ситуації із входженням до складу Північноатлантичного альянсу нових членів.» [2].

Проведений аналіз демонструє, що у зв'язку з високою ймовірністю військових конфронтацій — як у формі відкритих бойових дій, так і у площині гібридних загроз — держави по обидва боки глобального ідеологічного спектра, незалежно від того, чи йдеться про демократії чи авторитарні режими, змушені посилювати власний оборонно-безпековий потенціал. Одним із найбільш очевидних виявів цього процесу є системне зростання оборонних витрат, що поступово перетворюється на один із провідних трендів сучасних міжнародних відносин. Відповідно варто погодитися із дослідниками, які стверджують, що стагнація глобальних механізмів узгодження національних інтересів держав та зменшення керованості системою міжнародних відносин зумовили також зростання бажання та готовності держав до застосування сили. Про це свідчить, зокрема, значне нарощування військових видатків країн світу. Крім того, Китай і росія на офіційному рівні звинувачують США в несправедливому керуванні міжнародними процесами, скоєнні міжнародних злочинів і фактично відмовились діяти за встановленими США правилами [3].

Безперечно, саме Збройні Сили України стали вирішальним фактором у збереженні української державності та зірвали реалізацію російського плану швидкого захоплення країни (так званого «бліцкригу»). Вони забезпечили організований і результативний опір у перші дні повномасштабного вторгнення, спираючись на досвід, здобутий упродовж восьми років протидії гібридній агресії РФ.

Аналізуючи роль України в євроатлантичних процесах, можна виокремити щонайменше два стратегічні вектори, що сформувалися у відповідь на агресивну політику РФ. По-перше, повномасштабна війна зумовила якісне зближення України з євроатлантичними інституціями, насамперед із НАТО, що проявилося у розширенні військово-технічного співробітництва. Саме в цей період відбувся масштабний процес переозброєння української армії за стандартами Альянсу із врахуванням накопиченого нею унікального бойового досвіду. По-друге, центральним елементом нового формату стала платформа «Рамштайн», яка набула рис інституціоналізованого механізму колективної відповіді на російську агресію. У контексті сучасної анархічної міжнародної системи «Рамштайн» виконує функцію багатостороннього військово-політичного та логістичного партнерства, що відповідає принципам «комплексної взаємозалежності», концептуалізованим Джозефом Наєм і Робертом Кохейном у рамках неоліберальної інституціональної теорії міжнародних відносин. Отриманий досвід координації в межах цього формату може бути використаний у майбутньому для створення нових регіональних моделей безпеки, де роль України буде не лише вагомою, а й стратегічно незамінною.

Список використаних джерел

1. Kondratenko, O. (2020) 'Balto-Black Sea Commonwealth: origins and strategic opportunities for Ukraine', Bulletin of Taras Shevchenko National University of Kyiv. International Relations, (1), pp. 11–17. Available at: http://nbuv.gov.ua/UJRN/VKNU_mv_2020_1_4
2. Samchuk, Z., Levkulych, V., Shapoval, Yu., Chornyi, O. and Kovalevskyi, V. (2022) Modern political discourse on the problem of multipolar restructuring of the contemporary world. Kyiv: I.F. Kuras Institute of Political and Ethnic Studies, NAS of Ukraine.
3. Sytnyk, H. and Taran, Ye. (2024) 'Main trends of transformation of the international relations system (world order)', Bulletin of Taras Shevchenko National University of Kyiv. National Security, 2(2), pp. 5–12. doi:10.17721/3041-1912.2024/2-1/11

Ілля ТЯГУР
студент 2 курсу магістратури
ДВНЗ «Ужгородський національний університет»,
tiahur.illia@student.uzhnu.edu.ua

Ганна МЕЛЕГАНИЧ
кандидат політичних наук, доцент,
доцент кафедри міжнародних студій та суспільних комунікацій
ДВНЗ «Ужгородський національний університет»
hanna.melehanych@uzhnu.edu.ua

ЄВРОАТЛАНТИЧНА ІНТЕГРАЦІЯ УКРАЇНИ ЯК ФАКТОР ТРАНСФОРМАЦІЇ СИСТЕМИ ЄВРОПЕЙСЬКОЇ БЕЗПЕКИ

Проблематика забезпечення безпеки в сучасній Європі набуває особливої актуальності в умовах геополітичної нестабільності, спричиненої агресивною політикою росії. Традиційна архітектура європейської безпеки, сформована після завершення «холодної війни», виявилася неефективною перед новими викликами. У цьому контексті особливе значення має євроатлантична інтеграція України як чинник не лише зміцнення національної обороноздатності, а й переформатування всієї системи безпеки на континенті.

Мета дослідження – визначити вплив процесів євроатлантичної інтеграції України на трансформацію системи європейської безпеки, а також обґрунтувати стратегічну роль України в оновленій архітектурі безпеки.

Актуальність теми полягає в тому, що повномасштабна війна росії проти України зруйнувала стару модель європейської безпеки, базовану на домовленостях і дипломатичних гарантіях, і спричинила формування нової, колективної та ціннісно орієнтованої системи. Україна сьогодні виступає ключовим елементом цієї трансформації, захищаючи східні кордони євроатлантичного простору.

Наукова новизна полягає у визначенні євроатлантичної інтеграції України як динамічного фактора системних змін у безпековій архітектурі Європи, а не лише як політичного процесу наближення до НАТО. Уперше зроблено акцент на взаємозалежності між внутрішніми реформами сектору безпеки України та загальноєвропейськими процесами адаптації безпекової політики.

У процесі дослідження використано методи системного, порівняльного та інституційного аналізу, що дозволило простежити еволюцію політики НАТО щодо країн-партнерів та окреслити місце України в цій системі. Результати аналізу свідчать, що український досвід оборони проти російської агресії став каталізатором трансформації стратегічних підходів Альянсу. Відбувається посилення східного флангу НАТО, зміцнення оборонного потенціалу регіону Чорного моря, активізація співпраці з партнерами поза межами блоку. Україна інтегрується в оборонно-промислову, освітню та інформаційну складові безпеки НАТО, поступово досягаючи сумісності своїх Збройних сил зі структурами Альянсу. Значущим аспектом є також формування в Україні нової культури стратегічного мислення у сфері безпеки, що базується на принципах взаємодії з союзниками, прозорості оборонного планування та цивільного контролю над збройними силами. Це забезпечує поступове входження України в євроатлантичний безпековий простір не лише на інституційному, а й на ментальному рівні, створюючи передумови для стійкої адаптації до стандартів НАТО.

Висновки. Таким чином, євроатлантична інтеграція України сприяє переходу від постбіполярної моделі європейської безпеки до нової, багаторівневої системи, що ґрунтується на принципах спільної оборони, солідарності та демократичних цінностей. Це зумовлює формування якісно нового рівня транскордонного та міжнародного співробітництва, де Україна виступає не лише об’єктом, а й активним суб’єктом безпекових процесів у Європі.

Список використаних джерел

1. Gavin E.L. Hall. NATO And Ukraine: How Have We Gotten Here From 1991? Fair Observer. 2023y. URL: https://www.fairobserver.com/world-news/ukraine-news/nato-and-ukraine-how-have-we-gotten-here-from-1991/
2. Kuzio, T. Ukraine's NATO Path: Security Challenges and European Transformation. Journal of European Security Studies, 32(4), 245–261. 2023y.
3. Ministry of Foreign Affairs of Ukraine. Strategic Course toward NATO Membership. Kyiv.
4. NATO Annual Report 2023. Brussels: North Atlantic Treaty Organization. https://www.nato.int
5. Кручініна Оксана. Україна–НАТО: Проблеми та перспективи співпраці в умовах російсько- української війни. 2023р. URL: https://relint.vnu.edu.ua/index.php/relint/article/view/321/296
6. Тодоров І. Я. Євроатлантична інтеграція України. Історія та сучасність. Навчальний посібник. Ужгород. 2022р. ст. 117-125. URL: http://eurodev.uzhnu.edu.ua/images/files/2023_T.pdf

Данило ВЕРТАШ
студент
Дніпровський національний університет імені Олеся Гончара,
vertash@365.dnu.edu.ua

Юлія ВОЙТЕНКО
кандидат технічних наук, доцент
Дніпровський національний університет імені Олеся Гончара,
voitenko_y@365.dnu.edu.ua

ЗАХИСТ ЦИВІЛЬНОГО НАСЕЛЕННЯ УКРАЇНИ В УМОВАХ ВІЙНИ: СУЧАСНІ ВИКЛИКИ ТА ЕФЕКТИВНІ РІШЕННЯ

Повномасштабна війна в Україні сильно вплинула на всі сфери життя українців та поставила в складну ситуацію питання безпеки цивільного населення. За даними Моніторингової місії ООН з прав людини загинуло щонайменше 14 116 цивільних осіб, серед яких 733 дитини. Кількість поранених становить 36 481 особа, з них 2 285 — діти [1]. Очевидно, що жертв у реальності набагато більше, оскільки все випадки зафіксувати неможливо, але навіть ці цифри шокують. Гостро постає питання також фізичний та психічний стан населення – страх вибухів, смерті, невизначеності, нестабільності життя сильно впливають, що зменшують комфорт проживання в Україні. Проблема безпеки на сьогодні займає одну з ключових проблем, що потребують термінових заходів для мінімізації впливу на людей. Питання безпеки населення потребує комплексного рішення:

1. Попередження населення про небезпеки. В цьому напрямку було досягнуто гарних результатів та запропоновано ефективні рішення: основним засобом оповіщення залишаються сирени, паралельно з якими працюють державні додатки (Air Alert, eAlert, волонтерські карти), телеграм-канали, а за відсутності інтернету – SMS або Cell Broadcast. Основною проблему такої системи на зараз залишається ймовірність дезінформації [2].

2. Застосування БПЛА в широкому діапазоні функцій. Неможливо уявити сучасну війну без використання БПЛА у бойовому вигляді, проте вони здатні виконувати і гуманітарні місії та координувати дії - проводити розвідку, вивчати цивільну інфраструктуру, доставляти ліки та іншу допомогу [3], проводити демінінг, розробляти системи контрзаходів – збиття дронів перехоплювачами або коригування евуакуаційними коридорами [4].

3. Оптимізація укриттів та евакуаційних маршрутів. Використання ГІС, 3D-моделювання та оптимізаційних алгоритмів VGAE, RF, MILP, GA для розміщення укриттів, розробки маршрутів евакуації, оцінок доступності (G2SFCA) [5]. Також у 2024 році було створення та запущено функцію «Мапа укриттів» у Дії, що дозволяє обрати укриття та прокласти до нього найоптимальніший маршрут [6].

4. Створення мережі бригад медичної допомоги швидкого реагування. В умовах війни найважливішим параметром реагування є час, який здатна зменшити мережа мобільних бригад екстреної медичної допомоги, яка навчена за EMT-стандартами та SALT [7].

5. Впровадження системи психологічної допомоги. Війна дуже сильно впливає на психічний та, як наслідок, фізичний стан здоров'я людини. Цю проблему може вирішити MHPSS через цифрові інтервенції – мобільні додатки, чат-боти, телемедицину та онлайн-платформи, що дозволяють охопити ширшу аудиторію, зменшити навантаження на фахівців і надавати допомогу навіть у прифронтових зонах. В Україні впроваджено низку ініціатив – платформа «Tell Me», Aumora від UNEPA, U-RISE та FHI-360 за підтримки USAID [8].

6. Використання AI для прогнозування небезпеки та оцінки пошкоджень. Впровадження ШІ, особливо у БПЛА та супутники, показують ефективні результати для аналізу даних зі знімків, у моделюванні гуманітарних потреб та оптимізації розподілу ресурсів. Реалізувати

таку ідею можна через централізовані платформи прийому даних, моделі ML (ResNet50, ResNet101, YOLOv5 та VGG19) для оцінки шкоди та систем раннього прогнозування [9].

7. Громадська готовність і локальні ініціативи. Навчання першій медичній допомозі, правил поведінки під обстрілом, координація в умовах хаосу, дозволяє суттєво зменшити втрати серед цивільного населення. Для цього створюються навчальні центри, волонтерські об'єднання, що проводять тренінги, поширюють інформацію про дії та правила виживання під час атак.

8. Транскордонна співпраця та міжнародна допомога. Міжнародна координація в сучасних умовах війни залишається критичною для забезпеченнями ресурсами, обміну знаннями, наданням підтримки та забезпечення умов для прихистку населення, що виїжджає за кордон. Основними координаторами є організації OCHA, UNDP, WHO, ICRC, ЄС та НАТО, які створюють механізми реагування й платформи взаємодії із національними структурами [10].

Захист цивільного населення України під час війни потребує комплексного підходу, що поєднує технологічні, соціальні, психологічні та організаційні рішення, що здатні забезпечити ефективну безпеку, координацію та гуманітарну допомогу, слугуючи прикладом для інших країн у кризових умовах.

Список використаних джерел

1. Яновські, К., (2025). Втрати серед цивільного населення в Україні залишаються на тривожно високому рівні через постійне застосування зброї як ближнього, так і дальнього радіусу дії, яка руйнує життя людей по всій Україні — повідомляють спеціалісти ООН з прав людини [онлайн]. *Україна*. [Дата звернення 15 вересня 2025].
2. Kosheliuk, O. та Blahovirna, N., (2025). News in mobile air raid alert apps and media literacy in ukraine during the war time. *Media Literacy and Academic Research* [онлайн]. **8**(1), 178–193. [Дата звернення 28 вересня 2025]. Режим доступу: doi: 10.34135/mlar-25-01-09
3. Moroz, D., Shvachych, G., Moroz, B., Ievlanov, M. та Kabak, L., (2025). Концептуальна модель системи доставки медикаментів за допомогою безпілотних літальних апаратів. *COMPUTER-INTEGRATED TECHNOLOGIES: EDUCATION, SCIENCE, PRODUCTION* [онлайн]. (57), 120–127. [Дата звернення 5 жовтня 2025]. Режим доступу: doi: 10.36910/6775-2524-0560-2024-57-14
4. Gosselin-Malo, E., (2025). Interceptor drones are Europe's new hope for downing Russian Shaheds [онлайн]. *Defense News*. [Дата звернення 23 вересня 2025]. Режим доступу: https://www.defensenews.com/global/europe/2025/09/15/interceptor-drones-are-europes-new-hope-for-downing-russian-shaheds/
5. RE:Ukraine Shelters | balbek bureau's research project on developing a modern methodology for building air raid shelters — RE:ukraine [онлайн], (без дати). *RE:Ukraine*. [Дата звернення 5 жовтня 2025]. Режим доступу: https://www.reukraine.org/shelters-eng
6. Нова послуга в Дії: знаходьте найближче укриття в кілька кліків [онлайн], (2024). *Державні послуги онлайн | Дія*. [Дата звернення 5 жовтня 2025]. Режим доступу: https://diia.gov.ua/news/nova-posluga-v-diyi-znahodte-najblizhche-ukrittya-v-kilka-klikiv
7. *Головна - healthsol*. [Дата звернення 28 вересня 2025]. Режим доступу: https://healthsolutions.ngo/wp-content/uploads/2025/01/Modeli-roboty-mobilnykh-bryhad-v-Ukraini-v-umovakh-viyskovoi-ahresii-Kyiv-2024-Rezultaty-doslidzhennia.pdf
8. Supporting mental health and well-being in Ukraine [онлайн], (2024). *https://www.fhi360.org/*. [Дата звернення 5 жовтня 2025]. Режим доступу: https://www.fhi360.org/wp-content/uploads/2024/10/resource-mhpss-ukraine-fact-sheet.pdf
9. Artificial intelligence for better protection of civilians during urban warfare - lieber institute west point [онлайн], (2024). *Lieber Institute West Point*. [Дата звернення 5 жовтня 2025]. Режим доступу: https://lieber.westpoint.edu/artificial-intelligence-better-protection-civilians-urban-warfare/
10. United nations in ukraine [онлайн]. *UNHCR Ukraine*. [Дата звернення 2 жовтня 2025]. Режим доступу: https://www.unhcr.org/ua/en/united-nations-ukraine

Ігор ТОДОРОВ
доктор історичних наук, професор
професор кафедри міжнародних
студій та суспільних комунікацій
Ужгородський національний університет,
ihor.todorov@uzhnu.edu.ua

СУЧАСНІ БЕЗПЕКОВІ ВИКЛИКИ КРАЇНАМ ЦЕНТРАЛЬНО -СХІДНОЇ ЄВРОПИ В КОНТЕКСТІ ЛРУГОЇ КАДЕНЦІЇ ПРЕЗИДЕНТА США Д. ТРАМПА

В 2025 році США знову опинились під керівництвом Дональда Дж. Трампа, що відкриває новий етап трансформації трансатлантичної безпеки. Друга каденція Трампа супроводжується низкою політичних сигналів та практичних рішень, які можуть змінити баланс ризиків у Європі, зокрема у Центрально-Східному регіоні — Польщі, країнах Балтії, Чехії, Словаччині, Угорщині, Румунії та сусідніх державах. Ці держави опинилися в епіцентрі безпекових викликів, де поєднуються агресивна політика Росії, непевність щодо американських гарантій, залежність в енергетиці та вразливість до гібридних операцій. Вивчення впливу політики адміністрації Д.Трампа є необхідним для побудови надійних національних і колективних заходів стримування та адаптації.

В сучасних наукових дослідженнях можна виокремити кілька груп загроз для країн Центрально-Східної Європи: військові/конвенційні загрози на тлі російської агресії проти України [6], гібридні та інформаційні операції [1], енергетична вразливість і «зброя енергоресурсів» [2], економічні, політичні та соціальні ризики [7]. Втім поки нема робіт присвячених безпеці країн ЦСЄ кріз призму сучасної політики США.

Під час саміту НАТО в Гаазі в червені 2025 р. США підкреслювали підтримку Альянсу, зокрема — офіційні зустрічі демонстрували заяви щодо прихильності до Статті 5 Північноатлантичного договору, але на практиці адміністрація одночасно просувала підхід «поділу витрат» і добивалася значних підвищення внеску союзників. Спостерігалася тенденція до договірного підходу у відношенні до Росії у порівнянні з попередньою адміністрацією: зокрема — замороження введення нових санкцій у деяких випадках та прагнення до координації з ЄС перед діями, що може сповільнити швидку реакцію на агресивні кроки Москви. Це породжує занепокоєння у країнах ЦСЄ, котрі відчувають найбільший ризик від російської агресії [5]. Для країн південної Балтії та Польщі — які безпосередньо межують із РФ або її сателітами — це означає потребу в посиленні власних військових спроможностей. Збільшується стратегічна невизначеність щодо американської «мілітарної парасольки» в критичні моменти.

Політика щодо України — ключовий фактор регіональної безпеки. Якщо адміністрація США ускладнює або уповільнює введення нових санкцій проти РФ (або робить їх прив'язаними до європейських кроків), це може зменшити тиск на Москву і посилити її готовність до ескалації. Повідомлення про замороження нових санкцій 2025 року викликає занепокоєння серед партнерів, які спираються на санкції як інструмент стримування. Для України та її сусідів це означає необхідність готуватися до тривалої війни з обмеженими зовнішніми інструментами тиску — посилення ППО, логістики, оборонної індустрії, а також дипломатичної координації з ЄС.

Енергетична залежність від російських поставок залишається вразливістю для деяких країн ЦСЄ. У 2025 році питання енергетичної диверсифікації залишалось одним з ключови. При зміненій американській політиці, що більше орієнтується на умовні компроміси з РФ, країни ЦСЄ мають прискорити енергетичну диверсифікацію [3].

Росія продовжує практику гібридних операцій: порушення повітряного простору, напади на підводні кабелі, кібератаки, і використання енергетичних інструментів як зброї. Ці операції часто лежать нижче формального порогу, що викликає складності у швидкій колективній відповіді. Політична позиція країн ЦСЄ демонструє різні підходи до США і Росії: декотрі уряди (наприклад, уряди Угорщини та Словаччини) продовжують шукати тісніші економічні

зв’язки з Москвою, тоді як Польща і країни Балтії — консолідують позицію проти агресії. Адміністративні сигнали Вашингтона можуть стимулювати або послабити ці розбіжності [4].

Отже, друга каденція президента Д.Трампа створює для країн Центрально-Східної Європи як виклики, так і можливості. Навіть за офіційної риторики підтримки НАТО, операційні сигнали щодо «поділу витрат», уповільненої санкційної політики до Москви формують новий контекст стратегічної невизначеності. Країни регіону мають активізувати власні спроможності — військові, енергетичні, в кіберсфері та зміцнити регіональну координацію і зменшити ризики, пов’язані з можливими вибірковими діями з боку ключового трансатлантичного партнера. Водночас діалог з США лишається критично важливим. Однак ефективність майбутніх рішень залежатиме від поєднання зовнішніх гарантій і внутрішньої стійкості країн ЦСЄ.

Список використаних джерел

1. Cenusa D. Russia’s hybrid warfare on EU enlargement https://theloop.ecpr.eu/russias-hybrid-war-on-eu-enlargement/
2. Gritz A., Gas and energy security in Germany and central and eastern Europe, Energy Policy, 2024 https://ideas.repec.org/a/eee/enepol/v184y2024ics0301421523004706.html
3. From threat to opportunity: redefining energy security in Central and Eastern Europe https://ember-energy.org/latest-insights/from-threat-to-opportunity-redefining-energy-security-in-central-and-eastern-europe/
4. Tracking President Trump’s second-term Cabinet and appointees https://www.brookings.edu/articles/tracking-president-trumps-second-term-cabinet-and-appointees/
5. With freeze on new Russia sanctions, Trump abandons key Biden tactic https://www.washingtonpost.com/world/2025/09/19/trump-sanctions-russia-trade-putin/
6. Zięba R. (2024) Politics and Security of Central and Eastern Europe: Contemporary Challenges. Springer International Publishing, 353 p.
7. Лизун М., Ліщинський І., Віталішова К., Борсенкова К. Виклики регіональної безпеки для країн Центральної та Східної Європи // Журнал європейської економіки Західноукраїнський національний університет, Тернопіль. Том 24. № 1 (92). Січень–березень 2025. – С. 41-57.

Erzsébet MOLNÁR D.
PhD, associate professor
Ferenc Rakoczi II Transcarpathian Hungarian University,
molnar.d.erzsebet@kmf.org.ua

Orsolya MÁTÉ
International Relations III/1
II. Rákóczi Ferenc Transcarpathian Hungarian University

FINLAND'S SECURITY POLICY

Finland achieved EU membership in 1995 thanks to its long-standing policy of neutrality. Its unique security policy has traditionally been characterized by a flexible, pragmatic, and multidirectional approach. For a long time, the country sought to keep several options open at once, which was reflected in its debates on NATO and its gradual rapprochement with the alliance, as well as in its openness to dialogue with Russia.

One of the key elements of Finnish security policy is flexibility, which has enabled the country to build bilateral and multilateral defense cooperation simultaneously. Until February 2022, Finland actively participated in a number of defense partnerships, including within the EU, NATO, and Scandinavian cooperation frameworks. At the same time, Finnish decision-makers have always prioritized solutions that guarantee the greatest security, even outside of formal membership.

Historically, Finland has maintained more flexible relations with Russia than other Nordic countries, especially Sweden. Following the annexation of Crimea in 2014, Helsinki strongly supported EU sanctions against Russia, while at the same time seeking to maintain channels of communication with Moscow. This dual approach—loyalty to Western allies and maintaining pragmatic dialogue—was one of the main features of Finland's unique security policy identity until Russia's 2022 invasion of Ukraine, which fundamentally reshaped the country's strategic priorities.

Finland's characteristic flexibility in security policy can be seen as both a resource and a risk. On the one hand, this flexible approach allows the country to combine its defense cooperation in various ways, for example by establishing closer relations with the United States and Sweden, while retaining its own decision-making autonomy. This strategic openness also allows Finland to act as a reliable partner of the West and, at the same time, as a mediator between East and West.

On the other hand, this flexibility can also create uncertainty about the country's international position. There has long been debate among policymakers and analysts as to whether Finland should be seen as a European middle power, a strengthener of transatlantic relations, or rather as part of the Scandinavian security environment, where Sweden is the most important strategic partner.

However, Russia's 2022 invasion of Ukraine marked a turning point in this long-term search for balance. At that point, the Finnish leadership increasingly prioritized predictability and Western integration over its previous flexibility. The majority of political parties expressed support for NATO membership, which led to the official submission of a membership application in the summer of 2022.

All this raises new questions about Finland's future role in the international system. Although the country now clearly belongs to the military and political structures of the West, it is not yet clear how this will affect Finland's role as a mediator and "bridge builder" between East and West. The future will therefore show to what extent strategic predictability and alliance commitments will replace the flexibility that has prevailed until now.

Finland officially joined NATO on April 4, 2023, at an accession ceremony in Brussels. The ratification process was the fastest in NATO's history: within two months of the 2022 Madrid summit, 28 member states approved the accession of Finland and Sweden. Only Turkey and Hungary delayed for another seven months, and neither has ratified Sweden's membership to date.

Finland's previous security policy decisions facilitated its accession: it had participated in NATO's Partnership for Peace program since 1994, and its 2021 purchase of F-35 fighter jets also signaled its military compatibility and willingness to cooperate.

The decision to join NATO was made quickly after the outbreak of the Russian-Ukrainian war. Public opinion changed radically: within a few weeks, opposition turned to support, so it was not considered necessary to hold a referendum or organize a separate public consultation.

During the 2023 parliamentary elections, NATO membership was no longer a controversial issue, as there was broad consensus among parties and voters on the need for membership. Nevertheless, new questions will arise in the future, such as the presence of NATO troops in Finland and the role of nuclear weapons.

Membership will also lead to a significant increase in defense spending: although Finland already meets the NATO recommendation of 2% of GDP, the additional costs associated with the common budget and personnel assigned to NATO command are estimated at €70-100 million. According to a 2022 NATO survey, Finns are more than willing to increase defense spending. However, due to the austerity policy of the Orpo government, which took office in 2023, greater debate is expected in the future on the distribution of the state budget and the sustainability of defense spending.

Finland's current security strategy may not prove beneficial in the long term unless profound and concrete changes are made. Nordic and European Union cooperation has previously been seen as an alternative to NATO membership in Finnish security policy thinking.

The complexity of strategic decision-making stems from the fact that Finland must simultaneously take into account public opinion, its political relations, and its economic ties with both Russia and the European Union. As an EU member state, Finland cannot ignore any of these factors and must therefore rethink its foreign and security policy in order to align it with future decisions on the European security system.

Key words: NATO, EU, neutrality, multilateral, bilateral, invasion.

References

1. Amadae, S. M., Wass, H., Hentunen, M., Tukiainen, J., Weckman, A., & Laine, M. (2023). Top gear security: Finns' expectations for NATO membership (Policy Brief 1/2023). NATOpoll Research Project.
2. https://www.helsinki.fi/assets/drupal/2023-07/NATOpoll%20policy%20brief%201_2023%20English_6.7.2023.pdf
3. Brommesson, D. (2022). Finland's foreign and security policy: From bridge-building to the core of the West (UI Paper No. 5/2022). Swedish Institute of International Affairs.
4. https://www.ui.se/globalassets/ui.se-eng/publications/ui-publications/2022/ui-brief-no.-5-2022.pdf
5. Márton, A. (2013). Finland's security and defense policy changes from the end of the Cold War to present [Doctoral dissertation, Eötvös Loránd University]. Budapest.
6. https://www.academia.edu/81388573/Finland_s_security_and_defense_policy_changes_from_the_end_of_the_cold_war_to_present
7. Mattila, P. (2013). Finland's security solution in the future. United States Army War College.
8. https://apps.dtic.mil/sti/tr/pdf/ADA589427.pdf

DARCSI Karolina
II. Rákóczi Ferenc Kárpátaljai Magyar Egyetem
Történelem- és Társadalomtudományi
Tanszék adjunktusa és kutatója

HUBER Alex
III. évfolyamos
Nemzetközi kapcsolatok, társadalmi kommunikáció
és regionális tanulmányok szakos hallgató
II. Rákóczi Ferenc Kárpátaljai Magyar Egyetem

NÉMETORSZÁG BIZTONSÁGA

Németország biztonsága a 21. században összetett kérdés, amely magában foglalja a közbiztonság, a rendészet, valamint a társadalmi stabilitás fenntartását. A modern demokratikus állam nem támaszkodhat kizárólag a rendőrségi és hatósági eszközökre, hanem szüksége van a civil társadalom, a helyi közösségek és a magánbiztonsági szolgáltatások együttműködésére is. A közbiztonság megőrzése így nemcsak állami feladat, hanem közös társadalmi felelősség. Németország számára különösen fontos, hogy a rendészeti intézkedések, a polgári jogállam elvei és az emberi jogok tisztelete összhangban működjenek. A biztonság nem csupán a bűnözés visszaszorítását jelenti, hanem a polgárok mindennapi életének nyugalmát és biztonságérzetét is [1].

Bűnözési statisztikák Németország tartományaiban

Előfordultak pl:

Merénylet Mannheim belvárosában: egy autós a Paradeplatzon több embert elütött. A rendőrség megerősítette, hogy legalább egy ember meghalt, és többen súlyosan megsérültek. A helyszínen nagy erőkkel vonultak ki a hatóságok, és a gyanúsítottat őrizetbe vették.

Férfit késsel támadtak meg a berlini Holokauszt-emlékműnél

A hatóságok szerint a támadó eg 20 centis vadász késsel sebesítette meg az áldozatot, aki súlyos nyaki szúrásos sérülést szenvedett, sürgős műtéten esett át, és átmenetileg mesterséges kómába helyezték.

A támadás helyszínének közelében letartóztattak egy 19 éves szíriai menedékkérőt. A gyanúsított véres kézzel közelítette meg a rendőröket, és a hatóságok szerint azzal a szándékkal tervezte a támadást, hogy "zsidókat öljön".

Ezek az esetek rámutatnak arra, hogy a német közbiztonság romlása részben összefüggésbe hozható a migrációval. A 2015 óta tartó bevándorlási hullám következtében több, különböző hátterű és kultúrájú ember érkezett az országba, ami növelte a társadalmi feszültségeket. Egyes menedékkérők és bevándorlók körében a radikalizálódás, illetve a bűnelkövetés aránya magasabb, ami fokozott terhet ró a rendvédelmi szervekre. Mindez hozzájárult ahhoz, hogy a lakosság egy része bizonytalanságot érez, és gyengülni látszik a biztonságérzet Németországban [2].

Bűnözési statisztikák Németország tartományaiban
A német bűnügyi statisztikákat a Bundeskriminalamt publikálja minden évben

Összesen	Nem német lakosság aránya (%)	Rögzített esetek	Esetek száma	Minden hanyadik lakosra jut egy eset?	Nem német gyanúsítottak aránya (%)
Baden-Württemberg	11280257	17,8	550008	21	42,9
Bayern	13369393	15,5	619089	22	47,0

Berlin	3755251	22,2	519822	7	47,4
Brandenburg	2573135	7	170204	15	36,5
Bremen	684864	21	79713	9	43,5
Hamburg	1892122	19,2	211239	9	47,4
Hessen	6391360	18,7	368579	17	47,3
Mecklenburg-Vorpommern	1628378	6,5	106559	15	19,3
Niedersachsen 11,8	8140242	11,8	523996	16	29,9
Nordrhein-Westfalen	18139116	15,6	1366601	13	35,0
Rheinland-Pfalz	4159150	13,6	241779	17	33,8
Saarland	992666	14	68139	15	36,3
Sachsen	4086152	7,3	267312	15	35,2
Sachsen-Anhalt	2186643	7,4	178450	12	22,6
Schleswig-Holstein	2953270	10,2	221183	13	30,4
Thüringen	2126846	7,6	135911	16	22,8
Bundesrepublik Deutschland	84358845	14,6	5628584	15	37,4

A Nancy Faeser (SPD) szövetségi belügyminiszter be mutatta a 2023. évi német rendőrségi bűnügyi statisztikákat, amelyből kiderül, hogy jelentősen nőtt a lopások és az erőszakos bűncselekmények száma, valamint a külföldi és fiatal gyanúsítottak száma Németországban az elmúlt évben. Németországban regisztrált bűncselekmények száma 2016 óta a legmagasabb szintet érte el, a hatóságok összesen 5,941 millió bűncselekményt dolgoztak fel a szövetségi rendőrség 2023-as bűnügyi statisztikája szerint. Ez 5,5%-os növekedést jelent az előző évhez képest és 9,3%-os emelkedést a 2019-es, a COVID19 pandémiát megelőző évhez képest. Különösen meredek emelkedést mutatnak az adatok az erőszakos bűncselekmények és a lopások kapcsán [3].

A statisztikák szerint a növekedés részben a migrációval is összefügg, hiszen a bevándorlók és menedékkérők aránya az erőszakos és lopásos bűncselekmények gyanúsítottjai között az elmúlt években jelentősen megnőtt. Továbbá a fiatal, 18–25 éves korosztály körében is magas a bűnözési arány, ami szintén hozzájárul a rendőrségre nehezedő terhekhez. A regionális különbségek is jól láthatók: bizonyos tartományokban – például Berlinben és Baden-Württembergben – kiemelkedően magas az erőszakos cselekmények száma. Ezek az adatok azt jelzik, hogy a közbiztonság fenntartása egyre komplexebb feladat, amely egyszerre igényli a hatóságok, a helyi közösségek és a polgárok együttműködését [4].

Németország biztonsági helyzete

1. Statisztikai áttekintés

A 2023-as német rendőrségi statisztikák szerint a regisztrált bűncselekmények száma 5,9 millió volt, ami 5,5 %-os növekedést jelent az előző évhez képest. Különösen az erőszakos bűncselekmények mutattak meredek emelkedést: 214 099 esetet regisztráltak, ami 8,6 %-kal több, mint 2022-ben. A lopások, rablások és súlyos testi sértések száma is jelentősen emelkedett.

2. Okok és társadalmi tényezők

A statisztikák szerint a gyanúsítottak között nőtt a külföldi állampolgárok és a fiatal, 18–25 év közötti elkövetők aránya. A migráció kérdésköre emiatt gyakran kerül előtérbe a közbiztonsági vitákban. Az ifo Intézet elemzése szerint ugyanakkor a bevándorlás és a bűnözési ráta között nincs közvetlen ok-okozati kapcsolat: a magasabb bűnözési arány inkább a városias térségekhez köthető, ahol a bevándorlók nagyobb számban élnek [5].

3. Politikai radikalizmus és szélsőséges fenyegetések

2023-ban a politikailag motivált bűncselekmények száma is rekordot döntött: 60 028 esetet regisztráltak, amelyből 28 945 jobboldali indíttatású volt. Ezek közül 1 270 tartalmazott erőszakos cselekményt. A szélsőséges erők térnyerése a belső biztonság egyik legfontosabb kihívásává vált Németországban [6].

4. Kibervédelem és kritikus infrastruktúrák

A bűnözés mellett egyre jelentősebbek a kibertámadások és a kritikus infrastruktúrák elleni hibrid fenyegetések. A német kormány új stratégiát dolgozott ki a hálózatok és az energiaellátás védelmére, azonban az ágazat szereplői szerint a túlzott bürokrácia lassíthatja az energiaátmenetet.

5. Megoldási irányok

A német nemzeti biztonsági stratégia a védelem erősítésére több kulcslépést javasol: a rendőrség és a bűnüldözés modernizációját, a kibervédelmi képességek bővítését, a társadalmi kohézió és integráció támogatását, valamint a kritikus infrastruktúrák védelmét. Emellett a szélsőséges ideológiák elleni fellépés, a fiatalok radikalizációjának megelőzése és az energiabiztonság növelése is kiemelt feladatként szerepel [7].

Felhasznált irodalom

1. https://nemetorszagi-magyarok.de/infok/bunozesi-adatok-tartomanyonkent (25.09.23)
2. https://nemetorszagi-magyarok.de/infok/bunozesi-adatok-tartomanyonkent (25.09.23)
3. https://magyarnemetintezet.hu/rovid-hir/novekszik-a-buncselekmenyek-szama-nemetorszagban
4. https://nemetorszagi-magyarok.de/infok/bunozesi-adatok-tartomanyonkent (25.09.23)
5. https://www.bka.de/EN/CurrentInformation/Statistics/PoliceCrimeStatistics/2023/pcs2023.html?utm_source=chatgpt.com
6. https://www.ifo.de/en/press-release/2025-02-18/more-foreigners-do-not-increase-germanys-crime-rate?utm_source=chatgpt.com
7. https://www.cleanenergywire.org/news/germanys-cyber-defence-plans-risk-slowing-energy-transition-utilities-warn?utm_source=chatgpt.com
8. https://www.nationalesicherheitsstrategie.de/National-Security-Strategy-EN.pdf?utm_source=chatgpt.com (25.10.01)

CSERNICSKO Viktória
Nemzetközi kapcsolatok és regionális tanulmányok
II. évfolyam
Rákóczi Ferenc Kárpátaljai Magyar Egyetem
csernicsko.viktoria.bl22an@kmf.org.ua

DANCS György
docens
Rákóczi Ferenc Kárpátaljai Magyar Egyetem
dancs.gyorgy@kmf.org.ua

A HATALMI EGYENSÚLYTÓL A KOLLEKTÍV KÖZBIZTONSÁGIG

A nemzetközi biztonság fogalmát a 20. század közepétől hosszú ideig a realista iskola uralta, amely a nemzetközi rendszert anarchikusnak, a biztonságot pedig elsősorban az államok közötti hatalmi egyensúly zéróösszegű harcának tekintette. A tézisben megfogalmazott szemlélet ezzel szemben azt a jelentős paradigmaváltást tükrözi, amely az 1970-es évektől erősödött meg. A 21. századi nemzetközi együttműködésben a „biztonság" nem csupán a fenyegetések hiányát jelöli, hanem olyan többdimenziós erőforrást és közjavak-szerű koordinációs keretet, amely bizalmat épít, csökkenti a tranzakciós költségeket, és stabil elvárásokat alakít ki az államok, szervezetek, vállalatok és civil szereplők között (Baldwin, 1997; Keohane & Nye, 1977).

A biztonság ezért nem az együttműködés ellenpontja, hanem egyszerre előfeltétele és terméke. Ha a kölcsönös függés biztonsági garanciák nélkül marad, sérülékenységként jelenik meg; ha viszont intézményesen beágyazott, a kollektív cselekvés motorjává válik (Axelrod, 1984). A komplex interdependencia világa sokcsatornás kapcsolatrendszert feltételez, ahol a katonai erő nem mindenütt a domináns valuta (Keohane & Nye , 1977). Ilyen környezetben a kiszámítható biztonsági rend az ismételt interakciók logikáját erősíti: a felek hosszabb időhorizonton mérlegelnek, és érdemesebbé válik a kölcsönösség fenntartása, mint a rövid távú haszonért elkövetett csalás (Axelrod, 1984; Schelling , 1960). A fegyverellenőrzési rezsimek, a határigazgatási együttműködés vagy a kockázat-megismerési rendszerek nem pusztán technikai protokollok: hitelességi intézmények, amelyek a verifikáció és az átláthatóság révén mérsékelik a bizonytalanságot (Kydd , 2005).

A biztonság horizontjának kiterjesztése ugyanakkor nyelvi-politikai aktus is. A koppenhágai iskola rámutatott, hogy a „biztonságiasítás" (securitization) folyamatában gazdasági, környezeti, egészségügyi vagy technológiai problémák is „biztonsági kérdéssé" emelkedhetnek, ha a diskurzus és a közösségi eljárások úgy keretezik azokat (Buzan et al., 1998). A túlzott szekuritizáció kockázata ugyanakkor valós: ha minden kérdés „rendkívüli fenyegetéssé" válik, beszűkül a deliberáció tere, és sérülhet a demokratikus kontroll (Baldwin , 1997). A határon átnyúló együttműködés konkrét terepein a biztonság tipikusan határokon átívelő közjószág, amelynél a „leggyengébb láncszem" elve érvényesül. A közös standardok, az adatmegosztás és az interoperabilitás hálózati externáliákat hoznak létre, a normák és szabványok transznacionális terjedését pedig gyakran episztemikus közösségek – szakértői hálózatok – viszik végbe (Haas, 1992). Aki a biztonsági információmegosztásban megbízható és kiszámítható, az más területeken is könnyebben talál partnert; a reputáció a kooperatív egyensúlyok „láthatatlan biztosítéka" (Russett & Oneal, 2001).

Mindez nemcsak intézményi kérdés, hanem szociálpszichológiai alapokon is nyugszik. A bizalom hiánya információs aszimmetriákat és önbeteljesítő bizalmatlanság-spirálokat kelt: a másik fél szándékait hajlamosak vagyunk a legrosszabb olvasatban értelmezni (Kydd , 2005). Ezzel szemben az empatikus perspektíva-felvétel – amely Carl Rogers meghatározásában a „mintha" feltétel, azaz a másik világának átélésére tett kísérlet saját nézőpontunk elvesztése nélkül – képes csökkenteni a félreértéseket és az ellenséges attribúciót (Rogers , 1980, p. 140). Kollektív szinten ez az „ontológiai biztonság" érzetéhez járul hozzá: stabil identitás-narratívához, amelyben az államok értelmezik önmagukat és a másik viselkedését, mérsékelve a klasszikus biztonsági dilemmát (Mitzen , 2006). Ha a stratégiai kiegyensúlyozás sikerül, a biztonság nem zéróösszegű erőforrásként, hanem pozitív számú, megosztható közjószágként működik (Buzan et al., 1998; Baldwin, 1997). A tapasztalat azt mutatja, hogy a tartós nemzetközi rend alapja a megbízható ígéret, és ennek legjobb garanciája a

szabályokba öntött, reputációval megerősített és empatikus megértéssel áthatott biztonsági architektúra (Keohane & Nye, 1977; Kydd, 2005; Rogers, 1980; Mitzen, 2006).

A nemzetközi biztonság fogalmában bekövetkezett paradigma-váltás elszakadt a 20. századot uraló realista, anarchikus és zéróösszegű hatalmi egyensúly felfogásától. A 21. század biztonsága többdimenziós erőforrásként és közjószágként értelmezhető , amely a komplex interdependencia (Keohane & Nye, 1977) talaján, az ismételt interakciók logikája (Axelrod, 1984; Schelling, 1960) révén, intézményesen beágyazva termelődik. Az együttműködő biztonsági rendszerek hitelességi intézményeken (verifikáció) és a megbízhatóságon (reputáció) keresztül csökkentik a bizonytalanságot (Kydd, 2005; Russett & Oneal, 2001), miközben a biztonságiasítás (Buzan et al., 1998) kiterjeszti a biztonság hatókörét a nem katonai szektorokra. A tartós együttműködés legmélyebb garanciája azonban a szociálpszichológiai síkon valósul meg: az empatikus perspektíva-felvétel (Rogers, 1980, p. 140) és az ontológiai biztonság (Mitzen, 2006) révén kialakuló stabil identitás-narratíva, mely képes mérsékelni a klasszikus biztonsági dilemma negatív spiráljait. A stabil nemzetközi rend alapja egy olyan biztonsági architektúra, amely a bizalomra, a szabályokra és az empatikus megértésre épít.

A nemzetközi kapcsolatok kortárs biztonsági teóriái egyértelműen a hatalompolitikai megközelítés meghaladására mutatnak rá. A stabilitás kulcsa ma már nem az erőfölényben rejlik, hanem a kölcsönös előnyökön alapuló, szerződésekkel és intézményekkel megerősített hálózatokban. Az államok közötti tartós együttélés és együttműködés fenntartásához a szabályokhoz való következetes ragaszkodás, a bizalmi struktúrák folyamatos fejlesztése, valamint az emberi tényezők, mint az empátia tudatos integrálása szükséges, bizonyítva, hogy a hatékony nemzetközi rend elválaszthatatlan a szereplők normatív elkötelezettségétől.

Felhasznált irodalom

1. Axelrod, R. (1984) The Evolution of Cooperation. New York: Basic Books.
2. Baldwin, D. A. (1997) ‘The concept of security’, Review of International Studies, 23(1), pp. 5–26.
3. Buzan, B., Wæver, O. and de Wilde, J. (1998) Security: A New Framework for Analysis. Boulder, CO: Lynne Rienner.
4. Haas, P. M. (1992) ‘Introduction: Epistemic communities and international policy coordination’, International Organization, 46(1), pp. 1–35.
5. Keohane, R. O. and Nye, J. S. (1977) Power and Interdependence: World Politics in Transition. Boston: Little, Brown. [Használt kiadás: 2012, 4th ed., New York: Longman.]
6. Kydd, A. H. (2005) Trust and Mistrust in International Relations. Princeton, NJ: Princeton University Press.
7. Mitzen, J. (2006) ‘Ontological security in world politics: State identity and the security dilemma’, European Journal of International Relations, 12(3), pp. 341–370.
8. Rogers, C. R. (1980) ‘Empathic: An unappreciated way of being’, in Rogers, C. R. A Way of Being. Boston: Houghton Mifflin, p. 140. — Az empátia „as-if” („mintha”) feltételének klasszikus meghatározása, a hivatkozott részlet a 140. oldalon található.
9. Russett, B. and Oneal, J. R. (2001) Triangulating Peace: Democracy, Interdependence, and International Organizations. New York: W.W. Norton.
10. Schelling, T. C. (1960) The Strategy of Conflict. Cambridge, MA: Harvard University Press.

Ганна МЕЛЕГАНИЧ
кандидат політичних наук, доцент,
доцент кафедри міжнародних студій та суспільних комунікацій
директорка Центру сталого розвитку
ДВНЗ «Ужгородський національний університет»
hanna.melehanych@uzhnu.edu.ua

ВИКОНАННЯ УКРАЇНОЮ РЕЗОЛЮЦІЇ РАДИ БЕЗПЕКИ ООН №1325 «ЖІНКИ, МИР, БЕЗПЕКА»

Двадцять пять років тому вперше на міжнарожному рівні, а саме Організацією Обєднаних Націй було прийнято документ, який офіційно визнав важливу роль жінок у питаннях миру, безпеки та врегулювання конфліктів. Цей документ називається Резолюція Ради Безпеки ООН №1325 «Жінки, мир, безпека» і був ухвалений 31 жовтня 2000 року. Резолюція закликає до забезпечення рівної участі жінок у процесах прийняття рішень, захисту їхніх прав під час конфліктів та врахування гендерних аспектів у миротворчих зусиллях. І хоча Рада Безпеки ухвалила з того часу вже десять резолюцій, які містять конкретні зобов'язання для держав та системи ООН, але саме та яка під номером 1325 є провідною з резолюцій щодо жінок, миру та безпеки.Значення цієї Резолюції насамперед було важливе для тих країн, які мали чи мають військові конфлікти, але з огляду на те, що згідно Статуту ООН Рада Безпеки ухвалює рішення, обов'язкові для всіх країн, то імплементацію у національне законодавство почали спочатку робити країни ЄС: першою стала Данія у 2005 році, а станом на кінець 2024 року таких країн було 114 [1].

Україна була першою країною, яка перебуваючи у війському конфлікті прийняла Національний план дій 1325 (далі -НПД) у 2016 році. Розпорядженням Кабінету Міністрів України було затверджено Національний план дій з виконання резолюції Ради Безпеки ООН 1325 «Жінки, мир, безпека» на період до 2020 року [3]. Тоді цей документ був більше номінальним, хоча вже передбачаво рганізацію роботи міжвідомчих координаційних рад з питань виконання резолюції Ради Безпеки ООН 1325 «Жінки, мир, безпека» та поклав відповідальність за виконання на Міністерство соціальної політики. Це був перший крок до системної імплементації порядку денного «Жінки, мир, безпека» в Україні. Серед результатів – допуск жінок сержантського складу до бойових посад, відкриття військових ліцеїв для дівчат, зміни до законодавства про рівні можливості у військовій службі. Також почалося проведення освітніх кампанії, тренінгів для держслужбовців та покращено систему допомоги жінкам, які постраждали внаслідок конфлікту. Проте системна робота по резолюції «Жінки, мир, безпека» почала виконуватися низкою суб'єктів для різних цілей пізніше після прийняття вже другого Плану дій, до розробки якого вже були долучені й представники громадянського суспільства. Так, у 2020 році було ухвалено другий Національний план дій, який вже деталізував стратегічні та операційні цілі реалізації порядку денного «Жінки, мир, безпека» для України. У документі була визначена система індикаторів для оцінки прогресу, а також механізми міжвідомчої взаємодії. Значну роль почали відігравати не лише загальноукраїнські громадські організації, але й органи місцевого самоврядування та міжвідомча взаємодія. Початок повномасштабної війни у 2022 році повернув увагу багатьох до НПД і він був оперативно оновлений для врахування нових викликів в умовах воєнного часу. Було додано нові цільові групи та нових виконавців, нові напрямки діяльності та інтеграцію міжнародних стандарів й документів в цій сфері.

Зміст самої Резолюції та НПД в загальному визначає, що основні стратегічні цілі, а відтак вже й завдання й заходи спрямовані на: забезпечення повної та рівноправної участі жінок і чоловіків у прийнятті рішень на всіх рівнях, у тому числі в мирних переговорах, діяльності щодо встановлення миру, реінтеграції та примирення; запобігання насильству за ознакою статі, у тому числі шляхом притягнення до відповідальності за порушення міжнародного права; підтримка мирних ініціатив та процесів розв'язання конфліктів; захист прав і врахування потреб постраждалих в умовах конфліктів і після їх завершення, зокрема захист від різних форм насильства та переслідування; врахування особливих потреб жінок і дівчат, у тому числі вразливих категорій (зокрема біженців, внутрішньо переміщених осіб, жінок, які

постраждали від насильства за ознакою статі та сексуального насильства, пов'язаного з конфліктом), а також жінок-комбатанток, жінок-ветеранок під час надання послуг у сфері охорони здоров'я, психологічної та гуманітарної допомоги [4].

З огляду на те, що один з принципів діяльності ООН «Нікого не залишити осторонь», то очевидно, що глобальний документ та національний мали мати продовження на локальному рівні, щоб краще забезпечити його виконання. Саме тому в Україні кожна область після початку повномасштабного вторгнення розробила чи оновила свої обласні плани, адаптуючи національні цілі й завдання до конкретного локального контексту: безпекових викликів, демографії, потреб ВПО, наявних ресурсів тощо. Плани стали більш практичними: включили цивільний захист, роботу з ВПО, підтримку жінок-військових. В деяких областях навіть було передбачено фінансування з обласного бюджету (проте часто й без суми – у межах наявних програм), бюджети територіальних громад, державний бюджет (опосередковано – через соцпрограми/МВС/Мінветеранів) та за рахунок міжнародних та донорських організацій.

Аналізуючи вже сам процес виконання обласних планів дій, то варто зазначити, що важливу роль у цьому процесі відіграли саме останні, які підтримували й підримують локальні ініціативи на місцях. Саме це сприяло й активній міжвідомчій співпраця та активній включеності представників громадянського суспільства, адже за ініціативи та підтримки зокрема міжнародних та донорських організацій було утворено обласні коаліції – 1325. Діяльність цих коаліцій спрямована на всі види завдань НПД з огляду на їх актуальність в регіонах. Так, вони беруть участь у розробці та впровадженні регіональних планів дій (це можуть бути не лише обласні, а й місцеві на рівні громади), вони сприять налагодженню діалогу між органами влади, силовими структурами та організаціями громадянського суспільства, вони моніторять та самі беруть на себе співвідповідальність за виконання обласних планів дій, а також загалом виносять на порядок денний в регоінах питання ідей Резолюції 1325. Чисельний та якісний склад в кожній області може різнитися. Станом на 2025 рік найбільш чисельною є Коаліція «Одещина 1325», що створена у жовтні 2022 і об'єднує 72 учасниці та учасників. А найменш чисельною є коаліція «Миколаївщина 1325» створена 10 грудня 2024 року і яка нараховує 15 учасниць [2]. Проте незалежно від кількості людей в кожній з коаліцій, які створені по Україні до них ввходять представники чи представниці державних структур, громадського сектору та сектору безпеки і оборони. Така міжвідомча співпраця в рамках коаліцій створює майданчик для діалогу та інтеграції зусиль задля ефективного реагування на виклики безпеки, потреби постраждалих, інтеграцію ВПО та забезпечення участі жінок у прийнятті рішень.

Підсумовуючи варрто зазнчачити, що подальша координація дій та цілеспрямована робота на виконання Резолюції Ради Безпеки ООН 1325 «Жінки, мир, безпека» в Україні сприятиме запобіганню конфліктам і насильству; захисту жінок і дівчат і їхніх прав людини; повна, рівна та змістовна участь жінок у забезпеченні миру та безпеки; а також гендерно-чутлива допомога та відновлення.

Список використаних джерел:

1.Women's International League for Peace and Freedom (WILPF). 2016. *National Action Plans: Localising Implementation of UNSCR 1325*. Режим доступу: https://www.wilpf.org/national-action-plans-localising-implementation-of-unscr-1325/ [дата звернення 20.10.2025].

2.1325 Ukraine. n.d. *Коаліції в регіонах*. Режим доступу: https://1325ukraine.org.ua/koalicziyi/ [дата звернення 20.10.2025].

3.Верховна Рада України. 2016. *Про затвердження Національного плану дій з виконання Резолюції Ради Безпеки ООН 1325 "Жінки, мир, безпека" (2016-2020 роки): Закон України № 113/2016-РП*. 24 Режим доступу: https://zakon.rada.gov.ua/laws/show/113-2016-%D1%80 [дата звернення 20.10.2025].

4.Верховна Рада України. 2020. *Про затвердження Національного плану дій з виконання Резолюції Ради Безпеки ООН 1325 "Жінки, мир, безпека" на період до 2025 року: Розпорядження Кабінету Міністрів України № 1544-р*. 28 Режим доступу: https://zakon.rada.gov.ua/laws/show/1544-2020-%D1%80#Text [дата звернення 20.10.2025].

ІСТОРИЧНІ, КУЛЬТУРНІ ТА ФІЛОСОФСЬКІ АСПЕКТИ БЕЗПЕКИ В ПРИКОРДОННИХ РЕГІОНАХ

HISTORICAL, CULTURAL, AND PHILOSOPHICAL ASPECTS OF SECURITY IN BORDER REGIONS

A BIZTONSÁG TÖRTÉNELMI, KULTURÁLIS ÉS FILOZÓFIAI ASPEKTUSAI A HATÁR MENTI TERÜLETEKEN

Róbert VARGA
PhD, senior lecturer at the Department of History and Social Sciences
Ferenc Rákóczi II Transcarpathian Hungarian University

SECURITY CHALLENGES OF UNG COUNTY IN THE CONTEXT OF CROSS-BORDER ESPIONAGE, 1914 – 1915.

Abstract. The study aims to explore the security challenges of Ung County during the First World War in the context of cross-border espionage and intelligence operations. The research focuses on the activities of the Royal Hungarian Gendarmerie and the Uzhorod Municipal Police, both of which played a crucial role between 1914 and 1915 in maintaining internal security in the northeastern counties of the Kingdom of Hungary that were declared operational military zones, including Ung County itself.

The primary objective of the study was to present, on the basis of archival sources (notably the materials of Fonds 4 and 7 of the State Archives of the Transcarpathian Region) and contemporary press reports, how the gendarmerie and police organized counter-espionage operations, cooperated with the military, and applied various methods to identify and detain suspicious or hostile individuals. Furthermore, the study examines how the introduction of military administration and the expansion of law enforcement powers following the outbreak of war affected the everyday life of the civilian population and led, in several instances, to abuses committed in the name of state security.

The research methodology is based on the content analysis of archival documents, the reconstruction of specific case studies, and the historical interpretation of the security-political context. The study's scientific novelty lies in its comprehensive presentation of Ung County's counter-espionage experience, interpreted through the lens of local social and ethnic relations, thereby contributing to a deeper understanding of the First World War security history of present-day Transcarpathia.

The findings reveal that in the border regions—particularly in districts inhabited predominantly by Ruthenian populations—state distrust and suspicion were markedly intensified, frequently resulting in unfounded accusations, internments, and police excesses. The study also demonstrates that the weaknesses of the counter-espionage apparatus, combined with the ethnic heterogeneity of the frontier zone, created a new form of security threat that the central authorities were unable to manage effectively.

Keywords: war, spies, counter-espionage, Ung County, army, gendarmerie, police, abuses.

References

1. Kárpátaljai Területi Állami Levéltár. 4. fond (Ung vármegye főispánjának az iratai), 1. opisz, 691, 692, 694, 721, 723, 737. ügyiratok.
2. Kárpátaljai Területi Állami Levéltár. 7. fond (Ung vármegye alispánjának az iratai), 1. opisz, 2705, 2708, 2717. ügyiratok.
3. Asztalos Aladár (2000). Kémek az első világháborúban. Annó Kiadó
4. Boia, Lucian (2015). Vesztesek és győztesek. Az első világháború újraértelmezése. Csere Kiadó. Budapest
5. Clark, Christopher (2015). Alvajárók. Hogyan menetelt Európa 1914-ben a háború felé. Park Könyvkiadó, Budapest
6. Csapó Csaba (1990). A magyar királyi csendőrség története 1881–1914. Pannónia Kiadó. Budapest
7. Diószegi István (2001). Az Osztrák–Magyar Monarchia külpolitikája 1867–1918. Vince Kiadó. Budapest,
8. Dobai Péter (1985). A birodalom ezredese. Magvető Kiadó. Budapest
9. Hajdu Tibor–Pollmann Ferenc (2014). A régi Magyarország utolsó háborúja 1914–1918. Osiris. Kiadó. Budapest
10. Piekalkiewicz, Janusz (1997). A kémkedés világtörténete I-II. Zrínyi katonai kiadó. Budapest
11. Parádi József (1999). A magyar rendvédelem története. Budapest
12. Shipman, Pat (2008). Mata Hari. Budapest
13. Szijj Jolán (főszerk.) (1996). Magyarország az első világháborúban. Petit Real Kiadó. Budapest

SZAMBOROVSZKYNÉ NAGY Ibolya
PhD, a történelemtudományok kandidátusa, docens
Történelem és Társadalomtudományi Tanszék
II. Rákóczi Ferenc Kárpátaljai Magyar Egyetem
szamborovszkyne.nagy.ibolya@kmf.org.ua

KÖZÖSSÉG A LÉTBIZTONSÁG PEREMÉRE TOLVA: A NAGYBEREGI EGYHÁZKÖZSÉG 1944 ÉS 1948 KÖZÖTT

A kutatás célja, hogy történeti szempontból feltárja, s végig vezesse hogyan változtatta meg a szovjet csapatok térfoglalása következtében felállt Kárpátontúli Ukrajna átmeneti állama 1944–1946 januárja között, majd a Szovjetunió államhatalma Nagybereg község református sainak évszázados rendszerű működő közösségi létét. A téma problematikája abban rejlik, hogy bár immár több mint három évtizede széthullott a szovjet birodalom, azonban a kis közösségekre gyakorolt pusztító hatásainak feltárása csak részlegesen jelenik meg történeti kutatások szintjén. A cikk célkitűzéseinek megfogalmazása (a feladat kitűzése). Kutatásunkban a nagyberegi egyházközség történetének egy meghatározott szeletét mutatjuk be 1944 és 1948 közötti időszakban. Ebből kifolyólag – többek között – a következő kérdésekre kerestük a választ:

a) Milyen mélyreható változások kezdődtek el a községben 1944. október 26-án?

b) Hogyan hatott a közösségre az ún. háromnapos munkára történő elhurcolás, a málenykij robotra kiadott 0036. számú rendelet?

c) Hogyan csapódott le az új államhatalom (Zakarpatszka Ukrajina) szekularizációról szóló 1944. december 5-i dekrétuma a település felekezeti oktatásában?

d) Milyen következményeket hozott a közösség létfenntartása szempontjából az 1945. április 20-i egyházi vagyonról kiadott dekrétum?

e) Hogyan kényszerítette az egyházi vagyon elkobzása a községet saját anyagi lehetőségeinek legszélsőbb határaira?

f) Milyen anyagi teherrel sújtotta őket az újonnan megjelent állami adózás és a kötelező egyházközösségi bejegyzés bevezetése?

Módszertani megközelítésünk célja, hogy történeti szempontból, kronológiai rendben – egyben átfogóan és szerteágazóan – mutassuk be a nagyberegi egyházközség szempontjából milyen pusztítást végzett a szovjetesítés az 1944-ig gazdasági önfenntartó kis közösségben. Ebből kifolyólag általános tudományos és speciális történeti módszerek kombinációján alapuló munkát végeztünk. A téma kutatottságának hiányosságai és a megfogalmazott feladatok miatt elsődleges források feltárását tűztük célul, ami főképpen levéltári primer dokumentumokkal történő munkát jelentett, melyek zöme a mai napig publikálatlan állapotban találhatók. Mindemellett korabeli civil feljegyzéseket és az egyházközségi irattár anyagait is felhasználtuk. A tanulmány tudományos újdonsága (az eddig megjelent tudományos munkákhoz képest) abban rejlik, hogy az 1944-ben a vidéket elözönlő szovjet csapatok okozta politikai, gazdasági és társadalmi változásokat szinte csak makrotöténeti megközelítésben, leggyakrabban politikatörténeti szemszögből ismerhetjük meg. A kisebb közösségek – mint jelen esetben a nagyberegi egyházközség belső élete, amelyet csak alulról lehetett érzékelni, s amelyet az egyes egyházközségek éltek meg –, ritkábban kerül kutatási célkeresztbe. Jelen tanulmány pont ezt célozta meg – a mikrotörténeti kutatás sajátosságainak köszönhetően – alulnézeti perspektívából (bottom-up approach) közelíti meg és mutatja be azt, hogyan tolt az új hatalom az egzisztenciális biztonságból a létbiztonság peremére egy felekezeti közösséget. Legfontosabb eredmények és megállapítások. Elmondható, hogy Nagybereg egykori mezőváros múltja magán hordozza a kárpátaljai magyar közösségek 1944 után érintő minden nyomorúság jellegzetességét, ugyanakkor rendhagyó módon olyan események és történések helyszíne, terepe is volt, amelyek nem minden községben voltak megfigyelhetők. Miközben a települést az új szovjet irányítás a szovjetrendszer kirakattelepülésévé tette, minden politikai és pártvonalon tett vállalás – túlzássá és normán felülivé vált. Ezek érhetők tetten az egyházközséggel szembeni viselkedésben a falu új vezetői részéről (tanácselnök, jegyző, milicista), akik szinte kivétel nélkül homo novusok

voltak. Igaz ez úgy a település vezetésére, mint a községben fontos pozíciót betöltöttekre egyaránt, hiszen legtöbbjük nem nagyberegi születésű volt, csak a szovjet hadsereggel jelent meg a településen. A hatalom iránti teljes elköteleződésük hevében gyakran túllőttek a célon, mint például a hitoktatás vagy a harangozás betiltásakor. A református közösséget azonban felszámolni nem tudták, és a templomból nem lett sem raktár, sem múzeum.

Kulcsszavak: alulnézeti megközelítés, háború utáni átmenet, mikrotörténet, Nagybereg, reformátusok, szovjetesítés

Felhasznált irodalom

1. Füzesi, Eemér (1918–2001) egykori nagyberegi lakos feljegyzései (a család birtokában).
2. Hungaricana, Könyv- és Dokumentumtár (archív sajtó)
3. Kárpátaljai Református Egyház Levéltára és Múzeuma (KRELM)
4. Központi Statisztikai Hivatal Könyvtára (KSH Könyvtár)
    a. 1941. évi népszámlálás. Demográfiai adatok községenként. (Országhatáron kívüli terület.) Budapest, 1990. (Kézirat.)
    b. Az 1941. évi népszámlálás. Demográfiai adatok községek szerint. Budapest, Stephaneum Nyomda, 1947. (Kézirat gyanánt.)
5. Mester, Bálint néhai nagyberegi presbiter visszaemlékezése (a család birtokában.)
6. Molnár D. E. (2015): *Kárpátaljai magyarok a Szovjetunió hadifogoly- és munkatáboraiban (1944–1953)*. Doktori (PhD) értekezés. Debrecen: Debreceni Egyetem BTK, kézirat. https://dea.lib.unideb.hu/dea/bitstream/handle/2437/217124/dolgozat_Molnar_D._E.pdf (letöltve: 2025. október 1.).
7. Nagyberegi Református Egyházközség Irattára
8. Szamborovszkyné Nagy, I. (2016a): „Amiről sokáig beszélni sem volt szabad.” Lapok Nagybereg meg nem írt történelméből. Molnár D. Erzsébet–Molnár D. István (szerk.), *A kommunizmus áldozatai, rehabilitációs alternatívák Kelet-Közép-Európában*. Beregszász: II. Rákóczi Ferenc KMF, 130–153.
9. Szamborovszkyné Nagy, I. (2016b): A szovjet hatalom megjelenése és berendezkedése Beregszász magyar iskoláiban (1944–46). Történelmi vázlat. *Acta Academiae Beregsasiensis*, 2016 (15)/1. 83–99.
10. Szamborovszkyné Nagy, I. (2017): Koncepciós perek, politikai elítéltek, egyszerű emberek. Szovjet belbiztonsági tisztogatások Nagyberegen (1945–51). Molnár D. Erzsébet–Molnár D. István (szerk.): *Hadifogság, málenkij robot, Gulág. Kárpát-medencei magyarok és németek elhurcolása a Szovjetunió hadifogoly- és kényszermunkatáboraiba (1944–1953)*. Beregszász–Ungvár, Rik-U Kiadó, 226–244.
11. Державний архів Закарпатської області, Фонд Р-14. оп.1ю од.зб. 220, 1»а»
12. *Історія міст і сіл Української РСР. В 26 т. Закарпатська область*. Тронько П. Т. (голова редколегії. Бєлоусов В. І. (голова) [та ін.] (редколегія тому). Київ: УРЕ АН УРСР, 1969.
13. Федака Д. М. (ред.) (2004): *Реабілітовані історією. Закарпатська область. Книга друга*. Ужгород: ВАТ Видавництво „Закрпаття”.

Ярослав СКОЧИЛЯС
аспірант 2-року навчання
кафедри міжнародних студій та суспільних комунікацій
Ужгородський національний університет
yaroslav.skochylias@uzhnu.edu.ua

ВПЛИВ ЕТНОПОЛІТИЧНИХ КОНФЛІКТІВ НА ТРАНСКОРДОННУ БЕЗПЕКУ

Транскордонна безпека напряму пов’язана з етнополітичними конфліктами, безпосередньо цей аспект міжнародних відносин максимально проявився в міжвоєнний період а також під час Другої світової війни. Тому в даному дослідженні було поставлене завдання визначити як саме різні аспекти вплинули на міжнародні відносини під час цих історичних періодів.

В цьому історичному періоді транскордонна безпека зазнавала значних змін та викликів пов'язаних з етнополітичними та глобальними конфліктами які були закладені ще в попередніх історичних періодах. Серед факторів які впливали на транскордонну безпеку була мілітаризація та напруження навколо кордонів. Це суттєво впливало на погіршення безпеки оскільки агресори інколи використовували мілітаризацію кордонів майбутньої жертви як виправдання агресії [5]. Наступним фактором є території з невизначеним статусом які сильно розмивали зони впливу тих чи інших держав що призводило до конфліктів. Варто зазначити що перед конфліктами часто відбувалися прикордонні озброєнні інциденти коли відбувались або цілеспрямовані провокації або випадкові зіткнення що в обох випадках проводило до жертв і змушувало країни йти на подальшу ескалацію [3]. В наслідок буремних подій 1930-х років деякі кодони були змінені насильницьким шляхом, коли країни в наслідок ультиматуму війни були змушені змінювати статус територій [1]. Така зміна статусу не призводила до посилення транскордонної безпеки а натомість перетворювала прикордонні регіони в сіру зону яка ставала джерелом нових порушень міжнародного права. Одним з найбільших злочинів які відбувалися на прикордонних територіях стали масові депортації населення зі спірних регіонів, зокрема це була складова частина голокосту [4].

Окрема варто підкреслити проблему територій з невизначеним статусом. Ці території не підпадали під безпосередню юрисдикцію однієї держави, натомість використовувалася система мандатів від Ліги Націй. Іноді такі мандати видавались державами які опікувались тією чи іншою територією, однак був і інший сценарій коли територія безпосередньо керувалась Лігою Націй. Це був сценарій вільного міста Данциг на яке претендувала Польща. Ця була квазі держава яка мала лише деякі функції держави, тим не менш на її території знаходилась єдина польська військово – морська база і через територію цього утворення пролягав так званий польський коридор, єдиний вихід Польщі до балтійського моря. Польща контролювала деякі аспекти життя міста, однак місто налічувало понад 90% німецького населення. Через це Данциг став найважливішим прикладом провальної транскордонної безпеки яка призвела до Другої світової війни. Місто було предметом постійного транскордонного військового напруження а також провокацій та нападів на представників обох націй [2].

Список використаних джерел

1. Agreement concluded at Munich, September 29, 1938 (Munich Agreement). The Avalon Project: Documents in Law, History and Diplomacy, Yale Law School. – 1938. URL: https://avalon.law.yale.edu/20th_century/munich.asp
2. Blanke Richard. Orphans of Versailles: The Germans in Western Poland, 1918–1939. University Press of Kentucky. 1993. URL: https://archive.org/details/orphansofversail0000blan?utm_source=chatgpt.com
3. Buttin Félix. The Polish-Czechoslovak Conflict over Teschen Silesia (1918–1920): a case study. Perspectives: Central European Review of International Affairs. 2005. URL: https://ciaotest.cc.columbia.edu/olj/iirp/25_2005-06_winter/25_2005-06_winter_e.pdf
4. Douglas R. M. Orderly and Humane: The Expulsion of the Germans after the Second World War. Yale University Press. 2012. URL: https://archive.org/details/orderlyhumaneexp0000doug
5. Weinberg Gerhard L. The Foreign Policy of Hitler's Germany: Starting World War II, 1937–1939. University of Chicago Press. 1970. URL: archive.org/details/foreignpolicyofh0000wein

Сілвестер ІЖАК
Аспірант Школи історичних наук
Католицького університету ім. Пазманя Петера,
szilveszterizsak64@gmail.com

Наталія ВАРОДІ
габілітований доктор, доцент
доцент Кафедри історії та суспільних дисциплін
Закарпатського угорського університету ім. Ференца Ракоці II,
varadi.natalia@kmf.org.ua

БУДІВНИЦТВО ТЕРЕБЛЕ-РІЦЬКОЇ ГЕС (1949–1956): ІНДУСТРІАЛІЗАЦІЯ ЯК ІНСТРУМЕНТ ЗАБЕЗПЕЧЕННЯ ЕНЕРГЕТИЧНОЇ ТА СОЦІОПОЛІТИЧНОЇ БЕЗПЕКИ В РАДЯНСЬКОМУ ПРИКОРДОННОМУ ЗАКАРПАТТІ

Постановка проблеми. Прикордонні регіони в періоди геополітичних змін завжди були зоною підвищеної уваги центральної влади. Забезпечення їхньої безпеки має багатовимірний характер, що включає не лише військові, але й економічні, енергетичні та соціокультурні аспекти. В історичній ретроспективі масштабні інфраструктурні проєкти часто використовувалися як інструменти інтеграції, контролю та стабілізації таких територій. В цьому контексті вивчення радянської модернізації Закарпаття, зокрема будівництва ключових об'єктів енергетики, дозволяє зрозуміти механізми утвердження нового політичного режиму та трансформації суспільства в умовах прикордоння. Наукова проблема полягає в комплексному аналізі того, як гідроенергетичне будівництво формувало нові виміри безпеки регіону – від енергетичної незалежності до соціальної інженеії.

Мета та актуальність дослідження. Метою даної роботи є аналіз будівництва Теребле-Ріцької гідроелектростанції як складного соціотехнічного проєкту, спрямованого на забезпечення енергетичної автономії, трансформацію соціальної структури та утвердження радянської моделі управління в післявоєнному Закарпатті. Актуальність дослідження зумовлена сучасними дискусіями про безпеку прикордонних територій, де енергетична інфраструктура залишається ключовим чинником суверенітету та стійкості. Історичний досвід радянської індустріалізації Закарпаття надає важливий матеріал для розуміння довгострокових наслідків інтеграції периферійних регіонів, що має практичне значення для формування сучасної регіональної політики.

Наукова новизна. На відміну від існуючих робіт, що часто зосереджуються на техніко-економічних аспектах радянської індустріалізації, дане дослідження ґрунтується на комплексному аналізі раніше не використовуваних архівних документів з фондів Державного архіву Закарпатської області. Це дозволило вперше розкрити логістичні та кадрові труднощі як пряме наслідок специфіки прикордонного гірського регіону. Окрему увагу приділено соціальній ціні проєкту, включаючи масове переселення жителів сіл Вільшани, Бовцар та Нижній Бистрий, умови життя та праці будівельників, які формували нову соціальну реальность. Також розглядається міжнародний контекст будівництва – використання обладнання з Фінляндії та Швеції, залучення фахівців з країн соціалістичного табору, що відображає геополітичні умови ранньої «холодної війни».

Виклад основного матеріалу. Дослідження послідовно розглядає етапи реалізації проєкту Теребле-Ріцької ГЕС. Від нереалізованих чехословацьких та угорських планів 1920-х років, що свідчать про давній інтерес до енергетичного потенціалу річок Теребля та Ріка, до рішення радянської влади про будівництво в 1949 році. Детально аналізується організаційна структура: створення спеціалізованої організації «Закарпатгесбуд» на базі «Дніпрогесбуд», фінансові надходження, механізми постачання матеріалів, які супроводжувалися хронічними дефіцитами та логістичними проблемами. Окремо досліджується соціальний вимір будівництва – формування цілого робітничого селища з житловими будинками, соціальною інфраструктурою (школи, лікарні, клуб) та наслідки для місцевого населення, яке зазнало вимушеного переселення із виплатою компенсацій. На основі архівних звітів комісій

розкриваються причини серйозних відстань від графіка будівництва, зокрема брак кваліфікованих кадрів, незадовільний стан доріг та енергопостачання. Запізніле введення станції в експлуатацію у 1956 році замість запланованого 1954 року стало результатом подолання цих комплексних труднощів шляхом централізованого втручання та додаткового ресурсного забезпечення.

Висновки. Будівництво Теребле-Ріцької ГЕС було не лише енергетичним, але й ключовим геополітичним проєктом радянської влади, спрямованим на закріплення контролю над Закарпаттям через створення стратегічного об'єкта інфраструктури. Цей проєкт став символом індустріалізації, що супроводжувався глибокими соціальними трансформаціями: створенням нового соціуму будівельників, радикальною зміною природного та соціального ландшафту. Безпека регіону формувалася комплексно: через забезпечення власної енергогенерації, розвиток транспортної мережі (вузькоколійна залізниця) та створення постійного робочого поселення, що закріпило радянський соціокультурний вплив. Досвід будівництва наочно демонструє, що в радянській парадигмі безпека прикордонного регіону досягалася шляхом його інтеграції в єдиний економічний і адміністративний простір, часто без достатнього обліку локальних особливостей, що призводило до значних соціальних і екологічних витрат. Таким чином, історія Теребле-Ріцької ГЕС служить яскравим прикладом того, як інфраструктурні мегапроєкти використовуються для консолідації влади та формування нової ідентичності в прикордонних регіонах.

Список використаних джерел

1. Derzhavnyi arkhiv Zakarpatskoi oblasti (Derzharkhiv Zakarpatskoi obl.) (n.d.) F. P–1097, Op. 1, Spr. № 3, ark. 1–7.
2. Derzhavnyi arkhiv Zakarpatskoi oblasti (Derzharkhiv Zakarpatskoi obl.) (n.d.) F. P–1097, Op. 1, Spr. № 7, ark. 1–70.
3. Derzhavnyi arkhiv Zakarpatskoi oblasti (Derzharkhiv Zakarpatskoi obl.) (n.d.) F. P–1097, Op. 1, Spr. № 11, ark. 1–7.
4. Derzhavnyi arkhiv Zakarpatskoi oblasti (Derzharkhiv Zakarpatskoi obl.) (n.d.) F. P–1097, Op. 1, Spr. № 12, ark. 1–47.
5. Derzhavnyi arkhiv Zakarpatskoi oblasti (Derzharkhiv Zakarpatskoi obl.) (n.d.) F. P–1097, Op. 1, Spr. № 13, ark. 1–42.
6. Derzhavnyi arkhiv Zakarpatskoi oblasti (Derzharkhiv Zakarpatskoi obl.) (n.d.) F. P–1097, Op. 1, Spr. № 19, ark. 1–7.
7. Derzhavnyi arkhiv Zakarpatskoi oblasti (Derzharkhiv Zakarpatskoi obl.) (n.d.) F. P–1097, Op. 1, Spr. № 20, ark. 1–4.
8. Derzhavnyi arkhiv Zakarpatskoi oblasti (Derzharkhiv Zakarpatskoi obl.) (n.d.) F. P–1097, Op. 1, Spr. № 25, ark. 1–20.
9. Derzhavnyi arkhiv Zakarpatskoi oblasti (Derzharkhiv Zakarpatskoi obl.) (n.d.) F. P–1097, Op. 1, Spr. № 26, ark. 1–10.
10. Derzhavnyi arkhiv Zakarpatskoi oblasti (Derzharkhiv Zakarpatskoi obl.) (n.d.) F. P–1097, Op. 1, Spr. № 27, ark. 1–14.
11. Derzhavnyi arkhiv Zakarpatskoi oblasti (Derzharkhiv Zakarpatskoi obl.) (n.d.) F. P–1097, Op. 1, Spr. № 45, ark. 1–3.

Михайло ШЕЛЕМБА
кандидат політичних наук,
доцент кафедри міжнародних студій та суспільних комунікацій
ДВНЗ «Ужгородський національний університет»,
mychajlo.shelemba@uzhnu.edu.ua

ФІЛОСОФІЯ ПРИКОРДОННОЇ БЕЗПЕКИ ТА ВИКЛИКИ МІЖНАРОДНОЇ ПОЛІТИКИ: РОЛЬ РУМУНІЇ Й УКРАЇНИ В ЗМІЦНЕННІ СХІДНОГО ФЛАНГУ НАТО

Сучасна міжнародна система перебуває у стані динамічної трансформації, зумовленої геополітичними конфліктами, зміною структури глобальної влади та переосмисленням філософії безпеки. Гібридна агресія Російської Федерації проти України стала каталізатором нового усвідомлення ролі прикордонних держав у забезпеченні регіональної стабільності. В умовах посилення конфронтації між Заходом і авторитарними режимами поняття «філософія прикордонної безпеки» набуває нового значення, інтегруючи політичну, безпекову та гуманітарну складові.

Філософія прикордонної безпеки розглядає кордон не лише як лінію оборони, а як простір комунікації, взаємодії та обміну цінностями. Для України та Румунії це означає усвідомлення власної ролі не як периферії, а як активного гравця у формуванні нової архітектури євроатлантичної безпеки. У цьому контексті Чорноморський регіон набуває значення ключового плацдарму стабільності, де перетинаються інтереси НАТО, ЄС та партнерських держав.

Метою дослідження є обґрунтування філософсько-політичних засад прикордонної безпеки в контексті нових викликів міжнародної політики та визначення стратегічного значення співпраці України й Румунії у зміцненні Східного флангу НАТО. Завдання полягає в аналізі взаємозалежності між геополітичними інтересами, філософськими засадами безпеки та практичною реалізацією оборонних стратегій у регіоні.

Наукова новизна полягає у введенні поняття «філософії прикордонної безпеки» як інтердисциплінарного концепту, що поєднує елементи філософії, політичної теорії, стратегічних студій і культурології. Такий підхід дозволяє вийти за межі суто військового аналізу й зрозуміти прикордоння як соціокультурний феномен, де взаємодіють страх, довіра, цінності та політична відповідальність.

Східний фланг НАТО сьогодні є не лише зоною оборони, а простором стратегічного переосмислення колективної безпеки. Важливу роль у цьому процесі відіграє Румунія, яка з 2014 року послідовно підтримує політику посилення присутності Альянсу в Чорноморському регіоні. Її участь у створенні багатонаціональних бойових груп, у розвитку логістичної інфраструктури та координації регіональної взаємодії з Україною демонструє еволюцію від «спостерігача» до повноцінного гаранта стабільності.

Україна, зі свого боку, виступає лабораторією сучасних безпекових практик — від протидії гібридним загрозам до інновацій у сфері цивільно-військової співпраці. Її досвід ведення війни нового типу формує не лише практичну, а й ціннісну основу майбутньої моделі безпеки, де центральне місце посідає взаємна довіра та політична суб'єктність прикордонних націй.

Особливе значення має філософський вимір безпеки, який виходить за межі військових стратегій. Він передбачає розуміння безпеки як феномена свідомості — простору, де формується почуття колективної відповідальності за межі цивілізаційного світу. Прикордонні регіони, у цьому сенсі, перетворюються на «моральні лінії фронту», де гуманітарні, культурні та етичні аспекти безпеки стають не менш важливими, ніж технологічні чи військові.

Синергія України та Румунії створює унікальний прецедент регіональної співпраці, що базується на поєднанні оборонних спроможностей, дипломатичної ініціативності та культурної близькості. Спільні навчання, програми військової підготовки, співпраця у сфері енергетичної безпеки та протидії дезінформації демонструють практичну реалізацію принципів нової філософії безпеки.

Філософія прикордонної безпеки пропонує нову парадигму мислення, у якій периферія набуває центрального значення. Україна та Румунія виступають не лише як об’єкти міжнародної політики, а як суб’єкти формування нової системи безпеки, заснованої на довірі, партнерстві та відповідальності. Їхня взаємодія зміцнює Східний фланг НАТО, підсилює єдність євроатлантичної спільноти та створює передумови для філософського переосмислення безпеки як морального імперативу, що поєднує військові, гуманітарні та культурні виміри.

Список використаних джерел

1. Bădescu, G. (2023). Romania’s Strategic Role in the Black Sea Security Architecture. Journal of Strategic Studies, 46(2), 211–229. DOI: 10.1080/01402390.2023.2165889
2. Kravchenko, O. (2022). Ukraine and NATO’s Eastern Flank: Security Challenges after 2022. European Security Review, 31(4), 533–550. DOI: 10.1080/09662839.2022.2113421
3. Lungu, A. (2021). Border Security Philosophy and Regional Resilience in Eastern Europe. Security Dialogue, 52(6), 483–498. DOI: 10.1177/09670106211008972
4. NATO. (2023). Strengthening the Eastern Flank: Strategic Adaptation and Black Sea Resilience. NATO Review Magazine. DOI: 10.1787/2023natoeastern
5. Кравець, І. (2023). Чорноморський вимір євроатлантичної безпеки: філософські та політичні аспекти. Наукові записки ІПіЕНД НАН України, 3(101), 45–59.
6. Мельник, А. (2022). Україна і НАТО: еволюція безпекової співпраці у контексті війни. Політичний менеджмент, 2(94), 11–22.

György DANCS
associate professor
Department of History and Social Sciences
Ferenc Rakoczi Transcarpathian Hungarian University,
dancs.gyorgy@kmf.org.ua

INTERSTATE BORDER PROTECTION IN EAST-CENTRAL EUROPE IN THE 18TH–19TH CENTURIES

The study examines the highly complex system of interstate border protection in East-Central Europe during the 18th and 19th centuries, highlighting its political, military, economic, and social significance at the convergence point of the region's great powers: the Habsburg Monarchy, the Russian Empire, Prussia, and the Ottoman Empire.

At the turn of the 18th and 19th centuries, the Habsburg Monarchy possessed one of the most extensive border systems on the continent. Along the hundreds of kilometers of southern and eastern borders, the Military Frontier (Militärgrenze) was established in the 18th century. This institution simultaneously served military defense, the extension of state administration, and public health and police control. The organizational structure of the Military Frontier provided the institutional and personnel conditions that enabled the empire to effectively defend against epidemics (Rothenberg 1966, p. 45). The organizational structure and personnel numbers of the Military Frontier ensured the quick mobilization of the army for the empire, which was critical for the Habsburgs' 18th-century war efforts, particularly against the Turks. (Hochedlinger, 2003).

The Partitions of Poland created new borders and enforced strict control. Border surveillance also acquired an economic function at this time (customs, defense against smuggling). The Napoleonic Wars increased its strategic importance in the 19th century. During the era of the Holy Alliance, the function expanded to include police-political tasks (controlling revolutionary ideas). The Military Frontier became a key player during the events of 1848–49. The latter half of the century saw the formation of nation-states, bringing new border arrangements.

The practice of the "cordon sanitaire" was proven effective during plague defense as early as the 18th century. This involved securing the border line with military and civil guards to control the movement of goods and persons. This experience formed the basis for establishing a new type of public health border control during the cholera epidemics of the early 19th century.

In 1831, the Habsburg Monarchy established a triple military cordon in the region of Galicia, Bukovina, and Bessarabia, imposing a strict blockade along the Russian border. The cordon aimed to completely isolate infected areas and place so-called "second-class" individuals suspected of having the plague or cholera into quarantine before they entered the country.

The border closure was therefore not merely a medical measure, but also a tool for maintaining imperial order and security. During the cholera threat, the Habsburg government feared the spread of revolutionary ideas and national uprisings in addition to the epidemic ; thus, border control served both the protection of state order and ideological security.

For crossing the border, travelers required a passport and a health certificate. These documents had to include the place of departure, personal identification data, a certificate of being disease-free, and the route taken. These measures undoubtedly served as the precursors to modern personal identification and movement control. The urban citizenship documents, guild certificates, and border crossing permits of the early modern period were now standardized state travel documents aimed at population control and restricting mobility.

Torpey, who fundamentally researched the history of the passport and other movement documents, points out that states pursued the "monopolization of the means of legitimate movement"; the passport, as an institution, became the legal framework for state sovereignty and individual mobility (Torpey, p. 193). In the 19th century, this institution no longer functioned merely as a bureaucratic scattered measure, but as a central tool of state police control.

Military and public health border protection became closely intertwined by the early 19th century. The organizational model of the Military Frontier allowed quarantine stations and lazarettos to be

placed under military supervision. The lazarettos and border quarantines served both a health purpose and functioned as a means of realizing state border order (Panzac, 1986, p.64). This strict military supervision resulted in the close fusion of policing and health functions. This dual system established the foundations for modern state border administration and the concept of the "modern border state" in the peripheries, where maintaining security, health, and order became inseparable.

The infection originating from the Russian Empire during the 1830–31 cholera epidemic prompted strict border defense measures in Central Europe. Cordons were introduced along the borders of the Habsburg Monarchy and Prussia , aiming to physically stop the infection at the frontiers (Baldwin, p. 132).

The economic dimension—as exemplified by the formation of customs unions (such as in the German states)—not only reduced internal tariffs but also necessitated the consolidation of control at external borders. Thus, border control was also tightly linked to economic logic (Henderson, pp. 21–30). In the first half of the 19th century, the economic function of border defense became further differentiated. While the Habsburg Monarchy retained its internal customs system, the German Customs Union (Zollverein), established in 1834 between neighboring German states and Prussia, demonstrated the gradual blurring of economic borders on East-Central Europe's northern and western periphery. From a border defense perspective, the Customs Union served as a model for dismantling interstate trade barriers, contrasting sharply with the Habsburg Empire's mercantilist border surveillance practice (Henderson, 2019, p. 11). The region of the Prussian–Austrian–Russian tripoint was a particularly sensitive area, where the severity of economic control also reflected political tensions (Ingrao – Thomas, 2000).

The measures introduced on the northern-eastern border sections of the Kingdom of Hungary (e.g., Galicia, Bereg, Máramaros) during the 1831 cholera epidemic—border closures, passport and health certificate systems, military cordons—were the precursors to "modern border policing". Such procedures—epidemic cordons, movement restricted by passports, and the coordinated operation of military and police infrastructures—demonstrate that border restriction, personal identification, and movement control were put in the service of state economy, administration, and security as early as the 19th century. In 19th-century Europe, epidemics, particularly cholera, were "state-forming events" that facilitated the consolidation of administrative boundaries, health control, and personal identification systems (Baldwin, p. 418).

Conclusion

The 18th–19th century East-Central European border protection uniquely fused military, economic, policing, and epidemiological tasks. This functional multi-layered nature was crucial in shaping the border policy of the modern state and the nation-state. The responses to the 1831 cholera epidemic—such as the cordon service, health passports, and the quarantine system—can be seen as the direct antecedents of later modern border surveillance practice. The system of passport and personal identification institutions, customs and border traffic controls, and quarantine systems together established the logic where the border was no longer merely a physical line, but an administrative, legal, and state control zone.

References

1. Baldwin, Peter C. Contagion and the State in Europe, 1830–1930. Cambridge: Cambridge University Press, 1999.
2. Henderson, W. O. The Zollverein. (First published 1959.) London: Routledge (Routledge Revivals ed. 2019).
3. Hochedlinger, Michael: Austria’s Wars of Emergence: War, State and Society in the Habsburg Monarchy 1683–1797. London: Longman, 2003.
4. Ingrao, Charles – Thomas, Howard: The Habsburg Monarchy, 1618–1815. Cambridge: Cambridge University Press, 2000.
5. Panzac, Daniel. Quarantaines et lazarets : L’Europe et la peste d’Orient (XVIIe–XXe siècles). Aix-en-Provence: Edisud, 1986. 219 p.
6. Rothenberg, Gunther E. The Military Border in Croatia, 1740–1881: A Study of an Imperial Institution. Chicago: University of Chicago Press, 1966. xiv, 224 p.
7. Torpey, John C. The Invention of the Passport: Surveillance, Citizenship, and the State. Cambridge: Cambridge University Press, 2000.

Erzsébet MOLNÁR D.
PhD, associate professor
Department of History and Social Sciences
Ferenc Rakoczi II Transcarpathian Hungarian University,
molnar.d.erzsebet@kmf.org.ua

Ágoston RADVÁNSZKY
History and Archaeology MA II/3
II. Rákóczi Ferenc Transcarpathian Hungarian University,
radvanszky.agoston@kmf.org.ua

THE ACTIVITIES OF SOVIET INTERNAL SECURITY AGENCIES IN TRANSCARPATHIA IN 1944–1946

The aim of the study is to examine how Soviet internal security organs—principally the SZMERS, NKVD/MGB and their ad hoc judicial auxiliaries—were deployed to restructure politics, society, and religious life in Transcarpathia between late 1944 and 1946. We analyse the formation and practice of extraordinary jurisdictions, the criminal-law toolkit imported from the Ukrainian SSR, and the operational methods (arrests, investigations, show trials, extrajudicial violence) used to neutralize perceived opponents and consolidate Soviet power. By situating Transcarpathia within broader post-war patterns east of the Elbe, we show how "internal security" functioned as the cutting edge of annexation and regime change.

Objectives of the study. The study formulates the following objectives: (1) reconstruct the legal–institutional architecture enabling repression (with special attention to the December 18, 1944 Decree No. 22 establishing the Extraordinary Court at the People's Council of Transcarpathian Ukraine); (2) map the primary target groups and charge patterns; (3) document interactions between security organs and ordinary courts/procuracy, including the transfer of prisons under security control; (4) assess case-level outcomes for political elites and clergy; (5) interpret the security agencies' role in elite replacement and the integration of Transcarpathia into the Soviet administrative order.

Methodological approach. The article synthesizes archival records of the Transcarpathian Regional State Archive (fond and opis citations), contemporary press, juridical texts, and memoir literature from victims and clergy. Triangulating institutional decrees, indictments, and press narratives with ego-documents allows us to differentiate constructed (fictitious-fact) from tendentious (rule-abusing) show trials—both present in the region—and to relate legal form to coercive practice. This mixed evidentiary base supports both a structural account of institutions and a prosopography of targeted groups.

Scientific novelty. First, we offer a focused reconstruction of the Extraordinary Court as an instrument of internal security rather than justice, led by a politically credentialed but legally untrained chairman (Vasyl Rusyn), and positioned as a special collegium of the Supreme People's Court—thereby formalizing security priorities in a judicial idiom. Second, we show how the swift extension (January 25, 1946) of the Ukrainian SSR Criminal Code—especially §54 (the analogue of RSFSR §58)—standardized the repertoire of "counterrevolutionary" charges (treason, armed uprising, anti-Soviet agitation, etc.) and routinized mass sentencing. Third, we link the institutionalization of security control over carceral facilities to the downgrading of the procuracy and courts to mere "order maintenance," reframing adjudication as the execution of security decisions.

Findings and key results.

1.Institutionalization of coercion. Decree No. 22 (18 December 1944) created an Extraordinary Court to try a broad list of "enemies"—from former occupation officials and gendarmes to alleged "agents" and those "sowing national or religious hostility." This framed political competition, minor administrative acts, and ordinary pastoral activity as matters of state security.

2.Security primacy over justice. Prisons and detention sites were placed under internal security supervision, removing them from court/procuracy jurisdiction; sentencing effectively migrated into

investigative organs, while legal bodies handled public order. This reallocation produced a conveyor-belt from arrest to punishment with minimal judicial autonomy.

3.Criminalization of religious leadership. Security operations targeted the Greek Catholic Church most intensely, aiming at liquidation through arrests, forced “reunification” with Orthodoxy, and exemplary violence. Bishop Theodore Romzha’s assassination in 1947, following a staged traffic “accident” and hospital poisoning, crystallized the security–church conflict and terrorized clergy and laity. Although just beyond our core temporal frame, the operation’s preparation and logic were already present by 1946.

Discussion. The Transcarpathian case illuminates how internal security agencies exploited emergency courts to convert political aims into judicial outcomes. The Extraordinary Court’s capacious jurisdiction, the securitization of religious practice, and the codification of “enemy” categories produced a climate where law legitimated coercion ex post. The 1946 transplantation of the Ukrainian SSR’s criminal law harmonized local repression with all-Union practice, ensuring portability of charge formulas and sentence bands. The result was a layered system in which spectacular trials (of political figures) and mass, low-visibility cases (of parish clergy and activists) worked in tandem: the former defined enemies; the latter eroded community capacity.

Conclusions. Between 1944 and 1946, Soviet internal security in Transcarpathia built a coercive–legal regime that collapsed plural authority structures and reoriented society toward Soviet governance. Extraordinary courts, security-run carceral institutions, and standardized “counterrevolutionary” charges allowed swift neutralization of rival elites and confessional communities. These mechanisms set the template for later waves of repression (1947–52), including the liquidation of the Greek Catholic hierarchy and continuing prosecutions of Reformed and Roman Catholic clergy. Internal security agencies were thus not merely custodians of order but principal architects of regime consolidation.

Keywords: Transcarpathia; NKVD/MGB; Extraordinary Court; Decree No. 22 (1944); §54 USSSR Criminal Code; show trials; elite replacement.

References

1. Державний архів Закарпатської области, Фонд Р-14. оп.1ю од.зб. 220, 1»а»
2. Федака Д. М. (ред.) (2004): Реабілітовані історією. Закарпатська область. Книга друга. Ужгород: ВАТ Видавництво „Закрпаття”.
3. Botlik József: Egestas Subcarpathica. Adalékok az Északkeleti-Felvidék és Kárpátalja XIX. és XX. századi történetéhez. Budapest, 2000.
4. Dupka György: A szovjet hatóság megtorló tevékenysége Kárpátalján (1944–1991). Ungvár – Budapest, 2014.
5. Dupka György: Kárpátaljai Magyar Gulag-lexikon. Ungvár – Budapest, 1999.
6. Molnár D. Erzsébet – Szamborovszkyné Nagy Ibolya: A megszállástól a felszámolásig. Ruszinok és görögkatolikusok Kárpátalján a szovjet megszállást követő években (1944–1949). (Scopus Q2) Historia Ecclesiastica, XV, 2024/1. 105-118.
7. Szamborovszky-Nagy Ibolya; Chasar, Ishtvan: A situation of the Transcarpathian Reformed Church in the late stalinism period and its reflection in the press of the time. Новітня доба / гол. ред. Михайло Романюк; НАН України, Інститут українознавства ім. І. Крип’якевича. Львів, 2022. Вип. 10. pp. 127–140. ISSN 2409-434X.
8. Wyszkowski, Pavel OMI: Katolikusüldözés Ukrajnában és Kárpátalján. Esztergom, 2013.

István MOLNÁR D.
PhD, Associate Professor
Department of Geography and Tourism
Ferenc Rakoczi II Transcarpathian Hungarian University,
molnar.d.istvan@kmf.org.ua

THE DIFFICULTIES OF TEACHING GIS IN HIGHER EDUCATION INSTITUTIONS DURING WARTIME

Purpose of the research. This study investigates how armed conflict reshapes the conditions, content, and conduct of Geographic Information Systems (GIS) education in higher education, with a primary focus on the Ukrainian context. We examine the compounded effects of infrastructure disruption, displacement, psychological stress, constrained access to geodata and software, and heightened ethical and security risks on the integrity of practice-oriented GIS learning. Beyond diagnosing barriers, the study seeks to identify strategies that preserve core learning outcomes, professional socialization, and academic quality amid extreme volatility.

Statement of objectives. The article pursues six interlocking objectives: (1) to map the multi-level constraints—material, technological, pedagogical, psychosocial, and normative—affecting GIS education during wartime; (2) to document the specific mechanisms by which power outages, unstable connectivity, damaged laboratories, curfews, and campus closures degrade experiential learning and assessment; (3) to assess how student and staff displacement, mobilization, and trauma fragment cohorts, extend time-to-degree, and reduce feedback density; (4) to evaluate the feasibility of offline-first, low-bandwidth teaching models using open-source software, portable distributions, and compact didactic datasets; (5) to develop an operational ethics framework for spatial teaching under conflict conditions, including risk assessment for sensitive locations and data minimization in coursework and dissemination; and (6) to identify the role of international collaborations, humanitarian mapping projects, and policy flexibilities in sustaining learning continuity and quality assurance.

Methodological approach and its purpose. Methodologically, the paper integrates (a) a structured workflow analysis of the GIS teaching sequence—data acquisition, preparation, analysis, visualization, and communication—with (b) evidence from institutional practice in wartime universities and (c) a targeted review of literature on emergency higher education, remote/low-resource GIS instruction, and geospatial ethics. The workflow analysis "stress-tests" each instructional stage against wartime perturbations (e.g., denial of access to state geodatabases; cyberattacks or throttling of cloud services; hardware constraints on student devices; intermittent electricity). The purpose is twofold: first, to generate a granular causal map of failure points that is actionable for contingency planning and accreditation; second, to validate which adaptations—portable QGIS deployments, pre-rendered rasters, modular micro-projects, scripted labs with printable step-by-steps, asynchronous assessment with screenshot portfolios—maintain essential competencies when standard facilities and bandwidth are unavailable.

Scientific novelty. Existing discussions of emergency education typically treat "digital learning" as a homogeneous category. Our contribution isolates GIS as a lab-intensive discipline with distinctive dependencies (licensed or open-source software, performant hardware, high-bandwidth access, regulated geodata, and studio-style feedback cycles). We advance four novel claims. First, in GIS the collapse of infrastructure and data access is not merely logistical; it narrows the epistemic repertoire available to students, reshaping what methods (e.g., network analysis, big-raster processing, near-real-time remote sensing) they can actually learn by doing. Second, conflict conditions convert general data-ethics principles into operational security imperatives; the default of cartographic transparency must be replaced by context-sensitive disclosure control embedded in syllabi and assignment design. Third, wartime accelerates innovation toward open ecosystems—open-source tools, open educational resources, humanitarian mapping—while incentivizing lightweight, high-pedagogical-value tasks that are resilient to bandwidth and power constraints. Fourth, structured international partnerships can function as "surge capacity," offsetting local losses of infrastructure and staffing while providing students with authentic geospatial problem contexts and community support.

Key results and findings.

(1) Learning environment and infrastructure. Recurrent blackouts and unstable internet disrupt lab continuity and force migration to improvised venues; this pushes courses toward theory-heavy formats and erodes hands-on formation in data management, spatial analysis, cartography, and reproducible workflows. Programs that pre-position uninterruptible power supplies, offline copies of core datasets, and low-spec lab images maintain higher completion rates for practical assignments.

(2) Student and staff wellbeing. Displacement, mobilization, and sustained stress correlate with fragmented project trajectories, thinner peer interaction, and reduced instructor feedback. Introducing short, modular milestones, flexible deadlines, and reflective micro-deliverables helps preserve engagement without diluting standards.

(3) Technology and data access. Restrictions on state spatial portals, variable availability of commercial cloud services, and weak personal hardware impede canonical exercises. Offline-first toolchains (e.g., portable QGIS), pre-packaged plugins, and curated, small-footprint datasets (vector-first, tiled rasters) enable faithful approximation of core methods on low-end devices.

(4) Pedagogy and assessment. Asymmetric delivery—pre-recorded lab walkthroughs, printable guides, and short screencasts—reduces failure at connectivity bottlenecks. Assessment anchored in artifacts (project files, map exports, notebook snippets, and screenshot portfolios with brief method notes) preserves rigor while remaining bandwidth-light. Rubrics emphasizing method comprehension, parameter justification, and error discussion substitute for real-time demos when synchronous sessions are impossible.

(5) Ethics, safety, and publication control. Courses must include threat modeling, geoprivacy, and disclosure-risk audits of student outputs. Sensitive sites (e.g., critical infrastructure, shelters, logistics nodes) require generalization, masking, temporal lag, or complete exclusion; instructors should implement "safe defaults" for symbolization and scale, and restrict public repositories or delay posting until risks subside.

(6) Collaborations and policy enablers. Partnerships with foreign universities, NGOs, and humanitarian mapping initiatives supply authentic tasks, mentorship, and alternative infrastructure (temporary platform access, mirrored datasets). At the system level, quality assurance bodies can legitimize contingency assessment schemes and modular crediting to protect progression without sacrificing learning outcomes.

(7) Long-term effects. Wartime pressures risk a geospatial talent bottleneck due to interrupted studies and faculty outflows. At the same time, enforced experimentation yields durable gains: broader open-source literacy, modular curricula that travel across modalities, and an embedded culture of data ethics. These shifts align GIS education with national reconstruction priorities—damage assessment, infrastructure planning, environmental monitoring—once conditions stabilize.

Conclusions. Wartime exposes the fragility of GIS education's material and normative foundations but also reveals pathways to curricular resilience. Institutions that plan explicitly for offline-first operation; rebalance outcomes toward method understanding plus scaled practice; formalize OpSec-aware data ethics in teaching; and leverage transnational collaborations can safeguard the formation of a reconstruction-ready geospatial workforce. For Ukraine, these measures are not temporary stopgaps but strategic investments in capacity for evidence-based recovery and resilient spatial decision-support.

Keywords: wartime education; GIS pedagogy; higher education; Ukraine; offline-first instruction; open-source GIS; geospatial ethics; operational security.

References

1. Tetiana Marchenko, 2023: Higher Education During the War Time in Ukraine. Scientific Journal of Polonia University. (2023) 4. 49–57. DOI: https://doi.org/10.23856/5907.

2. Olena Polovko; Sergei Glotov, 2023: The Educational Process of Ukrainian University Students Following the Full-Scale Russian Invasion. London Review of Education. 21(1). Article 31. DOI: https://doi.org/10.14324/LRE.21.1.31.

3. Olena Labenko, 2023: Higher Education in Wartime: Challenges and Practices. INTED/EDULEARN Proceedings (IATED Library). (2023) https://library.iated.org/view/LABENKO2023HIG.

4. Olena Karpenko, 2025: Organization of the Educational Process in Higher Education Institutions of Ukraine During the Period of Martial Law. Social Work and Education. (2025). https://journals.uran.ua/swe/article/view/323874.

5. Eurydice, 2024: National Reforms in Higher Education – Ukraine. Eurydice – European Education and Culture Executive Agency. https://eurydice.eacea.ec.europa.eu/eurypedia/ukraine/national-reforms-higher-education.

6. Yevhen Nikolaiev; Ganna Riy; Iryna Shemelynets, 2023: War in Ukraine: Reshaping the Higher Education Sector. Analytical Report. Kyiv: Borys Grinchenko Kyiv University; Konrad Adenauer Stiftung. https://osvitanalityka.kubg.edu.ua/wp-content/uploads/2023/04/HigherEd-in-Times-of-War-EN.pdf.

7. Jana Vojteková et al., 2021: GIS Distance Learning During the COVID-19 Pandemic: Students' Perception. Sustainability. 13(8): 4484. DOI: https://doi.org/10.3390/su13084484

Katalin PALLAY
PhD, Associate professor
Department of Pedagogy, Psycholgy, Primary,
Pre-School Education and Management of Educational Institutions
Ferenc Rakoczi II Transcarpathian Hungarian University,
pallay.katalin@kmf.org.ua

Fedir MOLNAR
PhD, Associate professor
Department of History and Social Sciences
Ferenc Rakoczi II Transcarpathian Hungarian University,
molnar.ferenc@kmf.org.ua

SECURITY CHALLENGES IN CENTRAL EUROPEAN HIGHER EDUCATION

The transformation of higher education systems in Central Europe over the past three decades has created both opportunities and new security challenges. The expansion of international academic mobility, the implementation of the Bologna Process, and the rise of digital education have reshaped the institutional landscape while exposing universities to social, technological, and political risks. This study examines how higher education institutions (HEIs) in Central Europe – particularly in Hungary, Poland, Slovakia, the Czech Republic, and Ukraine – manage these complex challenges related to academic integrity, data protection, institutional autonomy, and the resilience of educational infrastructures.

The research objective is to identify the structural and human factors that influence the security and stability of higher education in the region. The paper analyzes how political transitions, internationalization, and technological modernization affect institutional governance and academic culture [1; 2]. The study applies a comparative approach that integrates insights from education policy, sociology, and security studies. By interpreting "security" not merely as physical or cyber protection but as the safeguarding of academic values, the research connects traditional risk management with intellectual and cultural resilience [3].

From a methodological perspective, the analysis relies on a synthesis of policy documents, international reports, and empirical studies. The COVID-19 pandemic and the war in Ukraine have further highlighted the fragility of higher education systems in the region, forcing universities to adapt rapidly to hybrid learning, digital communication, and crisis management [4].

The findings reveal several interrelated categories of security risks.

(1) Digital and information security: The rapid digitization of learning environments, particularly during the pandemic, increased the vulnerability of universities to cyberattacks, data breaches, and academic fraud. Institutions have been compelled to develop new regulatory frameworks for digital ethics and data governance [5].

(2) Institutional and political security: In several Central European countries, higher education autonomy remains under pressure from political centralization and funding dependency. These dynamics threaten the principle of academic freedom and weaken institutional resilience [1; 3].

(3) Social and cultural security: The diversification of the student population, growing internationalization, and demographic decline have reshaped academic communities. Universities must balance inclusiveness and competitiveness while maintaining the integrity of academic standards.

The scientific novelty of the study lies in defining educational security as a multidimensional concept that integrates digital, institutional, and cultural components. It demonstrates that Central European universities face not only technical or administrative threats, but also challenges to their intellectual and academic independence – the ability to sustain autonomous knowledge creation in the face of political, economic, or ideological pressures. The study argues that sustainable security in higher education requires a systemic approach combining transparent governance, ethical leadership, and cross-border cooperation.

In conclusion, the paper highlights that the resilience of Central European higher education depends on its ability to protect autonomy, ensure the integrity of research and teaching, and maintain openness to international collaboration. Strengthening academic security thus means defending the intellectual foundations of democracy and critical thinking. In a region marked by historical instability and current geopolitical uncertainty, universities remain not only centers of learning but also vital institutions of societal security and moral continuity.

References

1. Corbett A, Gordon C. Academic Freedom in Europe: The Central European University Affair and the Wider Lessons. History of Education Quarterly. 2018;58(3):467-474. doi:10.1017/heq.2018.25
2. European University Association (EUA) (2023) University Autonomy in Europe IV: The Scorecard 2023. Brussels: EUA. Available at: https://www.eua.eu/publications/reports/university-autonomy-in-europe-iv-the-scorecard-2023.html
3. Kwiek, M. (2018) Changing European Academics: A Comparative Study of Social Stratification, Work Patterns and Research Productivity. London: Routledge.0.
4. Oleksiyenko, A., Shchepetylnykova, I., & Furiv, U. (2023). Internationalization of higher education in tumultuous times: Transformative powers and problems in embattled Ukraine. Higher education research and development, 42(5), 1103-1118. https://doi.org/10.1080/07294360.2023.2193727
5. World Bank. (2021). Digital transformation and the future of education. World Bank Publications.

Fedir MOLNAR
PhD, Associate professor
Department of History and Social Sciences
Ferenc Rakoczi II Transcarpathian Hungarian University,
molnar.ferenc@kmf.org.ua

SECURITY CHALLENGES FACED BY NORTHEASTERN HUNGARY DURING THE 1848–1849 PERIOD

The revolutionary years of 1848–1849 reshaped the political and social order of the Habsburg Monarchy, posing complex security challenges in the multiethnic northeastern territories of the Kingdom of Hungary – regions corresponding to present-day Transcarpathia and its surrounding counties. These borderlands, inhabited by Hungarians, Rusyns, and Romanians, were not only military hinterlands but also zones of cultural contact and political tension. The present study investigates how the Greek Catholic Eparchy of Mukachevo, led by Bishop Vasyl Popovych, contributed to maintaining public order, interethnic balance, and social stability during the Hungarian Revolution and War of Independence.

The research objective is to reconstruct the mechanisms through which local ecclesiastical and civic actors managed to preserve stability in a period of state transformation. By analyzing the cooperation between the Batthyány Government and the Greek Catholic hierarchy, the study demonstrates that the Church functioned as a moral and social security institution, mediating between the revolutionary Hungarian authorities and the rural population [1; 2]. The significance of this research lies in its interdisciplinary approach: it interprets "security" not solely as military protection but as a composite of political legitimacy, cultural mediation, and moral integrity.

From a methodological perspective, the analysis relies on comparative historiography and on primary sources from the State Archives of Transcarpathian Oblast (Berehove Section), the National Archives of Hungary, and the Esztergom Primate Archives. These documents shed light on the dual role of the Greek Catholic clergy – as loyal supporters of the new Hungarian laws and as guardians of local peace in a volatile environment. The Eparchy's territory covered seven counties and the Hajdú district, which made it a key factor in sustaining the logistical and moral hinterland of the Hungarian revolutionary army [3; 4].

The findings indicate that the abolition of serfdom and the implementation of the April Laws in 1848 radically transformed the social hierarchy, creating uncertainty among the rural population. In this context, Greek Catholic parish priests played a stabilizing role by interpreting new reforms for largely illiterate communities and discouraging ethnic hostility. Bishop Vasyl Popovych's prudent leadership – avoiding confrontation with either the Hungarian government or the Viennese Court –helped maintain the fragile peace among diverse ethnic groups [2; 5]. Through pastoral mediation and community guidance, the Church prevented the escalation of unrest in Máramaros and Ugocsa counties, demonstrating that religious authority could substitute for state presence in ensuring local security.

The study also explores the socio-economic and ethical dimensions of security. The government's effort to provide state funding (congrua) for the lower clergy and educational institutions was welcomed by the Eparchy, as it recognized the Church's contribution to social welfare and cohesion [6]. This cooperation illustrated a broader transformation in the concept of national security – one rooted in civic responsibility, education, and moral governance.

The scientific novelty of the research lies in identifying the Eparchy of Mukachevo as an early security actor in a culturally diverse region. The clergy's efforts to promote understanding between ethnic groups and to preserve loyalty to the constitutional government show that stability in border areas depended not only on armies or administration but also on cultural and moral resilience. By combining archival evidence with modern theories of human and cultural security, the study contributes to a deeper understanding of how 19th-century frontier societies managed crises through ethical leadership and intercommunal cooperation.

In conclusion, the case of Northeastern Hungary during 1848–1849 demonstrates that sustainable security arises from the interaction of political reform, confessional tolerance, and shared moral values. The lessons of Bishop Vasyl Popovych's leadership remain relevant today: in border regions marked by ethnic plurality, peace can only endure where historical memory, trust, and dialogue form the pillars of security.

References

1. Bendász, I. (1997) Az 1848–1849-es szabadságharc és a Munkácsi Görög Katolikus Egyházmegye. Ungvár: KMKSZ.
2. Molnár, F. (2018) A Munkácsi Görögkatolikus Egyházmegye története 1848–1849-ben. [PhD dissertation] Eötvös Loránd University. Available at: https://edit.elte.hu/xmlui/handle/10831/40531
3. Molnár, F. (2016) 'Okremi aspekty biohrafii mukachivskoho hreko-katolytskoho epyskopa Vasylia Popovycha', Acta Academiae Beregsasiensis, 15, pp. 175–182.
4. Solymosi, J. (2013) Forradalom és szabadságharc Északkelet-Magyarországon 1848–1849-ben. Budapest: Hadtörténeti Intézet és Múzeum.
5. Pirigyi, I. (1998) 'Görög katolikusok az 1848-as szabadságharcban', in Takács, P. (ed.) A szabadság Debrecenbe költözött. Debrecen: Csokonai Kiadó, pp. 149–164.
6. Sarnyai, Cs. M. (2002) Polgári állam és katolikus egyház (1848. március – december). Budapest: METEM.

Надія МАРИНЕЦЬ
кандидат філософських наук, доцент
Кафедра історії та суспільних дисциплін
Закарпатський угорський університет ім.Ф.Ракоці ІІ
marinec.nagyija@kmf.org.ua

КОЛЕКТИВНА ПАМ'ЯТЬ І ФІЛОСОФІЯ ІСТОРІЇ У РЕПРЕЗЕНТАЦІЯХ ТРАВМАТИЧНОГО ДОСВІДУ РАДЯНІЗАЦІЇ В КУЛЬТУРІ ТА МИСЛЕННІ

Постановка наукової проблеми: Незважаючи на визнання травматичного характеру радянського періоду та його впливу на національну ідентичність, залишається недостатньо вивченим комплексний механізм трансформації травматичного філософсько-історичного досвіду радянізації на рівні колективної пам'яті та інтелектуальної традиції.

Мета дослідження: Здійснити міждисциплінарний філософсько-культурологічний аналіз репрезентацій травматичного досвіду радянізації в колективній пам'яті та мисленні, щоб визначити методологічні передумови для відновлення цілісності національної філософської традиції та побудови анти-тоталітарної філософії історії, що ґрунтується на ідеях свободи та відповідальності.

Актуальність дослідження: Сучасні дослідники стоять перед необхідністю критичного переосмислення радянської філософської спадщини як передумови подолання ідеологічної залежності. Аналіз понятійного розмаїття дозволяє інтегрувати психологічні, соціологічні та філософські моделі пояснення колективного досвіду.

Травматичний досвід (репресії, голодомори, етноцид), що призвів до руйнування структур культурної пам'яті, потребує актуалізації як чинник, що визначає сучасні моделі суспільної поведінки і колективне реагування (механізми пам'ятання і забуття) на виклики сьогодення. Усвідомлення травми необхідне для зміцнення стійкості суспільства та формування цілісної національної ідентичності.

Короткий виклад поставленого завдання: Історична травма постає як комплексне психосоціальне явище, що охоплює емоційний стан, способи осмислення та інтерпретації досвіду, переданого між поколіннями, який формує колективну ідентичність і визначає моделі суспільної поведінки. Її вивчення має міждисциплінарний характер, оскільки поєднує соціологічний, психологічний, культурологічний та філософський аспекти. У науковому обігу для позначення цього феномену вживають низку термінів, серед яких «культурна травма», «колективна травма», «міжгенераційна травма», «колоніальна травма». Наведене понятійне розмаїття відображає складність процесу засвоєння травматичного досвіду на індивідуальному та водночас на колективному рівні. Історична травма, з огляду на її масштабність, передбачає спільну ідентичність, колективне переживання події та її тривалий вплив на фізичне і ментальне здоров'я спільноти, а також на стійкість суспільства загалом [1, с. 85].

Історична пам'ять українців зазнала глибоких деформацій унаслідок тривалого перебування в умовах бездержавності, культурної асиміляції та політичного тиску. На сучасному етапі історична пам'ять перебуває у стані кризи, що виявляється у співіснуванні в колективній свідомості різних, часом суперечливих, проєкцій минулого. Одну з них формує власне український наратив, заснований на прагненні до самостійності, культурного відродження та історичної правди. Інша – малоросійська, що включає проросійські та радянські компоненти, утверджені десятиліттями імперського та тоталітарного впливу. Ці дві моделі пам'яті не є взаємодоповнювальними – навпаки, вони часто вступають у конфлікт, створюючи у суспільній свідомості антагоністичні картини історії, що ускладнює формування цілісного історіософського бачення [2, с. 265].

Радянський досвід, тривалий час формував спотворену історичну свідомість. Різні покоління українців упродовж радянського періоду були позбавлені доступу до інтелектуальних і мистецьких надбань Розстріляного Відродження – феномену, що уособлював спробу модерного українського мислення поєднати гуманізм, національну

самобутність і європейські культурні орієнтири. Системна ізоляція суспільства від цих здобутків призвела до втрати безперервності культурної тяглості, що своєю чергою вплинуло на формування колективної ідентичності. Замість автентичної історичної пам'яті утвердилася спотворена версія минулого, нав'язана через механізми пропаганди, соцреалістичну літературну критику та контрольовані медіа [3, с. 136].

Подолання впливу радянського минулого, особливо у сфері філософського знання, потребує не замовчування, а ґрунтовного вивчення його засадничих принципів і світоглядних постулатів. Змістовно це стосується аналітичного опрацювання досвіду з метою подальшого розпредметнення, критичного осмислення та звільнення від ідеологічних нашарувань. Саме через дослідження внутрішніх суперечностей радянської філософії стає можливим вироблення цілісного розуміння процесів, що сформували українську інтелектуальну традицію у XX столітті [4, с. 39-40].

Висновки: Вивчення радянської філософії є необхідним для реконструкції інтелектуальної атмосфери того часу. Цей процес дозволяє дослідникам не лише зрозуміти механізми ідеологічного контролю над думкою, але й ідентифікувати способи, якими окремі мислителі прагнули зберегти автономність розуму (резильєнтність) у межах репресивного дискурсу. Такий аналіз виходить за рамки простої критики, фокусуючись на стратегіях інтелектуального виживання.

Критичне переосмислення цієї спадщини має фундаментальне значення для становлення сучасної української філософської культури. Цей процес сприяє її орієнтації на критичне мислення, духовну самостійність та деколонізацію інтелектуального простору.

Список використаних джерел:

1. Семененко А., Кулик В., Цихуляк І. Філософські аспекти колективної пам'яті: історична травма та переосмислення минулого. Науково-теоретичний альманах Грані. 2025. № 28(2). С. 80-87.

2. Шершова Т. Культурна пам'ять у контексті формування національної ідентичності. Człowiek w historii vs historia człowieka. Monografia zbiorowa/ Warszawa-Paryż 2021. С. 264-270.

3. Сірик Л. Трагічні і травматогенні наслідки радянської політики в галузі української літератури. TEKA Komisji Polsko-Ukraińskich Związków Kulturowych. 2018. № 6(13). С. 127-140.

4. Козій І. В. Феномен української радянської філософії. Грані. 2018. Том 21, № 12. С. 34-41.

Fedir MOLNAR
PhD, Associate professor
Department of History and Social Sciences
Ferenc Rakoczi II Transcarpathian Hungarian University,
molnar.ferenc@kmf.org.ua

Melánia OROSZ
2st-year MA student, majoring in History and Archaeology
Ferenc Rakoczi II Transcarpathian Hungarian University,
orosz.melania.b20tm@kmf.org.ua

SECURITY CHALLENGES IN CENTRAL EUROPE, 1848–1849

The revolutionary years of 1848–1849 profoundly reshaped the political and social order of Central Europe, generating a complex set of security challenges that affected the Habsburg Monarchy and, within it, the Kingdom of Hungary and its surrounding regions. The collapse of imperial administrative structures, the rise of modern national movements, and the increasing involvement of great powers fundamentally transformed the security environment of the region. In this period, security cannot be understood solely in military terms; it encompassed political legitimacy, state sovereignty, ethnic coexistence, and social stability, all of which were simultaneously questioned and renegotiated [1].

With the outbreak of the revolution, the previously stable administrative system of the Habsburg Empire began to disintegrate at an unexpected pace. The authority of Vienna was shaken, the links between central and regional governance weakened, and a power vacuum emerged in many multiethnic areas [3]. Although the Hungarian government attempted to build a modern constitutional state, the rapid implementation of reforms and the unstable political environment heightened the likelihood of armed conflict [5]. As imperial authority weakened, local populations found themselves increasingly vulnerable: deficiencies in law enforcement, logistical shortages, and administrative uncertainty all contributed to the region's fragile security situation.

The strengthening of national movements fundamentally shaped the security landscape of mid-19th-century Central Europe. Hungarian, Croatian, Serbian, Romanian, and Slovak political elites followed divergent state-building agendas, leading to conflicts in which self-organised armed groups, national guards, and militias played a key role. These formations created parallel centres of authority, challenging state control and exposing the civilian population to new risks. National conflicts frequently escalated into ethnic tensions, exacerbated by communication gaps, political mistrust, and differing interpretations of loyalty. In such a multiethnic environment, the question of security was intertwined with competing national aspirations and fears [5].

Great power intervention represented another decisive security factor. From late 1848 onwards, the Habsburg government increasingly turned toward military measures, while preparations for Russian intervention began early in 1849. The eventual entry of the Russian imperial army not only sealed the fate of the Hungarian struggle for independence but also demonstrated the vulnerability of Central European regions to external geopolitical interests. The security of the region depended not only on internal stability but also on the strategic calculations of major powers [4]. This intervention cemented the role of Central Europe as a geopolitical buffer zone, a status it retained well into the second half of the nineteenth century.

The conflicts of 1848–1849 had serious social and economic repercussions. Constantly shifting battle lines, requisitions, supply crises, mass displacement, and the collapse of local economies all eroded the security of the civilian population [1]. For many communities, insecurity stemmed not only from military operations but also from the instability of governance, legal ambiguity, and the anxieties emerging from rapid social reform, such as the abolition of serfdom [2]. In this period, the modern dimensions of security – political, social, economic, and cultural – became deeply relevant, even if contemporaries lacked the conceptual vocabulary used today.

The ethnic diversity of the region played a crucial role in shaping its security challenges. Rapid changes in national identities often produced fear, distrust, and the construction of enemy images. The relationship between the state and society was further complicated by the fact that large segments of the population had limited understanding of political reforms. As a result, different ethnic communities interpreted the concept of security in diverging ways. For some, security meant military protection; for others, it was tied to cultural and linguistic self-preservation [2].

Understanding the security environment of 1848–1849 requires recognising that security was not confined to the battlefield or the sphere of high politics. Central Europe experienced a multifaceted crisis in which political reforms, social transformation, cultural identity struggles, national conflicts, and great power intervention intersected and reinforced one another. During this period, the region emerged unmistakably as an area whose stability depended as much on international power relations as on domestic developments. The experience of 1848–1849 underscores that the foundations of state stability lie in political dialogue, social trust, and the management of ethnic coexistence – elements that were in short supply during the revolutionary years and whose absence contributed significantly to the security crisis of the region.

References

1. Clark, Christopher: Revolutionary Spring: Fighting for a New World 1848-1849. London, Allen Lane, 2023.

2. Грицак, Ярослав: Нарис історії України. Формування модерної української нації XIX-XX століття. Київ, Генеза, 1996.

3. Judson, Pieter M.: The Habsburg Empire: A New History. Cambridge (MA), Harvard University Press, 2016.

4. Kosáry Domokos: Magyarország és a nemzetközi politika 1848–1849-ben. Budapest, História – MTA Történettudományi Intézete, 1999.

5. Sked, Alan: The Decline and Fall of the Habsburg Empire, 1815–1918. London, Longman, 2001.

DOBOS Sándor
adjunktus,
Történelem- és Társadalomtudományi Tanszék,
II. Rákóczi Ferenc Kárpátaljai Magyar Egyetem,

NYIKONOROVA Viktória
II. évfolyamos nemzetközi kapcsolatok, társadalmi kommunikáció
és regionális tanulmányok szakos hallgató,
II. Rákóczi Ferenc Kárpátaljai Magyar Egyetem

ERŐDÍTMÉNYRENDSZER ÉS VÉDELMI VONALAK MAI KÁRPÁTALJA TERÜLETÉN A MÁSODIK VILÁGHÁBORÚ KORÁBAN (1939–1945)

A második világháború időszakában Kárpátalja térsége nem csupán földrajzi, hanem stratégiai értelemben is kiemelt jelentőséggel bírt. A Kárpátok vonulata természetes védelmi határt képezett, amely a korszak katonai gondolkodásában a keleti védelem kulcsterületének számított. Az itt kiépített erődítményrendszerek nem pusztán építészeti és hadmérnöki teljesítmények, hanem a korabeli politikai és katonai döntések tükrei is. A téma kutatásának aktualitását az adja, hogy a Kárpátalja területén ma is számos, többé-kevésbé épen fennmaradt erődítményrészlet található. Ezek nem csupán a háborús múlt emlékei, hanem a határvédelem történetének fontos tanúi. A második világháborús erődítések vizsgálata nemcsak hadtörténeti, hanem örökségvédelmi és identitástörténeti szempontból is releváns, hiszen a határvidék mindig a nemzeti tér önazonosságának egyik legérzékenyebb pontja volt.

Kárpátalja sorsa a két világháború között többször is gyökeresen megváltozott. Az első bécsi döntés (1938. november 2.) következtében a terület déli része visszakerült Magyarországhoz, míg az északi zóna 1939 márciusáig Csehszlovákia fennhatósága alatt maradt. A Kárpáti Ukrajna néven rövid ideig fennálló államalakulat összeomlása után a magyar honvédség bevonult, és a teljes régiót annektálta. A térség katonai szerepe ezt követően jelentősen megnőtt. A Kárpátok természetes akadályként szolgáltak a keleti hadszíntér és a Kárpát-medence között. Magyarország hadvezetése felismerte, hogy a Szovjetunió felől érkező esetleges támadás esetén Kárpátalja lesz az első védelmi vonal. Ennek megfelelően a Honvédelmi Minisztérium Erődítési Főosztálya már 1939 végén megkezdte az előkészítő munkálatokat egy olyan védelmi rendszer kiépítésére, amely hosszú távon is képes ellenállni egy modern hadsereg támadásának.

A második világháború éveiben a magyar állam jelentős erőforrásokat fordított e célra. A hadmérnöki egységek és a munkaszolgálatos alakulatok együtt építették ki a Kárpátok vonalában húzódó állásokat. Az Árpád-vonal építése 1940-ben indult meg teljes erővel, majd 1943-ban tovább bővítették a védelmi rendszert a Hunyadi- és Szent László-vonalakkal, amelyek a belső területek védelmét hivatottak biztosítani {4}. A korszak katonai dokumentumaiban hangsúlyosan jelenik meg az a szemlélet, hogy a védelmi vonalak nem statikus erődítmények, hanem rugalmas, az ellenség mozgásához igazodó rendszerek. Ez a megközelítés a német hadműveleti elvekkel is összhangban állt, amelyek a mélységben tagolt védelem és a mozgó hadviselés kombinációját tekintették a korszerű háború alapjának.

A Kárpátalja területén kiépített magyar védelmi vonalak közül a legismertebb az Árpád-vonal, amely a történeti Magyarország legnagyobb hadmérnöki vállalkozásának tekinthető. A vonal hossza meghaladta a 600 kilométert, és több tucat erődített szakaszból állt. A tervezés során a mérnökök figyelembe vették a terep adottságait: a természetes sziklák, hegyoldalak és patakvölgyek integrálása révén a védelmi állások kiválóan illeszkedtek a környezetbe.

A védelmi rendszer fő elemei közé tartoztak a betonbunkerek, géppuskafészkek, tüzérségi állások, aknamezők, lövészárkok és fedezékek. Ezek láncolata követte a fő közlekedési útvonalakat, miközben az ellátó- és kommunikációs folyosók a völgyek között biztosították a kapcsolatot. A magyar katonai tervezők célja nem az volt, hogy áttörhetetlen falat építsenek, hanem hogy a terep adottságait kihasználva lassítsák és feldarabolják az ellenséges támadást.

A munkálatokban katonai alakulatok, műszaki egységek és munkaszolgálatosok ezrei vettek részt. Az építkezés nehéz, hegyvidéki körülmények között zajlott, gyakran kézi erővel, mivel a gépi szállítás a sziklás terepen nem volt lehetséges. Az anyagokat helyben termelték ki: követ, fát és cementet, amelyeket öszvérekkel és teherautókkal juttattak fel a magasabb részekre. A magyar hadvezetés törekedett arra, hogy a védelem a lehető legjobban illeszkedjen a domborzathoz, ezzel biztosítva a kis létszámú honvéd egységek számára is a hatékony ellenállást.

A hadtörténeti elemzések kiemelik, hogy a rendszer nemcsak hadászati szempontból volt jelentős, hanem a magyar hadmérnöki gondolkodás önállóságát is tükrözte. Az Árpád-vonal a korszak katonai technikájához képest rendkívül hatékony és gazdaságos megoldásnak bizonyult, hiszen a természetes terep adottságait használta fel védelmi célokra. A fő szakasz 1943-ra készült el, ekkor már több mint hatszáz kilométer hosszan húzódott a keleti határon, és a kor egyik legkorszerűbb hegyi védelmi rendszerének számított.

A második világháború éveiben a magyar hadvezetés a Kárpátalján kiépített védelmi rendszereket nem egyszerűen statikus akadályrendszerként, hanem összetett hadműveleti térként kezelte. A védelem hatékonyságát a terep adottságainak maximális kihasználása, a mélységben tagolt szerkezet és a rugalmas visszavonulási lehetőségek biztosították. Az Árpád-vonal, mint a keleti határ fő védelmi rendszere, három övre tagolódott: az első védelmi öv a Kárpátok gerincén húzódó, előretolt bunkerrendszer volt, a második öv a folyóvölgyek és hágók lezárását szolgálta, míg a harmadik öv a belső védelmi vonalakat jelentette. A fő szakaszok a legfontosabb stratégiai pontok mentén épültek: az Uzsoki-, Vereckei-, Tatár- és Borgói-hágó térségében, valamint a Munkács–Huszt–Rahó irányában.

A védelmi rendszer szerkezete korszerű és jól átgondolt volt. A bunkereket úgy alakították ki, hogy azok a tűzvezetést több irányba biztosítsák, a géppuskafészkek és a lövészárkok pedig egymást átfedő tűzmezőt alkottak. A bunkerek fala 1,5–3 méter vastag vasbetonból készült, a mennyezetet gyakran acélgerendákkal erősítették meg. Az állásokhoz föld alatti összekötő folyosók, tüzérségi megfigyelőpontok és aknavető-állások kapcsolódtak. A bunkerek bejáratait vasajtókkal zárták le, és szinte minden esetben ellátták szellőzőrendszerrel, lőszer- és élelmiszerraktárral. Az építményeket a hegyoldalba vájták, majd természetes anyagokkal álcázták, így a légi felderítés számára nehezen voltak észlelhetők.

Az Árpád-vonal mellett a Hunyadi- és Szent László-vonalak a belső védelmet biztosították, amelyek az első vonal áttörése után a tartalék erők visszavonulását és újbóli szervezését tették lehetővé. E rendszerek főként kisebb fedezékekből, gyalogsági állásokból és ideiglenes védelmi pontokból álltak, de a terephez hasonlóan illeszkedtek, mint az Árpád-vonal. A magyar hadvezetés célja nem a frontvonal végsőkig való tartása volt, hanem az ellenség mozgásának lassítása és kifárasztása, miközben a saját csapatok rendezetten vonulhattak vissza.

1944 nyarán, amikor a keleti front áthelyeződött a Kárpátok előterébe, a magyar 1. hadsereg vette át a védelem irányítását. A Vörös Hadsereg szeptemberben indította meg a Kárpáti hadműveletet, amelynek célja a Kárpátok hágóinak áttörése és a magyar területek elérése volt. Az ütközetek rendkívül hevesek voltak, különösen az Uzsoki- és a Tatár-hágó térségében, ahol a magyar és német egységek heteken keresztül tartották a frontot. A korabeli hadinaplók szerint a magyar állások sok helyen napokon át ellenálltak, miközben az ellenség súlyos veszteségeket szenvedett.

A védelmi harcok során a terep sajátosságai meghatározták a hadműveletek jellegét. A szovjet páncélos egységek a hegyvidéki környezetben korlátozottan tudtak mozogni, ezért a harcok elsősorban gyalogsági és tüzérségi összecsapásokban nyilvánultak meg. A védők a sziklás terepen és a mély völgyekben elhelyezett állásokból eredményesen lőtték az ellenséget, sok helyen tüzérségi tűzzel és aknamezőkkel akadályozták meg az előrenyomulást. Az Uzsoki-hágó környékén a magyar alakulatok mintegy három hétig tartották állásaikat, a Tatár-hágónál pedig az erősítések megérkezéséig sikerült megakadályozni a teljes áttörést.

A hadtörténeti kutatások kiemelik, hogy az Árpád-vonal védelmi koncepciója a valós harci helyzetben is bevált. A természetes terepre épülő rendszer kis létszámú csapatokkal is képes volt hatékonyan lassítani a sokszoros túlerőt, miközben a veszteségek viszonylag alacsonyak maradtak . A magyar védelmi stratégia tehát rövid távon elérte célját: a frontvonal 1944 szeptemberében még mindig a Kárpátokban húzódott, és a szovjet előretörés hónapokkal elhúzódott.

A védelmi rendszer gyengesége azonban az utánpótlás hiányában, a légitámadásokkal szembeni védtelenségben és a csapatok kimerülésében mutatkozott meg. Az 1944 októberében meginduló újabb szovjet támadások már áttörték az Árpád-vonalat. Az Uzsok–Beregszász–Munkács térségében több állás egymás után esett el, és a védők kénytelenek voltak fokozatosan visszavonulni a Tisza irányába.

Az összeomlás nem hirtelen következett be, hanem fokozatos folyamat volt. Az 1. magyar hadsereg parancsnoksága 1944. október 26-án rendelte el a visszavonulást, amikor már egyes szovjet egységek hátba kerülték a védelmi vonalakat. Az ellátási vonalak megszakadtak, a szállítás lehetetlenné vált, és a csapatok súlyos veszteségeket szenvedtek a hegyekből történő kivonulás során. A háború végére az Árpád-vonal teljes egészében megsemmisült, a bunkerek és fedezékek többsége elhagyatottá vált.

A hadtörténészek egybehangzó véleménye szerint az Árpád-vonal katonailag sikeres koncepció volt, amely a magyar hadmérnöki tudás egyik csúcspontját jelentette. Bár a háború menetét nem tudta megváltoztatni, mégis példája annak, hogy a terephez igazodó védelem és az emberi lelemény együttesen képes volt hónapokig feltartóztatni a túlerőt. Az Árpád-vonal ezzel a magyar hadtörténet egyik legösszetettebb és legjobban megtervezett védelmi rendszereként vonult be a történelembe.

A második világháború lezárását követően Kárpátalja a Szovjetunió fennhatósága alá került, és a magyar katonai örökség hosszú évtizedekre politikai tabutémává vált. Az egykori erődítmények sorsa ezzel gyökeresen megváltozott: a korábban stratégiai jelentőségű bunkerek, lövészárkok és fedezékek a háború utáni szovjet katonai és gazdasági érdekek számára értéktelenek, sőt, sok esetben gyanús objektumok lettek.

Az 1940-es évek végén és az 1950-es évek elején a Szovjet Hadsereg több helyen megkezdte a még használható erődítmények szisztematikus felszámolását. A vasbeton szerkezeteket felrobbantották vagy földdel temették be, másokat átalakítottak raktárakká, istállókká, vagy egyszerűen elhagyták. A helyi lakosság sokszor a beton- és fémelemeket széthordta építkezésekhez, így a védelmi rendszer jelentős része fizikailag is eltűnt.

A hidegháború éveiben a Kárpátok térsége fokozottan ellenőrzött határzónává vált, és az egykori Árpád-vonal maradványai gyakran a katonai tiltott övezet területére estek. A hozzáférés korlátozása miatt a kutatás szinte teljesen megszűnt. Csak néhány helytörténeti feljegyzés és szóbeli visszaemlékezés őrizte meg az emlékét, jellemzően az egykori katonák vagy helyi lakosok elbeszéléseiben.

A rendszerváltást követően, a 1990-es években kezdődött meg újra az Árpád-vonal iránti tudományos érdeklődés. Magyar és ukrán történészek, régészek, valamint helyi civil szervezetek kezdték feltérképezni a fennmaradt szakaszokat. Különösen a Volóci-, Szinevéri- és Rahói járásokban találhatók ma is viszonylag épen maradt bunkerek, amelyek az elmúlt években részben turisztikai látványossággá váltak.

E kutatások nyomán mára világossá vált, hogy az Árpád-vonal nemcsak hadtörténeti, hanem műszaki és kulturális örökségként is értékelhető. A fennmaradt objektumok betekintést engednek a korszak hadmérnöki gondolkodásába, a korabeli technológiai szintbe és a katonai stratégiai tervezés logikájába. A 21. században a cél már nem a katonai értékelés, hanem az örökségvédelem és az emlékezetpolitika: miként lehet méltón megőrizni és bemutatni ezt a múltat egy többnemzetiségű, történetileg sokrétű térségben.

Ma Kárpátalja több pontján újra felfedezik az Árpád-vonal emlékeit. Az utóbbi években helytörténészek, önkéntesek és civil szervezetek kezdeményezésére tanösvények, kisebb kiállítások és emlékhelyek jöttek létre. Ezek nem a háborút dicsőítik, hanem a múlt megértését szolgálják: bemutatják, hogyan élték meg az itt harcolók a front mindennapjait, és milyen hatással volt a háború a helyi közösségekre.

Az erődítmények így már nem csupán katonai objektumok, hanem emlékezésre hívó helyek. A bunkerek, lövészárkok és fedezékek némán idézik fel a háború borzalmait, ugyanakkor arra is emlékeztetnek, hogy a határvidék mindig az emberek kitartásának, félelmeinek és reményeinek színtere volt. A Kárpátok csendes erdői között ma már nem dörögnek fegyverek – csak a történelem visszhangja hallatszik.

Tehát az Árpád-vonal és a hozzá kapcsolódó védelmi rendszerek története jól tükrözi a magyar hadtörténelem 20. századi fordulatait. Ezek az erődítmények a katonai stratégia, a geopolitikai helyzet és a mérnöki tudás együttes termékei voltak. Megépítésük a magyar állam egyik legnagyobb hadmérnöki teljesítményét jelentette a korszakban, és a védelmi koncepció sikeresen ötvözte a természetes terepviszonyokat a technikai megoldásokkal.

Bár a háború kimenetelét az Árpád-vonal nem tudta megváltoztatni, szerepe mégis meghatározó volt: lassította a szovjet előrenyomulást, és lehetővé tette a magyar erők rendezett visszavonulását. A védelem összeomlása nem az erődítmények hibája, hanem az emberi és anyagi erőforrások kimerülésének következménye volt.

A háború utáni feledés és rombolás évtizedei után ma már újra felismerjük e rendszerek történeti és kulturális értékét. A fennmaradt bunkerek, fedezékek és lövészárkok a történelmi emlékezet részévé váltak, amelyek nemcsak egy háborús korszakot, hanem a határvédelem örök jelentőségét is megtestesítik. Igy zz Árpád-vonal nem csupán katonai építmény, hanem a történelem szimbolikus határvonala – a múlt tanúja, amely figyelmeztet a jövőre.

Felhasznált irodalom

1. Szabó József János “Az Árpád-vonal (A Magyar Királyi Honvédség védelmi rendszere a Keleti-Kárpátokban 1940-1944)
2. Mihályi Balázs “AZ ÁRPÁD-VONAL TÖRTÉNETE 1939-1944”
3. https://mki.gov.hu/hu/hirek-hu/minden-hir-hu/a-magyar-kiralyi-honvedseg-karpataljai-hadmuveletei
4. https://www.folyoirat.tortenelemtanitas.hu/2014/12/palinkas-denes-az-arpad-vedvonal-bunkerek-es-harcok-karpataljan-05-02-04/
5. https://akovekmeselnek.hu/az-arpad-vonal-maradvanyai-karpataljan/

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