ASEM
ACADEMY OF ECONOMIC STUDIES OF MOLDOVA

Department of
Information Technology and
Information Management

Proceedings

OF INTERNATIONAL CONFERENCE

TECHNOLOGICAL INNOVATIONS IN DIGITAL SECURITY

First Edition

May 15-16, 2025

CHIȘINĂU, 2025

ACADEMY OF ECONOMIC STUDIES OF MOLDOVA

Department of Information Technology and Information Management

PROCEEDINGS

of the First Edition of the International Conference

TECHNOLOGICAL INNOVATIONS IN DIGITAL SECURITY

May 15-16, 2025, Chișinău, Moldova

Chișinău, 2025

CZU 004.056(082)
T 32

Proceedings of Scientific Articles Presented at the International Conference "Technological Innovations in Digital Security", First Edition (May 15-16, 2025)

Copyright 2025

Layout and technical editor: LOZAN Victoria

DESCRIEREA CIP A CAMERELOR NAŢIONALE A CĂRŢII DIN REPUBLICA MOLDOVA

"Technological innovations in digital security", international conference (1 ; 2025 ; Chişinău). Proceedings of the First Edition of the International Conference "Technological innovations in digital security", May 15-16, 2025, Chişinău / scientific committee: Stratan Alexandru. – Chişinău : SEP ASEM, 2025. – 256 p. : fig., tab. color.
Cerinţe de sistem: PDF Reader.
Antetit.: Academy of Economic Studies of Moldova, Department of Information Technology and Information Management. – Bibliogr. la sfârşitul art.
ISBN 978-9975-168-48-9 (PDF).
004.056(082)
T 32

ISBN 978-9975-168-48-9 (PDF).
DOI: https://doi.org/10.53486/tids2025

© Academy of Economic Studies of Moldova
© Editura ASEM, 2025

The editors are not responsible for the content of published scientific papers or for the opinions of the authors presented in this collection of articles.

SCIENTIFIC COMMITTEE

STRATAN Alexandru, Academician, Hab. Dr., Professor, Rector of the Academy of Economic Studies of Moldova, Republic of Moldova

COCIUG Victoria, PhD, Vice-Rector for Research and Partnerships, Academy of Economic Studies of Moldova, Republic of Moldova

MIHAILA Svetlana, PhD, Academy of Economic Studies of Moldova, Republic of Moldova

IONESCU Bogdan, PhD, Professor, Bucharest University of Economic Studies, Romania

OHRIMENCO Serghei, Hab. Dr., Professor, Academy of Economic Studies of Moldova, Republic of Moldova

ČEKEREVAC Zoran, Hab. Dr., Professor, Editor-in-chief, MEST Journal, Belgrad, Serbia

GOGU Emilia, PhD, Bucharest University of Economic Studies, Romania

SHISHMANOV Krasimir, PhD, Professor, D. A. Tsenov Academy of Economics, Svishtov, Bulgaria

MANASTERSKA Tatiana, PhD, Professor, University of Kalisz, Poland

VELEV Dimiter, PhD, Professor, University of National and World Economy, Bulgaria

COSTAȘ Ilie, Hab. Dr., Professor, Academy of Economic Studies of Moldova, Republic of Moldova

PARȚACHI Ion, PhD, Professor, Academy of Economic Studies of Moldova, Republic of Moldova

PERJU Veaceslav, Hab. Dr., Professor, “Alexandru cel Bun” Military Academy of the Armed Forces, Republic of Moldova

CASIAN Angela, PhD, First Vice-Rector for Education, Academy of Economic Studies of Moldova, Republic of Moldova

GUJUMAN Lucia, PhD, Academy of Economic Studies of Moldova, Republic of Moldova

TOACA Zinovia, PhD, Academy of Economic Studies of Moldova, Republic of Moldova

ZGUREANU Aureliu, PhD, Academy of Economic Studies of Moldova, Republic of Moldova

ANDRONATIEV Victor, PhD, Academy of Economic Studies of Moldova, Republic of Moldova

BARACTARI Anatolie, PhD, Academy of Economic Studies of Moldova, Republic of Moldova

DOBRIANSKA Natalia, Dr., Professor, Odesa National Technological University, Ukraine

GEORGESCU Radu-Mircea, PhD, Professor, Alexandru Ioan Cuza University of Iasi, Romania

HERȚELIU Claudiu, PhD, Professor, Bucharest University of Economic Studies, Romania

CRISTESCU Marian-Pompiliu, PhD, Professor, Lucian Blaga University, Sibiu, Romania

SHEPELEVA Olga, PhD, Odesa National Technological University, Ukraine

ZACESOVA Natalia, Hab. Dr., Professor, Cherkasy National University named after Bohdan Khmelnytsky, Ukraine

IONESCU-FELEAGA Liliana, PhD, Professor, Bucharest University of Economic Studies, Romania

CIOBANU Ghenadie, PhD, Senior Researcher at National Research Institute for Labour and Social Protection, Bucharest, Romania

LOZAN Victoria, PhD, Academy of Economic Studies of Moldova, Republic of Moldova

VERES Cristina, PhD, University of Medicine, Pharmacy, Science and Technology “George Emil Palade” Targu Mures, Romania

HIRBU Eduard, PhD, Academy of Economic Studies of Moldova, Republic of Moldova

ORLOVA Dinara, Hab. Dr., Professor, Financial University under the Government of the Russia Federation, Russia

SENKOV Valeriy, PhD, Russian State University named after A.N. Kosygin, Russia

MACOVEI Anamaria-Geanina, PhD, Stefan cel Mare University of Suceava, Romania

COLESNICOVA Tatiana, PhD, Leading Scientific Researcher, Head of Department “Social Research and Standard of Living”, Academy of Economic Studies of Moldova, Republic of Moldova

TURCAN Aurelia, PhD, Academy of Economic Studies of Moldova, Republic of Moldova

CERNEI Valeriu, expert, CISA, CRISC, ITIL, Republic of Moldova

ORGANIZING COMMITTEE

COCIUG Victoria, PhD, Vice-Rector for Research and Partnerships, Academy of Economic Studies of Moldova, Republic of Moldova

OHRIMENCO Serghei, Hab. Dr., Professor, Laboratory of Information Security, Academy of Economic Studies of Moldova, Republic of Moldova

ČEKEREVAC Zoran, Hab. Dr., Professor, Editor-in-chief, MEST Journal, Belgrad, Serbia

SHISHMANOV Krasimir, PhD, Professor, Department of Business Informatics of the D.A. Tsenov Academy of Economic, Svishtov, Bulgaria

TOACA Zinovia, PhD, Academy of Economic Studies of Moldova, Republic of Moldova

GUJUMAN Lucia, PhD, Academy of Economic Studies of Moldova, Republic of Moldova

GEORGESCU Radu-Mircea, PhD, Professor, Alexandru Ioan Cuza University of Iasi, Romania

CRISTESCU Marian-Pompiliu, PhD, Professor, Lucian Blaga University, Sibiu, Romania

LOZAN Victoria, PhD, Academy of Economic Studies of Moldova, Republic of Moldova

CATRUC Adriana, PhD Student, Academy of Economic Studies of Moldova, Republic of Moldova

HINCU Veronica, Academy of Economic Studies of Moldova, Republic of Moldova

CEBAN Svetlana, Academy of Economic Studies of Moldova, Republic of Moldova

PREFACE

The proceedings volume includes the papers presented at the First Edition of the International Conference "Technological Innovations in Digital Security" organized by the Department of Information Technology and Information Management of the Academy of Economic Studies of Moldova. The conference represents a relevant and timely scientific initiative, designed to provide a platform for dialogue and experience exchange among researchers, practitioners, and specialists from both academic and economic sectors.

The first edition of the conference, held at the Academy of Economic Studies of Moldova, Chisinau, on May 15-16, 2025, brought together scientific contributions that address, from an interdisciplinary perspective, the challenges, trends and innovative solutions in the field of digital security and global technological transformation.

In the context of the exponential growth of modern society's dependence on digital technologies and the increasing complexity of cyber risks with economic, social, and institutional impact, the development of artificial intelligence, the expansion of cyberspace, and the transformation of economic and educational processes make ensuring information security a strategic priority at both national and international levels.

The conference proceedings are structured into four thematic sections:

Emerging Technologies and Innovations in Cybersecurity

Innovative Solutions for Information Security, Data Protection Regulations, and Compliance with International Standards

Cyber Risk Management and the Economic Impact of Digital Security

Digital Transformation and Security Challenges in the Economic, Governmental, and Educational Sectors

Through the diversity of topics addressed, the conference provides a scientific framework for analyzing new trends in areas such as post-quantum cryptography, cyber risk management, data protection regulations, the application of artificial intelligence in digital security, and the impact of digital transformation on the economy and education.

The participation of researchers and experts from the Republic of Moldova, Romania, Poland, Bulgaria, Ukraine, Germany, and other European countries gives the event an international and interdisciplinary character, fostering the development of an academic network dedicated to digital security and technological innovation.

This proceedings volume reflects the joint effort of the scientific community to respond to the challenges of the digital era and to promote a culture of information security based on research, cooperation, and academic responsibility.

Acknowledgements

We extend our gratitude to all participants, authors, and members of the scientific and organizing committees for their valuable contributions to the realization of this first edition of the Technological Innovations in Digital Security conference. The Scientific Committee gratefully acknowledges the support of the ASEM Scientific Library in the preparation and publication of this proceedings volume.

CONTENTS

CYBER FRAUD AND ARTIFICIAL INTELLIGENCE

UDC: [004.056.5+004.8]:[343.72:004.6](477)
DOI: https://doi.org/10.53486/tids2025.01

LUDMILA RYBALCHENKO
Ph.D, Associate Professor
Department of Cyber Security and Information Technologies
University of Customs and Finance
Dnipro, Ukraine
luda_r@ukr.net
ORCID ID: 0000-0003-0413-8296

Abstract. The role of artificial intelligence in the life of every citizen is becoming even more important in the modern world, especially with the ever-increasing number of cyberattacks. In various spheres of life, attention is focused on the application of effective methods to ensure effective protection against cyber fraudsters. The variety of methods used by cybercriminals is growing, which makes them more difficult to detect. Decision-making to ensure the protection of personal data is based on compliance with regulatory requirements and standards in the field of information security.

The development of innovative technologies in the field of cybersecurity also affects the use of new, unusual methods of attacks used by cybercriminals. Therefore, it is important to use the latest technologies to create and ensure information security at all levels of citizens' life. The latest technologies and artificial intelligence are used to protect the modern digital environment from cybersecurity. Artificial intelligence in the field of cybersecurity plays an important role in identifying risks and protecting confidential information.

Initially, artificial intelligence was used to monitor network traffic for suspicious activity. Subsequently, it was the application of deep learning algorithms that made it possible to effectively detect active threats to ensure reliable cybersecurity.

The purpose of this paper is to study the current state of cybersecurity in Ukraine and to identify the features associated with the use of effective mechanisms to combat cyber fraud using artificial intelligence. The use of artificial intelligence in the field of cybersecurity opens up new opportunities for detecting, predicting and preventing cyber threats.

Keywords: cyber fraudsters, artificial intelligence, information security, digital environment, innovative technologies.

JEL Classification: H56, D80.

INTRODUCTION

Cybersecurity is one of the most important issues affecting the security of the modern digital environment. The number of cyber threats and their complexity are constantly growing, so effective methods and approaches to protecting information systems must be more reliable and efficient. Cybersecurity incidents involving the theft of personal data, banking secrets, and various types of cyberattacks, including attacks on critical infrastructure, pose a threat to economic stability and national security.

The use of artificial intelligence (AI) to ensure cybersecurity and protect against cyber fraud is a promising area in the modern information environment. AI technologies offer special opportunities for cyber defence.

Identifying potential threats, responding to cyber incidents, detecting malware, assessing system vulnerabilities, and predicting potential cyber attacks is possible with the use of artificial intelligence.

The introduction of digital technologies has caused a number of risks that lead to a high level of cyber threats. The pervasiveness of risks in all areas of activity threatens the normal operation of businesses, entrepreneurial activities, and government organisations. Modern cyber threats are constantly changing, making them harder to detect.

Global cyberattacks exploit software vulnerabilities, data leaks, and hackers create various cases of cybercrime that cause large financial losses for industrial enterprises and institutions. To stay a few steps ahead of fraudsters, it is necessary to apply reliable cybersecurity measures, innovative technologies to protect confidential data and prevent financial consequences from cyber fraud.

MAIN CONTENT

Malicious attacks are becoming a serious threat, so the use of artificial intelligence methods to ensure cybersecurity of organisations and enterprises is a promising area of research. AI systems based on machine learning algorithms and linguistic neural networks are widely used to protect data in modern tools [2]. One of the main areas of application of artificial intelligence is the detection of unauthorised research of an information resource. Systems automatically detect malicious code or unusual Internet traffic and respond to unusual user behaviour.

Machine learning algorithms help filter spam messages and use email filters to reduce phishing emails. Alerting employees to suspicious email activity helps reduce the risk of receiving and opening unwanted fraudulent messages. Therefore, the use of artificial intelligence is effective in combating cyber threats and ensures a high level of security in the digital environment.

The introduction of artificial intelligence in cybersecurity allows for the improvement of models designed to detect, identify, eliminate and mitigate potential threats and hazards in businesses and organisations. Artificial intelligence is able to recognise patterns that humans may not be able to detect. Detecting threats through malware, malicious attacks, analysing large amounts of data and unwanted activity, preventing possible threats, blocking malicious threats, and more, all of this is done through artificial intelligence. It is important and relevant to increase the level of prediction of future events using artificial intelligence and the effectiveness of regulatory compliance to increase the fight against cyber threats.

With the development of information technology and the use of artificial intelligence to create reliable cybersecurity tools, it is important to remember that cybercriminals can also use artificial intelligence to commit crimes and cyber threats. Therefore, the confidentiality and integration of artificial intelligence systems into critical situations is a prospect for further opportunities to increase the level of national cyber defence and reduce dangerous threats.

The availability of the object of protection is an important component of information security. The creation of a monitoring system for information security in information systems is a mandatory tool. Monitoring systems are used for the efficient management of possible risks and events. The main purpose of the monitoring system is to track the status of network services and information security subsystems using various criteria.

Improving the detection of possible threats and dangers, real-time response to the behaviour of information systems, and the ability to detect and avoid cyber threats at the stage of their manifestation are among the important issues in applying artificial intelligence capabilities to digital security strategies.

1. Materials and Methods

Cybersecurity requires improving existing cybersecurity methods, creating reliable protection against possible new threats, updating existing protection measures, monitoring cyber threats and developing protection strategies that meet the current conditions of life.

The main methods of controlling the operation and ensuring reliable protection against cyber threats are collecting and combining various data and indicators to establish control, analysing and correlating the collected data to prevent possible attacks, and automated verification of event monitoring parameters. Testing scenarios of various events allows you to analyse and confirm the availability of services at different levels. The use of automated system response in case of significant deviations from the normalised values makes it possible to make effective decisions on identifying anomalies and preventing cyber threats.

The collected anomaly detection databases help to further identify and predict events and mechanisms for further activities to create effective strategies to protect against cyber incidents.

2. Results and Discussion

In today's world of digitalised information environment, artificial intelligence has become not only an innovation but also an integral part of everyday life. It is continuously transforming various areas, helping to automate boring and routine tasks, effectively solve complex problems, and significantly improve productivity. But one of the most important areas of AI application is cybersecurity. AI is gaining critical importance as machine learning algorithms, analysing large amounts of data, detecting anomalies in network traffic, and identifying potentially dangerous vulnerabilities. AI uses technologies that can be applied in various industries, economics, finance, banking, military, education, and healthcare [1].

Artificial intelligence makes it possible to analyse large amounts of data and identify unusual situations or suspicious activity. Such actions make it possible to recognise cyber threats and attacks that may occur faster. Important priorities in the use of artificial intelligence in cybersecurity include automating threat detection, minimising errors, processing large amounts of data, predicting undesirable events and preventing them.

The use of machine learning algorithms to analyse and identify fraudster activity and respond to new types of attacks and dangers indicates that it is possible to provide reliable protection against cyber threats. The latest intelligent systems are able to respond to cyber threats in a timely manner and provide timely protection against network access. Processing large volumes of information in a minimum amount of time helps to timely anticipate and prevent possible threats or cyber attacks. The speed of decision-making on threat detection is an effective component in the use of artificial intelligence to reduce cyber threats.

CONCLUSIONS

The problems of information security and protection of society from the negative impact of cybercrime can be countered by artificial intelligence. The main issues are malfunctioning of hardware and software, proliferation of information weapons, use of malware, leakage of confidential information, industrial espionage, technological influences, etc. Artificial intelligence technologies are one of the most effective tools in the field of cybersecurity. Fraud detection, unwanted intrusions, malware, risk assessment, network threats and other threats can be prevented and neutralised using artificial intelligence to improve the state of protection against cyber threats.

Artificial intelligence increases the ability of organisations to anticipate, prevent, defend against threats and control system access passwords, creating a strong defence against cybercrime. It is artificial intelligence that will expand the ability to protect the digital environment using the latest information technologies.

REFERENCES

1. The role of artificial intelligence in cybersecurity: predicting and preventing attacks. 2024. Available at: https://eba.com.ua/rol-shtuchnogo-intelektu-v-kiberbezpetsi-peredbachennya-ta-zapobigannya-atakam/ [Accessde 05.06.2025]
2. Rybalchenko L. V. (2022). Cybercrime in the global space. *Scientific Bulletin of the Dnipropetrovsk State University of Internal Affairs,* special Issue № 2 (121). pp. 524-530. https://doi.org/10.31733/2078-3566-2022-6-524-530
3. Rybalchenko L. V., Haborets O. A. & Prokopovych-Tkachenko D. I. (2024). Cyber Resilience: Global Threats And National Cyber Defense Strategies. *Systems and Technologies*, *68*(2), 95-101. https://doi.org/10.32782/2521-6643-2024-2-68.11
4. Carvalho, J.-P. (2025). The political-economic risks of AI. SSRN. https://doi.org/10.2139/ssrn.5137622

QUANTUM CRYPTOGRAPHY AND POST-QUANTUM SECURITY: CURRENT STATE, CHALLENGES, AND STRATEGIC DIRECTIONS

UDC: 004.056.55:530.145
DOI: https://doi.org/10.53486/tids2025.02

ZGUREANU AURELIU
Academy of Economic Studies of Moldova
zgureanu.aureliu@ase.md
ORCID ID: 0000-0003-3301-2457

ANDRONATIEV VICTOR
Academy of Economic Studies of Moldova
andronatiev@ase.md
ORCID ID: 0000-0002-0294-457X

Abstract. Quantum cryptography is a new field of research that tries to resolve the critical security concerns brought by quantum computing. There is an increasing effort to construct quantum-safe cryptographic solutions due to the threat that quantum algorithms, especially Shor's and Grover's, pose to popular cryptographic systems. Traditional cryptographic methods like RSA and ECC are based on problems that will be efficiently tackled by quantum computers, putting them at risk in a post-quantum world. Also, symmetric cryptography, despite being stronger against that threat, faces its own challenges as well, especially from Grover's algorithm, which effectively slashes the key length by half, increasing the necessary key size for maintaining security.

The rise of quantum technologies has come with additional risks such as cyber threats and security vulnerabilities, therefore creating a need for research in quantum as well as post-quantum cryptography. Quantum cryptography particularly Quantum Key Distribution (QKD) exploits quantum mechanical phenomena to safeguard the exchange of cryptographic keys with information-theoretic security. Eavesdropping in QKD is always detectable. However, due to stringent hardware requirements, QKD is limited for broader practical use. Meanwhile, post-quantum cryptography (PQC) seeks to devise traditional algorithms for cryptography which will continue to remain secure under attacks from quantum computers. Such algorithms include lattice-based cryptography and code-based cryptography which, among others, are being standardized by NIST.

This paper examines the current status of quantum cryptography alongside the vulnerabilities present in traditional systems as well as the efforts dedicated to implementing post-quantum algorithms. It covers the standardization and implementation challenges while also outlining prospective future research avenues aimed at reinforcing the cryptographic infrastructure in the era of quantum computing.

Keywords: Quantum Cryptography, Post-Quantum Cryptography, Quantum Key Distribution, Cryptographic Algorithms Quantum Computing.

JEL Classification: O33, D80, G23.

INTRODUCTION

The rapid pace of technological advancement has made quantum cryptography one of the most crucial domains in the world's race to protect digital infrastructure. The increasing competition in computing technology and the possible widespread adoption of quantum computers will put to test most traditional cryptographic techniques that provide secure communication channels, protect financial information, or safeguard data for governments. The consequences are dire. The existence of large-scale quantum computers would be catastrophic for the modern public key systems RSA, DSA, and ECC, which are used widely all over the world and could be broken in a matter of hours, exposing sensitive information that was previously considered secure for decades.

This concern is indeed valid, as both symmetric and asymmetric encryption systems have come under attack by quantum algorithms. Shor's algorithm, as an example, is able to factor large integers and calculate discrete logarithms at an exponential rate compared to classical algorithms. This essentially weakens the security of public key protocols that are used by almost everyone, making them vulnerable (Shor, P. W., 1994). On the other hand, symmetric encryption systems are not safe either. With his less destructive Grover's algorithm, symmetric encryption algorithms like AES are vulnerable too (Bennett *et al*., 1997). Because of both these algorithms, there is an added need for resilience in systems that rely on symmetric cryptography and an overhaul of the entire system's threat model in a post-quantum environment.

To address these newly developing challenges, researchers and organizations have created quantum cryptography and post-quantum cryptography as two complementary solutions. Quantum cryptography, and especially Quantum Key Distribution (QKD), uses the principles of quantum mechanics to provide security guarantees that are, in theory, impossible to break. It enables two parties to securely share keys with assurance of detection of any attempting eavesdropping due to quantum phenomena like superposition and the no-cloning theorem (Bennett, C.H. and Wiesner, S.J., 1992). Nevertheless, while QKD provides unmatched security, it is impractical for real world use because of physical range limitations, expensive equipment, and complex integration with traditional networks.

On the other hand, post-quantum cryptography (PQC) is a subclass of cryptographic algorithms meant to be secure against attacks from classical computers and quantum computers. They are based on certain mathematical problems believed to be very difficult to solve, even with the aid of quantum computers, such as those based on lattices, codes, and multivariate polynomials (ENISA, 2020). Unlike QKD, PQC can be implemented on traditional networks without the need for specialized quantum hardware, making it more readily scalable in the near term. Recognizing its strategic relevance, NIST commenced a pre-emptive globalization standardization initiative in 2016, which resulted in the selection of some promising post-quantum algorithms in 2022 (NIST, 2022a).

This paper examines the scope of quantum cryptography and countermeasures in post-quantum cryptography. It describes the shortcomings of traditional cryptography within information-theoretic frameworks, discusses quantum-initiated attacks, analyzes attempts to defend against them, and describes the actual work aimed at protecting information systems. It focuses on the normalization work, the policy implications considering the adoption barriers from the industrial side, and the impact on the cyberspace landscape, digital infrastructure, as well as policy making. The paper aspires to enhance the comprehension of the use of those measures expected to be taken on in the upcoming years.

MAIN CONTENT

1. Classical Cryptography vs. Quantum Computing

The bedrock of traditional cryptography, which has sustained digital security for over forty years now, rests on certain mathematical problems that are tough to solve using any conventional computing approaches. Solving large integer factorization, computing discrete logarithms, or even elliptic curve discrete logarithm problems are some of these hard problems. These hardships provide support for most public key cryptosystems employed today due to being hardware infeasible.

Quantum computing poses the most threat to asymmetric cryptography. Popularly known algorithms such as RSA, Diffie-Hellman and ECC face harsh issues due to underlying such weak frameworks. These asymmetric methods rely on problems solvable with quantum mechanics such as Shor's algorithm. For example, the security underpinning RSA relies on the difficulty of factorization of two large prime numbers. While classically it takes sub-exponential time for a computer to accomplish this, quantum computers using Shor's algorithm will be able to do so in polynomial time (Shor, P. W., 1994). This indicates that with adequate advancements in quantum computing, mainly requiring thousands of logical qubits with error correction, RSA and ECC would instantaneously lose relevance alongside.

There are risks to digital signatures, which are critical to authentication and non-repudiation in modern communications. Weaker points of ECC pose the same threat to ECDSA, which is prevalent in several blockchain use cases and secure messaging applications. The global public key infrastructure that supports HTTPS, email encryption, and VPNs would face existential rupture in a post-quantum world without the adoption of new cryptographic primitives.

In contrast, symmetric cryptography is relatively more resilient. AES and other algorithms undergo no change in-status in the post-quantum setting, but rather their effective power is crippled. Proposed in 1996, Grover's algorithm allows a quantum computer to search an unordered list of N items in $O(\sqrt{N})$ time, which in turn, shrinks brute-force attack (Bennett *et al.*, 1997). To illustrate, a quantum adversary would only receive a mere 64-bit protection from a 128-bit AES key. To counter this, NIST suggests adding extra brute-force replication layers by rising to AES-256. The same concept applies to hash-based functions where they shall be tested to ensure compliance to post-quantum standards for resistance against collisions and pre-images.

Regardless, the practical impact of Grover's Algorithm is much less pronounced than that of Shor's. The $\sqrt{N}$ exponential speedup provided by Grover's algorithm does not significantly change the security expectations for symmetric cryptosystems. Moreover, the quantum circuit depth and error correction layers suggest that the symmetric frameworks needed to effectively implement quantum algorithms are far too advanced for the available quantum resources in the near term.

The concept of "harvest now, decrypt later" is particularly perilous in the context of quantum computing threats. Bad actors could intercept encrypted communications protected by RSA or ECC, then await the emergence of sufficiently powerful quantum computers to decrypt the stored information. This scenario poses acute risk to sensitive governmental, military, and financial information that requires long-term, stringent confidentiality measures.

Thus, while symmetric cryptography remains a viable option in the quantum era (with strengthened parameters), the imminent collapse of asymmetric systems highlights the need for proactive migration strategies. There is an immediate need for cryptographers and cybersecurity experts to pivot from the out-dated public-key infrastructure to a post-quantum public-key framework that offers perpetual confidentiality and credibility.

2. Quantum and Post-Quantum Cryptography

In light of the functioning capabilities of quantum computers, there have been numerous paths explored within the field of cryptography. Each of these paths vary in their complexity, reasoning, and structure. One that stands out is quantum cryptography. It employs the foundations of quantum physics to create secure channels of communication, enabling optimal protection against eavesdroppers. This quantum-mechanics-based solution operates seamlessly alongside post-quantum cryptography, which relies on classical hardware and complex mathematical problems believed to be resistant to quantum attacks. Both approaches tackle the quantum threat, however, they do so from different angles, accompanied by different benefits and limitations.

Quantum cryptography, particularly QKD, is regarded as one of the most secure methods of communication. Using quantum particles like photons, QKD allows two parties to create a shared secret key. Its security is founded on the no-cloning theorem and Heisenberg's uncertainty principle, which guarantees that any eavesdropping on the system will disturb the particles' quantum state and hence be detectable (Bennett, C.H. and Wiesner, S.J., 1992). Protocols such as BB84 and E91 have been tested and put into pilot systems across the globe, including quantum-secured inter-bank and inter-agency communication for a government (NIST, 2018).

A cornerstone of QKD is the information-theoretic security of the system. Unlike other methods, information-theoretic security is not based on computational assumptions. Furthermore, it is immune to both classical and quantum attacks, as long as the implementation is perfect with no side-channel attacks. Despite this, practical issues with QKD remain:

- the distance of transmission is limited by photon loss in fibre-optic cables;
- for longer distances, trusted nodes or quantum repeaters are needed which reintroduce points of susceptibility;
- the expenditure required for quantum devices, such as single-photon detectors and quantum random number generators, is exorbitant;
- there are difficulties in integrating traditional systems with key management infrastructures.

Regardless of the setbacks, QKD networks are expanding. For instance, China's QUESS satellite has conducted space-based quantum key exchange, advancing contemporary quantum global communication (Liao, S. K. et al., 2017).

On the contrary, *post-quantum cryptography* aims to defeat both quantum and classical adversaries by designing new cryptographic algorithms. Because these algorithms can be executed on classical computers, they are easier to assimilate into existing infrastructure. Unlike QKD, PQC does not rely on the physical realization of quantum phenomena but rather depends on robust mathematical challenges which, to date, there is no efficient quantum solution known.

Several families of cryptographic primitives have been identified as strong candidates for PQC:

- *Lattice-based cryptography*: These algorithms rely on the hardness of problems like the Shortest Vector Problem and Learning With Errors (Gentry, C., and Peikert, C., 2010). Not only do lattice-based schemes support encryption and signatures, they also include advanced functionalities such as homomorphic encryption. NIST has selected CRYSTALS-Kyber (for key encapsulation) and CRYSTALS-Dilithium (for digital signatures) for their standardization (Lyubashevsky *et al*., 2010) (NIST, 2022a).
- *Code-based cryptography*: Originating from the McEliece cryptosystem, code-based schemes are characterized by high security, although they tend to have large key sizes (Weger, V. et al., 2024). They are most beneficial in scenarios where the speed and size of a signature are less important than strength.
- *Multivariate polynomial cryptography*: This scheme is centred on multivariate quadratic equations over finite fields and is mainly used for digital signatures. Even though some

multivariate systems have been broken, others continue to undergo scrutiny as strong candidates.

- *Hash-based cryptography*: This type of scheme works with the security provided by cryptographic hash functions. Hash-based systems are ideal for use in digital signatures within resource-constrained environments (Vidaković, M., and Miličević, K., 2023). One such example is the SPHINCS+ signature scheme, which is built entirely on hash functions and offers very conservative security guarantees.

Remaining adaptable and scalable is the most notable advantage of PQC. Reconfiguration becomes easier because existing infrastructure can be leveraged for software and hardware implementation of algorithms. Since 2016, NIST has been spearheading a standalone PQC standardization project, from which finalists as well as alternate candidates are undergoing validation for performance, side-channel resilience, and overall practicality of deployment (NIST, 2022a).

Despite these overcoming these milestones, PQC still poses some of the following challenges:

- public key and ciphertext size issued by some schemes can create bandwidth strain and performance hindrance;
- hardware and software compatibility need to be audited and updated;
- migration for legacy systems becomes complicated for embedded systems;
- a number of these schemes are considered safe today, though there always some risk of a currently unknown quantum algorithm emerging which renders them useless.

Quantum and post-quantum techniques combined create a robust and sophisticated defensive approach. While QKD offers unrivalled security in theory, PQC serves a more practical use and provides ease of mass scaling prematurely in anticipation for proposed quantum threats on the horizon.

3. Standardization and Implementation

Replacing obsolete algorithms with newer ones is not sufficient for transitioning to quantum-resistant cryptography. Instead, it requires a more comprehensive strategy that includes resolving technological, organizational, and policy issues within multiple spheres. Though the shift is vital for avoiding a cryptographic collapse in the face of advancing quantum computers, it simultaneously guarantees a difficult balance of securing systems, ensuring compatibility, and minimizing disruptions.

Organizations must begin by identifying systems that rely on quantum-vulnerable algorithms. This includes algorithms utilized in TLS/SSL, VPNs, Secure Email, Digital Signatures, and Certificate Authorities. A risk assessment should be able to correlate data boundaries such as confidentiality lifetime. For instance, medical documents have strict privacy requirements for extended periods. These are ideal for the “store now, decrypt later” attack strategy.

Everyone, particularly government operators and critical infrastructure, must inventory their cryptographic escrows and determine where immediate action is necessary most. CISA's PQC roadmap final draft from 2022 suggests federal bodies adopt post-quantum cryptography and incorporates crypto-agility, hybrid cryptographic schemes, and pilot testing aimed at PQC (CISA Insights, 2022).

The importance of *crypto-agility* – the ability to change cryptographic schemes without a full system overhaul – is pivotal in transitional phases. Systems must be modular, flexible, and balanced so that updates do not heavily impact performance benchmarks or security thresholds.

A more practical approach to this dilemma is accepting a combination of classical and post-quantum algorithms – dubbed the hybrid cryptographic approach. Imagine a TLS handshake that uses RSA together with a lattice-based key agreement. This approach provides a secure bridge to the future while current security measures are sustained (Peikert, C., 2016). Easing the departure from outdated algorithms stimulates gradual adoption as standards progress prevents stagnation.

While the need for some form of migration is evident, there are a number of unresolved operational and technical issues:

- *Performance*: some PQC algorithms come with increased key size and ciphertext size. A case in point, McEliece has public key sizes on the order of several hundred kilobytes which poses an issue for bandwidth, memory constrained systems.
- *Hardware limits*: embedded systems like IoT devices frequently lack the necessary resources to run high-demand PQC algorithms, rendering such retrofits nearly impossible.
- *Legacy systems*: older systems are likely to be hard-wired using classic algorithms and therefore need more flexibility than they can afford.
- *Standardization lag*: while NIST has chosen a handful of algorithms, formal final standards and interoperability guidelines are still in progress. This poses risks and reluctance for large-scale deployment.

In addition, the real-world testing of post-quantum algorithms is still ongoing. Organizations need to develop test environments and engage in pilot programs before committing to full implementation.

Cryptographic migration is a global issue, and successful transition will require international coordination. For all countries with differing levels of infrastructure maturity, regulatory framework, and threat models, convergence on applicable standards and practices is essential.

Institutions like International Telecommunication Union and European Union Agency for Cybersecurity (ENISA) have embarked on developing studies and frameworks to aid in the adoption of quantum-resistant technologies. Other organizations such as NATO and the European Commission have also incorporated quantum-safe resiliency in their cybersecurity strategies highlighting the need for collective resilience (ENISA, 2020).

At the national level, governments are:

- financing research and development in post-quantum cryptography:
- developing guidelines and timelines for the migration process;
- building quantum communication testbeds;
- building regulatory checklists and compliance mandates.

Ultimately, transitioning to quantum-resistant systems will require collaboration between governments, academia, and industry, as well as a proactive investment in education, tooling, and awareness.

4. Case Studies and Practical Applications

To better understand how quantum and post-quantum cryptography are being applied in real-world contexts, this section reviews several case studies across industries. These examples illustrate how organizations are preparing for quantum threats and deploying secure technologies in diverse environments - from national security to commercial systems.

Financial Sector: Secure Banking and Payments. Due to the financial industry relying on data confidentiality, reputation, and operational integrity, it remains one of the sectors most susceptible to quantum threats. Banking institutions heavily invest in cryptographic technologies for online banking, Secure SWIFT messaging, digital signature frameworks for transaction validation, and maintaining blockchain infrastructures.

A proactive example is ABN AMRO Bank in the Netherlands who, together with academic partners, investigated quantum key distribution (QKD) for secure interbank communications. In this project, a QKD link was used to secure high-valued communications between data centres using quantum channels augmented with classical encryption. The results not only proved the possibility of extending QKD into financial networks, but demonstrated significant problems in synchronization, mutual authentication, and scalability (ABN AMRO, 2019).

Other financial institutions have already joined PQC pilot projects, especially in relation to blockchain developments. PQC-based signature schemes are being implemented in testbeds of blockchain frameworks aimed at quantum resistance. This is vital since blockchain technologies supporting cryptocurrencies, including Bitcoin, utilize ECDSA for transaction signing which is known to be quantum vulnerable.

Government and Defence: National Quantum Communication Networks. Governments are investing in national infrastructures for quantum communication to safeguard classified information. China's Beijing-Shanghai quantum backbone, along with the Micius satellite (part of the QUESS program) are the most advanced QKD implementations to date. These systems have enabled secure video calls and data transmission through the use of entangled photons over thousands of kilometres (Liao, S. K. et al., 2017).

Similarly, the European Quantum Communication Infrastructure (EuroQCI) project aims to establish a QKD-based secure communication network between EU member states, expanding through fibre and satellite connections. This initiative is funded by the European Commission and the European Space Agency as part of the broader Digital Europe Programme. EuroQCI not only focuses on the technical deployment, but also on standardization and coordinated policy development among the member states (European Commission, 2020).

In the United States, the Department of Energy (DOE) partnered with several national laboratories and universities to develop the Quantum Internet Blueprint, which proposes a secure quantum communication layer to be integrated with the classical Internet (US DOE, 2020).

Industrial Applications: Cloud and IoT Security. One of the common cloud service providers, Amazon Web Services, Google Cloud, and Microsoft Azure are experimenting with post-quantum algorithms within their secure communication protocols. Post-quantum TLS key exchanges were tested in real world applications via Kyber (a lattice-based algorithm) integrated into Chrome Canary by Google in 2022. They aimed to prepare ecosystems in browsers to be able to switch seamlessly once PQC standards are issued. Their focus was ascertaining Experiential Value Optimization (Google Security Blog, 2022.).

IoT devices with their omnipresent nature and limited computational resources puts forth another challenging concern. Researchers are looking into PQC implementations that are more lightweight, specifically hash-based and lattice schemes that minimize operational and memory overhead (Cohn-Gordon, K., and Brierley, H, 2019). Embedded systems are being specially focused upon by the Internet Engineering Task Force (IETF) and NIST's Lightweight Cryptography Project as the develop pertinent guidelines and libraries.

An emerging trend is the development of hybrid encryption stacks for cloud and IoT systems that combine existing RSA or ECC protocols with post-quantum counterparts. With regard to future-safe architectures, this layered methodology offers quantum-elusive protection while still sustaining backward adaptability.

Academic and Research Institutions. Scholarly pursuits focus on advancing the frontiers of quantum and post-quantum cryptography. University and national laboratory collaborative projects have developed experimental quantum networks in Vienna, Tokyo, and Geneva where QKD and quantum repeaters are tested in live environments. These testbeds yield valuable data concerning photon loss, synchronization errors, and system resilience.

Moreover, leading universities are at the forefront of cryptanalysis, where newly developed post-quantum schemes are benchmarked against classical and quantum contenders. The MIT, ETH Zurich, KU Leuven, and University of Waterloo actively participate in algorithm design and review for the NIST PQC competition.

These efforts in practice illustrate the progress, albeit inconsistent in speed and scale, towards a globally integrated quantum-safe cryptography infrastructure.

5. Quantum cryptography: Future directions

The shift from theoretical models to functional quantum computers marks a new chapter for the field of cryptography, presenting it with one of the greatest challenges and unparalleled opportunities. Addressing challenges of post-quantum computing not only entails implementing novel algorithms and systems, but demands a fundamental restructuring of security frameworks, trust models, and coordination on technology around the world.

Thus, among the most important research and development directions, the following can be mentioned:

1. *Total standardization and implementation of post-quantum cryptographic algorithms*. Once NIST selects the finalist algorithms CRYSTALS-Kyber, CRYSTALS-Dilithium, SPHINCS+, among others, NIST released, on August 13, 2024, final versions of the first three Post Quantum Crypto Standards: FIPS 203, FIPS 204, and FIPS 205 (NIST, 202ab), (NIST, 2024). These standards will facilitate cross adoption throughout government, military, industry, and civilian entities. Simultaneously, IETF, ISO/IEC and other standardization bodies are also modifying and developing certain protocols such as TLS, VPNs, and SSH to accommodate PQC.

2. *The design of quantum-resistant systems and their components*. In addition to cryptographic primitives, system design must also account for larger key sizes, new certificate formats, and hybrid methods of authentication. This includes software such as OpenSSL and BoringSSL, operating systems, and secure hardware like Trusted Platform Modules and HSMs.

3. *The issues of identity and authentication from the quantum viewpoint*. Proven challenges and relevant research are being done as regards to authentication, especially with zero-knowledge proofs, biometrics, and quantum-resistant identity-based encryption. Blockchain identity solutions also face revision, as existing systems rely heavily on ECDSA and other vulnerable schemes.

4. *Development of quantum cryptographic networks and their hardware*. Quantum hardware innovations such as quantum repeaters, photonic chips, and room temperature single-photon detectors will enhance the accessibility and scalability of quantum communications. Quantum router, entanglement distribution, and quantum internet architectures are imminent areas of research that will redefine secure communication networks of the future.

5. *Global cooperation and policy alignment*. Due to the cross-border nature of digital communications, the open world society needs to establish common cryptographic frameworks for

international interoperability, trade controls, and collaborative research and development policies. Effective cyber diplomacy and information-sharing amongst the quantum leadership consortium (U.S., EU, China, Japan) will be essential to prevent fragmented or insecure transitions.

6. *Education and development of the workforce*. With the advancement of cryptographic systems, designing, implementing, and auditing such systems will require increasingly sophisticated skills. While universities are starting to create programs in quantum cybersecurity, organizations like ENISA and CISA have launched targeted campaigns focused on raising awareness and developing relevant competencies (ENISA, 2021). Bridging the talent gap in quantum-safe security is as crucial as the technologies themselves.

CONCLUSIONS

Quantum computing has the capacity to advance science, medicine and artificial intelligence; however, it poses an immediate, direct existential risk to traditional cryptographic systems. The sustained progress being made in quantum hardware brings with it the need to accelerate the adaptation of existing frameworks.

Symmetric cryptography, which is only moderately impacted by Grover's algorithm, can be defended against with greater key lengths in conjunction with proper cryptographic design. As for asymmetric cryptography, it is under immediate threat and must adapt a structured transition to quantum-safe substitutes without delay.

In response to the consequences of quantum technologies, two options are emerging: the theoretical securitization guarantees of quantum cryptography, such as QKD, and the more practical, scalable defence provided by post-quantum algorithms. It seems likely that both options will be present in future systems, each fulfilling different functions depending upon the system's sensitivity, size, and implementation expense.

The shift to a quantum-resilient cryptographic backbone will move through stages of development and refinement, research and testing, standardization, and the education of specialists in the field. This transition will take time and cannot be done overnight. It is equally important to realize that the consequences of inaction are profound. The time to act is now. By adopting post-quantum and quantum-cryptography technologies, we would be able to bolster global digital ecosystems in order to ensure privacy, integrity, and authenticity as fundamental guarantees even in the age of quantum technology.

REFERENCES

1. ABN AMRO, 2019. *Uses Quantum Key Distribution for Secure Bank Communication*. Available at: https://www.abnamro.com [Accessed 22.03.2025].
2. Bennett, C. H., Bernstein, E., Brassard, G. and Vazirani, U., 1997. The strengths and weaknesses of quantum computation. *SIAM Journal on Computing*. 26 (5), pp. 1510–1523.
3. Bennett, C.H. and Wiesner, S.J., 1992. Communication via One- and Two-Particle Operators on Einstein-Podolsky-Rosen States. *Physical Review Letters*, 69, pp. 2881-2884.
4. CISA Insights, 2022. *Preparing Critical Infrastructure for Post-Quantum Cryptography*. Available at: https://www.cisa.gov/sites/default/files/publications/cisa_insight_post_quantum_cryptography_508.pdf [Accessed 11.04.2025].
5. Cohn-Gordon, K., and Brierley, H, 2019. Lightweight Cryptography for the Internet of Things. *Proceedings of the IEEE European Symposium on Security and Privacy*, pp. 321-332.

6. ENISA, 2020. *Quantum-Safe Cryptography and Post-Quantum Cryptographic Algorithms*. Available at: https://www.enisa.europa.eu/publications/quantum-safe-cryptography [Accessed 09.04.2025].
7. ENISA, 2021. *Quantum Cryptography and Security Challenges in Europe*. Available at: https://www.enisa.europa.eu/publications/quantum-cryptography-in-europe [Accessed 12.11.2024].
8. European Commission, 2020. *EuroQCI: European Quantum Communication Infrastructure*. Available at https://ec.europa.eu/digital-strategy/our-policies/european-quantum-communication-infrastructure_en, [Accessed 07.02.2025].
9. Google Security Blog, 2022. *Chrome's Implementation of Post-Quantum Cryptography*. Available at https://security.googleblog.com/2022/06/chromes-post-quantum-cryptography-pilot.html, [Accessed 22.04.2025].
10. Liao, S. K., Cai, W. Q. , Liu, W. Y. *et al.*, 2017. Satellite-to-ground quantum key distribution, *Nature*, 549(7670), pp. 43–47.
11. Lyubashevsky, V., Peikert, C., and Regev, O., 2010. On the hardness of ideal lattice problems. *Journal of the ACM (JACM)*, 62(6), pp. 1-50.
12. NIST, 2018. NISTIR 8267: *Quantum Key Distribution and its Use in Secure Communications*. Available at: https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8267.pdf [Accessed 22.10.2024].
13. NIST, 2022a. *Post-Quantum Cryptography Project*. Available at: https://csrc.nist.gov/projects/post-quantum-cryptography [Accessed 03.11.2024].
14. NIST, 2022b. *Post-Quantum Cryptography Standardization: Finalists*. Available at: https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions [Accessed 03.11.2024].
15. NIST, 2024. *NIST Releases First 3 Finalized Post-Quantum Encryption Standards*. Available at: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards [Accessed 03.11.2024].
16. Peikert, C., 2016. Lattice cryptography for the masses. *Communications of the ACM*, 59(5), pp. 45-52.
17. Shor, P. W., 1994. Algorithms for quantum computation: Discrete logarithms and factoring. *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, pp. 124-134.
18. US DOE, 2020. *The Quantum Internet Blueprint: Building a Secure Quantum Network*. Available at: https://www.energy.gov/science/quantum-internet-blueprint [Accessed 13.04.2025].
19. Vidaković, M., and Miličević, K., 2023. Performance and Applicability of Post-Quantum Digital Signature Algorithms in Resource-Constrained Environments. *Algorithms*, 16(11), 518.
20. Weger, V., Gassner, N. and Rosenthal, J., 2024. *A Survey on Code-based Cryptography*. Available at https://arxiv.org/pdf/2201.07119, [Accessed 22.04.2025].
21. Gentry, C., and Peikert, C., 2010. Approximating the Shortest Vector Problem in Lattices. *Proceedings of the 41st Annual ACM Symposium on Theory of Computing*, pp. 237-246.

SECURITY INCIDENT ANALYSIS IN ELECTRICITY METERING SYSTEMS: UNAUTHORIZED ACCESS TO SMART MEASURING DEVICES

UDC: 004.056.5:621.317.78
DOI: https://doi.org/10.53486/tids2025.03

CONIUC SVETLANA
S.C. ADD-PRODUCTION S.R.L.
Svetlana.Coniuc@gmail.com
ORCID ID: 0009-0003-6796-9940

RUSANOV ALEXEI
S.C. ADD-TECHNOLOGY S.R.L.
Rusanov.Alexei@gmail.com
ORCID ID: 0000-0001-6573-9242

Abstract. Intelligent energy systems employ smart metering to enable bidirectional communication among operators, distributed energy resources (DER), and end users. Components include Advanced Metering Infrastructure for consumption data; metering devices and controllers for monitoring; communication networks linking assets; SCADA, EMS, and DMS systems coordinating DER; and renewable sources for sustainability. These reduce losses and optimize the supply – demand balance, enhancing reliability. Integrating renewables requires adaptive control and predictive models, which improves decision-making processes.

However, increased complexity enlarges the cyberattack surface. Millions of connected metering devices and controllers risk data integrity, confidentiality, and power delivery. Historical incidents illustrate this: RedEcho (attack originating from China, targeting India, 2021) used ShadowPad for exfiltration; Sandworm (Ukraine, 2022) targeted substation trip logic; Volt Typhoon (USA, 2024) conducted IT/OT reconnaissance; and Hydro-Québec (Canada, 2023) disrupted customer apps.

Since the mid-2000s, research has examined vulnerabilities arising from IoT integration and decentralized resources, necessitating multi-layered security. Standards such as NIST CSF, IEC 62351, and NERC CIP recommend layered architectures with cryptographic protection, firewalls, IDS/IPS, access control, and network segmentation. AI and machine learning enhance anomaly detection via real-time telemetry, while blockchain offers immutable transaction records for DER platforms despite challenges in scalability and energy consumption. Emerging directions include Post-Quantum Cryptography for secure communications and Zero Trust for continuous verification.

Comparative analyses reveal traditional methods – encryption, firewalls, IDS – lack adaptability and scalability against evolving threats. Future priorities include AI-based detection, blockchain-enabled architectures, PQC deployment, and phased Zero Trust adoption. Addressing implementation cost, data privacy, legacy-system compatibility, and regulatory gaps is vital for intelligent energy system resilience. This paper summarizes the challenges and proposed solutions for safeguarding critical infrastructure and ensuring international regulatory alignment.

Keywords: smart grid, cybersecurity, smart meters, DLMS/COSEM, vulnerability.

JEL Classification: L94, O33.

INTRODUCTION

The term “Smart Grid” refers to an evolutionary stage in the development of the electrical power system in which conventional electromechanical devices are augmented with intelligent sensors and equipment capable of collecting, transmitting, and analyzing real-time data. Unlike the traditional unidirectional flow of energy “from generation to consumption,” Smart Grids establish an interactive, decentralized architecture featuring bidirectional communication among operators, distributed energy resources, and end users [3, 10]. The key components of such grids include:

- Advanced Metering Infrastructure (AMI), which gathers real-time consumption data;
- Intelligent sensors and controllers, facilitating extended monitoring of line and equipment status;
- Communication and data transmission systems, interconnecting geographically dispersed assets into a unified network;
- Supervisory Control and Data Acquisition (SCADA), Energy Management Systems (EMS), and Distribution Management Systems (DMS), coordinating the operation of Distributed Energy Resources (DER);
- Renewable energy sources, such as solar and wind installations, integrated into the infrastructure to enhance environmental sustainability and supply flexibility.

Modern Smart Grids enable reduced transmission losses, optimize the supply – demand balance through load forecasting and adaptive distribution control, thereby contributing to the resilience and reliability of power delivery. However, the incorporation of distributed renewable sources necessitates adaptive control algorithms and predictive models to account for fluctuating power outputs and the unpredictability of renewable generation.

Concurrently, the expansion of functionality and increasing architectural complexity of Smart Grids significantly enlarge their attack surface. Millions of intelligent devices interconnected within a single network become potential entry points for adversaries. Without adequate protective measures, any device, communication channel, or control element can be compromised, threatening not only data integrity and confidentiality but also the uninterrupted delivery of electricity [2]. A successful attack on the power grid could trigger cascading consequences: healthcare systems, transportation, financial infrastructure, and public safety agencies might be deprived of power.

Historical examples of cyberattacks on energy networks demonstrate geographic breadth and diverse technical approaches:

- **RedEcho (China, January 2021):** Attackers injected the ShadowPad backdoor into India’s regional control centers, enabling clandestine data exfiltration and potential preparation for destructive assaults on critical assets [6].
- **Sandworm (Russia, April 2022):** A variant of the Industroyer2 malware attempted to alter the tripping logic at several Ukrainian substations with the aim of causing large-scale outages. Prompt intervention by CERT-UA and ESET prevented malware propagation and equipment shutdown [7].
- **Volt Typhoon (USA, February–November 2024):** Prolonged covert activities within the IT/OT networks of the Littleton Electric Light and Water Department (Massachusetts) allowed adversaries to gather data on load patterns and control system configurations, laying the groundwork for potential sabotage [9].

- **Hydro-Québec (Canada, 2023):** Compromise of public web and mobile applications responsible for notifying customers about power status led to a multi-hour loss of access to current information, eroding consumer trust. Nevertheless, the core electrical infrastructure remained intact.

Thus, Smart Grids represent a valuable yet vulnerable target for cyberattacks. Ensuring protection against such threats is a top priority for national security and the stability of critical infrastructure.

MAIN CONTENT

The cybersecurity concerns of Smart Grids have attracted the attention of researchers since the mid-2000s. Several seminal works focus on threat analysis and the development of models for constructing secure infrastructure.

Smart Grids are characterized by high interconnectedness and extensive integration of Internet of Things (IoT) devices, which substantially expands their attack surface [1]. According to multiple analytical reports, approximately 40 % of the most prevalent cyberattacks in recent years have targeted utility services. In Spain, for instance, a national assessment revealed that DoS attacks and data breaches pose serious risks to Smart Grid operations. The proliferation of intelligent sensors, controllers, and automated management systems leads to increasingly complex communication protocols, introducing additional vulnerabilities at the data link and transport layers.

The integration of Renewable Energy Resources (DER) presents particular challenges because decentralized installations require secure data exchange protocols for coordination and power flow management [8]. The literature emphasizes the necessity of a multi-layered security approach encompassing cryptographic protection at the link layer, anomaly detection systems, and application-level access control.

Among international standards relevant to Smart Grid cybersecurity are:

- **NIST Cybersecurity Framework (CSF)**, which offers comprehensive guidelines based on established standards for evaluating information security maturity and managing risks within the energy sector;
- **IEC 62351** series, specifying security requirements for communication protocols in the power industry (including encryption, key management, and access control);
- **NERC CIP (Critical Infrastructure Protection)**, mandating cybersecurity requirements for U.S. grid operators to safeguard critical infrastructure against cyber threats.

Overall, these standards propose a stratified security architecture, where each layer (physical, network, application) is fortified with dedicated measures. Cryptographic services, firewalls, and network segmentation secure communication channels; IDS/IPS (Intrusion Detection/Prevention Systems) detect and block intrusions; and access control systems manage user and device privileges.

Machine learning methods for anomaly detection can significantly enhance the accuracy of identifying previously unseen threats. In Lee and Wang [5], a convolutional neural network – based IDS was proposed to analyze real-time network traffic, substantially reducing false positives. This approach adapts to emerging attack patterns and enables rapid incident response. However, effective training of AI models demands substantial volumes of relevant data, and the models themselves may be susceptible to adversarial attacks – a subject of active research.

Other studies demonstrate the effectiveness of hybrid systems that combine traditional signature-based techniques with deep learning methods. In these approaches, collecting and anonymizing large datasets from thousands of sensors and meters plays a fundamental role in forming high-quality training samples and lowering false alarm rates.

Distributed ledger technologies (blockchain) have gained traction in scenarios involving transactions among DER, consumers, and operators. Blockchain provides immutability of records, transparency of operations, and protection against data tampering during energy trading. Architectures for peer-to-peer energy exchange platforms often leverage smart contracts to automate transaction settlement and payment. This reduces the load on centralized systems and broadens participation among energy market stakeholders.

However, scalability issues and high energy consumption inherent in consensus algorithms remain major obstacles for widespread blockchain adoption in Smart Grids. Proposed solutions include hybrid architectures where blockchain is used solely to record critical operations, while bulk energy exchange data are stored in external distributed databases with integrity ensured via cryptographic hashing.

With the rise of computational power and the advent of quantum computers, conventional encryption schemes may become vulnerable in the medium term. Consequently, Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD) are being explored to establish secure communications within future Smart Grids.

Simultaneously, the “Zero Trust Architecture” (ZTA) paradigm, based on “never trust, always verify,” is progressing. Under ZTA, each access request is subject to mandatory verification, and every session is monitored in real time [4]. Implementing ZTA in the energy sector can minimize “lateral” attack risks, where an intruder, having compromised one node, moves stealthily through the infrastructure.

To summarize and compare existing cybersecurity methods for Smart Grids, a comparative analysis was conducted across several key parameters. Table 1 presents the most widely used approaches, their characteristic limitations, and the primary metrics employed to assess effectiveness. This framework highlights the strengths and weaknesses of each method and identifies areas for further improvement of Smart Grid security architectures.

Table 1. Main Cybersecurity Methods, Their Limitations, and Measurable Parameters in Smart Grids

Method	**Limitations**	**Key Metrics**
Encryption	High computational overhead; vulnerability to quantum attacks	Security strength; latency; energy consumption
Firewalls	Ineffective against insider threats; static rule sets	Filtering accuracy; false positive rate; throughput
Intrusion Detection Systems (IDS/IPS)	False positives; limited effectiveness against zero-day attacks	Detection accuracy; response time
AI/ML for Anomaly Detection	Requires large datasets and computational resources; vulnerable to adversarial examples	Detection accuracy; training/response time; computational load

Method	Limitations	Key Metrics
Blockchain	Scalability challenges; high energy requirements; integration complexity	Transaction throughput; energy consumption; resilience
Multi-Factor Authentication (MFA)	Usability issues; potential vulnerabilities in the authentication chain	Success rate; lockout frequency; user convenience
Security Information and Event Management (SIEM)	Complexity of configuration; high cost; information overload	Event volume; alert time; accuracy
Public Key Infrastructure (PKI)	Management complexity; risk of certificate authority compromise	Key issuance time; key validation time; scalability
Network Segmentation	Implementation difficulties; does not guarantee complete prevention of attacks	Isolation level; effectiveness; deployment cost
Patch Management	Temporary vulnerabilities until patches are applied; potential impact on availability	Patch deployment time; coverage; compliance rate
Redundancy and Failover	High cost; possible replication of vulnerabilities	Recovery time; availability; cost-reliability ratio

Source: *According to the authors' research.*

The metrics listed—such as threat detection accuracy, response speed, energy consumption, and scalabilityserve as a basis for selecting the most promising protection approaches for critical energy infrastructure.

CONCLUSION

The study revealed critical Smart Grid cybersecurity gaps and evaluated existing defenses. Key evidence-based findings:

- Traditional controls' limitations: Encryption, firewalls, and IDS are inadequate against APTs, zero-day exploits, and distributed DoS.
- Comparative assessment: Adaptability, scalability, and resilience of legacy measures were benchmarked, confirming their shortcomings in a dynamic threat environment.
- Emerging approaches: AI-driven anomaly detection, energy-efficient blockchain, post-quantum cryptography, and Zero Trust were identified as essential for a layered security model.

Research prospects:

- Hybrid AI methods combining deep learning and statistical models for real-time telemetry threat detection.
- Decentralized, low-power blockchain platforms to handle high-volume microtransactions, especially for distributed energy resources.
- Post-quantum schemes tailored for resource-constrained metering devices.

- Phased Zero Trust rollout, covering access policy updates, micro-segmentation, and continuous authentication.

Study limitations & future work:

- Scope: Not all commercial solutions were evaluated; some hardware-software suites were underrepresented.
- Regional factors: Climatic and infrastructure variations require further adaptation studies.
- Validation: Cost and performance estimates for blockchain and PQC relied on literature rather than testbeds – field trials are needed.
- Regulatory engagement: Jurisdictional differences in standards and policies were not analyzed; additional legal research is required.

Unexpected findings & contradictions:

- Blockchain energy costs were higher than expected, questioning economic feasibility without consensus optimizations.
- Zero Trust pitfalls: Instant transitions cause operational disruptions without phased integration and trained staff, contrary to some optimistic projections.
- Outdated authentication: Some metering devices still use obsolete algorithms despite reports of decommissioning, highlighting a gap between practice and standards.

In sum, this work not only exposed vulnerabilities but also proposed a cohesive, multi-layered security framework and – combining security-by-design, AI monitoring, PQC, and Zero Trust. Despite its limitations, the findings chart a clear path toward a robust, future-ready, cyber-resilient Smart Grid.

REFERENCES

1. Alqarq M., Jung Y., *Security analysis of IoT-enabled smart grid devices.* Journal of Information Security, vol. 12, no. 3, pp. 145–161, 2019.
2. Hasan M. K., Mahmood K. T., Alqarni M., Khreisheh, A. T. *Review on cyber-physical and cybersecurity systems in the smart grid: Standards, protocols, constraints, and recommendations.* Journal of Network and Computer Applications, vol. 209, article 103540, 2023.
3. He H., Yan J., *Cyber-physical attacks and defenses in the smart grid: A survey.* IET Cyber-Physical Systems: Theory & Applications, vol. 1, no. 1, pp. 13–27, 2016.
4. Kindervag J., *Build Trust—Not Trust—Zero Trust Architecture (ZTA) Fundamentals.* Gartner Research, 2019. Available: https://www.gartner.com/en/documents/3973977/zero-trust-architecture-zta-fundamentals
5. Lee C. B., Wang J., *Deep Learning–Based Intrusion Detection for Smart Grid Communications.* IEEE Transactions on Industrial Informatics, vol. 16, no. 5, pp. 3469–3477, 2020.
6. *RedEcho: ShadowPad attack on regional dispatch centers in India.* Incident analysis, January 2021. Available: https://www.recordedfuture.com/shadowpad-backdoor-targets-india-power-sector
7. *Sandworm: Industroyer2 and attempted outage of Ukrainian substations*. CERT-UA report, December 2022. Available: https://cert.gov.ua/article/203493
8. Vähäkainu P., Lehto M., Kariluoto A., *Cyberattacks Against Critical Infrastructure Facilities and Corresponding Countermeasures in Cyber Security*. Critical Infrastructure Protection, Switzerland: Springer International Publishing, 2022, pp. 255–292.
9. *Volt Typhoon: Prolonged APT activity in the networks of the Littleton Electric Light and Water Department (Massachusetts, USA).* February–November 2024. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a
10. Yan Y., Qian Y., Sharif H., Tipper D., *A survey on cybersecurity for smart grid communications.* IEEE Communications Surveys & Tutorials, vol. 14, no. 4, pp. 998–1010, 2012.

CRYPTOGRAPHIC ALGORITHM BASED ON THE FOURIER TRANSFORM FOR DATA SECURITY

UDC: 004.056.55:004.6
DOI: https://doi.org/10.53486/tids2025.04

CERBU OLGA
Moldova State University
olga.cerbu@gmail.com
ORCID ID: 0000-0002-6278-7115

ȚURCAN AURELIA
Academy of Economic Studies of Moldova
cce.turcan@gmail.com
ORCID ID: 0009-0003-2512-2231

Abstract. This paper proposes a cryptographic algorithm that uses the Fourier transform to ensure data confidentiality and security. The presented method is based on representing signals or numerical data in the frequency domain, offering a cryptographic alternative to classical techniques based on modular arithmetic or permutations. By applying the Discrete Fourier Transform (DFT), the data is transformed into a form that is difficult to interpret without the correct decryption key. The steps of encryption and decryption, the advantages of the proposed method, as well as its computational complexity are discussed. In addition, security analyses and comparisons with other modern cryptographic methods are presented. Experimental results demonstrate that the algorithm can provide effective data protection, making it suitable for applications in secure communications and encrypted storage.

Keywords: algorithm, encryption, Fourier transform, data security.

JEL Classification: C63, D83, O33.

INTRODUCTION

In a global context where vast amounts of data are transmitted and stored daily, protecting information confidentiality has become a critical priority. Traditional cryptography is mainly based on mathematical concepts such as modular arithmetic, hash functions, permutations, and substitutions. This paper explores an innovative cryptographic alternative that uses the Discrete Fourier Transform (DFT) for data encryption and decryption, thereby proposing a new framework for numerical cryptosystems.

1. Theoretical Foundations

The Discrete Fourier Transform (DFT) is a fundamental mathematical technique through which a signal in the time domain is transformed into a signal in the frequency domain.

The DFT is defined for a vector:
$x = (x_0 , x_1 , \dots , x_{N-1})$ as:

$$X_k = \sum_{n=0}^{N-1} x_n \cdot e^{-2\pi ikn/N}, \qquad k = 0,1, \dots , N-1$$

This frequency-domain representation allows the analysis and manipulation of signals in a way that is difficult to intuit in their raw form, which makes it attractive for cryptography. Any complex signal (for example, a sound, an image, or a mathematical function) can be regarded as a sum of sinusoidal waves of different frequencies, amplitudes, and phases. The Fourier transform reveals which frequencies are present in that signal and how strong they are.

Formula (for the continuous transform)
For a function f(t), the Fourier transform is:

$$F(\omega) = \int_{-\infty}^{\infty} f(t) \cdot e^{-j\omega t} dt$$

where:

- f(t) is the function in the time domain,
- F(ω) is the function in the frequency domain,
- ω is the angular frequency (radians/second)),
- $e^{-j\omega t}$ represents the complex basis of the decomposition.

Types of Fourier Transforms

1. **Discrete Fourier Transform (DFT)** – for discrete and finite signals (used in digital signal processing).
2. **Fast Fourier Transform (FFT)** – an efficient implementation of the DFT, frequently used in software and hardware.
3. **Continuous Fourier Transform (FT)** – applied to continuous functions, in mathematical theory.

The Fourier transform is reversible – that is, we can reconstruct the original signal from its frequency components using the Inverse Fourier Transform (IDFT). The Fourier transform has interesting and innovative applications in cryptography, especially in modern contexts such as image encryption. It can also be used to hide data (steganography) or to encode information into certain frequency bands (as used in secure transmissions).

2. Proposed Algorithm

2.1 Encryption

1. **Preprocessing:** The data is converted into a numerical vector. *Conversion to the frequency domain:* Apply the Fast Fourier Transform (FFT) to an image.
2. **Applying DFT:** The Fourier Transform is applied to the data vector.
3. **Controlled Perturbation:** The obtained frequencies are modified using a secret key. *Modification of phase or amplitude:* A secret key (for example, a chaotic sequence) is applied to the phase or magnitude of the spectrum.
   Reconversion to the encrypted image: The Inverse Fourier Transform (IFFT) is applied to return to the spatial domain. The result is an encrypted image that visually does not resemble the original.
4. **Storage or Transmission:** The perturbed signal is transmitted or stored.

2.2 Decryption

1. Apply the inverse of the key.
2. Apply the Inverse DFT (IDFT) to return to the original data.

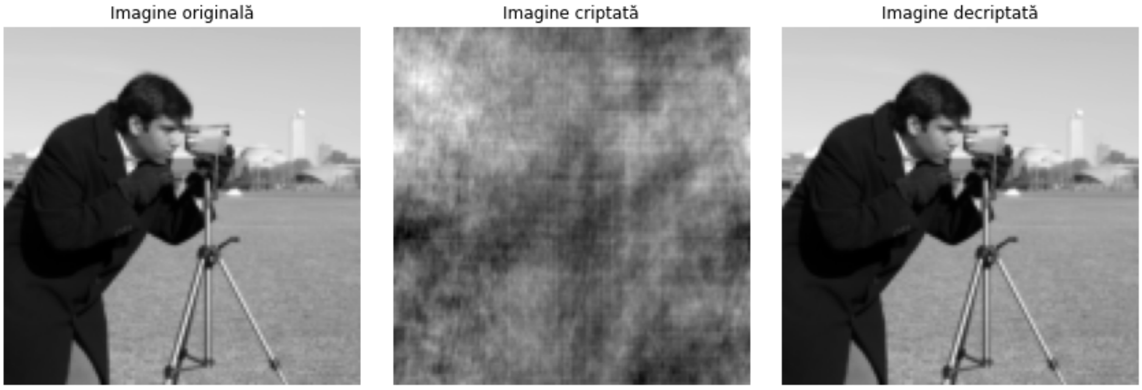
Next, we will create code that:

- Loads a grayscale image (`data.camera()`).
- Resizes it to 128×128 for speed.
- Generates a chaotic key using the Logistic Map.
- Encrypts the image in the frequency domain (FFT).
- Decrypts the image using the chaotic key.
- Displays the three images: original, encrypted, and decrypted.

```
import numpy as np
import matplotlib.pyplot as plt
from skimage import data
from skimage.transform import resize

# ===== Logistic Map for key generation =====
def logistic_map(x0, r, size):
    """
    Generate a chaotic sequence using the logistic function.
    """
    x = np.zeros(size)
    x[0] = x0
    for i in range(1, size):
        x[i] = r * x[i-1] * (1 - x[i-1])
    return x

# ===== Load a grayscale image =====
image = data.camera()  # the image is already grayscale
image = resize(image, (128, 128), anti_aliasing=True)

# ===== Chaotic key parameters =====
x0 = 0.7
r = 3.9
N = image.size
shape = image.shape

# ===== Generate chaotic mask (secret key)=====
chaotic_seq = logistic_map(x0, r, N)
chaotic_matrix = chaotic_seq.reshape(shape)
chaotic_phase = np.exp(1j * 2 * np.pi * chaotic_matrix)  # complex mask

# ===== Encryption =====
fft_image = np.fft.fft2(image)                   # FFT imagine
fft_encrypted = fft_image * chaotic_phase          # we mask the phase
encrypted_image = np.fft.ifft2(fft_encrypted).real  # encrypted image

# ===== Decryption =====
fft_decrypted = fft_encrypted / chaotic_phase       # we invert the phase
decrypted_image = np.fft.ifft2(fft_decrypted).real  # decrypted image
```

```
# ===== Display results =====
plt.figure(figsize=(12, 4))

plt.subplot(1, 3, 1)
plt.title("Original image ")
plt.imshow(image, cmap='gray')
plt.axis('off')
plt.subplot(1, 3, 2)
plt.title("Encrypted image ")
plt.imshow(encrypted_image, cmap='gray')
plt.axis('off')

plt.subplot(1, 3, 3)
plt.title("Decrypted image ")
plt.imshow(decrypted_image, cmap='gray')
plt.axis('off')

plt.tight_layout()
plt.show()
```

The result of encryption/decryption:



3. Advantages of the Proposed Method

- **Nondeterminism:** The transformed frequencies provide a representation of the raw data that is difficult to guess.
- **Key Sensitivity:** Without the correct key, even small errors lead to completely incorrect results.
- **Flexibility:** The algorithm can be applied to text, images, and sound.

4. Computational Complexity

The application of the DFT and IDFT can be efficiently performed using the FFT (Fast Fourier Transform) algorithm, with a complexity of O(Nlog⁡N)O(N \log N)O(NlogN). The cost of the added perturbations is linear with respect to the size of the vector.

5. Security Analysis

Unlike simple encryption in the spatial or temporal domain, frequency-domain encryption hides the visual structure of the data and is resistant to statistical attacks.

- **Resistance to brute-force attacks:** The key space can be significantly expanded.

- **Natural obfuscation:** The encrypted form does not preserve logical or statistical structure from the original data.
- **Limitations:** The algorithm requires integration into a complete encryption system.

6. Comparisons with other cryptographic methods

Criterion	Fourier	RSA	AES
Key complexity	Medium	High	High
Encryption speed	High	Low	High
Statistical resistance	High	High	High
Applications	Multimedia	Text	Various

7. Applications

- **IoT:** Encryption of sensor-collected data.
- **Secure storage:** Protection of multimedia files.
- **Military communication:** Difficult to intercept.

IoT: Encryption of Sensor-Collected Data

Encrypting sensor-collected data in IoT (Internet of Things) is an important process for ensuring the confidentiality, integrity, and authenticity of the data transmitted between smart devices and the processing infrastructure (cloud, controllers, servers).

Frequency-domain encryption of sensor-collected data in IoT is a cryptographic method that involves transforming the data from the time (or spatial) domain into the frequency domain, where masking and encryption techniques are applied. This approach differs from classical encryption (which operates directly on bits or characters) and offers advantages in the IoT context, especially for securing analog data or digital signals originating from sensors.

- Data from sensors are often continuous or discrete signals (e.g., sound, pressure, vibrations, variable temperature).
- These signals can be efficiently encrypted in the frequency domain, avoiding complex operations on each bit.
- It enables real-time encryption, particularly at edge nodes (microcontrollers).

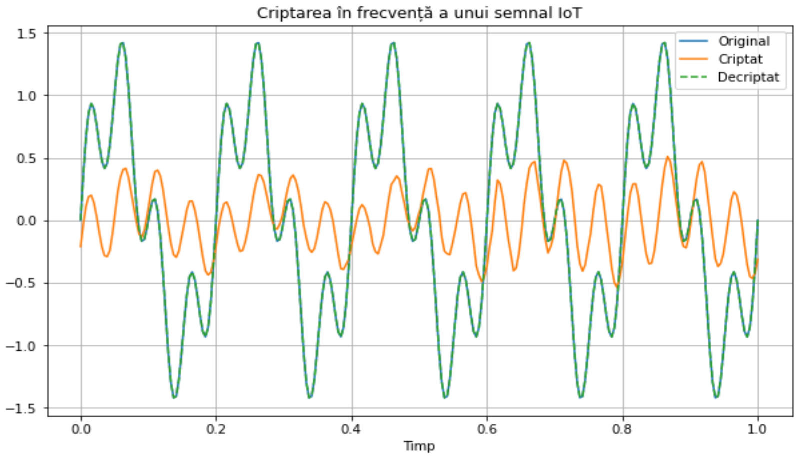
Simplified Example (image or sensor signal):

1. **Collection:** The sensor records a sequence of values (e.g., temperature over time).
2. **Fourier Transform:**
   $X(f)=F[x(t)]$
   The signal becomes a set of complex frequencies.
3. **Key application:**
   $X'(f)=X(f)\cdot e^{j\cdot\phi(f)}$
   The phase or amplitude is modified with a chaotic function or a key.
4. **Inverse transform:**
   $x'(t)=F^{-1}[X'(f)]$
   The encrypted signal in the time domain is obtained.
5. **Encrypted transmission:** The sensor sends the encrypted signal to the server.
6. **Decryption:** The server applies the inverse operation using the key,

```
import numpy as np
 import matplotlib.pyplot as plt
```

```
# Virtual sensor – vibration signal
t = np.linspace(0, 1, 256)
semnal_original = np.sin(2 * np.pi * 5 * t) + 0.5 * np.sin(2 * np.pi * 20 * t)

# Fourier Transform
fft_semnal = np.fft.fft(original_signal)

# Chaotic key (logistic map)
def logistic_map(x0, r, n):
    x = np.zeros(n)
    x[0] = x0
    for i in range(1, n):
        x[i] = r * x[i-1] * (1 - x[i-1])
    return x

key= logistic_map(0.7, 3.9, len(fft_semnal))
mask= np.exp(1j * 2 * np.pi * cheie)

# Encryption
fft_criptat = fft_semnal * masca
semnal_criptat = np.fft.ifft(fft_criptat).real

# Decryption
fft_decriptat = fft_criptat / masca
semnal_decriptat = np.fft.ifft(fft_decriptat).real

# Display
plt.figure(figsize=(10, 6))
plt.plot(t, semnal_original, label="Original")
plt.plot(t, semnal_criptat, label=" Encrypted ")
plt.plot(t, semnal_decriptat, '--', label=" Decryption")
plt.legend()
plt.title("Frequency-domain encryption of an IoT signal ")
plt.xlabel("Time")
plt.grid(True)
plt.show()
```

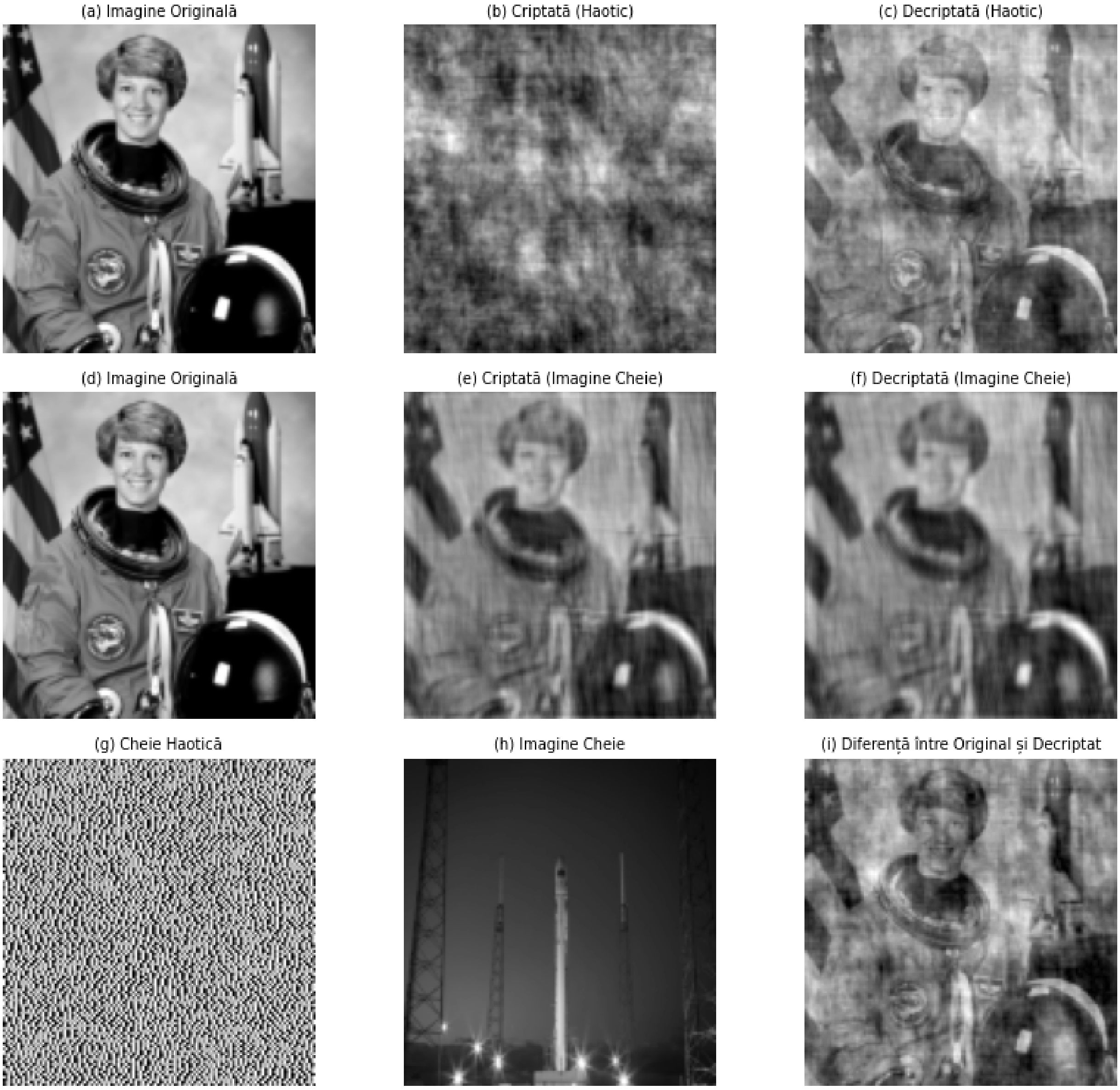
Practical example: vibration sensor



8. Experimental Results

The data was correctly encrypted/decrypted. The loss of fidelity is minimal.

```
import numpy as np
 import matplotlib.pyplot as plt
 from skimage import data, color
 from skimage.transform import resize

 # =====Function: Map haotic logistic =====
 def logistic_map(x0, r, size):
    x = np.zeros(size)
    x[0] = x0
    for i in range(1, size):
       x[i] = r * x[i-1] * (1 - x[i-1])
    return x

 # ===== Load the image to be encrypted =====
 image = color.rgb2gray(data.astronaut())
 image = resize(image, (128, 128), anti_aliasing=True)

 # ======== Chaotic encryption ========
 x0 = 0.7
 r = 3.9
 N = image.size
 chaotic_seq = logistic_map(x0, r, N)
 chaotic_phase = np.exp(1j * 2 * np.pi * chaotic_seq.reshape(image.shape))

 fft_image = np.fft.fft2(image)
 encrypted_fft_chaos = fft_image * chaotic_phase
 encrypted_image_chaos = np.fft.ifft2(encrypted_fft_chaos).real

 decrypted_fft_chaos = np.fft.fft2(encrypted_image_chaos) / chaotic_phase
 decrypted_image_chaos = np.fft.ifft2(decrypted_fft_chaos).real


 # ======== Encryption with KEY IMAGE ========
 key_image = color.rgb2gray(data.rocket())
 key_image = resize(key_image, image.shape, anti_aliasing=True)
 key_phase = np.exp(1j * 2 * np.pi * key_image)

 encrypted_fft_imgkey = fft_image * key_phase
 encrypted_image_imgkey = np.fft.ifft2(encrypted_fft_imgkey).real

 decrypted_fft_imgkey = np.fft.fft2(encrypted_image_imgkey) / key_phase
 decrypted_image_imgkey = np.fft.ifft2(decrypted_fft_imgkey).real

 # ===== Display results =====
 fig, axes = plt.subplots(3, 3, figsize=(12, 10))
 titles = [
    "Imagine Originală", "Criptată (Haotic)", "Decriptată (Haotic)",
    "Imagine Originală", "Criptată (Imagine Cheie)", "Decriptată (Imagine Cheie)",
    "Cheie Haotică", "Imagine Cheie", "Diferență între Original și Decriptat"
 ]
 images = [
    image, encrypted_image_chaos, decrypted_image_chaos,
    image, encrypted_image_imgkey, decrypted_image_imgkey,
    chaotic_seq.reshape(image.shape), key_image, np.abs(image - decrypted_image_chaos)
]
labels = ['(a)', '(b)', '(c)', '(d)', '(e)', '(f)', '(g)', '(h)', '(i)']
for ax, img, title, label in zip(axes.flatten(), images, titles, labels):
    ax.imshow(img, cmap='gray')
    ax.set_title(f"{label} {title}", fontsize=10)
    ax.axis('off')
plt.tight_layout()
plt.show()
```



(a) Original Image

This is the initial image, scaled to 128×128 pixels, represented in grayscale. It is used as the basis for applying chaotic and key-image-based encryptions.

(b) Encrypted Image (Chaotic)

The image was encrypted in the frequency domain using a chaotic phase generated by the logistic function. The result is a distorted image that no longer provides clear visual information about the original content.

(c) Decrypted Image (Chaotic)

After applying the inverse of the chaotic phase in the frequency domain, the image is recovered. We observe a good restoration of the original content, demonstrating the efficiency of the chaotic encryption method.

(d) Original Image (duplicate for comparison)

The original image is shown again here to be directly compared with the key-image-based encryption. It is identical to image (a).

(e) Encrypted Image (Key Image)

The image is encrypted using the phase derived from a key image (the rocket image). The result is again a distorted image, different from the original.

(f) Decrypted Image (Key Image)

By applying the inverse of the phase derived from the key image, the original image is successfully decrypted, highlighting the validity of the key-image-based method.

(g) Chaotic Key (logistic function)

This image represents the distribution of values generated by the logistic function and used as the chaotic phase. The values are scaled across the entire image and serve as the confusion element of the encryption.

(h) Key Image (for encryption)

The image used as the source for generating the phase in the key-image-based encryption method. The rocket image is scaled to the size of the image to be encrypted and converted into grayscale.

(i) Difference between Original Image and Chaotic Decryption

The absolute pixel-by-pixel difference between the original and the decrypted (chaotic) image highlights the minor errors introduced by the Fourier transformations and the chaotic phase. The dark areas indicate an almost perfect decryption.

9. Presentation of the chaotic function

Mathematical description:

$$x_{n+1} = r \cdot x_n \cdot (1 - x_n)$$

where:

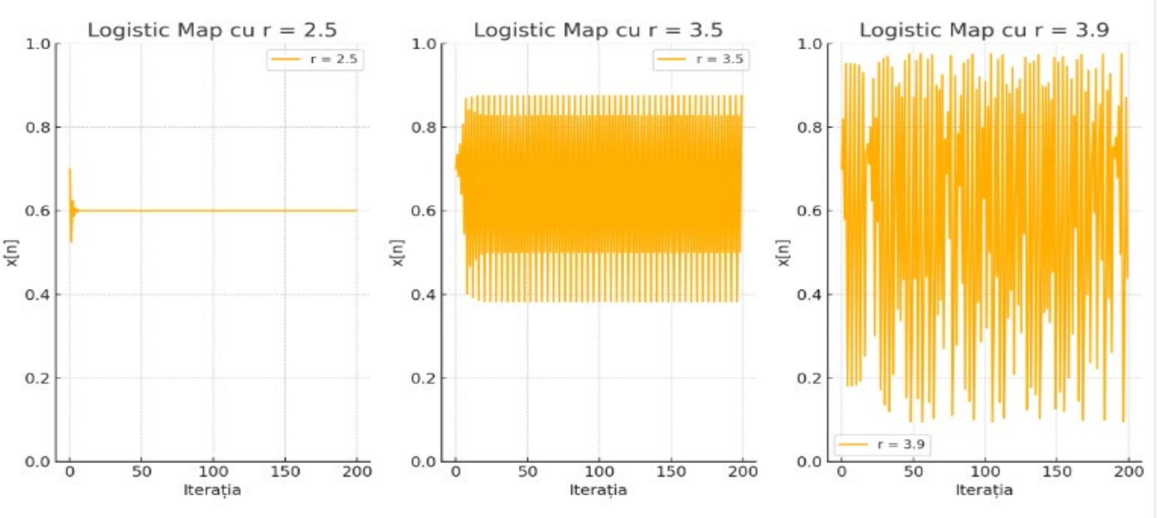
x_0 is the initial value (private key).

r is a control parameter:

- for maximum chaos: $r \approx 3.9$;
- for lower values (below 3.5), the behavior is not chaotic.

Cryptographic properties:

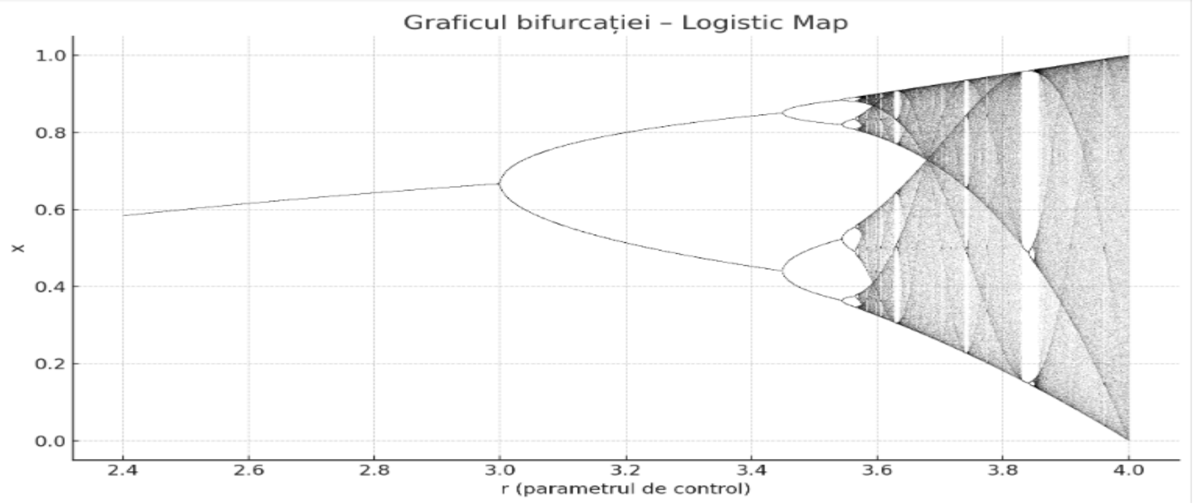
- Extremely sensitive to initial conditions.
- Can generate sequences that are hard to predict → used for dynamic keys.
- Easy to implement, yet provides nonlinear and chaotic behavior.



This visualization shows the evolution of the values generated by the Logistic Map chaotic function for different values of the parameter rrr. The parameter rrr in the Logistic Map chaotic function is a control parameter that determines the dynamic behavior of the system. Its value influences whether the system is stable, oscillatory, or chaotic.

- r = 2.5: Stable behavior – the values converge to a fixed point.
- r = 3.5: Regular oscillations – oscillations appear between several values (bifurcations).
- r = 3.9: Chaotic behavior – the values appear random and unpredictable (ideal for cryptography).

This chaotic behavior for r = 3.9 is exactly what makes it useful in cryptography for generating sensitive and hard-to-predict keys.



The role of *r*:

	Stable	
	periodic oscillation	
	chaotic behavior	

CONCLUSIONS

The Fourier transform can effectively mask information. It does not replace established methods but offers advantages in specialized applications such as IoT and encrypted storage. By combining the Fourier transform with deterministic chaos (chaotic maps) and visual key images, we obtain cryptographic methods that are efficient, hard to break, and suitable for encrypting images or multimedia data.

REFERENCES

1. Bracewell R. N. The Fourier Transform And Its Applications Bracewell : Ronald Bracewell : https://archive.org/details/TheFourierTransformAndItsApplicationsBracewell [Accessed 09.03.2025].
2. FFTW (*Fastest Fourier Transform in the West)* https://www.fftw.org/ [Accessed 03.03.2025].
3. IEEE Xplore: IEEE Transactions on Signal Processing https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=78 [Accessed 09.04.2025].
4. Schneier Bruce. Applied cryptography, second edition: Protocols, Algorithms, and Source Code in C:Table of Contents https://mrajacse.wordpress.com/wp-content/uploads/2012/01/applied-cryptography-2nd-ed-b-schneier.pdf [Accessed 29.04.2025].
5. Stallings William. *Cryptography and Network Security* https://www.uoitc.edu.iq/images/documents/informatics-institute/Competitive_exam/Cryptography_and_Network_Security.pdf [Accessed 29.03.2025].

THE INTERSECTION OF PROGRAMMING AND DATA PROTECTION: SECURE DEVELOPMENT WITH JAVA AND PYTHON

UDC: 004.43:004.056.5
DOI: https://doi.org/10.53486/tids2025.05

ȚURCAN AURELIA
Academy of Economic Studies of Moldova
cce.turcan@gmail.com
ORCID ID: 0009-0003-2512-2231

CERBU OLGA
Moldova State University
olga.cerbu@gmail.com
ORCID ID: 0000-0002-6278-7115

Abstract. In the context of accelerated digitization and strict data protection regulations, programming can no longer be analyzed exclusively from a technical perspective, but also as a tool for legal and ethical compliance. The article explores the intersection between programming and data protection, focusing on the role of Java and Python languages in secure software application development. The particularities of the two languages in implementing the principles of "privacy by design" and in complying with international regulations are highlighted. The comparative analysis emphasizes the advantages of Java in enterprise applications, where robustness and security are critical, and the advantages of Python in data-driven projects, where flexibility and a rich ecosystem of libraries facilitate data processing and protection. At the same time, the paper presents examples of tools and applications developed in both languages.

The conclusion emphasizes the need for convergence between technology and regulations to ensure both innovation and respect for fundamental rights regarding data privacy and security.

Keywords: Java, Python, cybersecurity, data protection, privacy by design, secure programming.

JEL Classification: C88, L86, O33

INTRODUCTION

The profound transformations brought about by global digitalization have led to a paradigm shift in the way software applications are developed. While in the early stages of programming the emphasis was placed on the *code first* principle—meaning the fastest possible implementation of technical functionalities—today the dominant paradigm is *privacy by design*. This concept, initially introduced by Ann Cavoukian and later enshrined in European and international legislation, entails the integration of data protection and privacy principles from the very design phase of applications. In such a context, programming languages are no longer merely technical tools but become vehicles for implementing legal and ethical principles [1].

Major international regulations—such as the European Union's General Data Protection Regulation (GDPR) [4], the European NIS2 Directive on the security of networks and information systems [5], or the California Consumer Privacy Act (CCPA) [19]—impose strict standards regarding the protection of personal data, cybersecurity, and the transparency of information processing. In practice, the application of these standards is achieved through a combination of organizational policies and technical solutions, with programming languages used in application development playing a crucial role.

In this regard, **Java and Python** occupy a central position. Today, they are among the most widely used languages in enterprise and data-driven application development, covering a broad spectrum of needs: from banking applications, distributed systems, and e-commerce platforms to applications based on artificial intelligence, big data analytics, and machine learning [23]. Java, with its robustness and object-oriented nature, is preferred in projects that require reliability, scalability, and compliance with strict security standards. **Python**, with its simplicity and flexibility, is favored in the rapid development of prototypes and data-centered applications, where the analysis, processing, and interpretation of information are essential [6].

Thus, the transition from *code first* to *privacy by design* is closely linked to the adoption of programming languages that allow not only the implementation of functionalities, but also the guarantee of fundamental principles such as:

- ✓ **security by default**, through the use of well-established libraries and frameworks (e.g., Spring Security for Java, Django and Flask with security extensions for Python);
- ✓ **transparency and accountability of coding processes**, through audit and logging tools integrated into the Java and Python ecosystems;
- ✓ **adaptability to regulations**—through the development of modules and APIs that implement GDPR requirements (e.g., the right to be forgotten, data portability), as well as compliance with regulations such as NIS2 or CCPA [4,5].

That is why the choice of Java and Python as the focus of this research is not accidental, as they represent the meeting point between technological demands and the legal and ethical imperatives of the information age. The purpose of this research is to analyze the role that the Java and Python programming languages play in contemporary information society, with emphasis on their technological, educational, and economic impact. The importance of the subject derives from the fact that both languages have become fundamental tools of digitalization, being used both in academia and in industry, in fields such as enterprise application development, data science, artificial intelligence, and cybersecurity. The practical relevance of this research lies in identifying the ways in which Java and Python contribute to the development of digital skills and the stimulation of technological innovation. On the theoretical level, the comparative analysis provides a framework for understanding the evolution of programming paradigms and their convergence in a globalized and digitalized society. Studying the role of these programming languages not only reflects the current level of science and technology but also offers benchmarks for the sustainable development of the digital ecosystem in accordance with the fundamental principles of data protection and cybersecurity.

2. Comparative Analysis of the Java and Python Languages

In the Tiobe global ranking [20], the Python programming language holds the first place, with a market share of approximately 13.97% in January 2024. An increase of nearly 12.7 times in 20 years is truly impressive. Java is also in the TOP 5 [22].

Next, we decided to compare these popular languages.

Java, officially launched in 1995 by Sun Microsystems, became established through the principle of *"Write Once, Run Anywhere"*, offering portability and robustness. According to Statista data, in 2023, it was used by over 30% of developers worldwide [9].

By contrast, Python, created by Guido van Rossum in 1991, focused on simplicity, readability, and a user-friendly syntax, which accelerated its popularity. In 2023, nearly 50% of developers worldwide used Python, making it one of the most popular languages in the industry. Its appeal lies in simplicity, readability, and an extensive ecosystem of libraries [9].

Both languages have evolved significantly, adapting to the needs of the information society: Java toward complex and scalable applications (banking systems, Android applications), and Python in areas such as data analysis, machine learning, and rapid prototype development.

To conduct a comparative analysis of the Java and Python programming languages, we will refer to the main differences between these languages, which are broadly presented in the following table.

Table 1. The Main Differences Between Java and Python

Parameter	Java	Python
What is a programming language?	Java is a multi-platform, object-oriented, and network-centered programming language. It is among the most widely used programming languages. It is also used as a computing platform and was first released by Sun Microsystems in 1995. Later, it was acquired by Oracle Corporation.	Python is a high-level, object-oriented programming language. It has built-in data structures combined with dynamic binding and typing, which makes it an ideal choice for rapid application development. Python also provides support for modules and packages, allowing for system modularity and code reuse. It is one of the fastest programming languages, as it requires very few lines of code. Its emphasis on readability and simplicity makes it an excellent choice for beginners.
Compilație	Java is a compiled language.	Python is an interpreted language.
Static or dynamic	Java is statically typed.	Python is dynamically typed.
String operations	Provides limited string-related functions.	Provides a wide range of string-related functions.
Learning curve	Complex learning curve.	Easy to learn and use.
Multiple inheritance	Multiple inheritance is partially achieved through interfaces.	Provides both single and multiple inheritance.
Braces vs. Indentation	Uses braces to define the beginning and end of each function and class definition.	Python uses indentation to separate code into code blocks.
Speed	Java programs run faster compared to Python.	Python programs run slower than Java.
Portability	Any computer or mobile device that can run the Java Virtual Machine can run a Java application.	Python programs require an interpreter installed on the target machine to translate Python code. Compared to Java, Python is less portable.
File reading	Java requires 10 lines of code to read from a file.	Python requires only 2 lines of code.
Architecture	The Java Virtual Machine provides the runtime environment to execute code and convert bytecode into machine language.	For Python, the interpreter translates the source code into machine-independent bytecode.
Famous companies using this technology	Airbnb, Netflix, Spotify and Instagram.	Uber Technologies, Dropbox and Google.
Best features	• Great libraries • Widely used • Excellent tools	• Readable code • Rapid development • Elegant code

Parameter	Java	Python
	• A huge amount of documentation available	
Best use cases	Java is the best for desktop GUI applications, embedded systems, web application services, etc.	Python: Excellent for scientific and numerical computing, machine learning applications, and more.
Database support	Provides stable connectivity.	Provides weak connectivity.

Source: elaborated based on [9], [10], [15].

Which is better, Python or Java?

The simplicity and readability of Python make it an excellent option for beginners and for developers in fast-growing environments, while Java's static typing and object-oriented features make it ideal for large-scale applications. The choice of the "better" language depends on your project requirements and personal preferences. Although Python is expected to run slower than Java, its development takes less time. Thanks to its built-in high-level data types as well as dynamic typing, Python programs are usually shorter than equivalent Java programs, which makes them simpler and faster to develop. Since Java requires more code and everything must be predefined, developers need more time to check everything and fix potential errors. Naturally, the more code there is, the more complex it becomes. However, the attention required to write good code can also lead to the creation of more stable and reliable software.

Simply put, Python runs slower but starts up faster. In contrast, Java starts up more slowly but stands out by running faster. Ultimately, the best programming language is the one that fits the type of software the developer wants to create. Ideally, as already mentioned, it would be useful for developers to learn both languages [15].

Considering that one of the essential dimensions in the comparative analysis of programming languages is typing and execution mode, we can make the following summary:

Java is a statically typed and compiled language, which means that type checking takes place at compile time, and the resulting code is transformed into optimized bytecode, executed on the Java Virtual Machine (JVM). This characteristic enhances the robustness of applications, reduces the risk of runtime errors, and provides superior performance in complex and critical environments (e.g., banking systems, government infrastructures). However, in terms of string manipulation, Java offers a relatively limited set of native functionalities, which often requires the use of additional libraries.

In contrast, Python is a dynamic and interpreted language, where type checking takes place at runtime. This model provides a high degree of flexibility, reducing development time and enabling rapid prototyping. Moreover, Python offers a vast range of functions and libraries dedicated to string manipulation, which makes it extremely efficient for data processing tasks, text analysis, or natural language processing. This orientation places it at the core of data-driven applications and artificial intelligence projects.

For a better study aimed at choosing between Java and Python and deciding which of these programming languages to use, it is necessary to focus on the characteristics and disadvantages of Java and Python, presented in the following table.

Table 2. Characteristics and Disadvantages of the Java and Python Languages

Characteristics of the Java	**Characteristics of the Python**
• Write code once and run it on almost any computing platform. • It is designed for building object-oriented applications. • It is a multithreaded language with automatic memory management. • It facilitates distributed computing as network-centered.	• Easy to learn, read, and maintain. • Can run on various hardware platforms using the same interface. • You can include low-level modules in the Python interpreter. • Python offers an ideal structure and supports large programs. • Python provides support for automatic garbage collection. • Supports an interactive mode for testing and debugging. • Offers high-level dynamic data types and also supports dynamic type checking. • The Python language can be integrated with Java, C, and C++ programming code.
Disadvantages of the Java	**Disadvantages of the Python**
Over the time I have used Java, I have encountered the following disadvantages: • The JIT compiler makes the program relatively slow. • Java has high memory and processing requirements. Therefore, hardware costs increase. • It does not provide support for low-level programming constructs such as pointers. • You have no control over garbage collection, since Java does not provide functions such as delete() or free().	

Source: elaborated based on [9], [10].

The decision to use Java or Python in a software development project must be based on the nature, objectives, and constraints of the project.

Python is often recommended for beginners due to its simple syntax, close to natural language, which facilitates the learning process. In addition, its open-source nature has led to the accelerated development of a vast ecosystem of tools and libraries covering areas such as statistical analysis, machine learning, and data visualization. Initial development costs are generally lower, making it attractive for startups and exploratory research projects.

Java, on the other hand, is designed as a general-purpose language, oriented toward portability through the principle of “write once, run anywhere”. This characteristic makes it suitable for large-scale projects where stability, security, and performance are priorities. Moreover, the Java ecosystem (Spring, Hibernate, Jakarta EE) provides strong support for enterprise applications, cloud infrastructures, and mobile applications (Android).

Therefore, the selection of the language depends on the balance between development costs, project complexity, and performance requirements. For applications focused on data exploration and rapid prototyping, Python is the optimal choice. Conversely, for critical applications requiring robustness, scalability, and adherence to strict security standards, Java remains the preferred solution.

2. Programming with Java and Python and Data Protection

In the era of strict regulations on privacy and digital security, programming can no longer be separated from the issue of data protection. According to the principle of "privacy by design", enshrined in the General Data Protection Regulation (GDPR), software development must integrate from the design phase both technical and organizational measures intended to ensure the protection of personal information [11].

The role of Java and Python in implementing the principles of GDPR, NIS2, and CCPA

Both Java and Python, through their extensive ecosystems, provide libraries and frameworks dedicated to ensuring compliance with security and privacy standards. In environments regulated by GDPR or NIS2, enterprise applications developed in Java rely on robust security architectures such as Spring Security and the Java Cryptography Architecture (JCA), which implement mechanisms for multi-factor authentication, encryption, and access auditing [8], [12].

At the same time, Python, due to its flexibility and popularity in data processing, integrates packages such as PyCryptodome or Fernet, used for the encryption and anonymization of personal data [2]. In the context of the California Consumer Privacy Act (CCPA), Python is frequently employed in building analysis and reporting tools that help companies demonstrate compliance with requests for access to or deletion of personal data [16].

Thus, both languages are not only "vehicles" for software development but also technical means of applying legislation in the field of data protection.

Table 3. Examples of tools and applications for security and data protection in Java and Python

a		Java
Monitoring and log analysis	• Scripts for parsing security logs (SIEM) with pyparsing, pandas. • Event visualization with matplotlib, seaborn. • Detection of multiple failed authentication attempts.	• Microservices that collect logs with logback / log4j and forward them via Kafka. • Real-time alerting rules (divergent geolocation, suspicious entries).
Traffic and packet analysis (detections)	• Scapy for packet capture and analysis. • Detection of data leaks through traffic analysis.	• Network analysis libraries in enterprise applications. • Integration with MLOps systems for intrusion detection at the gateway level.
Application-level data protection	• cryptography, pyca/cryptography libraries for encrypting PII and medical data. • Data masking in APIs/UI to protect sensitive information.	• javax.crypto, java.security for symmetric/asymmetric key encryption. • Tokenization of sensitive data in large databases.

Compliance and access rights management	• Scripts for audit and automated compliance reports. • Validation of RBAC/ABAC access policies on APIs.	• Access control through OAuth2, OpenID Connect in security gateways. • Privacy policies in enterprise workflows.
Automation of attachment management and data migration	• Scripts for migrating sensitive data between databases, with validation and in-transit encryption. • DLP (Data Loss Prevention) for detecting data in the cloud.	• Enterprise services for migration with logging, rollback, and full audit. • Integration with commercial/open-source DLP solutions via APIs.
Security and vulnerability testing	• SAST/DAST scripts for source code scanning. • Automated penetration testing with pytest.	• OWASP Dependency-Check for Maven/Gradle. • Automated evaluation of configurations (CSRF, XSS, CORS).
Data portability and migrations	• Export/import in CSV, JSON, Parquet with schema validations.	• Export/import in JSON, XML with XSD/JSON Schema validations.

Source: elaborated based on [2], [8], [12], [16].

Examples of real projects

- Security pipeline for a web application: prototype in Python, then ported to Java for production at scale.
- DLP tool for monitoring data in the cloud: analysis in Python, integration API in infrastructure in Java.
- Data protection in databases: Transparent Data Encryption (TDE) in Java at the JDBC driver level, monitoring and alerting in Python.

Table 4. Errors and consequences in the Java and Python languages

Common mistake	**Consequence**
Logging personal data	Accidental exposure in files, infrastructure, or cloud.
Lack of encryption at rest	Sensitive data stored in plain text in databases or files.
Lack of access control	Any user can access data that does not belong to them.
Storing passwords in plain text	Easy exploitation in case of a breach.

Source: elaborated based on [2], [3], [8].

Secure programming: security by design

Programming with Java and Python in the field of data protection involves using these languages to develop security solutions such as log analysis automation, packet analysis, and other specific tasks. Secure programming means not only writing functional code, but also adhering to fundamental principles: data minimization, encryption in transit and at rest, access control, audit and traceability, anonymization, and pseudonymization [2], [11], [12].

Java, through its security-oriented infrastructure, provides integrated solutions for implementing these principles in larger and more complex applications. Python, due to its simplicity and rich ecosystem, allows for the rapid development of prototypes and tools for compliance auditing and monitoring. Both languages can be used for developing data protection tools and systems, confirming the necessary convergence between technology and data protection legislation [3], [16].

CONCLUSIONS

Contemporary trends in the field of programming languages indicate a clear direction in the evolution of technologies, centered on innovation, security, and productivity. In a digital era defined by the rapid expansion of services and software applications, programming languages emerge not only as technical tools but also as structural foundations of the modern information society. Beyond functionality, the dimension of security becomes an essential criterion, while efficiency and productivity serve as benchmarks for evaluating the suitability of a language to the specifics of a project [14].

The research results confirm that Java and Python go beyond the status of mere programming languages, becoming true driving forces of digital transformation. In Eastern Europe, and especially in the Republic of Moldova, a clear distribution of preferences can be observed: Java is used predominantly in complex, enterprise-type applications, while Python dominates in data analysis and the field of artificial intelligence. Considering the complexity of learning C++, beginner programmers usually choose between Java and Python. This complementarity fosters not only technological innovation but also the sustainable development of the digital ecosystem, providing a framework for cooperation between industry, education, and research.

Looking to the future, three major directions of evolution are emerging:

- ✓ Strengthening the complementarity between Java and Python in interdisciplinary and large-scale projects;
- ✓ Expanding the educational role, with emphasis on training new generations of digital specialists;
- ✓ Deepening ethical debates, through the integration of security and privacy principles into programming practice.

Overall, the convergence of Java and Python creates the premises for collaborative, ethical, and innovative development, in which security and responsibility play a central role. This confirms the fact that programming languages constitute the pillars of the modern information society, and continuous research on their role and influence is an indispensable condition for technological progress and for strengthening an interconnected, resilient, and efficient digital world.

The security of programming languages has become one of the main issues, while their efficiency and productivity are key criteria in choosing the appropriate language for a project. Future-oriented programming languages have been defined as those that will shape technology in the coming years, and education and training in programming languages are considered vital for preparing future IT specialists.

Ultimately, it is evident that programming languages form the foundation of the modern information society, and their continuous study and the understanding of their influence across various domains are necessary for technological development and continuous innovation. It is important to remain open to change and adapt to new trends and technologies, in order to contribute to building an interconnected and efficient world.

REFERENCES

1. Cavoukian Ann. Privacy by Design. The 7 Foundational Principles Implementation and Mapping of Fair Information Practices. Disponibil la: https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf.
2. CodeVisionZ. (2023). *Python Cryptographic Libraries*. Disponibil la: https://codevisionz.com/lessons/python-cryptographic-libraries/
3. Dev.to. (2024). *Java Security: Protecting Your Applications with Secure Coding, Cryptography, Access Control*. Disponibil la: https://dev.to/adityabhuyan/java-security-protecting-your-applications-with-secure-coding-cryptography-access-control-26ej
4. European Union (2016). *General Data Protection Regulation (GDPR)*. Regulation (EU) 2016/679. Disponibil la: https://gdpr-info.eu/
5. European Union (2022). *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)*. Disponibil la: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng
6. GetWidget (2023). *Python vs Java: A Comprehensive Comparison*. Disponibil la: https://www.getwidget.dev/blog/python-vs-java/
7. Gosling J., Joy B., Steele G., Bracha G. (2005). The Java Language Specification. Addison-Wesley. Disponibil online: https://www.researchgate.net/publication/2290452_The_Java_Language_Specification
8. *Java Cryptography Architecture*. Disponibil la: https://en.wikipedia.org/wiki/Java_Cryptography_Architecture
9. Java vs Python - Comparison Guide (2025) Disponibil online: https://brightdata.com/blog/web-data/java-vs-python?ysclid=meokkuwsfd379795768
10. Java vs Python – Difference Between Them Disponibil online: https://www.guru99.com/java-vs-python.html
11. Moldstud. (2023). *Integrating Security and Privacy Considerations in Software Architecture*. Disponibil la: https://moldstud.com/articles/p-integrating-security-and-privacy-considerations-in-software-architecture
12. Oracle. *Java Cryptography Architecture (JCA) Reference Guide* (2023).. Disponibil la: https://docs.oracle.com/en/java/javase/21/security/java-cryptography-architecture-jca-reference-guide.html
13. Oracle. Java SE Documentation(2023). Disponibil online: https://docs.oracle.com/en/java/
14. Pirlog A., Turcan A. Programming languages in the information society era: evolution and analysis (2024).Disponibil online: x-natsionalnaya-nauchno-prakticheskaya-konferentsiya-problemy-i-vyzovy-ekonomiki-regiona-v-usloviyakh-globalizatsii-2024.pdf
15. Python and Java: key differences, performance, and use cases (2025) Disponibil online: https://www.imaginarycloud.com/blog/python-vs-java
16. Python Central. (2023). *How Python and Cybersecurity Services Help with Compliance and Regulatory Requirements*. Disponibil la: https://www.pythoncentral.io/how-python-and-cybersecurity-services-help-with-compliance-and-regulatory-requirements/
17. Python Software Foundation Python Documentation (2023). Disponibil online: https://docs.python.org/3/
18. Python Tutorial. Disponibil online: https://www.w3schools.com/python/default.asp
19. State of California (2018). *California Consumer Privacy Act (CCPA)*. Assembly Bill No. 375. Disponibil la: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375
20. TIOBE Index (2025). Programming Community Index. https://www.tiobe.com/tiobe-index/
21. Van Rossum G., Drake F. (2009). The Python Language Reference. Python Software Foundation. Disponibil online: https://archive.org/details/pythonlanguagere0000vanr
22. Which path should a beginner programmer take: Python vs Java / Habr (2024) Disponibil online: https://habr.com/ru/articles/788348/
23. *Why enterprises rely on JavaScript, Python, and Java*. Disponibil la: https://www.infoworld.com/article/2336936/why-enterprises-rely-on-javascript-python-and-java.html

IMPLEMENTING ISO/IEC 27001 IN SOFTWARE DEVELOPMENT: THE ROLE OF HUMAN RESOURCES IN ENSURING INFORMATION SECURITY[1]

UDC: 006.322:[004.056.5:004.4+005.963.1](478)
DOI: https://doi.org/10.53486/tids2025.06

LUCIA GUJUMAN
Associate Professor,
Academy of Economic Studies of Moldova
gujuman.lucia@ase.md
ORCID ID: 0000-0001-7940-4291

ZINOVIA TOACĂ
Associate Professor
Academy of Economic Studies of Moldova
toaca@ase.md
ORCID ID: 0000-0002-8304-1961

VITALIE URSACHI
PhD
Academy of Economic Studies of Moldova

Abstract. This paper examines the implementation of ISO/IEC 27001 in software development, emphasizing the critical role of human resources in ensuring information security. Based on international standards (ISO/IEC 27000 family, NIST CSF, COBIT, ITIL) and national legislation, the study highlights both the benefits and challenges identified through a survey of IT professionals in Moldova. The findings show that while awareness of ISO/IEC 27001 is high, training, flexibility, and organizational culture remain key factors for successful adoption. Recommendations are proposed to strengthen security practices and foster a resilient, innovation-oriented environment.

Keywords: Information Security Governance, Cybersecurity Frameworks, ISO/IEC 27001, resources, Infrastructure, standards, data.

JEL Classification: M15, M12, O32, L86

INTRODUCTION

In the digital age, the way entities collect, process, store and manage data and information is based on the use of information technologies. At the same time, the development and use of agile methodology with its Frameworks and Cloud infrastructures has accelerated the exposure of sensitive data to various types of threats. The increasing threat of cyberattacks and data leaks represents a significant challenge to the integrity of information security for all national and global entities.

According to official data published in the ENISA Threat Landscape 2024 report, by the European Union Agency for Cybersecurity, cyber threats in recent years have recorded continuous growth, affecting both private entities and public institutions. According to ENISA Threat Landscape 2024, the main risks identified at European level are the intensification of ransomware attacks, the exploitation of vulnerabilities in the supply chain and the increase in the number of attacks on critical

[1] The article was developed within the framework of Subprogram 030101 "Strengthening the resilience, competitiveness, and sustainability of the economy of the Republic of Moldova in the context of the accession process to the European Union", institutional funding.

infrastructures, which confirms the fragility of the digital environment in the face of technological and geopolitical pressures. (European Union Agency for Cybersecurity (ENISA), 2024)

According to the latest data published by Check Point Research, "the second quarter of 2025 completes this picture, highlighting a global increase in cyberattacks of 21% compared to the same period in 2024, reaching an average of 1,984 weekly attacks per organization." The same report states that "Education had 4,388 weekly cyberattacks per organization, being the most targeted sector, followed by Government (2,632) and Telecommunications (2,612)." (Check Point Research, 2025)

This growth requires the implementation of logical and standardized measures in the field of data and information security. Implementing the ISO/IEC 27001 standard in software development is not only a compliance requirement, but also an essential strategy for ensuring organizational resilience. And human resources are the most important in the successful implementation of the ISO/IEC 27001 standard within organizations. Organizations, through recruitment procedures, continuous staff training and the development of a security-oriented organizational culture, can contribute to the formation of a responsible and involved human resource in ensuring information security.

Thus, the article aims to analyze the principles and particularities of the ISO/IEC 27001 standard, with an emphasis on the ways of implementing it in the software development process and on the essential role of human resources. The paper aims to highlight the impact of applying the standard on development teams and the correlation between ISO/IEC 27001 requirements and organizational security policies, formulating conclusions and practical recommendations for strengthening information security.

THEORETICAL AND NORMATIVE FRAMEWORK OF INFORMATION SECURITY.

Security means protecting our assets. This can mean protecting them from attackers invading our networks, natural disasters, adverse environmental conditions, power outages, theft, vandalism, or other unwanted actions (Andress, 2014), and encompasses both physical protection measures and technical and organizational measures.

According to ISO/IEC 27000:2018 'Information security is defined as "maintaining the confidentiality, integrity, and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation, and reliability may also be involved" (SOURCE:ISO/IEC 27000:2018, Information Security Management Systems — Overview and Vocabulary).

The National Institute of Standards and Technology (NIST) defines information security as "the protection of information and information systems against unauthorized access, use, disclosure, disruption, modification, or destruction, in order to ensure confidentiality, integrity, and availability." (National Institute of Standards and Technology (NIST), 2018)

And the European Union Agency for Cybersecurity (ENISA) defines information security as "the set of policies, processes, and controls implemented to protect information assets and ensure the continuity of organizational activities." (European Union Agency for Cybersecurity (ENISA), 2024)

According to Law No. 299/2017 of the Republic of Moldova, information security is defined as "the state of protection of information resources, as well as the person, society, and the state, in the information space." (Parlamentul Republicii Moldova, 2017)

The analysis of the definitions presented shows that information security is based on three fundamental characteristics: confidentiality, integrity and availability, and their assurance is achieved through a management process, supported by policies, procedures and controls implemented at the organizational level. These characteristics are considered the core of information security and recognized by major reference frameworks, such as: ISO/IEC 27000 and NIST SP 800-12.

Information security is an essential condition for the efficient functioning of contemporary institutions and organizations. The application of international standards and frameworks provides integrated methodologies for developing information security management that would contribute to reducing risks and strengthening cyber resilience.

The ISO/IEC 27000 family of standards covers a wide range of information security standards published by both the International Organization for Standardization and the International Electrotechnical Commission. ISO/IEC 27000 recommends best practices for managing information risks by implementing security controls within an overall information security management system (ISMS).

The ISO/IEC 27000 family of standards is recognized as a reference and starting point in the development of information security management systems globally, being composed of several interconnected standards, each having a specific role in the overall framework. ISO/IEC 27000 covers security, confidentiality and IT issues, and the structure of this family of standards is presented in Figure 1.

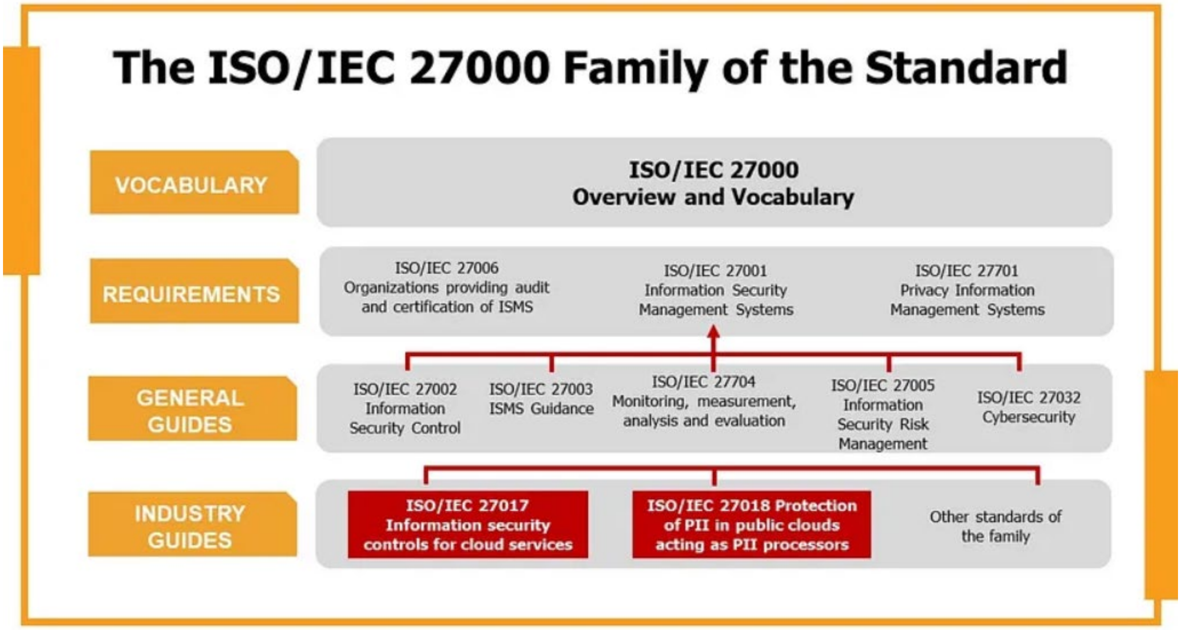

The ISO/IEC 27000 Family of the Standard
VOCABULARY
ISO/IEC 27000
Overview and Vocabulary
REQUIREMENTS
ISO/IEC 27006
Organizations providing audit and certification of ISMS
ISO/IEC 27001
Information Security Management Systems
ISO/IEC 27701
Privacy Information Management Systems
GENERAL GUIDES
ISO/IEC 27002
Information Security Control
ISO/IEC 27003
ISMS Guidance
ISO/IEC 27704
Monitoring, measurement, analysis and evaluation
ISO/IEC 27005
Information Security Risk Management
ISO/IEC 27032
Cybersecurity
INDUSTRY GUIDES
ISO/IEC 27017
Information security controls for cloud services
ISO/IEC 27018 Protection of PII in public clouds acting as PII processors
Other standards of the family

Figure1. Structure of the 27000 family of standards.

Source: *The ISO/IEC 27000 Family of Standards (CFE Certification, 2023)*

ISO/IEC 27001 is the most widely recognized international standard for information security management systems (ISMS) and their requirements. Additional practices for data protection and cyber resilience are covered by numerous other standards in the ISO/IEC 27000 family. Together, they enable organizations of all sizes and sectors to manage the security of assets such as financial information, intellectual property, employee data, and information entrusted to third parties. (CFE Certification, 2023)

ISO/IEC 27001 is a standard that helps organizations manage the security of important information in a structured and risk-focused way. It gives a clear guide for setting up, carrying out, keeping up, and regularly improving their information security practices.

The main purpose of ISO/IEC 27001 is to assist organizations in safeguarding the confidentiality, integrity, and availability of their information assets. The standard highlights the necessity of creating an information security management system (ISMS) that is customized to meet the specific requirements and risk levels of the organization, aiming to reduce confusion and frustration caused by unclear or inconsistent information security practices, which can result in operational disruptions and undermine trust. Implementing a tailored ISMS is crucial for ensuring that information is handled appropriately, securely, and in line with the organization's goals and regulatory requirements.

ISO/IEC 27001 is built on some important ideas, like being committed to managing risks in a careful and organized way, always trying to improve security practices, and making sure that security measures fit with the organization's goals and needs. A key part of this standard is the Plan-Do-Check-Act (PDCA) cycle, which helps organizations plan and set up an information security management system, carry out security controls, keep track of how well things are working, and keep making improvements over time.

An important aspect in the development of the ISO/IEC 27001 standard in our view is the role of human resources, which represents a key element in the development of an information security management system. The standard contains a specific set of human resources security controls, emphasizing the importance of staff involvement throughout the information security lifecycle.

By implementing ISO/IEC 27001, organizations demonstrate their commitment to best practices in information security and can provide assurance to stakeholders, customers, and partners that their information assets are managed with care and diligence.

Certification to ISO/IEC 27001 demonstrates that an organization has defined and implemented best practices for information security. However, not all organizations choose to obtain ISO/IEC 27001 certification; some use the standard as a framework for a best practice approach to information security management.

ISO/IEC 27001 certification can help an organization demonstrate compliance with international standards, making it more attractive to potential customers. ISO/IEC 27001 compliance helps companies demonstrate good security practices, which can improve customer relationships and give them a competitive advantage. Having an internationally recognized certification, regularly reviewed by an independent auditor, demonstrates an ongoing commitment to improving and protecting an organization's important digital assets.

ISO/IEC 27001 is the most widely known and widely used international standard for the development of information security management systems, based on risk management principles. However, organizations are not limited to this standard alone, but also use other reference frameworks, such as the NIST series (e.g. NIST SP 800-171), COBIT, PCI DSS, SOC2, NERC-CIP, GDPR or FISMA, which provide complementary guidance and controls depending on the industry and regulatory context. Typically, in practical work, organizations combine elements from several frameworks to meet regulatory requirements and their own security objectives. In order to highlight the main differences and complementarities, the following table presents a comparative summary of the most relevant information security management standards and frameworks depending on their focus, strengths and limitations.

Table 1. Comparison of the main information security management frameworks.

Frame / Standard	Main focus	Strengths	limitation
ISO/IEC 27001 (SMSI)	Requirements for implementing an Information Security Management System (ISMS); based on risk management and PDCA.	Certified international standard; globally recognized; applicable to any organization; provides systematic and risk-based approach	Complex and costly implementation; requires mature organizational culture
ISO/IEC 27002	Good practices and control objectives (access control, cryptography, HR security, incident response).	Practical model for information asset protection; supplement to ISO/IEC 27001	Not certifiable; secondary role to 27001
NIST CSF (Cybersecurity Framework)	5 key functions: Identify–Protect–Detect–Respond–Recover; strategic and flexible orientation.	Easy to apply in any sector; widely used for assessing security maturity; good for internal/external communication	Does not provide certification; does not prescribe exactly which controls to implement
NIST SP 800-53	Detailed set of security controls (access, risks, incident response, assessment).	Very detailed technical guidance; widely adopted also in the private sector; flexible and adaptable	The statement can be rephrased as: "It is complex and challenging to implement for small organizations or those with limited resources."
COBIT 2019	IT is about governance in TI and connection to project objectives.	The framework links business and IT together, which is helpful for management and meeting compliance requirements.	It's not just about security, but also about general IT governance.
GDPR	Protection of personal data and privacy.	European laws on data protection that affect the whole world; these rules apply to any company that handles information about people living in the European Union.	It is not a management system, but a law; it only covers personal information.

Source: *developed by the author, based on (National Institute of Standards and Technology (NIST), 2018), (ISACA, 2019), (Parlamentul European și Consiliul Uniunii Europene, 2016).*

We think that ISO/IEC 27001 is still the best standard for creating an information security management system because it offers certification and is easy for any organization to use. It's not right to say that companies should only use one framework or that one is better than the others. In reality, multiple frameworks can be used together in one organization because they work well with each other and can greatly improve the safety of data and information.

IMPLEMENTING ISO/IEC 27001 IN SOFTWARE DEVELOPMENT

Knowing the details and background of the organization, as outlined in clause 4.1 of the ISO/IEC 27001 standard, helps us properly recognize the risks and weaknesses that could affect its information assets. The organizational context includes internal elements, such as organizational structure and culture, available resources, processes and contractual relationships, as well as external elements, such as market trends, legal regulations (e.g. GDPR), economic conditions and technological developments. The analysis of these factors contributes to defining the objectives of the information security management system (ISMS) and to the appropriate allocation of resources necessary for its implementation.

Risk assessment, as a fundamental part of the implementation process, aims to identify threats to the confidentiality, integrity and availability of information. In practice, this involves the involvement of security teams in the analysis of system architecture and in the development of plans to mitigate the identified risks. Examples such as those applied by companies in the software industry show how each project includes the consideration of risks and the selection of appropriate actions to minimize them.

Implementing ISO/IEC 27001 in software development means making security a key part of the whole product life cycle. Key secure practices include:

- Secure software design – making sure security needs are considered from the start, including things like user login systems, and building the software structure in line with international standards.
- Secure development and coding – following good coding rules, checking code for errors, making sure all inputs are safe, managing changes properly, and using encryption methods.
- Testing and quality assurance – including security checks at every step of development, using fake data for testing, and doing penetration tests to find any hidden weaknesses.
- Keeping environments separate and managing access – having different areas for building, testing, and running the software, setting up strict rules for who can access what, and keeping track of changes.
- Using third-party and open-source software – choosing external tools carefully, checking for security risks, and making sure the software licenses meet the needs of the customer.
- Classifying and protecting information – deciding who is in charge of data, and setting up access rules that match how important the data is.
- Keeping records, making backups, and planning for continuity – watching for security events, saving copies of data, and having a plan in place to handle emergencies so important processes can keep going without stopping.

These policies make sure that security is part of every step in making software, which helps lower the chances of problems that could put the organization's or customers' data at risk.

Using good practices for building information management systems helps organizations in several ways: it lowers the costs from security issues, makes customers more trusting, improves how processes are planned and managed, saves time on maintenance, and gives a competitive edge by showing they follow ISO/IEC 27001 standards.

Implementing ISO/IEC 27001 comes with some challenges such as: high costs, the need for a mature organizational culture and possible differences between customer and internal requirements can be major obstacles. These aspects confirm that the success of applying the standard depends on both technical integration and the organization's ability to manage change.

The first line of defense against cyberattacks is represented by employees. Awareness of the importance of policy compliance and continuous security training are essential to prevent data leaks and incidents. Thus, the role of human resources becomes a central element of the success of ISO/IEC 27001 implementation.

THE ROLE OF HUMAN RESOURCES IN ENSURING INFORMATION SECURITY

To describe the role of human resources in the implementation of the ISO/IEC 27001 standard, with the aim of ensuring information security in IT organizations in the Republic of Moldova, a questionnaire was used as a research tool. This method allowed for the collection of direct data from specialists involved in software development processes, providing an applied perspective on how security policies influence daily activities and organizational culture. The respondents to the questionnaire were 25 specialists of an IT company employed in different roles and seniority levels, namely: 8 senior developers, 7 junior developers, 4 senior testers, 3 junior testers, 1 delivery manager, 1 scrum master, 1 business analyst. The survey aimed to identify the opinions and perceptions of development teams regarding the processes and procedures involved in the implementation of the ISO/IEC 27001 standard within the company.

Following the completion and processing of the survey data, we note that 88% of respondents consider it necessary to implement the ISO/IEC 27001 standard, because it offers an increased level of security and perceives its importance, and there is a significant recognition of the importance of implementing the standard within the company. The majority of team members perceive this implementation as necessary, recognizing the benefits brought by an increased level of security, do not identify conflicts between the requirements of the ISO/IEC 27001 standard and the daily work within the company, and regarding security policies, the majority of respondents consider them transparent, reflecting the approach to all current trends and vulnerabilities.

However, there are also divergent views among respondents. Approximately 22% of respondents perceive the implementation of the standard as necessary, but express concerns about potential obstacles and delays in development projects or believe that they are too frequent and would take away from the time that can be allocated to the activity within the project. This perspective emphasizes the importance of ensuring that all employees realize the need to be aware of the risks related to information security and the vital role that each one plays in adhering to these requirements, but also indicates an important aspect of the balance between security and flexibility within the development processes.

And 12% see room for improvement by providing more rigorous security awareness training and better assessment of understanding of the material presented, suggesting increased attention to training and awareness needs.

These findings highlight the existence of robust and extensive practices designed to ensure information security, effectively support and inform teams on the implementation of the ISO/IEC 27001 standard, and the importance of continuing efforts to adopt the ISO/IEC 27001 standard within organizations, suggesting that there is significant support, but also challenges and opportunities for improvement to ensure a harmonious integration of the standard into the company's culture and processes.

Within IT companies in the Republic of Moldova, there is awareness of the importance of adopting relevant and current practices and policies aimed at ensuring information security as well as training employees on the development of information security management through the implementation of the ISO/IEC 27001 standard.

RECOMMENDATION

The survey results provide the necessary premises for formulating recommendations, namely:

1) Intensifying and diversifying the training process - an aspect highlighted by 12% of respondents. This recommendation highlights the importance of strengthening training programs in the field of information security, through a more detailed structuring of the content and by introducing rigorous evaluation mechanisms, which would contribute to a better understanding of the key concepts associated with information security management and the ISO/IEC 27001 standard, facilitating their coherent and uniform application within entities.

2) Flexibility to maintain operational efficiency by developing a compliance strategy adapted to the specifics and complexity of ongoing projects. Identifying a balance between security and adaptability is essential to support innovation and creativity in software development processes.

3) Periodically review and update security policies to continuously adapt to technological and environmental changes. Thus, regular evaluation of policies and procedures can help maintain their relevance and ensure that they remain effective in the face of changes in the information security field. These practices must be designed and implemented in a way that promotes a deep understanding of the principles and requirements of this information security management standard.

4) Two-way communication. It is essential to develop two-way feedback mechanisms so that employees can share experiences, suggestions or concerns related to the implementation of the standard and the development of effective information security management. This open communication process would support the rapid identification of any uncertainties and would facilitate the taking of corrective measures or adjustments effectively.

By addressing these comprehensive support and awareness practices, IT companies can strengthen the commitment and involvement of the team in the implementation process of the ISO/IEC 27001 standard, thus contributing to the success and continued effectiveness of the information security program.

Implementing these recommendations can strengthen the commitment and conscious involvement of each team member in the implementation process of the ISO/IEC 27001 standard, thus contributing to ensuring information security.

REFERENCES

1. Andress, J. (2014). *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice.* SUA: Elsevier Science.
2. CFE Certification. (2023). *The ISO/IEC 27000 family of standards.* The ISO/IEC 27000 family of standards.
3. Check Point Research. (2025). *Global Cyber Attacks Surge 21% in Q2 2025 — Europe Experiences the Highest Increase of All Regions*. Preluat de pe Check Point Research: https://blog.checkpoint.com/research/global-cyber-attacks-surge-21-in-q2-2025-europe-experiences-the-highest-increase-of-all-regions
4. European Union Agency for Cybersecurity (ENISA). (2024). *ENISA Threat Landscape 2024.* Luxembourg: Publications Office of the European Union.
5. European Union Agency for Cybersecurity (ENISA). (2024). *ENISA Threat Landscape 2024.* Luxembourg: Publications Office of the European Union.
6. ISACA. (2019) *COBIT 2019 Framework: Governance and Management Objectives.* Schaumburg, IL: Information Systems Audit and Control Association (ISACA).
7. National Institute of Standards and Technology (NIST). (2018). *An Introduction to Information Security (NIST Special Publication 800-12 Rev. 1).* Gaithersburg, MD: U.S. Department of Commerce.
8. National Institute of Standards and Technology (NIST). (2018). *Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1).* Gaithersburg, MD: National Institute of Standards and Technology.
9. Parlamentul European și Consiliul Uniunii Europene. (2016). *Regulamentul (UE) 2016/679 – Regulamentul general privind protecția datelor (GDPR).* Bruxelles: Jurnalul Oficial al Uniunii Europene.
10. Parlamentul Republicii Moldova. (2017). *Legea nr. 299/2017 privind securitatea informațională.* Chișinău: Monitorul Oficial al Republicii Moldova.

CYBER RISK MANAGEMENT AND THE ECONOMIC IMPACT OF DIGITAL SECURITY

CONCEPTUAL AND TECHNOLOGICAL PARTICULARITIES OF CYBER INSURANCE

UDC: 004.056.5:[368.022+368.03](100)
DOI: https://doi.org/10.53486/tids2025.07

IVAN LUCHIAN
Moldova State University
ivan.luchian@usm.md
ORCID ID: 0000-0002-8683-7228

SVETLANA GHERJAVCA
Moldova State University
svetlana.gherjavca@usm.md
ORCID ID: 0009-0002-2994-8412

Abstract. Cyber insurance (also called cyber liability insurance or cybersecurity insurance) encompasses insurance products designed to cover financial losses incurred by companies as a result of cyber incidents. These assurances are becoming increasingly important for all companies as the problems of cyber-attacks against applications, devices, networks, and users worsen, consequently requiring protection against cyber events, including acts of cyber terrorism, and can help remediate security incidents. This article aims to examine the specific characteristics of cyber insurance as a distinct financial product. The screening of open sources placed on the Internet was applied as a research method. Cyber insurance is an insurance product designed to protect corporate clients from risks related to information technology infrastructure and activities (such as data destruction, data extortion, theft, hacking, and denial-of-service attacks), as well as the liability of companies to third parties for damages caused, for example, by errors and omissions, failure to protect data, or defamation. Such insurance policies may also provide for regular security audits, post-incident public relations and investigation expenses, and criminal reward funds. The main areas that cyber insurance covers include: customer notifications; recovering personal identities; data breaches; data recovery; system damage repair; ransom demands; attack remediation; and liability for losses incurred by business partners with access to business data. Cyber insurance currently forms a continuously growing market segment of the global insurance market. This trend is maintained by the continuous development of the digital economy and e-commerce, the significant increase in the size of damages to companies following cyber incidents, as well as the permanent growth of technologies applied in cybercrime. At the same time, its size remains tiny compared to the global insurance market and the global cybersecurity market. Cyber insurance has a significant set of benefits. However, its spread is hindered by certain factors, the main ones being the specific conditions for the sale of insurance policies and the limits of insurance companies in assuming financial commitments.

Keywords: cyber insurance; liability; damage; security incident; cyber-attack.

JEL Classification: G22, L86

INTRODUCTION

Since the second half of the 1990s, the development of the digital economy and the information society has become a reality, and to this day, processes of deepening and development are taking place.

And as in any field of human activity, related malicious activities are simultaneously manifested, which affect the activity of companies in cyberspace.

In this context, Stocklytics experts (2024) state: “Despite the maximum efforts to prevent and minimize cybercrime damage, cyber-attacks, including ransomware attacks, data breaches, cyber espionage, phishing, and other espionage, are still the biggest threats in the business sector. According to the Allianz Risk Barometer survey, 40% of respondents called cybercrime their biggest potential threat in 2023, ahead of inflation, energy crises, and supply chain disruptions.”

According to some estimates, 57% of business leaders believed that cyberattacks were inevitable (IBM, 2025).

In 2019, FM Global surveyed CFOs of companies with revenues of over $1 billion. It found that 71% of respondents said they believed their insurer would cover all or most of the potential losses in the event of a cyberattack (Granato, Polacek, 2019).

Therefore, modern companies, following the development of digital activities, have a growing need to ensure cybersecurity as a complex of methods and tools to protect systems, networks and programs from manifestations of cybercrime, which tend to alter, access or destroy sensitive information, extort users' funds, or disrupt normal economic activity (Fortune Business Insights, 2025).

One of the solutions aimed at strengthening the cybersecurity of companies is cyber insurance, which comes to supplement the cybersecurity system of corporate clients through a special insurance product.

Traditional insurance products for corporate clients, such as general liability and errors and omissions policies, typically do not cover losses caused by cyber incidents, leaving companies vulnerable to the full and significant cost of ransomware attacks, business email compromise scams, and other cybercrimes. For example, a ransomware attack costs an average of $4.54 million, not including ransom payments (IBM, 2025).

Cyber insurance policies are designed to fill this gap. By covering losses caused by cyber incidents, cyber insurance policies can help companies limit their damage, recover faster, and increase their overall level of cyber resilience (IBM, 2025).

The purpose of this article is to explain the essence of cyber insurance and present its technological particularities.

MAIN CONTENT

1. Materials and Methods

As a primary research method, screening of information available in various open publications on the Internet in the form of reports from specialized companies and views of experts in the field of cyber insurance was applied. Then the accumulated information was subjected to analysis and synthesis to obtain a complex picture of this specific insurance product.

2. Results and Discussion

The presentation of the results of the research begins with the definition of cyber insurance.

Cyber insurance (also known as cybersecurity insurance, cyber risk insurance, cyber liability insurance) is a specialty insurance product that allows companies to mitigate the consequences of the risk of cybercrime activities by covering the costs associated with data recovery after a cyber incident. This insurance product provides financial assistance and assistance in a cyber incident that could compromise private information, stop business activities, or cause financial damage (Fortinet), (IBM, 2025).

That is, it is a protection of corporate clients of insurance companies from dangers capable of affecting IT infrastructure, information governance, and information policy, which are not covered by traditional insurance policies. This insurance product works in the same way as if companies were to contract insurance against physical risks and natural disasters. Only the object of insurance differs (Fortinet).

The study identified the factors behind the increase in corporate customers' interest in cyber insurance.

First of all, it is about the rapid advancement of the process of developing the information economy, the expansion of electronic commerce, and the digitalization of companies' activities.

Secondly, there has been a rapid increase in corporate losses from cybercrime (Figure 1).

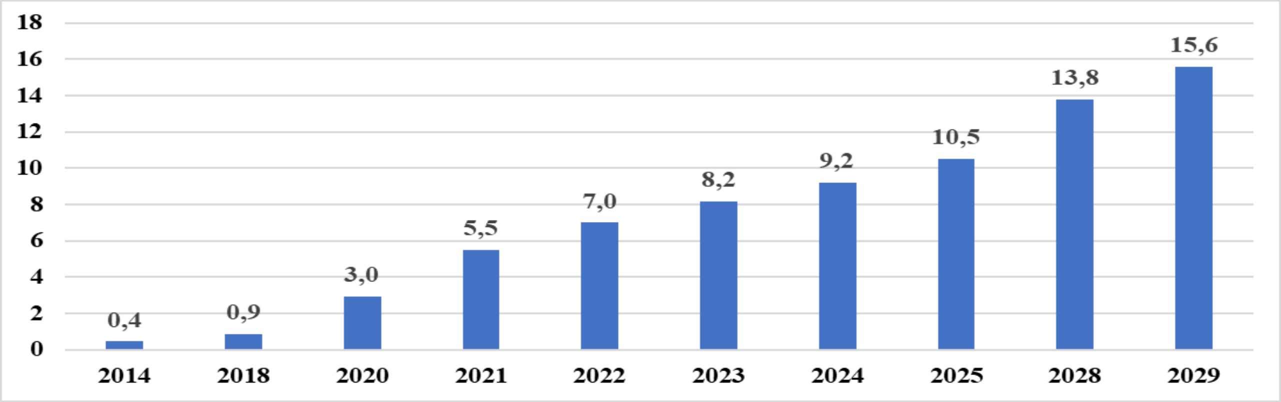


Figure 1. Dynamics of Global Cybercrime Costs (trillion U.S. dollars).

Sources: *(Fox, 2024), (Nakashima, Peterson, 2014), (Statista, 2024), (Stocklytics, 2024)*

Thus, if in 2014 the global costs of cybercrime amounted to about 445 billion US dollars, then for 2029 this indicator is estimated at 15.6 trillion US dollars.

IBM specialists (2025) report the following: "Security breaches are growing more common and more costly. According to IBM's Cost of a Data Breach report, 83% of organizations have had more than one data breach, and the average breach costs USD 4.35 million. Cyber insurance can lessen the financial impact of these breaches, making it an important part of risk management for businesses today."

Thirdly, it is essential to note the ongoing trend of cybercriminals continually improving their techniques to achieve their criminal objectives.

In the view of Embroker experts (2025), this insurance product is particularly advisable for certain industries that have an increased cyber risk: manufacturing, finance, insurance, energy and utilities, healthcare and pharmaceuticals, and technology.

On the other hand, considering that more and more companies are asking their employees to work from home and many companies are offering online services, it is very likely that social engineering attacks and data breach attempts will be on the rise for companies of all sizes and industries (Embroker, 2025).

The fourth factor is regulatory compliance requirements. Many countries have adopted robust regulatory frameworks to address cyber threats. In some jurisdictions, cyber insurance is mandatory, while in others, guidelines or incentives have been implemented for companies to obtain such coverage voluntarily (LAMDA Broking, 2023).

For example, in some countries, legislation requires companies that have contracts that have access to sensitive government data to have cyber insurance (Abacus).

Under the impact of these factors, the value of the cyber insurance market has grown rapidly (Table 1).

Generalizing the data in the table, we can conclude that in 2024 the average size of the cyber market was 15.6 billion US dollars, slightly exceeding the level of 2023 (15.3 billion US dollars), and for 2025, an increase to 16.3 billion US dollars is expected. For the next ten years, a CAGR level of 18.4% is likely.

Table 1. The current and prospective global cybersecurity market size.

Expert company	Market size (billion US dollars)						CAGR (%)
	2023	2024	2025	2032	2033	2034	
Imarc Group		**14,2**			**73,5**		**17,9**
Fortune Business Insights	**16,7**	**20,9**		**120,5**			**24,5**
Skyquestt	**14,0**	**16,8**		**71,8**			**19,9**
Insight Ace Analytic		**11,0**				**32,3**	**11,5**
Munich Re		**15,3**	**16,3**				

Sources: *(Fortune Business Insights, 2025), (Imarc Group, 2024), (Insight Ace Analytic, 2025), (Munich Re, 2025), (Skyquestt, 2025)*

Geographically, North America accounted for 36.61% of the market share in 2023. (Fortune Business Insights, 2025)

The total volume of premiums collected in the global cyber insurance market in 2023 amounted to 14 billion US dollars, increasing to 15.3 billion US dollars in 2024. For the future, an increase of up to 29 billion US dollars is forecasted by 2027 (Cobalt, 2024), (Munich Re, 2025).

In 2024, North America earned $10.6 billion in premiums, accounting for 69% of global premiums. And premiums earned in Europe were $3.3 billion, accounting for 21% of global premiums (Munich Re, 2025).

Despite the fact that cyber insurance is a rapidly growing business, it is still a relatively small part of the insurance market. For example, according to data provided by Swiss Re (2024), the size of the global insurance market was 3.1 trillion US dollars, which means that the share of the global cyber insurance market in the global insurance market is 0.49%. And the global cybersecurity market is 193.7 billion US dollars (Fortune Business Insights, 2025).

According to data provided by Embroker (2025), in 2024, the average payment amount of a company for cyber insurance was between 1,200 and 7,000 US dollars annually, with an average cost of approximately 2,000 US dollars per year. And the limits of cyber liability coverage are between 500 thousand US Dollars and 5 million US Dollars per insurance case.

The following variables can be mentioned as variables taken into account: company size, industry, amount and sensitivity of data, annual revenue, strength of security measures, and cyber liability coverage limits, claims history (Embroker, 2025).

The history of cyber insurance began in 1997, when insurance policies were intended for information technology companies responsible for managing networks and systems used by other companies and consumers (Granato, Polacek, 2019).

In the early 2000s, online media insurance policies began to cover unauthorized access, network security, data loss, and damage related to computer worms or viruses (Prowriters).

Cyber insurance policies also did not include both direct and third-party coverage at the same time. It was not until the mid-2000s that these policies, in response to cyber threats, included some direct coverage to protect companies themselves and potentially intellectual property. New policies included coverage for cyber business interruption, cyber extortion, and damage to network assets.

In 2003, the California Information and Security Breach Act, which affected both exposure and cyber insurance, went into effect. Companies operating in the state were required to provide notice to any affected residents of a personal data breach by an unauthorized party. Many other states then passed similar laws. Cyber insurance companies quickly adjusted their offerings with direct coverages such as IT forensics and information security, public relations, credit monitoring, and customer notification. New coverages were also developed for third-party, regulated defense, and fines and penalties that could be tied to notification of affected parties.

To the present moment, the examined market has widened, and three forms of cyber protection through insurance can be identified at the moment:

- Third-party coverage;
- First-party coverage;
- Silent cyber coverage.

Third-party cyber insurance (third-party cyber liability insurance) is designed to provide liability coverage for companies responsible for a client’s online security. That is, it is liability coverage for companies responsible for the online security and data of their clients, but who fail to prevent a data breach or cyberattack on a client. For example, if an IT company’s client suffers a ransomware attack or data breach and sues the IT company, third-party cyber insurance can cover the necessary legal expenses (Insureon), (TechInsurance).

First-party cyber insurance is intended to directly cover the policyholder from the financial consequences of cybersecurity breaches in a company's own network (Coalition), (Insureon).

Silent cyber (also known as unintended or non-affirmative) coverage provides coverage for unknown (or unquantified) exposures arising from cyber hazards that may be triggered under traditional property and liability insurance policies (GuyCarpetenter).

Cyber insurance policies usually offer the following (*5 Types…,* n.d.):

1. Privacy liability coverage. It is important for companies that handle sensitive employee and customer information. It helps protect the company in the event of a data breach that exposes private data and exposes the company to liability. This coverage protects against liabilities resulting from breaches of privacy law or cyber incidents involving private data. These events often result in third-party liability costs due to contractual obligations or regulatory investigations.

2. Network security. This protects a company during network security failures such as data breaches, cyber extortion requests, malware infections, business email compromise events, and ransomware. This covers direct costs incurred by the first party as a result of a cyber incident, including IT forensic investigations, legal fees, data restoration, ransomware negotiation and payment, consumer notification of the security breach, public relations expenses, call center setup, credit monitoring, and identity restoration.

3. Network business interruption. Network business interruption insurance helps companies exposed to operational cyber risk. This includes losses resulting from system failures (such as human error or a failed software patch) and security failures (such as a third-party cyber-attack).

4. Errors and omissions (E&O) coverage. In this case, it is about protecting companies from cyber incidents that prevent the provision of services to customers and the execution of contractual obligations. This includes claims of errors or performance failures in services, such as software and consulting services, as well as professional services. Errors and omissions coverage refers to allegations of negligence or breaches of contract, covering legal defense costs incurred due to lawsuits or disputes with customers.

5. Media liability coverage. This insurance is designed to protect companies from intellectual property damage, excluding patent infringement. It is typically used in print and online advertising, including company posts on social media.

A cybersecurity insurance policy will often exclude issues that were caused by human error or negligence or could have been prevented, such as (*5 Types…*, n.d.), (Fortinet):

- *Poor security processes:* cyber-attacks become possible due to security gaps or ineffective configuration management.
- *Prior breaches:* these are security incidents that occurred before the company purchased a cyber insurance policy.
- *Human error:* these are cyberattacks caused by human errors committed by company employees.
- *Insider attacks:* data loss or theft caused by an internal attack, which made a company employee vulnerable.
- *Pre-existing vulnerabilities:* this is the case when a company suffers a data breach as a result of not addressing or remediating previously known vulnerabilities.
- *Technology system improvements:* this includes any costs related to technological improvements, such as network and application improvements.

Expert Dan Burke (2025) presented the new trends in cyber risk management in 2025:

- *Technology supply chain attacks*. Given that some companies take a relatively long time to patch known vulnerabilities, attackers can exploit these vulnerabilities as long as they exist, generating losses for companies with cyber insurance.
- *Securities and Exchange Commission (SEC) enforcement*. Recent SEC decisions in the United States point to a less risky regulatory environment regarding cybersecurity for public companies and their Chief Information Security Officers. The SEC recently launched the Cyber and Emerging Technologies Unit (CETU) to address cybersecurity misconduct and protect individual investors from malicious cyber actors. The CETU will focus on the following priority areas: fraud committed using emerging technologies, such as artificial intelligence and machine learning; use of social media, the dark web, or false websites to perpetrate fraud; hacking to obtain material nonpublic information; takeovers of retail brokerage accounts; fraud involving blockchain technology and crypto assets; regulated entities' compliance with cybersecurity rules and regulations; public issuer fraudulent disclosure relating to cybersecurity (SEC, 2025).
- *Artificial intelligence (AI) risk*: The adoption of artificial intelligence is accelerating rapidly, and many of the risks associated with it have yet to be discovered. When there is such uncertainty, an insurance policy can help a company leverage the power of artificial intelligence without taking on too much risk. Likewise, many experts warn about the use of AI to carry out cybercrime.
- *Non-breach privacy claims.* Legal issues related to litigation under US privacy laws, particularly the Video Privacy Protection Act (VPPA), highlight the need for companies to improve their data practices and ensure they obtain explicit consent from users before sharing any personal information.

CONCLUSIONS

Cyber insurance is a special insurance product designed to limit the liability of a corporate policyholder and help manage recovery costs in the event of a cyber incident.

Cyber insurance helps protect companies against security risks, the diversity of which increases year by year. And threats to companies' cybersecurity are constantly evolving.

It is a complex product made up of three basic components: third-party coverage, first-party coverage, and silent cyber coverage.

At present, we can speak of the existence of a global cyber insurance market, the essential part of which is located in the US. Although its share is relatively modest within the global insurance market, the dynamics of its expansion are impressive.

REFERENCES

1. *5 Types of Cyber Security Insurance Coverage and what to watch out for*. Available at: https://www.bluevoyant.com/knowledge-center/5-types-of-cyber-insurance-coverage-and-what-to-watch-out-for [Accessed 08.05.2025]
2. Abacus. *How Cyber Insurance Plays A Role in Risk Management and Regulatory Compliance*. Available at: https://goabacus.com/how-cyber-insurance-plays-a-role-in-risk-management-and-regulatory-compliance/ [Accessed 10.05.2025]
3. ABI. What does cyber insurance cover?. Available at: https://www.abi.org.uk/products-and-issues/choosing-the-right-insurance/cyber-insurance/what-does-cyber-insurance-cover/ [Accessed 10.05.2025]
4. Burke Dan, 2025. *Cyber Insurance in 2025: What to Expect*. Available at: https://woodruffsawyer.com/insights/cyber-looking-ahead-guide [Accessed 17.05.2025]
5. Cobalt, 2024. *Top Cybersecurity Statistics for 2025*. Available at: https://www.cobalt.io/blog/top-cybersecurity-statistics-2025 [Accessed 10.05.2025]
6. Embroker, 2025. *How much does cyber insurance cost in 2025?*. Available at: https://www.embroker.com/blog/cyber-insurance-cost/ [Accessed 12.05.2025]
7. Fortinet. *What Is Cyber Insurance? Why Is It Important?*. Available at: https://www.fortinet.com/resources/cyberglossary/cyber-insurance Accessed 12.05.2025]
8. Fortune Business Insights, 2025. *Cyber Insurance Market Size, Share & Industry Trends Analysis, By Insurance Type (Standalone and Tailored), By Coverage Type (First-party and Liability Coverage), By Enterprise Size (SMEs and Large Enterprise), By End-user (Healthcare, Retail, BFSI, IT & Telecom, Manufacturing, and Others), and Regional Forecast, 2024-2032*. Available at: https://www.fortunebusinessinsights.com/cyber-insurance-market-106287 [Accessed 09.04.2025]
9. Fortune Business Insights (2025) *Cybersecurity Market Size, Share & Industry Analysis, By Component (Solutions and Services), By Deployment (On-premises and Cloud), By Security Type (Network Security, Cloud Application Security, End-point Security, Secure Web Gateway, Application Security, and Others), By Enterprise Size (Small & Medium Enterprises (SMEs) and Large Enterprises), By Industry (BFSI, IT and Telecommunications, Retail, Healthcare, Government, Manufacturing, Travel and Transportation, Energy and Utilities, and Others), and Region Forecast, 2024-2032*. Available at: https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165 [Accessed 09.04.2025]
10. Fox Jacob (2024). *Top Cybersecurity Statistics for 2025*. Available at: https://www.cobalt.io/blog/top-cybersecurity-statistics-2025 [Accessed 05.05.2025]
11. Granato Andrew, Polacek Andy, 2019. *The Growth and Challenges of Cyber Insurance*. Available at: https://www.chicagofed.org/publications/chicago-fed-letter/2019/426#:~:text=In%20July%202019%2C%20FM%20Global,would%20suffer%20in%20a%20cyberattack. [Accessed 16.05.2025]

12. GuyCarpetenter. *Affirmative versus silent syber: an overview*. Available at: https://www.guycarp.com/insights/2018/11/affirmative-versus-silent-cyber-an-overview.html#:~:text=Non%2Daffirmative%2Fsilent%2Funintended,every%20type%20of%20insurance%20policy [Accessed 06.05.2025]
13. IBM (2025). *What is cyber insurance?*. Available at: https://www.ibm.com/think/topics/cyber-insurance [Accessed 09.04.2025]
14. Imarc Group (2024) *Cyber Insurance Market Size, Share, Trends and Forecast by Component, Insurance Type, Organization Size, End Use Industry, and Region, 2025-2033*. Available at: https://www.imarcgroup.com/cyber-insurance-market [Accessed 03.05.2025]
15. Insight Ace Analytic (2025) *Cyber Insurance Market Research Report*. Available at: https://www.insightaceanalytic.com/report/cyber-insurance-market/1634 [Accessed 03.05.2025]
16. Insureon. *Third-party cyber insurance coverage*. Available at: https://www.insureon.com/small-business-insurance/cyber-liability/third-party [Accessed 16.05.2025]
17. LAMDA Broking, 2023. *Cyber Insurance and Regulatory Compliance: Safeguarding Data in a Global Context*. Available at: https://www.linkedin.com/pulse/cyber-insurance-regulatory-compliance [Accessed 03.05.2025]
18. Markets and Markets (2024) *Cybersecurity market size, share, industry, overview, growth, latest trends*. Available at: https://www.marketsandmarkets.com/market-reports/cyber-security-market-505.html#:~:text=the%20global%20cybersecurity%20market%20size,projected%20to%20reach%20%24298.5%20billion [Accessed 02.05.2025]
19. Munich Re (2025) *Cyber Insurance. Risks and Trends 2025*. Available at: https://www.munichre.com/en/insights/cyber/cyber-insurance-risks-and-trends-2025.html#:~:text=Cyber%20insurance%20market%20trends,the%20insurance%20industry%20going%20forward [Accessed 02.05.2025]
20. Nakashima Ellen, Peterson Andrea (2014) *Report: Cybercrime and espionage costs $445 billion annually*. Available at: https://www.washingtonpost.com/world/national-security/report-cybercrime-and-espionage-costs-445-billion-annually/2014/06/08/8995291c-ecce-11e3-9f5c-9075d5508f0a_story.html [Accessed 02.05.2025]
21. Prowriters. *Cyber Insurance Blog*. Available at: https://prowritersins.com/cyber-insurance-blog/history-cyber-insurance/ [Accessed 17.05.2025]
22. Securities and Exchange Commission, 2025. *SEC Announces Cyber and Emerging Technologies Unit to Protect Retail Investors*. Available at: https://www.sec.gov/newsroom/press-releases/2025-42 [Accessed 17.05.2025]
23. Silverfort. *Cyber Insurance*. Available at: https://www.silverfort.com/glossary/cyber-insurance/ [Accessed 08.04.2025]
24. Statista (2024) *Annual cost of cybercrime worldwide 2018-2029*. Available at: https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide [Accessed 05.05.2025]
25. Stocklytics (2024) *Annual Cybercrime Cost to Jump by 70% and hit $13.8 Trillion by 2028*. Available at: https://www.globalsecuritymag.com/annual-cybercrime-cost-to-jump-by-70-and-hit-13-8-trillion-by-2028.html [Accessed 05.05.2025]
26. Skyquestt (2025) *Cyber Insurance Market Size, Share and Growth Analysis*. Available at: https://www.skyquestt.com/report/cyber-insurance-market [Accessed 03.05.2025]
27. Swiss Re, 2024. sigma 5/2024: Global economic and insurance market outlook 2025-26. Available at: https://www.swissre.com/institute/research/sigma-research/sigma-2024-05-global-economic-insurance-outlook-growth-geopolitics.html [Accessed 07.05.2025]
28. TechInsurance. *Third-party cyber liability insurance*. Available at: https://www.techinsurance.com/insurance-terms/third-party-cyber-liability [Accessed 16.05.2025]
29. Wikipedia. *Cyber insurance*. Available at: https://en.wikipedia.org/wiki/Cyber_insurance [Accessed 08.05.2025]

PSYCHOLOGICAL ASPECTS OF CYBERCRIME PREVENTION

UDC: 004.056:[343.451+343.971]
DOI: https://doi.org/10.53486/tids2025.08

BARBĂNEAGRĂ OXANA
Academy of Economic Studies
oxana.barbaneagra@ase.md
ORCID ID: 0009-0008-2567-0170

Abstract. Cybercrime is any criminal activity using information devices and/or digital networks which exploit various information vulnerabilities, involving the criminal use of technologies, identity theft, data breaches, computer viruses, scams, and other malicious activities. A number of current publications demonstrate important psychological aspects that have become an integral part of cybercrime. The main goal of the research conducted is to determine the psychological mechanisms of cybercrime and use specific techniques to prevent it. The research was based on examining open Internet publications from experts and specialized companies. The study demonstrated that the basic psychological aspects of cybercrime are the primary motivations and psychological vulnerabilities of the victims. The first refers to the thirst for financial gain, the sense of power and control over victims, and ideological motivations. In their quest for illicit gains, cybercriminals typically target individuals and legal entities with valuable assets, using ransomware attacks, credit card theft, online banking fraud, large-scale money laundering operations, identity theft, phishing, and the creation of fraudulent websites. For some perpetrators, the feeling of power and control over their victims is important due to the anonymity offered by the online environment (which shields them from the fear of identification or retaliation) and the feeling of invincibility. Similarly, cyberbullying and online harassment can be used with the intention of hurting, humiliating or intimidating. Ideological motivations are related to political, extremist, or ethical hacking goals. In terms of victim vulnerability, we differentiate cybercrimes based on manipulation of human behavior, phishing attacks and deceptive techniques, exploiting cognitive biases, impulsiveness and the psychology of online addiction. This involves manipulative techniques with emotions such as fear, greed, curiosity, empathy, or excitement, as well as abuses based on trust and the building of false relationships. One of the solutions to the problems generated by cybercrime is the use of certain psychological techniques, which can be divided into three groups: deducing behavioral profile and risk assessment; undertaking awareness and education measures; carrying out psychological intervention and rehabilitation activities.

Keywords: psychology, cybercrime, motivation, technique, prevention.

JEL Classification: D91, G41, L86

INTRODUCTION

Cybercrime is a general term that is related to any illegal activity with the use of a computer, network, or digital device (Brush Kate, Cobb Michael, 2024), (Proofpoint).

The Council of Europe Convention on Cybercrime defines cybercrime "as a wide range of malicious activities, including the illegal interception of data, system interferences that compromise network integrity, and availability and copyright infringements" (Brush Kate, Cobb Michael, 2024).

Cybercrimes have a certain diversity, with some specialists dividing their typology into the following categories (Brush Kate, Cobb Michael, 2024):

- Crimes in which the computing device is the target, whose purpose, for example, may be to gain access to the network;
- Crimes that use the computer as a weapon; for example, to carry out a denial-of-service attack;

- Crimes in which the computer is used as an accomplice; for example, when it comes to using it to store illegally obtained data.

Cybercrime can be further divided into four categories (Cybertalents):

1. *Individual cybercrimes*, which are related to the activity of individuals. Examples include phishing, spoofing, spam, cyberstalking, and others;

2. *Organizational cybercrime*, which primarily targets organizations and is usually committed by teams of criminals, including malware and denial of service attacks.

3. *Property cybercrimes*, which target property such as credit cards or intellectual property rights.

4. *Society cybercrimes* are the most dangerous form, as they include cyberterrorism.

The conducted research has uncovered important psychological aspects that can be considered as part of the motivation and mechanisms behind cybercrime.

In this context, expert Jonathan Reed (2025) states: "To truly understand cybersecurity is to understand the human mind — both as a weapon and as a shield. …At the core of every cyberattack is a human, driven not just by code but by complex motivations and psychological impulses. Cyber criminals aren't merely technologists. They are people with intentions, convictions, emotions and specific psychological profiles that drive their actions."

A cybercriminal is a person who applies their technological skills to carry out malicious acts and illegal activities in the form of cybercrimes. These criminals can be individuals or form teams (Cybertalents).

These criminals exploit security gaps and vulnerabilities discovered in cyber systems to gain entry into the target environment. These security breaches can take the form of weak authentication methods and passwords, but they can also arise from the lack or ineffectiveness of security models and policies (Cybertalents).

As expert Bhagat Singh Sharma (2023) states, cybercriminals are motivated by a variety of factors, such as financial gain, personal gratification, and even specific political or ideological beliefs. They also exhibit certain psychological traits, such as impulsivity, thrill-seeking, and lack of empathy, which can lead to a lack of concern for the consequences of their actions, including the harm they cause.

Understanding these psychological aspects of cybercrime can be an important component for developing preventive cybersecurity measures, which in turn can reduce the risk of individuals and companies becoming victims of cybercrime.

This article has two main purposes:

- To study the psychological aspects of cybercrime.
- To examine the analysis of behavioral patterns and address psychological issues in order to mitigate the risks associated with cybercrime.

MAIN CONTENT

1. Materials and Methods

The research was based on examining open Internet publications from experts and specialized companies. The conducted research has allowed us to outline the essence and basic psychological aspects of cybercrimes. Then, the psychological possibilities of developing strategies to identify cybercriminals and prevent their activity were studied. The research was completed by drawing up the related conclusions.

2. Results and Discussion

The first part of the study conducted was dedicated to examining the psychological aspects of cybercrimes.

Some experts say that one of the basic psychological foundations of cybercrime is the anonymity provided by activity in cyberspace, which can encourage some individuals to commit crimes that they would not dare in the physical world. Cybercriminals often assume that they can more easily avoid punishment for breaking the law online (Loughtec, 2024).

The expert Jonathan Reed (2025) states: "Many cyber criminals share distinct personality traits: an inclination for risk-taking, problem-solving prowess and an indifference to ethical boundaries. Furthermore, the physical and digital distance inherent in online crime can create a psychological disconnect, minimizing the moral weight of their actions. This environment enables cyber criminals to justify their behavior in ways they might not if they had to face their victims in person."

Opportunistic behavior is also possible. That is, in some cases cybercriminals take advantage of vulnerabilities and weaknesses in software, hardware, or networks without having a specific motive, but with the intention of exploiting the weaknesses for personal gain (Loughtec, 2024).

From a criminological perspective, the following theories can be highlighted to explain the motivation of cybercrimes (*Criminological…*, n.d.):

1. *Rational choice theory*. Individuals engage in cybercrime under the influence of the belief that it is a profitable and low-risk activity. That is, their actions are the result of weighing the potential benefits of committing the crime against the potential risks of being discovered and punished.

2. *Social learning theory*. Criminal behavior by some individuals is the result of observing the behavior of others, especially those close to them. It may also be influenced by the media's portrayal of hackers as charming and successful.

3. *Strain theory*. Individuals may engage in cybercrime when they are dealing with tensions or pressures in their lives, such as economic problems or social exclusion. In this case, criminal activities may become a way to relieve stress or gain a sense of power and control.

4. *Routine activities theory*. Cybercrimes can occur when three factors converge: a motivated perpetrator, a suitable target (e.g., a vulnerable computer system), and the absence of capable protectors (e.g., lack of effective cybersecurity measures).

5. *Self-control theory*. Individuals who commit cybercrimes often have low levels of self-control. This means that many of them are prone to acting impulsively and making decisions without considering the consequences.

Some experts have examined the psychological motivations of cybercriminals (Figure 1) **(**The Hackers Meetup, 2024), (Coretech, 2022), (Loughtec, 2024):

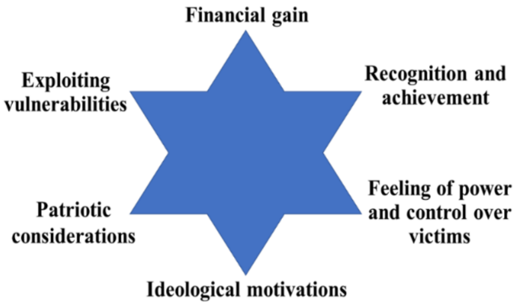

Financial gain
Exploiting vulnerabilities
Recognition and achievement
Patriotic considerations
Feeling of power and control over victims
Ideological motivations

Figure 1. The main psychological motivations of cybercrimes

Sources: (The Hackers Meetup, 2024), (Coretech, 2022), (Loughtec, 2024)

➢ *Financial gain*. According to many experts, financial gain (obtaining economic profits) is the main motivation of cybercriminals, the difference being the methods of obtaining the funds.

This can include:

- Direct access to a bank or investment account, stealing the password of a financial site followed by transferring the assets to one of the criminals;
- Swindling an employee into making a money transfer using a specific technique;
- Carrying out a ransomware attack on the entire organization.

With the stated goal in mind, cybercriminals typically target individuals and businesses with valuable assets, carrying out ransomware attacks, credit card theft, online banking fraud, large-scale money laundering operations, identity theft, phishing, and the creation of fraudulent websites. Cybercriminals may also target an individual's private information or corporate data for theft and resale.

➢ *Recognition and achievement*. Some criminals are motivated by the sense of accomplishment (self-affirmation) that can come with breaking into an important system.

They may operate in groups or independently, but to some extent they crave recognition. By nature, most cybercriminals are competitive and love the challenge that their actions bring. They often encourage each other to carry out sophisticated cyberattacks.

➢ *The feeling of power and control over victims*. For some perpetrators, the feeling of power and control over their victims is important due to the anonymity offered by the online environment and the illusion of invincibility. Cyberbullying is often carried out with the intention of hurting, humiliating or intimidating.

➢ *Ideological motivations*. In this case, it is cybercrime committed with political, extremist, or ethical hacking goals. Typically, these crimes are organized by criminal groups that target entities that challenge their worldviews, often focusing on religious beliefs or geopolitical conflicts.

Cyberterrorism involves the use of technology to cripple a nation's infrastructure or disrupt critical services. Driven by political or ideological agendas, cyberterrorists may launch attacks on government agencies, financial systems, or vital utilities to create chaos and instill fear.

Extremist groups use information technologies to impose and spread their ideology, recruit members, and conduct propaganda campaigns. Cyberspace has become a global terrain for these groups to radicalize individuals and incite violence.

A specific form of cybercrime committed under the impact of ideological factors is *ethical hacking*, also known as *hacktivism*, related to unauthorized access to computer systems with the intention of promoting social or political change.

Although criminals believe their motives are noble, the illegal methods used can cause substantial damage and create ethical issues.

Some cybercriminal groups use their hacking skills to attack large organizations. The motives are usually related to a cause, such as respecting human rights or alerting a large corporation to vulnerabilities in their system. They may also target groups whose ideologies do not align with their own. These groups may steal information and claim to practice free speech, but more often than not, these groups carry out DDoS (Distributed Denial of Service) attacks to overload a website with too much traffic and cause it to crash.

➢ *Patriotic considerations*. Patriotic sentiments are sometimes supported by funding and assistance from a particular state. "Patriots" use cybercrime methods to advance their nation's own interests. Typically, this involves stealing information (including intellectual property), personally identifiable information, and money to fund or advance espionage and exploitation causes. In this case, state-sponsored actors carry out malicious cyberattacks and claim that their cyberespionage activities are legitimate activities on behalf of the state.

➢ *Exploiting vulnerabilities*. This includes cybercrimes based on the manipulation of human behavior, phishing attacks and deception techniques, exploiting cognitive biases, impulsivity and the psychology of online addiction. In most cases, the addictive nature of the digital world and inherent human impulsivity are exploited. The Internet in the modern world offers instant gratification and escape from reality, leading to the development of online addictions. Individuals with a propensity for addiction may engage in cybercrime as a means of fueling their compulsive behaviors.

Some experts point to *the exploitation of the human factor through social engineering* (Reed, 2025).

As Jonathan Reed (2025) notes, the vulnerability of the human mind is one of the most powerful weapons in a cybercriminal's arsenal. Social engineering attacks, such as phishing, exploit non-technological human factors such as trust, fear, urgency, and curiosity, which have become alarmingly effective. A Verizon report notes that the human element was included in 68% of data breaches, highlighting the vulnerability of human interactions.

Phishing attacks focus on creating a sense of urgency, fear, or curiosity. Attackers manipulate users of information products into clicking on malicious links or revealing sensitive information. The success of these attacks depends on creating an illusion of trust and authority, taking advantage of innate human tendencies.

Impulsivity plays an important role in the conduct of cybercrime, as impulsive individuals are more likely to engage in risky behaviors without considering the potential consequences. Cybercriminals capitalize on impulsive behavior to exploit victims and gain unauthorized access to sensitive information. To do this, they use techniques of manipulating emotions such as fear, greed, curiosity, empathy or enthusiasm, as well as abuses based on trust and building false relationships.

Expert Nilesh Roy (2024) focuses attention on the psychological features of cybercrimes:

➢ *Cognitive biases and decision making* are systematic patterns of deviation from the norm or rationality in judgment (reasoning), which can affect both attackers and defenders. They can take the form of confirmation bias and risk assessment bias.

Confirmation biases occur in attackers, when they fall victim to biases manifested only by seeking information confirming pre-existing beliefs, which can lead them to underestimate a target's defenses or to ignore the potential consequences of their actions.

Risk assessment biases occur in both attackers and defenders, who may misjudge risks due to optimism (underestimating the possibility of negative outcomes) and anchoring (overly relying on the first piece of information encountered). These biases can lead to overconfidence in security measures or underestimating the capabilities of an attacker.

➢ *Social engineering* uses human psychology to gain unauthorized access to systems or information and can take one of the following forms:

– *Psychological manipulation* relies on exploiting victims' emotions, such as fear, greed, or curiosity. For example, by crafting persuasive messages, victims are persuaded to reveal sensitive information or click on malicious links;

– *The impact of social dynamics* by appealing to the perceived authority of the sender, the urgency of the message, or the familiarity of the source, to increase the effectiveness of the attacks.

➢ *Stress* can significantly influence decision-making, especially in high-stakes situations, such as responding to a cyber incident. This influence is twofold:

– *The impact on defenders* is manifested by the pressure on cybersecurity professionals, especially during active incidents. Stress can impair judgment, leading to hasty decisions that may not be optimal;

– *The impact on attackers* is exerted when engaging in prolonged or complex activities. Stress can lead to mistakes or deviations from the preliminary plan, which defenders can uncover if they are vigilant and adaptable.

The second part of the study focused on examining the importance of understanding the psychological aspects of cybercrime for developing effective prevention strategies.

By analyzing behavioral patterns and addressing psychological issues, proactive measures can be taken to mitigate the risks associated with cybercrime **(**The Hackers Meetup, 2024):

- Behavioral profiling and psychological risk assessment;
- Education and awareness;
- Psychological interventions and rehabilitation.

Behavioral profiling and psychological risk assessment tools are designed to assist in identifying potential cybercriminals and preventing their actions.

Authors Kitty Kioskli and Nineta Polemi (2020) report the following: “Psychological profiling (or just ‘profiling’) is broadly defined as the various techniques of identifying and analyzing behaviors performed in a crime. …Profiling assists the investigation by either selecting the offender from a pool of suspects or by providing the offender’s description for future identification.”

Psychological profiling involves examining the psychological factors that drive individuals to commit criminal acts. It aims to understand the complex motivations, personality traits, and behavioral patterns that contribute to a person becoming a cybercriminal. Psychological profiling draws on principles from psychology, criminology, and behavioral science to profile potential criminals and understand their actions in the digital realm. An important aspect of psychological profiling is examining the personality traits associated with cybercriminals. Research has identified traits such as narcissism, Machiavellianism, and psychopathy as prevalent among individuals involved in cybercrime. These traits can manifest themselves in actions such as manipulation, lack of empathy, and risk-taking, which are typical of participating in criminal cyber activities (Reynolds, 2024).

A psychological risk assessment is a tool designed to identify potential dangers and risks to the mental health and well-being of individuals and to take measures to minimize or eliminate them (Weidl, 2023).

In this context The Hackers Meetup (2024) mentions the following:

1. *Identifying potential cybercriminals*. Analyzing behavioral patterns (e.g., online activities, communication style, and history of previous cybercrime) can help experts detect individuals with a heightened propensity to engage in cybercriminal activities.

2. *Analyzing behavioral patterns*. Behavioral patterns can reveal clues to potential cyberbullying. They include excessive secrecy, exaggerated online activity, and a tendency to exploit or manipulate others.

3. *Assessing risk factors for cybercrimes*. Assessing risk factors related to a person's use of information technologies, personal and social circumstances, and motivations, contributes to understanding the likelihood of this individual's involvement in cybercrime and developing related prevention strategies.

In this context, we can talk about a special field of research known as *cyber forensic psychology* related to the application of psychological principles and techniques in the investigation of cybercrimes, which is extremely important for understanding the behaviors and motives of attackers, as well as for developing effective investigative strategies (Roy, 2024).

User behavior analytics has become an intersection of information technology and psychology. By analyzing behavioral patterns and detecting deviations, organizations can proactively identify potential threats. This approach is based on the principle that individuals, even in the digital environment, follow predictable patterns. Behavioral analytics can uncover abnormal behaviors, such as an unexpected attempt to access restricted files or logins at unusual times, signaling a potential security breach. The combination of psychology and technology allows for dynamic and adaptive security measures that detect threats early, even before they escalate into full-blown incidents (Reed, 2025).

Enhancing psychological education and promoting awareness about safe digital behavior are basic elements in preventing cybercrime.

These activities refer to the specific field called *cybersecurity psychology* which examines how people perceive, interact with, and respond to cyber threats, with the aim of researching the thought processes that guide their actions (Anders, 2023).

In other words, cyber psychology is the study of the psychological aspects of the interaction of human thought with information technology, with an emphasis on the Internet and digital environments. This field investigates how psychological principles influence both attackers and defenders (Roy, 2024).

In this area the complex of activities may contain (The Hackers Meetup, 2024):

1. *Psychological education for safer cyber behaviors*. By educating individuals about the psychological techniques used by cybercriminals, they become able to recognize and resist manipulation attempts. Promoting critical thinking skills and digital literacy can help individuals be informed, make informed decisions, and identify potential threats.

2. *Enhancing digital literacy*. Digital literacy programs aim to improve knowledge about online security, privacy protection, and responsible digital citizenship. Informing individuals about the risks of cybercrime allows them to take proactive steps to protect their online activity.

3. *Cybersecurity awareness programs in institutions* can help educate interested individuals about best practices, potential risks, and the importance of maintaining a secure online environment.

Psychological interventions and rehabilitation programs are designed to address the issues contributing to cybercrime, assisting individuals in the rehabilitation process and preventing relapse by:

1. *Understanding rehabilitation methods* focus on examining the psychological, behavioral, and social factors that determine a person's involvement in cybercrime, including therapy, counseling, skills development programs, and support networks geared toward positive behavior change.

2. *Addressing underlying psychological issues*. Many cybercriminals have specific psychological issues, such as low self-esteem, trauma, or feelings of helplessness. Psychological interventions aim to identify and address these issues, helping individuals develop healthier coping mechanisms and reducing the likelihood of recidivism.

3. *The role of therapy in cybercrime prevention*. Therapy plays an important role in preventing cybercrime by examining the root causes of criminal behavior. Individual and group therapy sessions can form a supportive environment in which individuals can vent their emotions, gain perspective on their actions, and develop strategies for better decision-making.

Jonathan Reed (2025) mentions the mental strength of cyber professionals.

Protecting against cyber threats, along with technical skills, requires resilience, ethical conviction, and a deep understanding of human behavior. Cyber professionals face constant psychological pressure, and mental resilience allows them to quickly plug gaps, restore security, and learn from incidents.

Creativity and adaptability are also mandatory for cybersecurity. As cybercriminals constantly refine their tactics, security professionals are forced to anticipate these moves and must innovate by developing new countermeasures before an attack occurs.

The aforementioned author also mentions the importance of ethics by virtue of the fact that cybersecurity professionals have access to sensitive data and important tools. In case of their improper use or negligence, substantial damage becomes possible. Implementing a solid code of ethics can create a psychological anchor, helping professionals navigate the moral complexities of their work, respecting the privacy and security of users.

Of great importance is the promotion of a *psychologically sound cybersecurity strategy*. An effective cybersecurity strategy is not only about blocking attacks, but also about adapting to human behavior. Therefore, security measures must be tailored to natural human tendencies. This will work best if users adhere to comprehensive security protocols (Reed, 2025).

Promoting a culture of psychological safety within a company can also encourage employees to be open to security concerns. When employees can freely discuss potential threats and even mistakes, they are able to identify risks early and a collective commitment to cybersecurity is formed within the company.

CONCLUSIONS

The conducted research has demonstrated that cybersecurity is not just a technical issue, but has fundamental human aspects. Psychology's role in cybersecurity is currently very broad, encompassing user behavior as well as attacker prediction and profiling. Its goal is to understand the goals, cognitive patterns, and emotional factors that drive cybercriminals to take action to combat and prevent cybercrime. The psychology of cybercriminals is complex, demonstrating a high adaptability to new technologies, the ability to use multiple tools and techniques to exploit weaknesses in software, networks, and human psychology. And the psychological motivation for illegal behavior is very diverse. Simultaneously, international practice has developed effective techniques designed to help prevent cybercrime. Modern cybersecurity strategies must combine technology and psychology to form effective protection that takes into account both the technical vulnerabilities of the system and human behavior. Combating cyber threats by professionals relies on their mental toughness, creativity, and ethical strength. Implementing behavioral analytics, incorporating the human perspective into cybersecurity strategies, and launching training programs based on psychological principles contribute to the formation of a more adaptive and robust defense system.

REFERENCES

1. Anders Larkin, 2023. The Importance of Teaching Cybersecurity Psychology to Employees. Available at: https://www.hooksecurity.co/blog/importance-of-teaching-cybersecurity-psychology. [Accessed 16.05.2025]
2. Brush Kate, Cobb Michael, 2024. What is cybercrime and how can you prevent it?. Available at: https://www.techtarget.com/searchsecurity/definition/cybercrime#:~:text=Cybercrime%20is%20any%20criminal%20activity,directly%20damage%20or%20disable%20them. [Accessed 10.05.2025]

3. Coretech, 2022. 6 Motivations of Cyber Criminals. Available at: https://www.coretech.us/blog/6-motivations-of-cyber-criminals. [Accessed 12.05.2025]
4. Criminological Explanations of Cybercrime. Available at: https://cod.pressbooks.pub/crimj1165/chapter/module-3/ [Accessed 14.05.2025]
5. Cybertalents. *What is Cybercrime? Types, Examples, and Prevention*. Available at: https://cybertalents.com/blog/what-is-cyber-crime-types-examples-and-prevention [Accessed 12.05.2025]
6. Kioskli Kitty, Polemi Nineta, 2020. Available at: A Socio-Technical Approach to Cyber-Risk Assessment. https://core.ac.uk/download/586551524.pdf. [Accessed 15.05.2025]
7. Loughtec, 2024. Exploring the motives behind cybercrime. Available at: https://www.loughtec.com/exploring-the-motives-behind-cybercrime. [Accessed 13.05.2025]
8. Proofpoint. *What Is Cyber Crime?*. Available at: https://www.proofpoint.com/au/threat-reference/cyber-crime [Accessed 12.05.2025]
9. Reed Jonathan, 2025. *Hacking the mind: Why psychology matters to cybersecurity*. Available at: https://www.ibm.com/think/insights/hacking-the-mind-why-psychology-matters-to-cybersecurity [Accessed 08.04.2025].
10. Reynolds, A'shya Latrice, 2024. *Profiling Cybercriminals: Behavioral Analysis and Motivations Behind*
11. *Cybercrime Activities*. Available at: https://digitalcommons.odu.edu/cgi/viewcontent.cgi?params=/context/covacci-undergraduateresearch/article/1094/&path_info=COVA_Research_Paper____Profiling_Cybercriminals__Behavioral_Analysis_and_Motivations_Behind_Cybercrime_Activities.____3_.pdf. [Accessed 24.05.2025]
12. Roy Nilesh, 2024. *Cyber Psychology in CyberSecurity: A Comprehensive Analysis*. Available at: https://www.linkedin.com/pulse/cyber-psychology-cybersecurity-comprehensive-analysis-roy--5x5ac#:~:text=Cyber%20psychology%20is%20the%20study,influence%20both%20attackers%20and%20defenders. [Accessed 10.04.2025].
13. Sharma Bhagat Singh, 2023. *The psychology of cybercriminals: understanding the mind of a hacker*. Available at: https://www.linkedin.com/pulse/psychology-cybercriminals-understanding-mind-hacker-sharma [Accessed 10.04.2025].
14. The Hackers Meetup, 2024. *Understanding the Psychology Behind Cyber Crimes*. Available at: https://thehackersmeetup.medium.com/understanding-the-psychology-behind-cyber-crimes-235ab3360078 [Accessed 08.04.2025].
15. Weidl Christof, 2023. What to *Consider in a Psychological Risk Assessment, Who Should Conduct It, What it Brings, and Best*. Available at: https://www.lemin.ai/en/post/what-to-consider-in-a-psychological-risk-assessment-who-should-conduct-it-what-it-brings-and-best#:~:text=A%20psychological%20risk%20assessment%20(PBG)%20is%20an%20important%20tool%20for,to%20minimize%20or%20eliminate%20them. [Accessed 14.05.2025].

ADAPTIVE MULTI-FACTOR AUTHENTICATION IN A DOCUMENT-CENTRIC SYSTEM

UDC: 004.056.523
DOI: https://doi.org/10.53486/tids2025.09

GHENADIE BELINSCHI
Information Security Laboratory of the Academy of Economics Studies,
ghenadie.belinschi@ase.md
ORCID ID: 0009-0009-3361-9890

Abstract: Static authentication methods are increasingly vulnerable to social engineering and phishing, especially in cloud-based document workflows. This paper presents an adaptive multi-factor authentication model that escalates security measures with higher document criticality or anomalous user behavior. By merging biometric data with cryptographic safeguards under Zero-Trust principles, continuous verification is achieved while balancing usability. Preliminary findings suggest a notable increase in protection for sensitive documents and underscore the need to standardize event-driven controls.

Key words: Multi-factor authentication, document-centric systems, data protection.

JEL Classification: C 88, O 33, M 15

INTRODUCTION

In the era of digital transformation, the need for reliable user authentication when handling sensitive data is steadily increasing. Traditional authentication methods—such as relying solely on passwords—are no longer sufficient to ensure security. Passwords can be easily guessed or stolen through phishing and data breaches. According to Verizon, approximately one-quarter of all data breaches involve the use of stolen credentials (Verizon, 2022). Even the implementation of static two-factor authentication (2FA) does not fully resolve the issue: social engineering and phishing attacks can still bypass one-time codes, while the constant demand for additional authentication steps significantly reduces user convenience.

The Zero Trust concept calls for a fundamental shift in how access security is approached. At its core is the principle of "never trust, always verify," meaning that every attempt to access a resource is treated as potentially unsafe until proven otherwise (NIST, 2020). Traditional perimeter-based security models assume that internal users and devices can be trusted by default. In contrast, Zero Trust is built on a presumption of distrust: authentication and authorization must be performed for every access request, regardless of whether it originates inside the corporate network or from outside (NIST, 2020). In practice, Zero Trust architecture requires continuous verification of both user and device during every session or transaction, along with enforcing the minimum necessary access level for each request. This approach significantly reduces risks associated with both external attacks and internal threats, including compromised employee credentials or devices.

Nonetheless, applying Zero Trust principles introduces a challenge to user convenience: if all possible authentication factors are requested for every action, the user experience becomes excessively burdensome. Therefore, a key objective is to strike a balance between stringent access control and usability. One effective approach is adaptive multi-factor authentication—a dynamic method where the system tailors verification procedures according to the current risk level. In an adaptive model, low-risk actions are executed with little to no disruption for the user, whereas higher-risk situations trigger requests for additional identity verification. This risk-based strategy has gained significant attention from experts, as it addresses the long-standing trade-off between security and convenience (Brodsky, A., 2018). Specifically, risk-based authentication (RBA) determines not only whether authentication is required, but also which and how many factors should be used, based on a real-time assessment of the current context (Brodsky, A., 2018).

Document-centric systems have specific authentication requirements. Access to protected documents must be granted only to verified users with the appropriate permissions, and each operation—such as opening, editing, or sending a document—should be explicitly confirmed. At the same time, employees require convenient and seamless access to documents in order to work efficiently. This creates a demand for adaptive verification mechanisms that can strengthen security in response to abnormal or high-risk activities, while remaining unobtrusive during routine, low-risk actions.

The aim of this study is to design and analyze an architecture for adaptive multi-factor authentication in a document-centric system, aligned with the principles of Zero Trust.

1. METHODOLOGY

This study is applied in nature and follows the design science methodology commonly used in information security research. It begins with an analysis of the shortcomings of traditional authentication mechanisms and the requirements imposed by the Zero Trust concept. Based on this analysis, the architecture of an adaptive multi-factor authentication (MFA) system tailored for a document-centric environment was developed. The system's core components were implemented in a prototype and tested using model scenarios involving access to protected documents. To evaluate the outcomes, a combination of comparative analysis and experimental simulation of access attempts—both legitimate and malicious—was employed.

The authentication system comprises several modules that interact through an event-driven model. The key components of the architecture and their roles are as follows:

The authentication module serves as the central component responsible for processing access requests to documents. Each time a user attempts to access a protected document, this module initiates a verification process—prompting the user to provide the necessary authentication factors based on the assessed risk level. It supports a range of factors, including passwords, one-time passcodes (OTP), biometric data (such as fingerprints or facial recognition), and hardware tokens. Under normal, low-risk conditions, a single-factor check (e.g., password) may be sufficient. However, when the risk level increases, additional factors are automatically enforced. In this way, the module implements the Step-Up authentication approach, escalating the verification requirements as needed.

The Risk Engine is a dedicated module for risk assessment that analyzes the context of each session and assigns it a dynamic risk level. It collects input data from multiple sources—such as user identity, device characteristics, network details, time of access, and the type of operation being requested. Using this data, it calculates a real-time risk score based on predefined rules and models. Relevant risk factors include the user's geographic location and deviations from their typical patterns, whether the device and browser are recognized or new, the time of access (e.g., during or outside working hours), and whether the user's current behavior aligns with their historical activity patterns (Verizon, 2022), (Brodsky, A., 2018).

The Risk Engine can also leverage behavioral biometrics, such as typing speed and rhythm or mouse movement patterns, to help identify users by their unique behavior. Based on the combination of these inputs, the system classifies each session as low, medium, or high risk. The authentication module then adjusts its response accordingly: low-risk sessions proceed transparently, medium-risk sessions require an additional verification factor, and high-risk sessions are blocked—prompting extended checks or outright denial. This adaptive strategy enables the system to enhance security without disrupting the experience for legitimate users.

The event model is designed to be event-driven. This means that all significant events and context changes are captured and formalized as structured records, which are then transmitted to the Risk Engine and other system modules. The model encompasses various types of events, including authentication events (e.g., successful login, failed login attempt, additional factor request), application events (e.g., document opening, file upload or transmission), and system events (e.g., session IP address change, new device connection, privilege escalation).

Each event is described using a defined set of attributes—such as event type, timestamp, user ID, and contextual data like geolocation or device status. This standardized event format ensures consistent and reliable information flow into the Risk Engine. The model builds on established approaches in security event management and user and entity behavior analytics (UEBA). However, the Zero Trust paradigm currently lacks a unified standard for event modeling, making the integration of disparate systems more complex (Morrow *et al.*, 2022). To address this, our solution uses a custom event format and vocabulary, which may serve as a foundation for future standardization efforts.

Cryptographic Protection. Confidential user data—such as password hashes and biometric templates—is stored in the authentication database in encrypted form. Robust, standardized encryption algorithms are used to ensure data security (e.g., AES-256 for data storage and TLS 1.3 for data transmission), meeting the requirements for confidentiality and integrity.

Additional safeguards are implemented to prevent the compromise of authenticators themselves. For example, biometric data is transmitted with a cryptographic signature that verifies both its authenticity and its origin from a trusted sensor. When hardware tokens are used (e.g., smart cards or USB keys), their private keys never leave the device; instead, the token signs authentication challenges internally, eliminating the risk of secret interception. In this way, the architecture adheres to Zero Trust principles by securing all communications—regardless of network location—and validating the authenticity of data sources (NIST, 2020).

Sequence diagrams and use case models were developed to illustrate the system architecture and the interaction between its components. The paper also includes pseudocode for the Risk Engine rules and examples of event formats to demonstrate the system's logic. Following the architectural design, a prototype was implemented: a web-based document management service integrated with the authentication module and a simplified version of the Risk Engine. This prototype enabled simulation testing, the results of which are discussed in the following section.

2. COMPARISON OF TRADITIONAL AND ADAPTIVE AUTHENTICATION SCHEMES

To assess the effectiveness of the proposed system, we conducted a comparative analysis against traditional approaches. In a document-centric environment, traditional authentication typically relies on static multi-factor authentication (MFA)—for example, a user is always required to enter a password followed by a one-time code sent to their phone upon login. While this method offers better security than password-only access, it has notable limitations.

First, it lacks contextual awareness—additional factors are always required, even in low-risk situations (such as when an employee logs in from their usual workstation in the office). Second, static MFA does not respond to changes in real time. Once the initial check is passed, access remains open, and the system does not continue to monitor or evaluate subsequent activity.

The proposed adaptive authentication approach is characterized by the following key features.

Context-awareness – The decision to require MFA is based on real-time contextual information about the session. The system evaluates factors such as the device and location from which the request originates, the type of document being accessed, the time of day, and more. If no anomalies are detected, additional authentication steps are skipped, enhancing the overall user experience (Brodsky, A., 2018).

Dynamic and continuous – Risk assessment is performed for every new access event. Under the Zero Trust model, each action must be verified independently, meaning that even after a successful login, the system may require re-authentication when accessing highly sensitive documents or when contextual changes occur—such as a sudden change in the session's IP address (NIST, 2020). In contrast, traditional models often grant broad access after the initial login, which poses a risk if the session is compromised. The adaptive model follows a "per request" decision-making principle—each request is evaluated in real time to determine whether additional verification is necessary.

Balance of security and convenience – The system is designed to deliver strong security where it is necessary, without overburdening users in low-risk scenarios. As noted, risk-based authentication helps reconcile the tension between security and user convenience (Brodsky, A., 2018). In typical conditions, users barely notice the protection mechanisms—login is seamless, and access to standard documents requires no extra steps. In contrast, when the situation is atypical, the system escalates the level of verification. According to recent research, users find adaptive (risk-based) authentication more convenient than constant two-factor authentication, while also perceiving it as more secure than password-only access (Wiefling et al., 2021). As a result, the proposed approach improves user satisfaction without compromising security.

Resistance to credential compromise – If an attacker obtains a user's password, traditional MFA may still prevent access—provided the second factor is enabled. However, many users disable the second factor due to inconvenience, or use weaker methods such as SMS, which can be intercepted. In an adaptive scheme, the compromise of a password alone is not enough to breach the system. If a login attempt is made from an unfamiliar device or an unusual location, the Risk Engine assigns a high risk level and prompts for additional factors that the attacker likely cannot provide (such as biometrics or a hardware token). The system can also fully block suspicious attempts if the assessed likelihood of an attack is high (Brodsky, A., 2018). This significantly reduces the risk of account takeover through stolen credentials.

To illustrate how the scheme functions, consider the following example scenarios.

Scenario 1 (typical access): An employee logs into a document-centric system from their office computer. The device is registered, the geolocation matches the office location, and the system recognizes that the user has previously logged in from this device. In addition, behavioral indicators—such as typing speed—match the user's typical pattern. The Risk Engine classifies the session as low risk. As a result, only basic authentication is required—for example, entering a password—after which the user is granted immediate access to documents without additional checks. From the user's perspective, this feels like a simple, seamless login.

Scenario 2 (high risk): The same employee attempts to log in from an internet café in another country and requests access to a financial report marked "Confidential." In this case, the context is unusual: the device is unknown, the location is atypical, and the requested document is highly sensitive. The Risk Engine assigns a high risk level to the session. Consequently, the system may require multiple authentication factors: in addition to the password, the user must confirm the login via a mobile app (e.g., push notification or OTP) and complete biometric verification. Access is granted only if all required factors are successfully provided. If the attempt is fraudulent—such as when an attacker cannot supply valid biometrics or the correct OTP—access is denied, and the incident is forwarded to the security monitoring system. In this way, the adaptive mechanism responds intelligently to context: in the first case, the user experiences no friction, while in the second, a potential attack is thwarted through multi-layered verification.

3. SYSTEM SECURITY AND THREAT MANAGEMENT

Security Analysis of Adaptive MFA – The proposed system offers a significantly higher level of protection compared to static authentication schemes. Even if an attacker manages to bypass one factor—such as by guessing or stealing a password—the likelihood of simultaneously overcoming multiple independent factors, while also passing behavioral and contextual checks, is extremely low. Particular emphasis is placed on resilience against common types of attacks.

As noted earlier, a password alone does not guarantee secure access—phishing and password guessing remain significant threats. In cases of suspicious login attempts, the system requires additional authentication factors that phishing sites cannot easily intercept, such as biometric data or a push notification to a trusted device. Moreover, the Risk Engine can detect anomalies characteristic of automated attacks—for instance, unusually high-speed credential entry or login attempts using bulk username lists—and immediately flag such sessions as high-risk, thereby blocking mass brute-force attempts.

In traditional models, if an attacker gains access to an active session cookie, they can often continue interacting with the system without further authentication. In contrast, the adaptive model enforces re-authentication for every critical action. For example, even with a stolen session cookie, an attacker attempting to open a protected document or perform actions on behalf of the user would be prompted for additional authentication (re-authentication). Furthermore, the system can detect if the session has been transferred to a different device or IP address, flag it as potentially hijacked, and require the user to re-authenticate entirely.

A dishonest employee or an external attacker who gains access to the internal network cannot move freely across resources without oversight. In a Zero Trust model, every action across different nodes requires explicit authorization (NIST, 2020). To mitigate internal threats and privilege escalation, the system logs all document access requests and can identify suspicious patterns of behavior—even from users who are legitimately logged in. For instance, opening a large number of documents in rapid succession or attempting access at unusual hours may trigger a higher risk classification. As a result, the system may prompt the user to re-authenticate or temporarily suspend access pending further investigation. In this way, the system hinders insider attacks and lateral movement within the network.

An important component of the system is the use of biometrics—such as fingerprint, facial, or voice recognition—as one of the authentication factors. Biometric authenticators offer a significant advantage: they cannot be forgotten or shared, are inherently linked to the individual user, and—unlike passwords or tokens—cannot be accidentally lost. However, biometrics also come with known vulnerabilities. One issue involves identification errors (false acceptances and false rejections), where the system may confuse one user for another. While modern algorithms minimize these errors, a more serious concern is spoofing—i.e., the forgery of biometric data. An attacker might try to trick the system using a fake fingerprint or a photograph of a face instead of a live person. It is well-documented that simple techniques, like showing a printed photo to a camera, can deceive some facial recognition systems if no additional checks are in place (Zakuanova *et al*., 2018).

To counter such threats, the system incorporates anti-spoofing mechanisms, collectively referred to as Presentation Attack Detection (PAD). The first layer of protection involves a liveness check during biometric capture: the camera or scanner analyzes features such as micro-movements of the face, pupil response, or finger temperature to verify that a real, live user is present. Secondly, the Risk Engine evaluates the metadata associated with the biometric authentication channel. As noted in a Sberbank study, the highest risks are linked to remote authentication scenarios, where the user's device is outside the system's direct control. Accordingly, the system applies differential trust: biometrics captured in controlled environments (e.g., on a corporate device with a certified sensor) are granted a higher level of trust, while those obtained from regular user devices are treated with greater caution. In the latter case, even a successful biometric match may require additional verification to mitigate potential fraud. This approach aligns with NIST recommendations—for example, the SOFA-B document, which assesses the reliability of biometric factors based on the channel through which they are collected.

Thus, the integration of biometrics into adaptive MFA enhances overall system security by adding another barrier for attackers, while incorporating safeguards against biometric-specific threats.

As part of the study, the prototype was tested using a set of experimental scenarios. The evaluation focused on several key metrics: average user authentication time under different conditions, the number of additional verification steps at various risk levels, the number of blocked unauthorized access attempts, and overall user satisfaction. The results confirmed the theoretical assumptions. Under typical conditions (low risk), users logged in with minimal delay: in 85% of cases, access to documents was granted after entering only the primary factor (a password), with no need for additional verification. In contrast, the baseline static MFA system always required extra codes, which increased the average login time by approximately 30%. Thus, in terms of convenience—measured by login time and number of required actions—the adaptive scheme showed a clear advantage.

From a security perspective, simulated attack scenarios demonstrated the system's ability to detect anomalies. Login attempts using clearly stolen passwords from unfamiliar locations were either blocked outright or triggered requests for additional factors inaccessible to the attacker. Separate tests addressed biometric spoofing: attempts to log in using a photo instead of a live face were detected by the system through the absence of liveness indicators, and access was denied, with the event logged as an attack. These results confirm that the combination of the Risk Engine and modern authentication methods can significantly enhance the security of a document-centric system—without compromising convenience for legitimate users.

The proposed approach is applicable to a wide range of systems that require flexible access control to sensitive data—particularly corporate systems, government infrastructures, and cloud-based platforms for exchanging confidential files. In environments where employees work remotely or in hybrid formats, adaptive authentication makes it possible to implement the Zero Trust model in practice, enabling secure document access from anywhere in the world.

Moreover, key components of the system—such as the Risk Engine and the event model—can be integrated into identity and access management (IAM) platforms and broader cybersecurity solutions. Overall, adaptive multi-factor authentication aligns with the strategy of Continuous Adaptive Trust, which is increasingly recognized as an essential element of modern cybersecurity frameworks. Industry reports indicate that major technology companies—including Google, Amazon, and Microsoft—are already employing risk-based authentication mechanisms to protect user accounts (Wiefling *et al.*, 2021). This demonstrates the practical viability and effectiveness of the concept.

CONCLUSIONS

This paper presents an architecture for adaptive multi-factor authentication in a document-centric system, built on the principles of Zero Trust. The analysis demonstrates that combining the Risk Engine, an event-driven approach, and a diverse set of authentication factors results in a higher level of security compared to traditional models—without placing unnecessary burden on the user. The key strengths of the proposed model lie in its dynamic risk response (adjusting the depth of verification based on contextual factors) and improved user experience for legitimate users (most routine operations in familiar environments require no extra steps). Experimental validation confirmed that the adaptive scheme effectively detects unauthorized access attempts—such as those involving stolen credentials or spoofed biometric data—and substantially reduces the risk of compromising protected documents.

The main findings of the study can be summarized as follows: First, risk-based authentication resolves the long-standing trade-off between security and usability, enabling continuous access control without significantly impairing the user experience (Brodsky, 2018), (Wiefling *et al.*, 2021). Second, incorporating biometric factors into MFA enhances overall protection, but requires the implementation of spoofing countermeasures and robust management of biometric data collection channels (Zakuanova *et al.*, 2018), (Brodsky, 2018). Third, the event model is essential to the effective application of Zero Trust principles: by consolidating and analyzing events from multiple sources—such as authentication systems, applications, and networks—it provides a comprehensive understanding of context, allowing the decision engine to function with greater precision and reliability.

Despite the promising results, the proposed solution has several limitations. First, the effectiveness of the Risk Engine depends heavily on the quality and volume of available data related to user behavior and environmental context. In cases where data is limited—such as with new users or devices—the system may produce false positives (triggering unnecessary MFA prompts) or, conversely, fail to accurately assess risk. Future improvements should focus on refining machine learning models and heuristic risk assessments, as well as collecting more behavioral data to improve reliability over time. Second, introducing adaptability adds complexity to the authentication infrastructure. It requires the integration of multiple components, rule configuration, and compatibility with a range of devices and authentication factors. This increases initial deployment costs and demands skilled personnel to manage and maintain the system. Third, not all organizations or resource types are prepared to adopt the Zero Trust model. For some smaller companies, a traditional static MFA approach may be more practical and cost-effective. As such, adaptive MFA should be viewed as part of a broader organizational security strategy, whose feasibility depends on the risk landscape and available resources.

Future Directions and Standardization – One of the key areas for future work is the development of standardized event models for Zero Trust systems. As previously noted, there is currently no widely accepted specification that defines the format and semantics of authentication and access events within a Zero Trust context (Morrow *et al.*, 2022). Establishing a unified standard would enable consistent data exchange between the Risk Engines of different solutions, simplify system integration, and improve the reliability of risk assessments through aggregated event data from diverse sources.

Promising directions also include the advancement of adaptive biometric methods, where the system not only validates biometric templates but also dynamically adjusts the required biometric factor or threshold based on contextual factors. Another critical area is the integration of artificial intelligence into the Risk Engine. More sophisticated machine learning algorithms and event correlation techniques will enhance the system's ability to detect complex attacks and anomalies with greater accuracy.

A major objective is to create a self-learning system that incorporates behavioral biometric profiling—analyzing typing dynamics, mouse movement patterns, and individual work styles to continuously refine user identification. To rigorously define system security, it will also be necessary to formalize the models of events and authentication states.

Finally, transitioning from prototype to full-scale deployment will require extensive testing. Evaluating system performance across a broad range of scenarios will enable precise tuning of the balance between security and usability.

REFERENCES

1. Brodsky, A., 2018. Risk-Based Authentication: Balancing Security and Usability (in Russian). *BIS Journal – Information Security of Banks №2(29)/2018*.
   Available at: https://ib-bank.ru/bisjournal/post/665 [Accessed 10.05.2025].
2. Morrow, T., Popeck, M., & Brown, R., 2022. *Zero Trust Industry Day Experience Paper*. Software Engineering Institute, Carnegie Mellon University. Available at: https://insights.sei.cmu.edu/documents/621/2022_019_001_888817.pdf [Accessed 10.05.2025].
3. NIST, 2020. *SP 800-207: Zero Trust Architecture*. National Institute of Standards and Technology. Available at: https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf [Accessed 10.05.2025].
4. Verizon, 2022. *Data Breach Investigations Report – 2022*. Verizon Enterprise. Available at: https://www.verizon.com/business/resources/T30f/reports/2022-dbir-data-breach-investigations-report.pdf [Accessed 10.05.2025].
5. Wiefling, S., Dürmuth, M., and Lo Iacono, L., 2021 Verify It's You: How Users Perceive Risk-Based Authentication. *IEEE Security & Privacy*, 19(6), pp. 26–36. Available at: https://www.stephanwiefling.de/papers/rba-perceptions-spm2021.pdf [Accessed 10.05.2025].
6. Zakuanova, M.R., Kalinovskii, I.A., 2018. Detection of Spoofing Attacks in Facial Biometric Systems via Texture Analysis (in Russian). In: ITMO University, *Scientific Almanac of ITMO University*, vol. 2, pp. 174–177. Research advisor: Shchemelinin, V.L. Available at: https://science.itmo.ru/wp-content/uploads/2021/08/almanah_2018_tom2.pdf [Accessed 10.05.2025].

MODERN METHODS OF DETECTING AND COUNTERING PHISHING ATTACKS IN THE DIGITAL ENVIRONMENT

UDC: 004.056.53
DOI: https://doi.org/10.53486/tids2025.10

OLHA HABORETS
PhD, Associate Professor
Department of Operational and Investigative Activities and Information Security
Faculty No. 3, Donetsk State University of Internal Affairs, Ukraine
ORCID ID: 0000-0001-7791-6795

LUDMILA RYBALCHENKO
PhD, Associate Professor
Department of Cyber Security and Information Technologies
University of Customs and Finance, Dnipro, Ukraine
luda_r@ukr.net
ORCID ID: 0000-0003-0413-8296

Abstract. Phishing attacks have evolved into a major cybersecurity threat, leveraging advanced technologies and human vulnerabilities to achieve unauthorized access, data exfiltration, and financial exploitation. This article explores the transformation of phishing tactics, identifies the latest detection technologies including artificial intelligence and behavioral analysis, and evaluates the strategic countermeasures adopted across various digital sectors. Through a comprehensive review of modern techniques such as Natural Language Processing, threat intelligence sharing, and multi-factor authentication, the article emphasizes the importance of an adaptive and collaborative approach to phishing defense.

Hackers use deception to lure users out of their account passwords and compromise personal information, creating a threat to the confidentiality of information. With phishing attacks, which are a common form of digital threats to accounts, attackers hack into accounts using hypertext links with malicious codes. The issue of phishing attacks is one of the of the most common methods of gaining access to confidential user data. With the growth of information technology comes the development of various technologies for creating phishing attacks that are related to messaging and mobile devices. Attackers often intercept and crack codes to gain access to accounts and create a cyberattack using malware. Often, fraudsters use phishing attacks to gain access to accounts and sell the data to criminals. Data breaches for large enterprises can become the basis for various cyberattacks, which can result in the loss of large amounts of money.

Keywords: phishing, cyber threats, artificial intelligence, behavioral biometrics, Natural Language Processing, social engineering, threat intelligence, cybersecurity strategy, phishing detection, phishing mitigation.

JEL Classification: H56, D80.

INTRODUCTION

Phishing remains one of the most sophisticated and persistent threats in the contemporary digital landscape, evolving rapidly to exploit vulnerabilities in both human behavior and technological infrastructure. As digital communication and online services expand globally, cybercriminals continue to adapt phishing methodologies to bypass traditional security mechanisms, often employing advanced social engineering tactics and automation. Consequently, the necessity for modern, integrated approaches to phishing detection and prevention has become a focal point in cybersecurity research and practice.

Phishing attacks have diversified significantly in recent years, moving beyond simplistic email-based scams to encompass more complex forms such as spear-phishing, smishing, vishing, pharming, and clone phishing. Each vector is designed to manipulate the target through various channels – email, SMS, voice calls, manipulated websites, or forged communications – to extract credentials, financial information, or other sensitive data. The polymorphic and context-aware nature of these attacks complicates detection and response, requiring a layered and adaptive defense strategy. Notably, attackers increasingly exploit current events, such as global pandemics or geopolitical conflicts, to increase the success rate of their campaigns.

MAIN CONTENT

1. Materials and Methods

Contemporary methods for phishing detection increasingly rely on the integration of artificial intelligence (AI) and machine learning (ML) algorithms. These technologies enable the continuous analysis of large volumes of data to identify subtle anomalies and predictive indicators of phishing behavior. Natural Language Processing (NLP) is applied to scrutinize the semantic and syntactic features of messages, detecting urgency, coercion, and deceptive intent commonly embedded in phishing content. Similarly, heuristic and signature-based systems continue to serve as foundational elements, particularly for recognizing known patterns of malicious activity.

Advanced phishing detection systems now combine AI-driven threat modeling with real-time data feeds, enabling predictive analytics and early warnings. Sandboxing techniques are also employed to isolate suspicious attachments and observe their behavior in a controlled environment. Email security gateways equipped with anomaly detection mechanisms can effectively intercept phishing emails before they reach end-users. Furthermore, phishing simulators are widely used to test employee readiness and improve organizational response mechanisms.

Another crucial aspect of modern phishing mitigation is the use of URL and domain analysis, which assesses the trustworthiness of links based on registration data, structural characteristics, and real-time comparisons with threat intelligence databases. Browser extensions and endpoint security software further augment this analysis by providing real-time alerts and blocking access to flagged content. Behavioral biometrics represents a promising frontier, enabling systems to detect fraudulent access attempts based on deviations in user interaction patterns, such as typing rhythms or mouse dynamics. Coupled with geolocation data and device fingerprinting, these methods can create robust authentication profiles.

To counter phishing effectively, organizations must adopt a proactive and holistic approach. Multi-factor authentication (MFA) serves as a vital line of defense, reducing the risk of unauthorized access even when credentials are compromised. Concurrently, comprehensive security awareness training fosters a culture of vigilance among employees, enhancing their ability to identify and report suspicious communications. The implementation of email authentication protocols – such as SPF, DKIM, and DMARC – significantly curtails email spoofing, reinforcing trust in organizational correspondence.

2. Results and Discussion

Moreover, the integration of threat intelligence sharing mechanisms across sectors facilitates a collaborative response to emerging phishing campaigns. Platforms for real-time exchange of indicators of compromise (IOCs) and attack signatures empower security teams to anticipate and neutralize threats with greater efficiency. This collective intelligence, when augmented with automated analytics, provides a scalable defense framework adaptable to the evolving tactics of threat actors. International cooperation, including joint initiatives by governmental and private cybersecurity organizations, further strengthens global resilience.

Nevertheless, significant challenges persist. Adversaries are increasingly leveraging AI to enhance the believability of phishing messages and to automate the customization of attacks based on publicly available personal data. As a result, defensive systems must evolve beyond static rule sets to incorporate dynamic, self-learning capabilities capable of anticipating novel attack vectors. Future research should prioritize the development of context-aware detection models, interdisciplinary strategies combining human cognition with machine reasoning, and regulatory frameworks that mandate transparent data sharing and accountability.

CONCLUSIONS

In conclusion, the dynamic and multifaceted nature of phishing necessitates a strategic fusion of technological innovation, informed policy-making, and continuous education. Modern countermeasures – when applied coherently – can substantially reduce the effectiveness of phishing campaigns and fortify the resilience of digital ecosystems against exploitation. The path forward lies in the collaborative advancement of intelligent systems that not only detect threats but also preemptively disrupt adversarial operations in the cyberspace continuum. As digital environments continue to expand, so too must our capacity to protect them through adaptive, ethical, and intelligent cybersecurity practices.

The increasing complexity of cyberspace presents a profound challenge to achieving cyber resilience, exacerbating inequities that leave less-resourced organizations vulnerable. Geopolitical tensions are prompting organizations to re-evaluate their strategies, balancing security concerns with global operations. Such tensions often drive targeted attacks, as state-sponsored actors exploit vulnerabilities for espionage and disruption. This dynamic landscape requires adaptive strategies that account for shifting global risks and supply chain dependencies.

REFERENCES

1. Haborets, O. A. (2024). The impact of cyber threats on community and citizen security: Analysis and perspectives on resolution. In Interaction between state bodies and the public in counteracting criminal offenses in the central regions of Ukraine: Roundtable materials (April 17, 2024, Kropyvnytskyi) (pp. 36–37). Kropyvnytskyi: DonDUVS. Access mode: https://dnuvs.ukr.education/wp-content/uploads/2024/06/ zbirnyk_ materialiv_kruglogo_stolu_ord_ta_ib-2.pdf
2. Global Cybersecurity Outlook 2025. World Economic Forum. 2025. p. 49. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

CYBERSECURITY AMONG USERS: PERCEPTIONS, KNOWLEDGE, AND REALITIES

UDC: [004.056+004.8]:[658.89+366.14]
DOI: https://doi.org/10.53486/tids2025.11

VERONICA HÎNCU
Academy of Economic Studies of Moldova
soltanici.veronica@ase.md
ORCID ID: 0009-0002-9291-088X

Abstract. In an increasingly digital world, cybersecurity has become a fundamental concern for both individuals and organizations. This paper explores users' perceptions, knowledge, and real-world behaviors related to digital security, based on the analysis of a questionnaire applied to a sample of 100 participants. The study investigates five thematic areas: awareness of cyber threats, personal and organizational experiences, individual security practices, openness to cybersecurity education, and expert perspectives on emerging solutions such as artificial intelligence.

The results reveal a significant gap between theoretical awareness and actual behavior. While 93% of respondents correctly defined a cyberattack, only a small percentage actively apply good cybersecurity practices – such as updating software, using two-factor authentication, or changing passwords regularly. Furthermore, 37% of participants reported having been affected by cyber incidents, yet only a third of organizations reportedly use vulnerability detection tools on a regular basis. A notable proportion of respondents (58%) expressed willingness to participate in cybersecurity training if it were accessible and easy to understand, and over one-third recognized the value of artificial intelligence in enhancing security capabilities.

This contrast between awareness and action underscores the urgent need for targeted digital education, user responsibility, and organizational investment in automated tools. The findings suggest that cybersecurity culture must be redefined as a shared responsibility, where users, institutions, and policymakers align efforts to foster a safer digital environment. The study contributes to a better understanding of the human factor in cybersecurity and outlines key directions for future training, policy, and technological adoption.

Keywords: Cybersecurity, User Awareness, Digital Behavior, Vulnerability Detection, Cyber Threats, Artificial Intelligence.

JEL Classification: D83, L86, O33.

INTRODUCTION

In recent years, the digitalization of everyday life has led to a growing dependence on technology, making cybersecurity not just a technical issue, but a societal necessity. Individuals, organizations, and governments face increasing risks related to data breaches, phishing attacks, identity theft, and other cyber threats. Consequently, the role of users as both potential targets and active participants in ensuring digital safety has become more relevant than ever.

Several studies (Anderson & Moore, 2007; ENISA, 2022) have emphasized that while users may have a general understanding of cybersecurity, their real-life practices often lag behind. This discrepancy between knowledge and behavior has sparked interest in exploring the human factor in cybersecurity – particularly in relation to awareness, preparedness, and willingness to adopt safe practices.

This paper seeks to address the following research questions:

- How aware are users of current cyber threats and vulnerabilities?

- What are their personal and organizational experiences with cyber incidents?
- What behaviors and security measures do they adopt in daily digital interactions?
- Are users open to cybersecurity education and innovation, such as AI-driven tools?

The theoretical framework is grounded in behavior-based cybersecurity models, which highlight how risk perception influences the adoption of protection strategies. The study is exploratory and descriptive, aiming to fill a gap in understanding the digital habits and attitudes of general users – not IT specialists.

The main objective of this research is to analyze the perceptions, knowledge, and realities of cybersecurity among users, based on the results of a structured questionnaire applied to a sample of 100 respondents. The paper contributes to the growing literature on user-centered cybersecurity by identifying gaps between awareness and practice, and by proposing concrete directions for future education, policy, and technological adaptation.

METHODOLOGY

This study employed a quantitative research approach based on the application of a structured questionnaire. The objective was to assess users' perceptions, knowledge, and behaviors related to cybersecurity, focusing on both individual and organizational contexts.

The questionnaire was distributed online and completed by a total of 100 respondents. The sample included participants from various professional backgrounds and age groups, with no prior requirement for technical expertise in cybersecurity. The anonymity of respondents was ensured to encourage honest and accurate responses.

The questionnaire was divided into five thematic sections:

1. **Awareness of Cyber Threats and Vulnerabilities** – aimed to evaluate the respondents' understanding of common cyber risks and threats such as phishing, data breaches, and financial fraud.
2. **Personal and Organizational Experiences** – explored whether respondents had been personally affected by cyber incidents and the extent to which their organizations implemented protective measures.
3. **Cybersecurity Behaviors and Practices** – investigated individual security habits, such as updating software, password management, and use of multi-factor authentication.
4. **Attitudes and Openness to Learning** – examined perceptions regarding responsibility, data protection awareness, and willingness to participate in educational initiatives.
5. **Expert Perspectives (Optional)** – provided respondents with the opportunity to share opinions on advanced topics such as artificial intelligence, organizational vulnerabilities, and proposed solutions.

The collected data were analyzed using descriptive statistical methods, with results presented as percentages to illustrate key trends and behaviors. No personal identifying information was collected. The approach enabled the identification of discrepancies between awareness and actual practice, as well as gaps in organizational preparedness and individual responsibility.

1. FINDINGS AND DISCUSSION

1.1 Awareness of Cyber Threats and Vulnerabilities

The results indicate that most users possess a theoretical understanding of cybersecurity threats. Specifically, **93% of respondents correctly defined a cyberattack** as an unauthorized attempt to access data or systems. This finding reflects a relatively high level of basic awareness regarding the nature of digital risks.

However, when analyzing practical exposure to threats, a more nuanced picture emerges. Nearly **47% of respondents reported having received at least one suspicious email or message** requesting personal information - indicating that phishing remains a common issue, despite general awareness of its existence.

In terms of perceived risks, respondents ranked **financial fraud** as the most significant threat (48%), followed by **system access disruption** (32%), and **loss of personal data** (14%). This prioritization highlights users' concern with direct, tangible consequences of cyber incidents, particularly those with potential financial impact.

These results suggest that while users may be familiar with cybersecurity terminology and concepts, their perception of threats is shaped primarily by personal relevance and perceived severity. It also reflects a reactive mindset, where awareness exists but is not always translated into preventive behavior.

Furthermore, the emphasis on financial fraud as the top concern points to a need for enhanced education on the broader scope of cybersecurity risks, including social engineering, ransomware, identity theft, and data manipulation – threats that can be equally damaging but may not be immediately visible to non-expert users.

1.2 Personal and Organizational Experience

The survey results reveal that cybersecurity incidents are not merely hypothetical for many users. 37% of respondents reported having been directly affected by cyberattacks, including data loss and unauthorized access to personal or work-related accounts. This figure underscores the tangible impact of digital threats and confirms that cyber incidents are a lived reality for a significant portion of the sample.

On the organizational side, the findings are equally concerning. Only 37% of respondents indicated that their organizations regularly use vulnerability detection tools. This suggests that even in professional environments, proactive measures for identifying and mitigating threats are not consistently implemented. The lack of systemic protection may further expose users to risks, especially in hybrid work environments where personal and professional digital spaces often overlap. Moreover, 70% of respondents identified the lack of financial resources and proper training as the main reasons for their organizations' vulnerability to cyber threats. This reflects a structural issue that extends beyond individual behavior, highlighting gaps in strategic investment and workforce development at the organizational level.

These results suggest a dual-layered challenge: on one hand, users face real consequences due to cyber incidents; on the other, the institutions meant to support and protect them may not be adequately prepared. The findings emphasize the need for targeted investment in both technological infrastructure (e.g., vulnerability scanners, monitoring systems) and human capital (e.g., training, awareness programs).

1.3 Cybersecurity Behaviors and Practices

Despite a relatively high level of awareness regarding cyber threats, the actual behaviors of users indicate a worrying lack of proactive security practices. The data reveal a significant gap between knowledge and action:

- Only 7% of respondents reported updating their applications immediately after a new update becomes available. This low percentage highlights a critical vulnerability, as outdated software is a common entry point for cyberattacks.
- 43% of respondents never use two-factor authentication (2FA), despite its growing availability and importance in securing accounts. This omission leaves accounts more susceptible to unauthorized access, especially in cases of password leaks.
- Password hygiene is also poor: 54% of respondents admitted they never change their passwords, while 35% do not check the source of applications or websites before accessing them. These findings indicate that many users engage in risky digital behaviors, either due to lack of awareness of best practices or underestimation of potential consequences.

The results suggest that users tend to adopt a minimal or even passive approach to digital protection. Security behaviors such as regular updates, password management, and source verification – though simple and effective – are not yet embedded in the daily routines of a majority of users.

This behavioral gap points to the need for simplified and accessible cybersecurity training that focuses on habit-building, not just knowledge transmission. Moreover, the low adoption rate of even basic practices reinforces the idea that usability and perceived convenience often override caution, especially in non-technical user populations.

1.4 Attitudes and Openness to Learning

Beyond behavior, users' attitudes toward cybersecurity and their willingness to engage in learning opportunities are critical indicators for long-term improvement. The survey results show a generally positive inclination toward acquiring cybersecurity knowledge – 58% of respondents stated they would participate in a data protection course if it were easy to understand. This openness represents a valuable opportunity for designing educational initiatives tailored to non-specialist audiences.

However, gaps in awareness of existing tools and responsibilities persist. For example, 52% of respondents reported not knowing what vulnerability detection tools, if any, are used within their organizations. This suggests not only a lack of transparency from organizational leadership but also limited communication between IT departments and regular users. Additionally, 59% of participants consider organizations to be primarily responsible for data protection, which may indicate a tendency to delegate responsibility rather than see cybersecurity as a shared duty.

While users recognize the importance of protecting personal and organizational data, there is still a need to strengthen their sense of agency and personal accountability. Bridging the gap between interest and action will require communication strategies that are clear, relatable, and context-specific. Moreover, the findings suggest that many users are not resistant to cybersecurity education – they simply need it to be accessible, relevant, and embedded in their digital routines. Institutions and policymakers should seize this opportunity to introduce tiered learning platforms, awareness campaigns, and gamified content that foster active engagement.

1.5 Perspectives on Emerging Solutions

As part of the optional section of the questionnaire, respondents were invited to share their views on the use of advanced technologies – particularly artificial intelligence (AI) – and to suggest improvements for cybersecurity practices within organizations. The responses provide valuable insight into users' openness to innovation and their perception of future-oriented solutions.

Notably, 37.6% of respondents believe that AI can contribute "very significantly" to the detection of vulnerabilities in digital systems. This reflects a growing trust in intelligent, automated tools as essential components of modern cybersecurity strategies. AI-powered solutions are increasingly being integrated into intrusion detection systems, threat analysis, and anomaly monitoring, offering scalability and speed that human teams alone cannot match.

However, the feedback also suggests a cautious optimism. While many users see the potential of AI, others expressed concerns about its complexity, cost, and implementation transparency. This highlights the importance of combining AI deployment with user education and clear communication, ensuring that such technologies are not perceived as "black box" solutions but as accessible tools that enhance – not replace – human decision-making.

Respondents also offered practical suggestions for improving cybersecurity, such as:

- Developing more interactive and personalized training programs.
- Increasing visibility of security protocols within organizations.
- Encouraging regular internal audits and simulations of attack scenarios.
- Establishing dedicated communication channels between IT departments and general staff.

These perspectives demonstrate that users are not passive actors - they are willing to engage and contribute, provided they are equipped with the right tools, knowledge, and support.

CONCLUSIONS AND RECOMMENDATIONS

This study set out to explore how users perceive cybersecurity, what they know, and how they behave in practice. The results reveal a clear disparity between theoretical understanding and real-world actions. While most respondents were able to identify key threats such as cyberattacks or financial fraud, their day-to-day security habits remain inconsistent and, in many cases, insufficient.

A significant portion of users (37%) have experienced cyber incidents firsthand, yet fundamental security practices such as software updates, two-factor authentication, and password management are not widely adopted. Organizational responsibility is acknowledged, but often not matched by transparent communication or adequate resource allocation. Despite these shortcomings, users show promising openness to learning, and many express trust in the potential of artificial intelligence to improve cybersecurity.

Based on the findings, several key recommendations emerge:

1. **Implement continuous digital education programs** tailored to different knowledge levels, using accessible language and interactive formats.
2. **Promote shared responsibility models** where users, organizations, and policymakers all play active roles in maintaining digital security.
3. **Encourage the adoption of good security habits** by integrating them into routine digital behaviors through gamification, nudges, or policy requirements.
4. **Strengthen organizational infrastructure** by investing in vulnerability detection tools, regular security audits, and transparent communication practices.

5. **Leverage AI responsibly**, ensuring that its implementation is accompanied by adequate user training and ethical oversight.

In conclusion, transforming cybersecurity culture requires more than tools and policies – it demands behavioral change, continuous education, and collaboration. The human factor remains both the weakest link and the greatest potential in digital security.

REFERENCES

1. Anderson, R. and Moore, T., 2007. The economics of information security. *Science*, 314(5799), pp.610–613.
2. ENISA, 2022. *Cybersecurity Culture Guidelines: Behavioural Aspects in Cybersecurity*. European Union Agency for Cybersecurity. Available at: https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity [Accessed 1 Jun. 2025].
3. Liang, H. and Xue, Y., 2010. Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, 11(7), pp.394–413.

THE PARTICULARITIES OF CYBER SECURITY RISK MANAGEMENT IN CRYPTOCURRENCY TRANSACTIONS

UDC: 005.334:[336.747.5:004.056.55]
DOI: https://doi.org/10.53486/tids2025.12

LUCHIAN IVAN
Moldova State University
ivan.luchian@usm.md
ORCID ID: 0000-0002-8683-7228

DONCEV TRAIAN
Most Organic
tdoncev@gmail.com

Abstract. Cryptocurrency is a digital asset based on blockchain technology, enabling decentralized and secure digital transactions. The acquisition, trading and investment in cryptocurrencies are based on the operation of a specialized infrastructure, which includes cryptocurrency exchanges, crypto banks, crypto friendly banks, crypto gateways, platforms and apps. The exponential growth in the number of cryptocurrencies and their integration into financial systems have led to an increased risk of cyber threats, including fraud, theft, and hacking. The article aims to explore the specific cybersecurity vulnerabilities associated with cryptocurrency transactions and reviews the contemporary risk management practices designed to mitigate them. The analysis is based on expert opinions, industry reports, and academic studies. Particular attention is given to the architecture of cyber-attacks and scams in the crypto domain. The research revealed a wide variety of cyber threats to cryptocurrency transactions, which are essentially cyber-attacks and various scam schemes. The objects of criminal activity are the elements of the cryptocurrency market infrastructure and cryptocurrency holdings in digital wallets. All procedures undertaken for to secure cryptocurrency transactions aimed at ensuring protection against fraudulent activities and maintaining the security of digital currency ownership meets the notion of cryptocurrency security. In international practice, complexes of techniques have been developed aimed at ensuring the cyber security of cryptocurrency transactions. The paper examined layered defense strategies that incorporate cryptographic protocols, regulatory frameworks, and artificial intelligence tools. The study emphasizes that effective cybersecurity in cryptocurrency transactions requires a combination of technological, organizational, and legal measures. The findings contribute to a deeper understanding of risk exposure and the practical steps necessary to secure digital assets in an evolving threat landscape.

Keywords: cryptocurrency; crypto security; threats; cybercrime; risk management.

JEL Classification: B17, F31, L86.

INTRODUCTION

A cryptocurrency is a digital or virtual currency created by applying encryption algorithms. The use of encryption technologies means that cryptocurrencies function as both a currency and a virtual accounting system. Encryption means the use of algorithms and techniques that protect these inputs, such as elliptic curve encryption, public-private key pairs, and hashing functions. Cryptocurrency is based on a distributed network across a large number of computers, which allows it to operate outside the control of governments and central authorities. The basis of cryptocurrency operation is blockchain technology, which is used to make secure digital payments using tokens. Storage and transmission of cryptocurrency data between wallets and to public ledgers (Inhope, 2022), (Oswego), (The Investopedia Team, 2024).

According to the information presented by Fabio Duarte (2025), the global number of cryptocurrencies has increased from 50 in the year 2013 to 17134 in April 2025.

Powered by CoinGecko (2025), in the period 01.01.2014-12.05.2025 the level of capitalization of the global cryptocurrency market increased through fluctuations from $10.6 billion to $3450.7 billion.

According to Triple A (2024) in 2024 an estimated 562 million people worldwide (up 34% from 420 million in 2023) owned cryptocurrencies. And for the 2025, the number of people who will use cryptocurrencies was estimated at 861.0 million, which constitutes 11.0% of the world population (Kumar, 2025).

The purpose of this article is to examine the essence of cyber risks of cryptocurrency transactions and their management technologies

MAIN CONTENT

1. Materials and Methods

Cryptocurrencies themselves and the market formed by them remain a relatively little studied field, with advertising information about the attractiveness of investing in them and their use as a payment instrument prevailing in the internet space. At the same time, potential investors remain relatively poorly informed about the associated risks. The research on the topic was based on screening information provided by specialized companies, expert opinions, and academic papers available on the internet. The study examined the essence of cryptocurrencies and provided expert advice on the risks of cryptocurrency transactions, as well as technologies for managing the cybersecurity of these activities. As a result, a summary presentation was developed on the essence of cyber risks of cryptocurrency transactions, followed by a complex vision of their management.

2. Results and Discussion

The complex of activities carried out to secure cryptocurrency transactions against criminal activities and to maintain the security of digital currency are collectively known as cryptocurrency security (Arkose Labs).

In this setting, specialists from Darktrace expressed that cybersecurity for cryptocurrency (crypto cybersecurity) is a fundamental thought within the quickly advancing world of digital assets. As more people and businesses grasp cryptocurrencies, the move to digitizing assets presents important vulnerabilities that require security measures. Moreover, as cryptocurrency develops in ubiquity, these digital assets are progressively uncovered to threat actors.

Additionally, cryptocurrency transactions are digital in nature and involve a sophisticated backend process, according to the experts at Arkose Labs. Blockchain, which is basically a distributed database or ledger that is shared among several computer network nodes, is the technology that powers cryptocurrency security. Blockchain uses cybersecurity frameworks and best practices to offer comprehensive risk management against cyber threats. Information and communication are protected by cryptography, which employs codes to make sure that only those with permission may access them.

Cybercrime in the cryptocurrency market refers to criminal activities related to the theft (or otherwise illegal acquisition) of cryptocurrencies and some methods or security vulnerabilities exploited.

In 2021, 0.15% of known cryptocurrency transactions were linked to illicit activities such as cybercrime, money laundering, and terrorist financing, with a total volume of $14 billion (Mengqi Sun, David Smagalla, 2022).

The Immunefi Crypto Losses 2022 Report cites losses from fraud and hacking as a combined total of $3.9 billion for the year and $8 billion for 2021 (Melinek, 2023).

In 2023, the FBI reported on cryptocurrency fraud that cost American investors $4.8 billion (Yaffe-Bellany, 2025).

Two types of cybercrimes are committed in the cryptocurrency market: cyber-attacks and scams.

A cyber-attack is any criminal activity with the intent to steal, expose, modify, disable, or destroy data, applications, or other information assets through unauthorized access to a network, computer system, or digital device (IBM, 2025).

In this field, the main form of illegal activity is hacking aimed at gaining unauthorized access to a computer system or network.

Examples include attacks on cryptocurrency exchanges and digital wallets (Malmqvist, Maartmann-Moe, 2025):

- *Exchange hacking*. Cryptocurrency exchanges are basically digital platforms where individuals can buy, sell, or keep their coins. Because these exchanges often maintain significant amounts of cryptocurrencies, they are attractive targets for cybercriminals. Hackers employ different attack methods, including phishing and social engineering, to take coins that are stored in active wallets on the exchange.
- *Bridge attack*. A bridge attack is a type of cyberattack on cryptocurrency trading services, whereby cybercriminals focus on cryptocurrency while it is being transferred between different blockchains.
- *Wallet hacking*. Digital wallets are designed to hold, oversee, and exchange cryptocurrencies. Cybercriminals can take advantage of software or network vulnerabilities to break into a user's device, gain access to the crypto wallet, and steal the currency stored in it.
- *Phishing attack*. Users are deceived into disclosing their private keys. If an individual loses access to the private key associated with a wallet, the assets become irretrievably lost. A prevalent form of digital attack is executed by criminals who send emails, thereby misleading users into divulging sensitive information or downloading malware, which can enable the hacker to gain access to the crypto wallet and misappropriate their assets.
- *Malware*, or malicious software, is any program or file that's intentionally harmful to a computer, network or server (Kinza Yasar, Ben Lutkevich, 2024). Due to their code-based nature, cryptocurrencies and associated software may have flaws that hackers might take advantage of. Any vulnerability in the crypto architecture allows them to alter the code. For instance, they are able to conduct bridge attacks and hack bitcoin exchanges.
- *Theft of crypto keys.* Users must utilize keys to access their cryptocurrency wallets and exchanges, and if hackers are able to obtain these keys or the passwords that secure them, they can launch attacks on cryptocurrencies.

- *DDoS attacks on cryptocurrency exchanges*. A Distributed Denial-of-Service (DDoS) attack aims to disrupt the operation of a target system by overwhelming it with a massive stream of Internet traffic. When it comes to blockchain networks, DDoS attacks take a unique form due to the decentralized nature of the technology and lead to several negative effects for cryptocurrency users. One of them is the delay in transactions. As spam transactions clog the network, legitimate transactions can experience processing delays or even get stuck in queues waiting for confirmation. The situation can be especially serious for users who need timely completion of transactions for trading or other financial activities. During periods of high congestion caused by DDoS attacks, transaction fees can increase sharply as users compete for limited processing capacity (Trust, 2025).

A cryptocurrency scam is a complex of fraudulent activities aimed at deceiving a person or organization into dispossessing them of their digital assets. It can take many forms and is often based on emotions such as fear or greed (Allie Grace Garnett, 2025).

The most common types of cryptocurrency scams are considered to be the following (Allie Grace Garnett, 2025):

- *Cryptojacking* is the act of using a computer to mine cryptocurrencies, often through websites, against the user's will or while the user is unaware (Caprolu et al., 2021). Cryptojacking can lead to slowdowns and crashes due to the demand on computing resources. Proof-of-work mining for cryptocurrencies such as Bitcoin requires significant computing power and resources. Cryptojackers reap all the benefits of mining cryptocurrencies at no cost, while the device owner consumes electricity and the device malfunctions. Visiting an infected website or downloading compromised software can allow malicious code from a cryptojacker to enter the digital device.
- *Fake ICOs*. Although it lacks the infrastructure and technology necessary to support it, a fake initial coin offering (ICO) has all the characteristics of a real one. In essence, it is the launch of a coin that exists in name only. A fake ICO usually ends with the developers disappearing once the ICO proceeds are collected.
- *Sensitive information theft*. Hackers often target private keys, which are important for accessing digital wallets. Once these keys are compromised, the hacker gains full control over the victim's assets, leading to their loss.
- *Crypto mining*. Crypto mining involves using certain computing resources to validate transactions and secure the blockchain network. Cybercriminals sometimes deploy mining malware, which covertly uses the victim's computer power to mine cryptocurrencies for the attacker. This not only slows down the victim's device, but also increases their electricity costs.
- *Cloud mining scams*. Cloud mining services, often referred to as mining-as-a-service, represent a legitimate business model; however, certain cloud mining companies engage in fraudulent activities. A company might assert that it provides cloud mining services, frequently guaranteeing appealing returns in return for an initial payment. The anticipated returns may never be realized, as the company may not possess the mining equipment.
- *Social engineering schemes* are designed to manipulate individuals into revealing confidential information. Scammers often pose as trustworthy individuals or offer investment opportunities that seem too good to be true.
- *Insider threats* come from individuals within an organization (companies, institutions) who have access to sensitive information and who can abuse their positions to steal digital currency or sabotage security measures.

- *Fake wallets*. A fraudulent (fake) wallet scheme deceives individuals into thinking they are utilizing a genuine digital wallet for asset storage. This counterfeit wallet prompts users to input their private keys, which the scammers subsequently exploit to misappropriate cryptocurrency assets. Fake wallet apps can be found in app stores or promoted through phishing emails.
- *Pump-and-dump schemes*. Scammers use a variety of strategies to artificially raise (or pump) the price of a digital asset in this cybercrime. The scammer sells his tokens on the open market right away when the price is inflated. The rapid increase in the supply of tokens causes their price to plummet, but not before the scammer has made a profit. By making false or misleading claims and purchasing huge amounts of a low-value token all at once, scammers can artificially boost its price.
- *Blockchain-wide attacks***.** Scammers can target entire cryptocurrency networks, and techniques may include the following:

  – *51% attacks*, which involve a single entity obtaining control over more than half of the mining power of a blockchain or cryptocurrency;

  – *Sybil attacks*, or the creation by a single entity of multiple false identities (nodes) to criminally influence network operations;

  – *Routing attacks* involve the participation of a malicious actor that manipulates data routing information to illicitly intercept, alter, or block communication among blockchain nodes;

  – *Time jacking attacks* occur when a malicious actor modifies the timestamps of a network's nodes, creating confusion and enabling the attacker to double-spend cryptocurrencies;

  – *Eclipse attacks* are carried out by hoodlums segregating one or more blockchain hubs with the point of giving wrong data to the isolated node;

  – *Long-range attack* are a hypothetical shape of assault that includes hoodlums making a modern fork of a blockchain from a far-off point within the past, making false exchanges show up genuine;

  – *Selfish mining attacks* happen when mineworkers effectively prepare a modern square but don't transmit this data to the arrange, furtively mining another piece. Such attacks have not however been recognized, but is hypothetically conceivable.

To uncover criminal activities in the cryptocurrency market, experts recommend using the ten red flags system (Merkle Science, 2025):

1. *Smurfing* involves splitting large transactions into smaller transactions to avoid compliance alerts;

2. *Peel chains*. To distribute stolen money, criminals frequently practice transferring money between several wallets. This idea is carried out by a peel chain, which transfers progressively smaller sums to more wallets;

3. *Rapid movement of funds*. Predictable patterns, like keeping a current balance or holding coins for a long time, are indicative of legitimate wallet activity. Within minutes of receiving the money, a criminal wallet can be completely depleted, indicating a brief halt end route to its ultimate destination;

4. *Incongruous trading volume*. Users are required to reveal their sources of pay and assessed exchange sums as portion of the Know Your Client (KYC) handle. A major red flag is when exchange volume distant surpasses these declarations;

5. *Involvement with high-risk jurisdictions*. Blacklisted nations are often regarded as high-risk. Additionally, there is a grey list of countries that are being enhanced monitored for strategic flaws in their counterterrorism finance and anti-money laundering regulations;

6. *Association with dark net marketplaces*. By buying products and reselling them for clean fiat money, criminals can use dark net markets to launder cryptocurrency. They also facilitate and enable the illicit trade of commodities and services. Sometimes, these products might end up in the hands of terrorist or criminal groups;

7. *Use of coin mixers or tumblers*. Coin mixers, sometimes referred to as tumblers, combine money from several users, severing the connections between transactions. When a user deposits cryptocurrencies into a mixer, for instance, they receive an equivalent amount from other funds that have been pooled;

8. *Sending funds to clustered wallets*. Multiple crypto addresses can be created by an individual. Clustering algorithms are used in blockchain analytics to find wallets that are probably under the control of the same person. Transferring money to many wallets may be a sign of wash trading, which is used to conceal illegal transactions or increase currency trade volumes;

9. *Chain hopping*

10. *Use of privacy coins*. Privacy coins prioritize user anonymity. Criminals can use them to hide their transactions from regulatory scrutiny.

International cyber practice has developed a set of recommended measures for managing risks related to cryptocurrency transactions (Arkose Labs):

- *Risk assessment*. It is essential to carry out a thorough risk evaluation to pinpoint possible weaknesses, dangers, and risks related to cryptocurrency operations, in addition to prioritizing efforts for mitigation;
- *Private key protection*. Cryptocurrency transactions involve the use of cryptographic keys, particularly private keys, to access and control ownership of these digital assets. It is essential to safeguard private keys through methods like encryption, secure storage solutions, and hardware wallets;
- *Wallet security*. It is necessary to use strong passwords, multi-factor authentication, and regular updates of wallet software to improve wallet security;
- *Two factor authentication*. It is advised to enable two-factor authentication (2FA) to add an extra level of protection to cryptocurrency accounts;
- *Secure transactions*. It is necessary to use extra security features like transaction signing and encryption to confirm the recipient's wallet address;
- *Network security*. Network monitoring and cryptographic algorithms are necessary to defend blockchain infrastructure against bot-generated attacks like DDoS attacks. Strong encryption, virtual private networks, firewalls, intrusion detection and prevention systems, and frequent network device application and updates are also necessary;
- *The security of cryptocurrency exchanges* encompasses strategies to safeguard user accounts and ensure secure storage of assets, two-factor authentication, anti-money laundering and know-your-customer procedures, regular security audits, and compliance with regulatory standards. Additional security features like IP restrictions or withdrawal whitelists must be enabled, and careful consideration must be given when choosing trading partners;

- *Data encryption*. It is imperative to implement encryption measures for sensitive data, both during transmission and while stored, employing a variety of encryption methodologies available to safeguard information against unauthorized access or interception;
- *Smart contract and token security*. The adoption of secure coding methodologies is imperative, and comprehensive testing protocols must be executed prior to deployment;
- *Strong password practices*. Strong password creation advice is required, as are suggestions for using password managers to safely store and handle login information;
- *Access control and user privileges*. Strict user privileges and access controls are advised in order to limit access to sensitive information and systems;
- *Software and firmware updates*. Periodically updating hardware wallet firmware, software clients, and cryptocurrency wallets is necessary since these processes may include security fixes and enhancements for better defense against known threats;
- *Backup and recovery*. Regularly backing up bitcoin wallets and keeping backups safe are essential;
- *Continuous monitoring*. Cryptocurrency security networks and systems must be continuously monitored in order to identify and address any suspicious activity or any security breaches. This will involve the use of monitoring tools, security information and event management systems, intrusion detection systems, and threat intelligence feeds to detect and mitigate security incidents;
- *Incident response and recovery*. Developing an incident response plan, which contains procedures for reporting and analyzing incidents, limiting and mitigating damage, recovering lost funds, and strengthening the security system in order to avoid incidents in the future;
- *User education and awareness*. This is a comprehensive attempt to inform cryptocurrency users about common attack vectors, security best practices, and potential hazards, including social engineering and phishing attempts, as well as the significance of upholding personal security hygiene, which includes creating strong passwords, updating software frequently, and refraining from disclosing sensitive information;
- *Partnering with a security vendor*. After evaluating the security system in terms of data management, access controls and incident response capabilities, it is necessary to select a reliable security provider;
- *Security audits and assessments.* The periodic conduct of audits and assessments is required by the need to assess the efficiency of the security system and detect any vulnerabilities.

Government regulations are of paramount importance in improving the security of cryptocurrency transactions. The Financial Action Task Force's recommendations require cryptocurrency exchanges to implement know-your-customer and anti-money laundering policies to prevent illicit activities. In the United States, the Securities and Exchange Commission enforces compliance regulations for Initial Coin Offerings and other financial activities related to cryptocurrencies (Anifowose et. al., 2022). The Markets in Crypto-Assets Regulation establishes legal rules across the European Union for the issuance and trading of crypto-assets, including transparency, disclosure, authorization and supervision of transactions and the activities of crypto-asset service providers (Abramova, Andreeva, 2025).

In all of these regulatory measures, challenges persist in enforcing global compliance due to the decentralized nature of cryptocurrencies. Regulatory arbitrage, where entities operate in jurisdictions with lax regulations, undermines the effectiveness of security measures. International collaboration between regulatory agencies is needed to address this issue (Anifowose et. al., 2022).

The emphasis on privacy and anonymity in the cryptocurrency market makes it difficult to identify criminals. However, there are certain tools that law enforcement agencies operate to identify criminal users. They work closely with cryptocurrency companies to track transactions on the blockchain and conduct on-chain investigations. Given that the technology is developing at a rapid pace, collaboration between law enforcement and the crypto financial market is vital to ensure that government institutions are informed about the latest technologies (Inhope, 2022).

Artificial intelligence (AI) has become a tool for detecting and preventing cyber threats in cryptocurrency transactions. AI-based fraud detection systems examine transaction behaviors and identify suspicious activity in real time. Machine learning models are trained on historical fraud data to increase detection accuracy. For example, AI algorithms can flag transactions related to money laundering, such as rapid movement between multiple wallets. These solutions provide an additional layer of security, supplementing cybersecurity measures. At the same time, AI-based systems also face challenges, including adversarial attacks in which hackers manipulate AI models to avoid detection (Anifowose et. al., 2022).

An important aspect of ensuring the security of cryptocurrency companies and platforms is conducting audits, which include code reviews, penetration tests, and risk assessments to detect potential vulnerabilities before fraudsters take advantage of them. A crypto audit also provides a comprehensive review of a company's operations, systems, and processes to ensure compliance with external and internal security standards (Malmqvist, Maartmann-Moe, 2025).

CONCLUSIONS

The dynamic expansion of the cryptocurrency market has made it a prime target for increasingly sophisticated cyberattacks. Although blockchain technology provides inherent security features such as decentralization and cryptographic validation, these alone are insufficient to ensure comprehensive protection. Cyber threats-including hacking, phishing, insider threats, and advanced scam schemes-highlight the urgent need for robust cybersecurity strategies.

This study has shown that an effective defense against cryptocurrency-related cyber risks must include a multi-layered approach that combines: technical safeguards (e.g., key encryption, secure wallets, AI-based monitoring); regulatory compliance (e.g., KYC/AML frameworks, international standards); and user education to build awareness of potential vulnerabilities.

The role of artificial intelligence in real-time fraud detection is growing, though it must be supplemented by continuous audits and adaptive risk management practices. Furthermore, international cooperation among regulators, cybersecurity firms, and crypto platforms is essential to close jurisdictional gaps and ensure effective enforcement.

Future research should explore quantum-resistant cryptographic protocols and the integration of decentralized AI in securing blockchain infrastructures. Only through a holistic and proactive approach can the long-term security and trustworthiness of cryptocurrency ecosystems be maintained.

REFERENCES

1. Abramova Alisa, Andreeva Julia, 2025. *EU Crypto Regulations 2025*. Available at: https://sumsub.com/blog/eu-crypto-regulations/. [Accessed 14.05.2025]

2. Anifowose Victor, Mei Song, Nicole Reed (2022) *Cybersecurity Frameworks for Crypto Transactions*. Available at: https://www.researchgate.net/publication/389079078_Cybersecurity_Frameworks_for_Crypto_Transactions. [Accessed 28.04.2025]
3. Arkose Labs. *Guide to cryptocurrency security*. Available at: https://www.arkoselabs.com/explained/guide-to-cryptocurrency-security/. [Accessed 28.04.2025]
4. Caprolu Maurantonio, Raponi Simone, Oligeri Gabriele, Di Pietro Roberto, 2021. *Cryptomining makes noise: Detecting cryptojacking via Machine Learning*. Available at: https://www.sciencedirect.com/science/article/pii/S0140366421000797?via%3Dihub. [Accessed 10.05.2025]
5. CoinGecko, 2025. Available at: https://www.coingecko.com/en/global-charts#:~:text=The%20global%20cryptocurrency%20market%20cap,a%20Bitcoin%20dominance%20of%2061.03%25. [Accessed 12.05.2025]
6. Darktrace. *What is crypto cyberseucity?*. https://www.darktrace.com/cyber-ai-glossary/crypto-cybersecurity#:~:text=Cybersecurity%20for%20Crypto%20is%20an,vulnerabilities%20that%20require%20security%20measures. [Accessed 07.05.2025]
7. Duarte Fabio, 2025. How Many Cryptocurrencies are There In 2025?. Available at: https://explodingtopics.com/blog/number-of-cryptocurrencies. [Accessed 07.05.2025]
8. Garnett Allie Grace, 2025. *Cryptocurrency scams: 8 crypto cons to avoid*. Available at: https://www.britannica.com/money/cryptocurrency-scams. [Accessed 01.06.2025]
9. IBM, 2025. *What is a cyberattack?*. Available at: https://www.ibm.com/think/topics/cyber-attack. [Accessed 06.05.2025]
10. Inhope, 2022. *What is Cryptocurrency?*. Available at: https://www.inhope.org/EN/articles/what-is-crypto. [Accessed 08.05.2025]
11. Kumar Naveen, 2025. How Many Cryptocurrencies Are There in 2025?. Available at: https://www.demandsage.com/number-of-cryptocurrencies/#:~:text=The%20Future%20Of%20Cryptocurrencies&text=The%20number%20of%20cryptocurrency%20users,by%20the%20end%20of%202025. [Accessed 12.05.2025]
12. Malmqvist Ritva, Maartmann-Moe Carsten, 2025. *Summary of Cryptocurrency and Blockchain Risks, Protections, and the Importance of Audits*. Available at: https://advisense.com/2025/03/13/cryptocurrency-and-blockchain-risks/. [Accessed 07.05.2025]
13. Melinek Jacquelyn, 2023. *Crypto losses in 2022 dropped 51% year on year to $4B*. Available at: https://techcrunch.com/2023/01/05/crypto-losses-in-2022-dropped-51-year-on-year-to-4b/. [Accessed 07.05.2025]
14. Merkle Science, 2025. *Top 10 Red Flags to Watch for in Crypto Transactions*. Available at: https://www.merklescience.com/blog/top-10-red-flags-to-watch-for-in-crypto-transactions. [Accessed 19.05.2025]
15. Oswego. *The Basics about Cryptocurrency*. Available at: https://www.oswego.edu/cts/basics-about-cryptocurrency. [Accessed 07.05.2025]
16. Sun Mengqi Smagalla David, 2022. *Cryptocurrency-Based Crime Hit a Record $14 Billion in 2021*. Available at: https://www.wsj.com/articles/cryptocurrency-based-crime-hit-a-record-14-billion-in-2021-11641500073. [Accessed 07.05.2025]
17. The Investopedia Team, 2024. *Cryptocurrency Explained With Pros and Cons for Investment*. Available at: https://www.investopedia.com/terms/c/cryptocurrency.asp. [Accessed 08.05.2025]
18. Triple A, 2024. *Global Crypto Ownership Reaches 562 Million People in 2024: New Report*. Available at: https://www.triple-a.io/blog/crypto-ownership-report. [Accessed 19.05.2025]

19. Trust, 2025. *DDoS attacks in blockchain networks, explained*. Available at: https://trustwallet.com/blog/security/ddos-attacks-in-blockchain-networks-explained. [Accessed 19.05.2025]
20. Yaffe-Bellany David, 2025. *The Cryptocurrency Scam That Turned a Small Town Against Itself*. Available at: https://www.nytimes.com/2025/02/19/magazine/cryptocurrency-scam-kansas-heartland-bank.html. [Accessed 06.05.2025]
21. Yasar Kinza, Lutkevich Ben, 2024. *What is malware? Prevention, detection and how attacks work*. Available at: https://www.techtarget.com/searchsecurity/definition/malware. [Accessed 06.05.2025]

THE ROLE OF CROWDFUNDING IN STIMULATING INNOVATION AND ECONOMIC GROWTH IN MOLDOVA

UDC: [004.738.5:330.322.12]:[658.14+330.341.1](478)
DOI: https://doi.org/10.53486/tids2025.13

DOROGAIA IRINA
Academy of Economic Studies of Moldova
Chisinau, Republic of Moldova
dorogaia.irina.ion@ase.md
ORCID ID: 0000-0003-4625-8616

SCUTARI ALEXANDR
BALKANIKA SRL
Chisinau, Republic of Moldova
alscut@gmail.com
ORCID ID: 0009-0005-7979-605X

Abstract. Modern economic transformations increasingly necessitate the adaptation of funding mechanisms through digital integration. In the Republic of Moldova, the emergence of the crowd economy introduces alternative opportunities for mobilizing capital, particularly in support of innovation-driven initiatives. This article examines crowdfunding as a non-traditional tool for financing, outlining its key actors, operating models, and sectoral applications. Drawing on best practices from the European Union and recent data provided by ESMA, the study identifies pressing regulatory and infrastructural challenges. Based on the analysis, the article proposes recommendations for strengthening Moldova's legal and institutional framework to better support the growth of digital investment platforms. The *aim of the study* is to explore the possibilities of using innovative financing methods, such as crowdfunding, to create and promote innovative activities of enterprises. To this end, the following *objectives* have been formulated: to study the characteristics of crowdfunding, to conduct a cross-country analysis of the implementation of crowdfunding, and to develop recommendations for the use of crowdfunding in innovative activities. The study used *methods* of analysis of theoretical aspects, global statistics, synthesis of information, and generalization of the data obtained.

Keywords: innovation, financing, crowd economy, crowdfunding, investment platform, small and medium-sized enterprises.

JEL Classification: O31, G23, M13

INTRODUCTION

In a market-driven economy, attracting investment is a critical component of sustainable growth, particularly for small and medium-sized enterprises (SMEs) that serve as the backbone of economic resilience. In the Republic of Moldova, however, the regulatory environment for crowdfunding as a financing mechanism remains underdeveloped and insufficiently structured. Advancing the technological and operational capabilities of SMEs requires active support for innovation, with digital crowdfunding platforms emerging as one of the most accessible and flexible instruments for mobilizing capital.

To effectively implement innovation-driven initiatives, crowdfunding must evolve into a well-established investment tool, grounded in voluntary participation and transparent reward mechanisms. This development calls for a clear understanding of the methodological foundations and research approaches necessary for shaping the institutional framework and governance of crowdfunding—particularly in relation to state oversight and legal regulation.

Interest in digital collective investment platforms has increased significantly since the enforcement of Law No. 181/2023 "On Collective Financing Services" in March 2024. The legislation outlines the principal actors involved in the ecosystem: platform operators, investors, project initiators, and third-party service providers. Nevertheless, critical financial and legal challenges remain unresolved, including low levels of public and corporate trust in new financial instruments, and the lack of analytical expertise needed to adequately assess and compare project proposals *Law No. 181/2023 (2023).*

At the same time, the rapid evolution of digital technologies is introducing a new generation of investment instruments and assets. This shift necessitates the urgent development of coherent methodological and regulatory frameworks to ensure the safe, effective operation of digital finance tools.

This article aims to explore the feasibility and relevance of integrating modern digital financing models—particularly crowdfunding—into the national innovation and economic development strategy of the Republic of Moldova.

MAIN CONTENT

1. Materials and Methods

The study used quantitative and qualitative methods. Qualitative methods included an analysis of literature on the subject, as well as legislative acts of the Republic of Moldova to establish the characteristics of the legal framework and create conditions for the functioning of crowdfunding platforms with the aim of developing innovative projects. At the same time, an analysis of quantitative values related to global trends in these processes was conducted.

2. Results and Discussion

2.1. Crowdfunding Platform as a Digital Investment Ecosystem

The ecosystem approach views a crowdfunding platform as a structured environment that facilitates interaction among participants in the allocation of financial resources and execution of investment agreements (Lafuente, *et al.,* 2021). Its primary objective is to ensure sustainability through mechanisms of self-organization.

A digital ecosystem is defined as a scalable system composed of interconnected digital elements, driven by collaboration and innovation (Ghjg Elia, *et.al*, 2020). A digital platform (DP) leverages technology to connect participants, offering services via the internet, including financial tools and advisory support. These platforms accelerate the launch of startups. Key ecosystem actors include borrowers, investors, regulatory authorities, banks, technology developers, and support institutions (Tretiacova, *et.,al*, 2022).

Ecosystem Participants

- Borrowers (Founders): Enterprises seeking funding.
- Investors (Backers): Individuals backing projects.
- Regulators (NCFM, NBM): Authorities overseeing operators.

- DP Operator: Manages operations, mitigates risks, and provides risk-reduction strategies and auto-investment options.
- Banks and Organizations: Offer support services.

The operator handles marketing activities, publishes project offers, and calculates return forecasts based on risk factors. Borrowers undergo a due diligence process, and their offers are promoted using a marketing mix framework (7P theory) (Korsun, 2022).

Investors independently select projects and reduce risk exposure through diversification. Funds are pooled in an escrow account and are released only upon successful closure of the funding round. Profits are distributed to investors in the form of interest payments or dividends.

Given the current regional climate and Moldova's strategic direction toward implementing European Union directives, the promotion of innovation remains a key priority of national economic policy. To date, Moldova’s system of public support includes targeted programs, research grants, special economic zones, and SME support funds. A comparative assessment of these mechanisms and their counterparts in international practice is presented in Table 1.

Table 1. Methods of Financing Innovative Projects on International Capital Markets

Financing Method	Brief Description	Key Features
IPO (Initial Public Offering)	Initial public offering of company shares on a stock exchange	High disclosure requirements, regulatory compliance; demands extensive preparation
SPO (Secondary Public Offering)	Issuance of additional shares by a public company	Used for business expansion, M&A financing, or debt refinancing
Corporate Bonds	Raising funds through debt securities issuance	Debt financing tool, often applied in medium- to long-term projects
Venture Capital	Investments in innovative firms for equity stakes	Targets high-growth startups; high risk, high reward
Crowdfunding	Capital raised from numerous investors via digital platforms	Effective for early stages; available in equity, debt, or hybrid formats

Source: *compiled by the authors based on research*

In international practice, the most widely used methods for financing innovation activities are presented in Table 2.

Table 2. Comparative Analysis of Innovation Support: Moldova vs. International Practice

Criterion	Moldova	International Practice
Government Programs	National targeted programs, research grants, industrial park creation	Programs like SBIR (USA), direct state investments, tax incentives, tech accelerators
Project Selection Criteria	Regional priorities, significance of scientific and applied research	Commercial viability, export potential, alignment with global challenges and ESG principles

Funding Conditions	Co-financing, phased approach, strict reporting, deadlines	Flexible terms, MVP/prototype support, acceleration programs, tailored funding paths
Expected Economic Impact	Local employment, regional value added, research infrastructure growth	Global scalability, tech startup growth, contribution to global innovation chains

Source: *compiled by the authors based on research*

Crowdfunding is a form of alternative finance that typically involves small contributions from a large number of individuals — commonly referred to as the "crowd" — via digital platforms.

These platforms serve as intermediaries that connect potential investors or lenders with businesses seeking capital, most often startups and small or medium-sized enterprises (SMEs). Unlike traditional banking systems, crowdfunding enables direct interaction between funders and recipients, bypassing financial intermediaries. Funding may take the form of loans or transferable debt and equity instruments. Crowdfunding plays a particularly critical role for businesses operating in smaller or emerging markets, where access to capital is often limited (*World Investment Report (2022).*

2.2. The Role of Crowdfunding in Innovation Activities

As previously noted, in a competitive market environment, small and medium-sized enterprises (SMEs) require access to alternative sources of funding to successfully implement their projects and strengthen their positions both domestically and internationally. However, in the Republic of Moldova, the volume of investment has been declining, which necessitates new approaches to capital mobilization. Crowdfunding, as a financing tool, enables external investment into projects at early development stages, bypassing traditional financial intermediaries.

A critical enabler of crowdfunding success is the digitalization of society, as supported by Moldova's National Digital Transformation Strategy for 2025–2027, approved in May 2025. This strategic plan focuses on fostering a digital society, expanding the ICT sector, and boosting the growth of the digital economy (*Logos Press* (2025).

By the end of 2027, the implementation of this programme is expected to accelerate national economic development. The export share of ICT services is projected to grow to 14%, up from 10% two years prior. Annual public investment in the IT sector will amount to MDL 2.7 billion. Entrepreneurs will access 85% of public services online, and 45% of the population will be actively using digital identification [7].

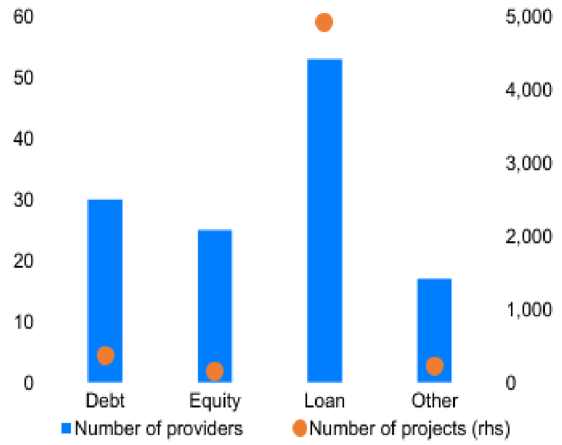
Digital platforms unlock new opportunities for financing startups, social initiatives, and charitable projects due to their high return potential and streamlined processes. Crowdfunding represents a collaborative model of resource mobilization through digital platforms in support of business ideas or social causes. Beyond funding, these platforms offer cost-effective promotional tools for public engagement and marketing outreach.

Among the most widely used global crowdfunding platforms are:

1. Kickstarter – A leader in fundraising for creative projects, including music, film, and environmental initiatives.
2. Indiegogo – Supports a wide variety of initiatives, from tech innovations to social impact projects.
3. Republic – A digital investment platform that has raised over $800 million from 1.5 million investors across 100 countries for startups, arts, and real estate initiatives (*Republic* (2025).

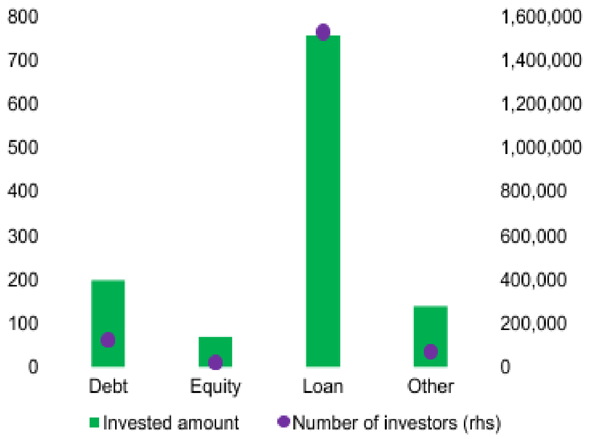
In Moldova, loan-based crowdfunding is the most prevalent model, involving repayment of funds with interest. By early 2025, the total amount of capital raised through crowdfunding had reached approximately EUR 9 million (*Fagura* (2025).

Since 2024, Moldova's crowdfunding market has been in a formative phase, demonstrating steady progress in terms of the few of active platforms, transaction volume, and user base expansion. The positive momentum aligns with EU best practices and is supported by statistical data provided by ESMA (2025). According to ESMA, total crowdfunding investment volumes in the EU exceeded EUR 1 billion in 2023. Loan-based crowdfunding accounted for the majority (65%) of this funding, followed by debt-based models (17%) and equity crowdfunding (6%) (ESMA (2025). (Figure 1, 2)



Note: Number of EU crowdfunding service providers and number of projects (rhs), by type of funding, 2023. "Other" includes admitted instruments for crowdfunding purposes. Data from 17 NCAs, as detailed in the appendix.
Sources: Data reported by NCAs, ESMA

Figure 1: Providers by funding type: Most projects are loan-based
Source: *ESMA*



Note: Invested amount, in EUR mn, and number of investors (rhs), by type of funding, 2023, "Other" includes admitted instruments for crowdfunding purposes. Data from 17 NCAs, as detailed in the appendix.
Sources: Data reported by NCAs, ESMA.

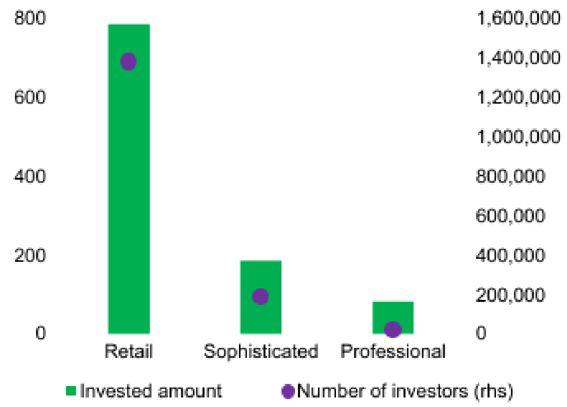
Figure 2: Investing by funding type Large majority of fundings is loan-based
Source: *ESMA*

Interestingly, the average amount raised per loan-based project was approximately EUR 15,000 — significantly lower than the average for debt-based models (EUR 53,000) and equity-based models (EUR 46,000).

The majority of crowdfunding participants (87%) were classified as retail investors. An additional 12% were identified as sophisticated investors, while only 1% qualified as professional market participants. According to ESMA data, the average investment per individual was as follows:

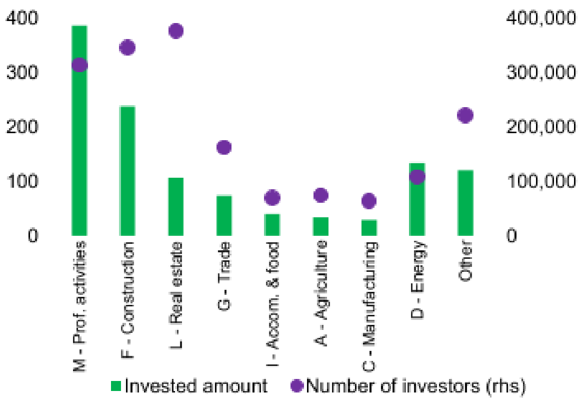
- Retail investors: ~EUR 590
- Sophisticated investors: ~EUR 990
- Professional investors: ~EUR 4,200.

The most attractive sector for investors was professional, scientific, and technical services, which attracted approximately EUR 390 million — accounting for one-third of the total raised capital. The construction sector ranked second, with EUR 240 million raised, while the real estate market led in terms of investor participation, engaging over 380,000 individuals. (Figure 3, 4)



Note: Note: Invested amount, in EUR mn, and number of investors (rhs), by investor type, 2023. Sophisticated investors are those classified by providers under ESCPR; professional are classified by investment firms under MiFID. Data from 17 NCAs, as detailed in the appendix.
Sources: Data reported by NCAs, ESMA.

Figure 3: Investors by type: Retail investors predominate
Source: ESMA



Note: Invested amount, in EUR mn and number of investors (rhs) by economic sector, 2023. "Prof. activities" = professional, scientific and technical activites; "Accom." = accommodation. Sector codes are the NACE Level 1 classification, revision 2, per Regulation (EC) 1893/2006, which gives definitions. Data from 17 NCAs, as detailed in the appendix.
Sources: Data reported by NCAs, ESMA.

Figure 4: Projects by economic sector: Range of economic activity supported
Source: ESMA

France remains the European Union's largest crowdfunding market in terms of both the number of platforms (30) and total funds raised (EUR 292 million). The Netherlands ranks second on both counts, with 17 platforms and EUR 291 million raised. Lithuania, meanwhile, leads in the number of investors (500,000) and projects (2,840) (*ESMA*, 2024).

It is worth noting that Lithuania and France began developing national crowdfunding regulations well before the adoption of the EU-wide framework — in 2017 and 2014 respectively.

Approximately 17% of all funds raised were contributed by cross-border investors. Austria and Estonia recorded the highest proportions of cross-border financing (around 80%), while in nine countries this figure remained below 10%.

Particular attention has been drawn to Lithuania, where nearly 500,000 residents have participated in crowdfunding — representing more than 20% of the country's adult population. This reflects both the early adoption of national legislation and the country's broad digital penetration (*ESMA*, 2024).

Despite the rapid development of crowdfunding in EU countries, the Republic of Moldova continues to face a number of systemic challenges — particularly related to the underfunding of key sectors such as science, education, and innovation.

An analysis of capital allocation patterns in the EU compared to Republic of Moldova reveals a low degree of intersectoral capital redistribution within the Moldovan economy. On one hand, this highlights a continuing conservatism among local investors; on the other, it points to the untapped potential for expanding the crowdfunding sector, provided there is proper institutional support. Shifting the national economy toward an investment- and innovation-driven model could be a critical factor for sustainable growth during the period of structural transformation.

The most promising sectors for attracting funds through digital platforms remain the IT industry, computing systems development, telecommunications, and digital infrastructure. These areas are essential pillars of the modern information-rich economy and require ongoing investment — including from alternative sources.

At present, Republic of Moldova lacks a comprehensive legal framework that governs crowdfunding in its broader sense. This creates uncertainty for all parties involved — from project initiators to potential investors. The key goals of state regulation should include: the development of a legitimate and transparent crowdfunding environment, increased attractiveness of digital platforms, legal recognition of project income, and the formation of a stable base of private investors willing to support projects of varying scales.

To unlock this potential, Republic of Moldova requires a clearly structured model of government engagement — from regulatory frameworks to the design and oversight of crowdfunding project mechanisms. Publishing and executing projects via specialized digital platforms offer a cost-effective and time-efficient way to attract capital, which is especially crucial for startups and SMEs.

In conclusion, active government support in fostering and regulating crowdfunding could become a powerful tool to overcome existing development gaps, boost digitalization, and stimulate entrepreneurial activity. Crowdfunding allows entrepreneurs to launch innovative initiatives with minimal overhead and without the need for large marketing budgets — a vital option given the limited access to traditional banking finance.

CONCLUSION

In summary, the development of crowdfunding is a key driver for the emergence of innovative solutions, new products, and advanced technologies on the market. It creates additional opportunities to stimulate investment in innovation and production in the Republic of Moldova. Furthermore, this practice can help mitigate the outflow of scientific talent and skilled professionals by enabling them to implement their ideas domestically. Crowdfunding is increasingly recognized as a promising mechanism to support entrepreneurial initiatives. The experience of implementing such projects reflects growing societal interest in modern financial tools for launching new business ventures.

At present, crowd-based technologies represent a rapidly evolving segment of alternative investment and business financing. The market continues to expand year after year, offering attractive returns for investors and accessible financing solutions for entrepreneurs.

Compared to economically advanced countries, Moldova's crowdfunding ecosystem remains in an early development stage. This is largely due to limited investor trust and a delayed start relative to international trends. Nevertheless, recent trends indicate steady growth in both the number of crowdfunding projects and platform users. In this context, businesses—particularly small and medium-sized enterprises (SMEs)—are encouraged to actively explore and leverage the potential of available digital platforms for attracting capital.

Key Challenges Identified:

- Low public awareness and limited penetration of crowdfunding within the SME sector due to a lack of systematic educational initiatives on this topic.
- Limited transparency regarding platform activities, making it difficult for both entrepreneurs and investors to make informed choices.
- Gaps in the legal framework, including the absence of clear regulations for specific types of crowdfunding technologies.

Recommended Actions:

- Expanding the scope of legal regulation: there is a need to formalize governance mechanisms for donation-based and reward-based crowdfunding models at the legislative level.
- Establishing professional and ethical standards for the operation of investment platforms.

- Mandating the definition of procedures for investor-project initiator interactions in the event of unforeseen circumstances or force majeure.

From a public policy perspective, a systematic approach is needed to support the development of crowdfunding infrastructure, alongside the introduction of a transparent, coherent, and comprehensive legal framework capable of effectively governing the activities of digital investment platforms.

The work represents **scientific novelty** in that it combines two related areas—alternative financing methods and innovation management—as well as the economic characteristics of the Republic of Moldova, which is in the process of establishing this interconnection.

The study is limited by time constraints, given that the concept of crowdfunding is only beginning to gain interest in the Republic of Moldova, but for many, this term is still unfamiliar, so the next limitation is its weak perception by the population. Given the national characteristics of doing business, successful examples from other countries cannot always be transferred to the Moldovan economy, which is also a limitation.

Looking ahead**, further research** should focus on analyzing the quality and maturity of the infrastructural components of the crowd economy. This will be essential for broadening the range of available projects and attracting new flows of capital to Moldova's emerging alternative finance ecosystem.

REFERENCES

1. Law of the Republic of Moldova No. 181/2023 "On Collective Financing Services", Available at: https://www.legis.md/cautare/getResults?doc_id=138188&lang=ro [Accessed 31.05.2025]
2. ESMA, Crowdfunding in the EU 2024 // Market Report – 2025, pp. 6-11, ESMA50-20852710188 January 2025-4039, Available at: https://www.esma.europa.eu/sites/default/files/2025-01/ESMA50-2085271018-4039_ESMA_Market_Report_-_Crowdfunding_in_the_EU_2024.pdf [Accessed 04.06.2025]
3. Lafuente E., Ács Z. J., Szerb L., 2021. A composite indicator analysis for optimizing entrepreneurial ecosystems. *Research Policy*. Vol. 51. Is. 9, 104379, Available at: https://doi.org/10.1016/j.respol.2021.104379 [Accessed 02.06.2025]
4. Ghjg Elia G., Margherita A., Passiante G., 2020. Digital entrepreneurship ecosystem: How digital technologies and collective intelligence are reshaping the entrepreneurial process. *Technological Forecasting and Social Change*. Vol. 150(1), 119791, Available at: https://doi.org/10.1016/j.techfore.2019.119791 [Accessed 03.06.2025]
5. Tretyakova E. A., Freiman E. N., 2022. Ecosystem approach in modern economic research. *Management Issues*. No. 1. pp. 6–20, Available at: https://doi.org/10.22394/2304-3369-2022-1-6-20. EDN: QPUHDQ [Accessed 02.06.2025]
6. Korsun O., 2024. MARKETING 7P // Marketing Link – 2024, Available at: https://marketing.link/ru/marketing-7p-2/ [Accessed 03.06.2025]
7. World Investment Report, 2022. UNCTAD. INTERNATIONAL TAX REFORMS AND SUSTAINABLE INVESTMENTS, Available at: https://unctad.org/system/files/official-document/wir2022_overview_ru.pdf [Accessed 04.06.2025]
8. *Business Publication - 2.7 billion lei will be allocated annually to the IT sect*or, 2025, LOGOS PRESS, Available at: https://logos-pres.md/ru/novosti/kak-dostignem-czelej-v-oblasti-czifrovizaczii/ [Accessed 04.06.2025]
9. Republic, investment platform, https://republic.com/learn/investors/how-it-works [Accessed 05.06.2025]
10. Fagura, investment platform, Available at: https://fagura.com/ [Accessed 05.06.2025]

CYBER RISK ASSESSMENT IN EDUCATION

UDC: 378.1:[004.056+005.334]
DOI: https://doi.org/10.53486/tids2025.14

VIOLETA BOGDANOVA
"Ion Creanga" State Pedagogical University of Chisinau
bogdanovaleta@gmail.com
ORCID ID: 0000-0003-4140-6317

Abstract. Cyber risk assessment in educational institutions is related to the processes of risk identification, analysis and assessment. The educational environment, as well as other sectors of the economy, is exposed to quite strong digital threats and vulnerabilities. Due to the growing integration of technologies into teaching, learning, administration and communication processes, educational institutions face various cyber risks. Proper risk assessment helps to protect data, ensure compliance and maintain business continuity.

Keywords: cyber security, training, data protection, business processes in education.

JEL Classification: I29.

INTRODUCTION

In the modern world, education is subject to certain requirements related to the demands of a rapidly changing economic environment. Information technologies penetrated all spheres of education from kindergarten to higher education institutions, from engineering to creative specialties.

The development of digital pedagogy, which began to be actively implemented in the Republic of Moldova during the pandemic, is dictated by the requirements of sustainable development of national education at all levels.

Risks related to threats of violations of integrity, confidentiality and availability of information arise when using digital technologies.

The academic environment is quite open. The peculiarity of the university is its openness due to the constant influx of new students, the organization of scientific events, such as conferences.

Cyber threats are realized due to:

– data leaks and unauthorized access;
– ransomware attacks;
– phishing;
– internal threats;
– outdated system vulnerabilities (Liluashvili, G. B., 2021).

An analysis of scientific literature, represented by numerous articles and conference materials, shows that the rapid digitalization of education has significantly increased the security risks of information systems of educational institutions.

Cyber risks in the educational environment are considered in various works from the position of:

– educational process security (features of online learning, difficulties in monitoring students' knowledge, etc.);
– student security (leakage of students' personal data, easy access to the Internet and AI technologies in the process of studying and assessing knowledge, use of unreliable and dangerous information, cyber resistance to information and psychological influence, etc.);

– financial and economic risks (availability of licensed software and timely updates, availability of sufficient material and technical base in terms of information protection and countering threats, insufficient equipment with auxiliary digital technologies and training of teachers in their use, etc.);

– legal aspects, etc.

Analysis and assessment of cyber risks in the educational environment are presented in the works of the authors: Burov, O. Yu. (2024), Ulven, J. B., & Wangen, G. (2021). Bandara, I., Ioras, F., & Maher, K. (2014). And many others. The increase in cyber attacks on educational institutions is mentioned in the works (Vajpayee, P., & Hossain, G. 2024).

The wide interest in this topic is caused by the fact that Industrial Revolution 4.0 has had a significant impact on education due to the expansion of the use of new digital technologies. The issues of ensuring the safety, integrity, authenticity and confidentiality of information, the safety and operability of university information systems, the confidentiality and integrity of information resources are becoming increasingly relevant.

The purpose of this article is to consider cyber risks in the educational activities of a university from the perspective of the business processes being implemented.

To achieve the goal, the following tasks were solved:

1) the goals of the university were formulated taking into account the modern challenges facing the education system;

2) the main business processes of the university were examined in detail;

3) recommendations were presented for training employees and students to reduce the likelihood of cybersecurity threats.

MAIN CONTENT

Informatization affects all the main, auxiliary and management business processes in the university. A business process is a repeating chain of actions that creates value for an educational organization, students, parents, the labor market, and the state. Value is usually understood as products and services, money, and information.

From the point of view of an educational system, which is a non-profit structure, value can be the achievement of specific results that allow an educational institution to increase efficiency, reduce training costs, and improve the quality of educational services. The goal of an educational institution cannot be formulated, as in a commercial one, in the form of a single position. If we consider in detail the process of goal setting in the educational system, the goal itself becomes a subsystem containing various directions, such as: optimization of the university's work, cost reduction, quality improvement, increasing transparency and control, flexibility and scalability, increasing student satisfaction.

In the implementation of the goal "Optimization of the University's work" it is implied:

- a set of measures aimed at improving the learning process and its quality;
- automation of processes;
- use of analytics systems;
- optimization of the class schedule;
- creation of comfortable conditions for independent work of students;
- use of individual approaches to learning;

- introduction of new technologies in learning;
- use of modern methods of knowledge assessment.

Such a goal as "Cost reduction" for a university is always relevant, since higher education needs additional funding to purchase new equipment, materials for laboratories and much more. To achieve this goal, the following usually occurs:

- transfer of information sources and document flow to electronic form;
- optimization of technical support for the university's activities;
- use of financial assistance.

The sphere of higher education is a highly competitive environment. Therefore, the goal of "Quality Improvement" is permanent for any university

- improving the educational process;
- creating conditions for motivating students;
- improving material and technical support;
- supporting an individual approach;
- implementing a quality management system;
- regular monitoring.

The implementation of the goal "Increasing transparency and control" is dictated by the requirements of the environment in the form of control from the state, the interest of the business environment in the quality of graduates, parents of students. To achieve this goal, it is necessary:

- creation of an information platform for interaction with society;
- development of social network communications of the university;
- implementation of the principle of openness and accountability;
- conducting an open audit of financial activities;
- involvement of the academic staff in decision-making processes.

In today's rapidly changing world, the goal of "Flexibility and Scalability" is aimed at promptly making changes and adapting it to changes in the external and internal environment of the university by:

- ensuring flexibility in planning and implementing programs;
- building programs on a modular principle;
- increasing international student mobility;
- implementing access control systems to educational resources.

No less important is the goal of "Increasing student satisfaction". According to the author's observations, the number of people in the Republic of Moldova who want to obtain higher education is currently decreasing. This is due to both demographic problems and changes in the value system of the younger generation. In order to attract more students to the system of higher professional education, it is necessary to:

- update curricula;
- improve and timely update information on academic disciplines;
- uninterrupted connection to electronic library systems;
- support educational and industrial practices;
- participation in grant activities;
- involvement of students in scientific activities;
- timely and high-quality response to all requests.

Each specific university, depending on its operating conditions, sets specific goals for itself.

The main business processes of the university can be divided into:

– educational activities;

– research activities.

. Many universities provide additional education services, so we will classify it as a main business process.

Table 1 presents the main business processes in the university.

Table 1 Structure of the main business processes in the university

Educational process	Research activities	Additional education
– admission and enrollment of students; – development of curricula; – conducting classes and practical training; – current monitoring and assessment of knowledge; – intermediate monitoring of students' knowledge; – final monitoring of students' knowledge. – issuance of educational documents	– preparation and implementation of scientific projects; – organization of conferences and other scientific and scientific-practical events; – participation in grant research; – interaction with the business environment within the framework of scientific research activities; – work of postgraduate schools; – work of scientific research laboratories	– organizing advanced training courses; – organizing professional retraining; – conducting courses, trainings, master classes for the teaching community and business environment

Source: *developed by the author*

Most of the above core business processes can be targeted for financial gain or reputational damage to a higher education institution.

Data leaks can occur for accidental or deliberate reasons. Data leaks usually occur when unauthorized persons gain access to confidential information. This can happen as a result of cyber attacks or security vulnerabilities. Legal consequences, reputational and financial losses for the university are inevitable.

Cases of ransomware being used in cyber attacks have become more frequent. Most often, the university's information system is blocked, the data is encrypted. The attacker demands payment for restoring access to resources.

Since higher education institutions do not have sufficient financial resources, the data is partially or completely destroyed, the university suffers reputational losses and legal risks.

Phishing is becoming an increasingly common cybersecurity problem. Attackers disguise messages in such a way that deceived university employees voluntarily or involuntarily provide access to confidential information. Phishing messages are used to introduce various malicious software into the university's information system, including ransomware. Fake letters and messages encourage employees to follow suspicious links, enter passwords and other important information. Internal threats are especially dangerous, since employees, due to insufficient qualifications or deliberately steal or destroy the university's information system. The actions of employees can lead to data leaks, unauthorized access by unauthorized persons. At the same time, system vulnerabilities can remain unnoticed for quite a long time.

Universities lack resources for advanced security. Antivirus software and firewalls alone are not enough to counter fraudulent attacks. In addition to classic malware, university security services face social engineering, zero-day exploits, compromised accounts, Living off the Land (LotL) attacks, and the like.

According to cybersecurity companies Arcticwolf and Asimily, a table of cyber threats faced by universities and colleges from USA in 2020 - 2023 has been compiled (Table 2).

Table 2. Cyber threats faced by US universities in 2020-2023

Year	University/College	Attack Type	Impact/Details
2020	University of California, San Francisco	NetWalker ransomware	Paid $1.14 million ransom to recover encrypted research data
2021	Howard University	Ransomware	Forced cancellation of online/hybrid classes; campus Wi-Fi shut down
2022	Mount Saint Mary College	Ransomware	Data stolen and published on the dark web after refusing ransom
2023	University of Michigan	Data breach	230,000 records stolen; included financial, health, and personal data
2023	Stanford University (Dept. of Public Safety)	Ransomware	430GB of confidential data claimed stolen by Akira ransomware gang
2023	University of Manchester	Ransomware	1.1 million people affected; health records and PII exfiltrated via VPN exploit

Source: *Extracted from official sites of. Arcticwolf and Asimily*

As you can see from the table, most often large universities faced financial extortion `by ransomware attack.

The education system stores a large amount of personal data of students, their parents, guardians, teachers and staff. Attackers encrypt such data for financial gain. The universities presented in Table 2 are only the tip of the iceberg. These educational institutions reported attacks and their consequences. It is obvious to assume that even more educational institutions did not inform the public about such incidents.

Attackers are also aware of the lack of cybersecurity specialists in the university, software and hardware. This allows attackers to use social engineering methods more often and more effectively.

CONCLUSIONS

In the work, cyber risks will be considered within the framework of various university processes.

A modern university faces a wide range of threats. The implementation of cyber threats can lead to financial and reputational losses. To minimize risks, the university must apply reliable access restrictions and regularly audit the information security system. The implementation of information security standards will be effective: NIST SP 800-171, Cybersecurity Maturity Model Certification (CMMC) 2.0, GDPR etc.

REFERENCES

1. 4 Cyberattacks that Shook Universities and Colleges in the Last Year. Available at: https://asimily.com/blog/4-cyberattacks-universities-and-colleges/ [Accessed 01.05.2025].
2. 10 Cybercrimes Against Colleges and K-12 Schools, and How To Prevent Them Available at: https://arcticwolf.com/resources/blog/cyber-attacks-against-schools-and-colleges/ [Accessed 01.05.2025].
3. Gremalschi A., (2021) Lecția Pandemiei: de la simpla alfabetizare digitală la o pedagogie digital autentică, Univers Pedagogic, Nr. 6 (748), p.3
4. Jomir, E., Belostecinic, G. (2022) Educația şi cercetarea universitară ca factor de ameliorare a securităţii naţionale. In: The Collection. : Economic security in the context of sustenable development, 17 decembrie 2021, Chisinau. Chişinău: Departamentul Editorial-Poligrafic al ASEM, 2022, 2, pp. 45-50.
5. Liluashvili, G. B., (2021) Cyber risk mitigation in higher education. Law & World, 17, 15.
6. Vajpayee, P., & Hossain, G. (2024, October). Cybersecurity Education in High School: Exploring Cyber Assets, Cyber Value at Risk, and Authentic Assessment. In 2024 IEEE Frontiers in Education Conference (FIE) (pp. 1-9). IEEE.
7. Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. Future Internet, 13(2), 39.
8. Bandara, I., Ioras, F., & Maher, K. (2014). Cyber security concerns in e-learning education. In ICERI2014 Proceedings (pp. 728-734). IATED.
9. Chiriac L., Bogdanova V. (2024) Modeling of information system security by fuzzy logic methods. In CAIM 2024. Proceedings of the 31th Conference on Applied and Industrial Mathematics, 2024, Bucharest: MATRIX ROM, p. 24-27.
10. Буров, О.Ю., Литвинова, С.Г. Пінчук, О.П. (2024) Cybersecurity in the digital educational environment: external and internal risks. ІЦО НАПН України, м. Київ, Україна, pp. 64-74.
11. Буров, О.Ю. (2021) Cyber risks and the use of artificial intelligence in networking In: Автоматизація та комп'ютерно-інтегровані технології у виробництві та освіті: стан, досягнення, перспективи розвитку. Черкаський національний університет імені Богдана Хмельницького, м. Черкаси, Україна, pp. 60-62.

POLITICAL ECONOMY ASPECTS OF THE SHADOW DIGITAL ECONOMY

UDC: 004.056+339.19:004
DOI: https://doi.org/10.53486/tids2025.15

DINARA ORLOVA
Financial University under the Government of the Russian Federation
DOrlova@fa.ru
ORCID ID: 0000-0002-2901-070X

SERGHEI OHRIMENCO
Academy of Economic Studies of Moldova
osa@ase.md
ORCID ID: 0000-0002-6734-4321

Abstract. The article analyzes the shadow digital economy (SDE) as a modern threat to cybersecurity. The article formulates and proposes definitions of the SDE, based on the specifics of software production and the life cycle of information services of a criminal nature.

In the course of the research, the political economy foundations and general features of the SDE were determined. These include latency, coverage of all phases of the process of social and economic reproduction, the parasitic nature of the activity, and others. Future cyber threats such as Quantum Computing Threats, AI-enabled cyberattacks, Internet of Things (IoT) vulnerabilities, Cyberwarfare, and political manipulation are presented.

Keywords: Digital Economics, Cybersecurity, Shadow Digital Economics, Digital Threats, Cyberattack.

JEL Classification: D74 E26 F51 K24

INTRODUCTION

The currently used and prevailing technical approach to covering cybersecurity issues ignores many crucial socio-economic aspects. We argue that a political economy approach should address the social relations developing within the shadow digital economy. This includes production, distribution, exchange, and consumption of information, software, and services with criminal intent, as well as their impact on the value chain.

The peculiarity of the political economy approach is, firstly, the analysis of objective production relations, the nature of man in the system of market relations, and his objective interests (maximization of value income and minimization of costs). Secondly, political economy assumes that the existing relations are limited through the regulation of the economy (including the structure of production, the quality of products, a range of prices, the introduction of environmental and social standards, the distribution of development funds in the spheres of education and health care, the establishment of progressive tax on income, etc.). Thirdly, political economy links economic decisions to the socio-economic and political interests of social groups.

1 Definition of the shadow digital economy

We define the shadow digital economy based on its specificity in the production of goods and services, and their life cycle.

In the context of rapid digitalization of all aspects of life, insufficient attention is paid to the emerging negative trends where the shadow digital economy and cybercriminals play a key role. That is why, with the widespread introduction of the latest information technologies into society's everyday life, a new branch of knowledge has arisen – the shadow digital economy (SDE), which combines activities to promote products and services with a "shadow" focus. We define the digital shadow economy as "all illegal and hidden products and services that use information technology." The most important economic elements of this area are the following: illegal economic relations, illegal activities associated with the production, distribution, and use of prohibited products and services (Ohrimenco, 2021), (Ohrimenco, 2020).

The basis of the SDE is the shadow business activity, the general features of which have a hidden, latent (secret) character, meaning the activity is not registered by the organizations or state authorities and is not reflected in the official reporting; it covers all phases of the process of social reproduction (production, distribution, exchange, and consumption); and has a parasitic nature in all processes, ranging from the disclosure of the source code of a software product to the monetization of botnets by renting (Ohrimenco & Cernei, 2024).

From an economic perspective, the SDE represents a sector of economic relations that encompasses all types of production and economic activities which, by their nature, content, and form, contradict existing norms and legislation. These activities are carried out in violation of state regulation and bypass control mechanisms. The key economic elements of this sphere include: illegal economic and commercial relations, as well as illegal activities associated with the production, distribution, and use of prohibited or malicious products and services.

From a technological perspective, the SDE involves both individual and collective activities that are illegal, including the design, development, distribution, support, and use of information and technology components (such as processes, software, hardware, and communication systems), all of which are hidden from society. Thus, the SDE encompasses all illegal and concealed goods and services that rely on, are built upon, and operate with the support of information technology (IT) components.

A range of actions is undertaken by hacker groups, including targeted attacks, insider threats, social engineering, malicious mailings, espionage, and fraud. The main types involve hacking (e.g., credit card theft), denial-of-service attacks, identity theft, virus dissemination, online fraud, software piracy, and malicious code.

2. Cybercrime Economics

A separate and very important issue is the study of the economic foundations of cybercrime. In this regard, the data on the cybercrime economy looks stunning against the background of the collected statistics on the activities of the shadow digital economy. According to the study conducted by Bromium, cybercrime activity in 2018 was estimated at $1.5 trillion. This was the first study of its kind aimed at studying the "dynamics of cybercrime" in the context of revenue flow and profit distribution (Williams, 2019). In the course of the study, new criminal platforms and a thriving cybercrime economy were identified, which is self-sufficient and erases the boundaries of legality. Gregory Webb, CEO of Bromium, commented on the results of the study as follows: "It is shocking how widespread and profitable cybercrime has become. The crime model is to create malware and provide it to cybercriminals as easily as shopping online. Not only is it easier to access the tools, services and expertise of cybercriminals, it means that businesses and governments will face more sophisticated, costly and destructive attacks as the profit-driven web gains momentum. We cannot solve this problem with old thinking or outdated technology. It is time for new approaches."

3. Taxonomy of cybercrime

The proposed taxonomy is based on approaches to defining a set of criteria, which include technical experience, behavior, motivation, and level of moral development. The proposed model includes seven categories and is based on the recording of behavior:

1. Script Kiddies (SK) - individuals with limited technical knowledge and abilities who run pre-compiled software to cause harm to individual users, systems, and networks.

2. Cyber-punks (CP) – these people have a clear disrespect for authority and its symbols and disregard for social norms. They are driven by the need for recognition or fame from peers and society. The moral level remains low.

3. Haktivist (H) – Calling yourself a hacktivist sounds more respectful than calling yourself a petty criminal. People tend to justify their destructive behavior, including defacing websites, by labeling it as civil disobedience and ascribing political and moral correctness to it.

4. Thief (T) – This group targets information systems for financial gain and as such, targets credit card and bank account numbers that can be used for immediate personal gain. This group can accurately be described as petty criminals, given that the activities of its members are usually not sophisticated, namely simple wire transfer fraud and fraudulent use of credit card numbers.

5. Virus Writers (VW) – This category of individuals can include both technically skilled and novices. This category includes four subcategories, namely: teenager, college student, adult, and former virus writer. Even though viruses have been around in one form or another for many decades, they still constitute a very profitable segment of the crimeware market.

6. Professionals (P) – This is the most elite of the cybercriminal groups and is associated with competitive intelligence and the activities of so-called "white hat" and "gray hat" hackers. Members of this group may be involved in sophisticated scams or corporate espionage. They will sell information and intellectual property to the highest bidder. Very little is known about this underground group as they use strict anonymity to hide their activities. For them, their criminal activities are a job and they are consummate professionals.

7. Cyber terrorist (CT) – members of this group may be part of the armed forces or paramilitary formations of a nation state and are considered soldiers or freedom fighters on the battlefield of the new cyberspace. Their activities are associated with the commission of terrorist acts in cyberspace.

Taking into account the motivation of criminals, cybercrimes can be divided into the following categories:

- cyber fraud with the purpose of acquiring funds;
- cyber fraud with the purpose of acquiring information (for personal use or for subsequent sale);
- interference with the operation of information systems with the purpose of gaining access to automated control systems (for intentional damage for a fee or to damage competitors).

4. The Future of Cybersecurity

We will assume that cybersecurity policies are aimed at ensuring the security and resilience of digital technologies. For this reason, cybersecurity is an integral part of any government strategy aimed at developing the digital economy: reducing risk means reducing the expected costs of the economy and increasing the likelihood of adoption through greater trust. Cyber risk can entail huge costs for the economy, businesses, and ordinary users.

The main source of concern is purely technical: cybercriminals can exploit the limitations of software to hack it. Several factors support this thesis (Mariniello, 2022). It should be recognized that software is a very sensitive component and is subject to many errors. There are many reasons for this thesis. First, software code is extremely complex. Second, software always requires interaction with other software. Third, software code is necessarily built on previously coded software, which may have vulnerabilities that have never been fixed.

At the same time, users rely on other additional software such as antivirus, firewall, and traffic monitoring software (which may also be vulnerable to attacks) to track and counter potential attack attempts.

Thus, the cornerstone of cybersecurity effectiveness is the ability to withstand a variety of attacks. Historically, the evolution of cyberattacks spans from the emergence of simple malware to complex threats driven by artificial intelligence (Rusinova V., 2024), (Alaba, 2025), (S. Armstrong-Smith, 2024), (Shipley, 2024), (Kestner, 2024). Consider the evolution of cyberattacks, using et al.

Check Point experts identify five generations of cyberattacks. Generation 1 - late 1980s, virus attacks on autonomous personal computers affected all businesses and led to the first antivirus products. Generation 2 - mid 1990s, attacks from the Internet affected all businesses and led to the creation of the firewall. Generation 3 - early 2000s, exploitation of vulnerabilities in applications affected most businesses and led to the emergence of Intrusion Prevention Systems (IPS). Generation 4 - around 2010, the rise of targeted, unknown, evasive, polymorphic attacks affected most enterprises and led to the emergence of bot attack countermeasures (anti-bot) and sandboxes. Generation 5 - circa 2017, large-scale, multi-vector, mega-attacks using advanced attack tools and the introduction of advanced threat prevention solutions.

Let's consider expert assessments. Thus, Steve Morgan, editor-in-chief of Cybercrime Magazin, presented to the experts' judgment an article describing the five most significant facts on cybersecurity (Morgan, 2021). In particular:

1. Global cybercrime costs are projected to reach $10.5 trillion per year by 2025.Cybersecurity spending will exceed $1 trillion from 2017 to 2021. Experts predict that the global cost of cybercrime will grow by 15 percent per year over the next five years, reaching US$10.5 trillion per year by 2025, up from US$3 trillion in 2015. Innovation and investment in cybersecurity will significantly exceed the damage caused by natural disasters in a year, and will be more profitable than the global trade in all major illicit products combined (including drugs, pornography, arms trafficking, etc.). The costs of cybercrime include the cost of data damage and destruction, theft of money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, disruption to normal business operations following an attack, forensic investigation, recovery and removal of hacked data and systems, and reputational damage.

2. Global cybersecurity spending between 2021 and 2025 will total more than $1.75 trillion. The increasing pace of digitalization will drive global spending on cybersecurity products and services to a combined $1.75 trillion over the five-year period from 2021 to 2025. By comparison, the global cybersecurity market was valued at just $3.5 billion in 2004, and is now one of the largest and fastest-growing sectors of the information economy. The cybersecurity market is expected to grow at a compound annual growth rate of 15 percent from 2021 to 2025.

3. By the end of 2021, there will be 3.5 million unfilled cybersecurity jobs worldwide. Every IT job is also a cybersecurity position. Every IT worker, every technology worker, must play a role in protecting applications, data, devices, infrastructure, and people. According to Cybersecurity Ventures, there will be 3.5 million unfilled cybersecurity jobs worldwide in 2021. That's up from Cisco's previous estimate of 1 million unfilled cybersecurity jobs in 2014. The cybersecurity unemployment rate in 2021 will be zero percent (for experienced workers, not entry-level positions), where it has been since 2011. The rise in cybercrime will lead to just as many unfilled positions over the next 5 years.

4. Global ransomware damage is projected to exceed $265 billion by 2031. Global ransomware damage is projected to reach $20 billion per year in 2021, up from $325 million in 2015, a 57-fold increase. Ten years from now, costs will exceed $265 billion. Experts expect that by 2021, a business will fall victim to a ransomware attack every 11 seconds, up from 14 seconds in 2019. This makes ransomware the fastest growing form of cybercrime. The frequency of ransomware attacks on governments, businesses, consumers, and devices will continue to increase over the next 5 years, reaching every two seconds by 2031. The average ransom amount is estimated (Report, 2021), to be a significant $220,298 ($220,298 vs. $154,108, up 43% from Q4 2020), with the median ransom amount being $78,398 ($78,398 vs. $49,450, up 59% from Q4 2020), foreshadowing a quantitative and qualitative increase in new attacks.

5. The average ransom amount estimated by (Schwartz, 2021), is a significant $220,298 ($220,298 vs. $154,108, up 43% from Q4 2020), with the median ransom amount being $78,398 ($78,398 vs. $49,450, up 59% from Q4 2020), suggesting a quantitative and qualitative increase in new attacks.

Leading experts make an interesting suggestion that if cybercrime, from an economic point of view, were a sovereign country, it would rank 13th in the world by GDP. The total revenue, according to rough estimates, is $1.5 trillion and includes: $860 billion - activities in illegal, illicit online markets; $500 billion - theft of trade secrets, IP; $160 billion - data trading; $1.6 billion - cyber fraud and cybercrime as a service; $1 billion - ransomware. The report indicates that cybercrime operates on several levels, with some large "corporate" style trading operations bringing in more than $1 billion, and "small and medium business" style orders - from $30,000 to $50,000.

As information and communication technologies evolve, so too do the strategies used by cybercriminals. Cyber attacks have evolved significantly since the first computer viruses emerged. Experts note that the spectrum of cyber risks is constantly changing – from sophisticated malware to state-sponsored cyber warfare (cyber blockades).

Historical context includes: The Morris worm (1988); email-borne viruses (1990s); phishing attacks (early 2000s) to expropriate passwords and financial data.

Current status: Modern attacks are becoming increasingly sophisticated, using artificial intelligence, automation, and social engineering to evade detection. Key trends include:

Ransomware as a Service (RaaS), where criminal organizations provide ransomware toolkits that allow individuals with little or no technical knowledge or skills to carry out large-scale attacks;

Advanced Persistent Threats (APT): state-sponsored intrusions that infiltrate networks to spy or sabotage infrastructure;

Cloud Security Threats: as enterprises migrate to the cloud, attackers are taking advantage of misconfigurations and inadequate authentication protocols;

Deepfakes and AI-powered attacks: cybercriminals are using AI-generated audio and video to deceive individuals and organizations.

Future Cyber Threats: As technology evolves, cyber threats will also adapt, and potential future attacks include:

Quantum Computing Threats: quantum decryption has the potential to undermine existing encryption methods, thereby compromising sensitive information;

AI-enabled cyberattacks – cybercriminals will use AI to automate and optimize attacks, making them more difficult to detect;

Internet of Things (IoT) vulnerabilities: the proliferation of connected devices will create new attack vectors, especially in smart homes and industrial systems;

Cyberwarfare and political manipulation: nation-state actors will continue to use cyber strategies for espionage, sabotage, and influence operations.

CONCLUSIONS

The processes of digitalization have affected all leading economies, on the one hand, and the availability of modern tools and the growth of criminal competencies, on the other hand, are accelerating the criminalization trend, turning the underground infrastructure of the digital economy into an influential force capable of generating new threats at cosmic speed. This is why the shadow digital economy is now seen as a powerful, financially sustainable catalyst for cybercrime, providing attackers with access to services, resources, and technologies, thus expanding the scale and complexity of global attacks.

Additional difficulties were created by the COVID-19 pandemic, which revealed many problems related to remote user access and "home" work. First of all, these are information security problems - connecting personal computing devices to information networks, which activated phishing, which exploited the COVID-19 problem, and others. Additional threats were the remote access devices used, the volume of work performed using cloud technologies increased and, as a result, the number of DDOS attacks increased. The goals of cybercriminals have changed - if earlier financial organizations were considered the main target of cyberattacks, then during the pandemic there was a shift and the main targets became government organizations, industrial enterprises, energy, and medical institutions.

REFERENCES

1. Alaba, F. A. &. R. A., 2025. *The Implication of Cyberattacks on Big Data and How to Mitigate the Risk.*. s.l.:Springer.
2. Kestner, P., 2024. *The Art of Cyber Warfare.*. s.l.:Springer.
3. Mariniello, M., 2022. *Digital economic policy: The economics of digital markets from a European Union perspective.* s.l.: Oxford University Press.
4. Morgan, S., 2021. *Top 5 Cybersecurity Facts, Figures, Predictions, And Statistics For 2020 To 2021.* [Online] Available at: https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2019-to-2021/ [Accessed 25 June 2025].
5. Ohrimenco, S. &. B. G., 2020. Challenges for Digital Transformation in the Manufacturing Industry. In: *Socio-Economic Development-Interdisciplinary Ecosystems Perspective,*. Krakov: s.n., pp. 139-154.
6. Ohrimenco, S. B. G. &. C. V., 2021. *Estimation of the key segments of the cyber crime economics.*. Harkiv, IEEE.
7. Ohrimenco, S. B. G. &. T. B., 2019. *Shadow of digital economics.*. Harkiv, IEEE.

8. Ohrimenco, S. & Cernei., G. B. &. V., 2024. The Digital World Has a Long Shadow.. In: D. R. R. a. J. WŁODARCZYK, ed. *The Elgar Companion to Information Economics.* s.l.:Edward Elgar Publishing, pp. 481-.
9. Report, 2021. *Ransomware Attack Vectors Shift as New Software Vulnerability Exploits Abound.* [Online]. Available at: https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound [Accessed 25 June 2025].
10. Rusinova V., &. M. E., 2024. Fighting cyber attacks with sanctions: Digital threats, economic responses. *Israel Law Review.,* 57(1), pp. 135-174.
11. S.Armstrong-Smith, 2024. *Understand the Cyber Attacker Mindset: Build a strategic security programme to counteract threats.* s.l.: Kogan Page Limited.
12. Schwartz, M. J., 2021. *Cyber Extortion Thriving Thanks to Accellion FTA Hits.* [Online] Available at: https://www.bankinfosecurity.com/blogs/cyber-extortion-thriving-thanks-to-accellion-fta-hits-p-3024 [Accessed 25 June 2025].
13. Shipley, T. G. &. B. A., 2024. *Surviving A Cyberattack: Securing Social Media and Protecting Your Home Network.* s.l.: Stylus Publishing, LLC.
14. Williams, J., 2019. *Cybercrime as an Economy.* [Online] Available at: https://thefintechtimes.com/cybercrime-economy/ [Accessed 25 June 2025].

INFORMATION SECURITY ASPECTS IN HIGHER EDUCATION

UDC: [378.14:004.056.5]:005.342
DOI: https://doi.org/10.53486/tids2025.16

KRASIMIR SHISHMANOV
Professor, PhD
k.shishmanov@uni-svishtov.bg
ORCID ID: 0000-0001-9874-2149

EMIL TSANOV
Head Assist. Prof., PhD
e.tsanov@uni-svishtov.bg
ORCID ID: 0009-0003-0957-1301

ISKREN TAIROV
Head Assist. Prof., PhD
i.tairov@uni-svishtov.bg
ORCID ID: 0000-0002-2971-5451

Abstract. Recent studies indicate that information security plays an increasingly critical function in businesses today. Higher education is not an exemption. The growing number of safety incidents reported by higher education organizations in the past few years exemplifies the significance of privacy, reliability, and information accessibility in universities. The current review attempts to improve the authors' grasp of the views, methodology, and tendencies that define this emerging field of study. A literature review is conducted, and a direction for future research is suggested. The article suggests the fact that data protection in higher education is a profoundly unstudied topic. Other studied subjects include data safety habits, study evaluations of management information security in areas other than higher education, comparing studies between educational institutions, as well as security monetary theory and administration.

Keywords: smart cities, security, measures, deep learning.

Classification JEL: L86

INTRODUCTION

Recently, the advent of technological innovations has provided individuals, companies, and society as entirety with new opportunities. Improved chances for government and business enterprises to collect, analyze, and control data, as well as produce novel insights have appeared, becoming handling information an essential corporate component. The dominant alternatives given by the age of computers have led to novel protection requirements, which manifest in a variety of means: an environment of constantly shifting IT techniques; new laws for protecting data, and the emergence of ethical difficulties. Each of the demands has a cohesive source: a computerized, allowed, and social response to the increasing incidence of events involving information security.

Data safety is based on the principles of privacy, reliability, and accessibility of information (Whitson, 2003), and it has grown in significance and effect on present-day organizations. The rise in IT security expenses relates to the growing relevance of security concerns as a component in company decision-making, including topics such as the responsibilities of the corporate authority (Curry, 2017), a data security culture, and managerial support.

Because of the acknowledged importance of privacy and security in computerized assessments (Lowry et al., 2017), academic research remains behind, and subjects like the managerial approaches for information assurance awareness of information security (Parsons et al., 2017) and the importance of psychological factors have only lately become subjects of research. In general, the scientific community recommends additional studies on information security's organizational and executive parts to supplement the conventional, scientific tackle (Soomro et al., 2016). The current study answers these inquiries and investigates the managerial components of information security, emphasizing a specific field: higher education.

THEORETICAL BACKGROUND

Higher education institutions are located at among the greatest congested crossroads of the global digital economy. Such open-by-design (Borgman, 2018), decentralized, multi-stakeholder, ephemeral systems are typically linked with information technology, studies, and creativity. Students, educators, employees, and arrivals use higher education computer networks to acquire and generate knowledge in a variety of ways, including their cellphones and wearables (bring-your-own-device, BYOD), business desktops and notebooks, testing detectors, and scroll authentication mechanisms. Data transfer between educational institutions as organizations and their different consumers is ongoing (Chapman, 2019).

Higher education institutions, like many innovative companies, are expanding online, increasing their vulnerability to assaults by hackers and mandating continual surveillance and confidentiality of activities. However, the higher education setting appears to have an inherently unique connection to the security of information due to its multilayered method, inflexible construction, and central oversight. Most institutions lack the capacity for offering centralized safety measures, so substantial licensing of information security is frequently the favored alternative (Liu et al., 2017). The fact that this happens in one conjunction allows for quicker and more successful responses to cyber-attacks, but it also expands educational organizations' digital footprints and necessitates sufficient administration and contract administration.

A further challenge is that various kinds of customers in colleges have different levels of expertise in information security standards, making education efforts difficult at best. This last component is compounded by a historically high level of turnover and a typically lax perception of information security. Based on a threat actor's perspective, the period of educational institutions not owning any appealing resource is over: with computing resources (utilized, for instance, for launching distributed-denial-of-service assaults or, lately, for "mining" digital currencies) to private information, to trademarks, and some research information, educational institutions are swiftly ascending hackers' curiosity specifies.

As a consequence of all these complicated factors, the quantity of known information security catastrophes in higher education is increasing globally (Chapman, 2019), with some high-profile cases reaching the news lately. University research into the administration of information security in higher education is yet in its early stages (Okibo, 2014). At the very same time, previous work (Doherty et al., 2009) has shown that information security on campuses varies from other organizations, making managing information security in higher education a distinct studying subject. To determine and evaluate the latest developments in this newly developing area of investigation, the current paper presents a comprehensive assessment of academic studies on information security administration in higher education.

METHODOLOGY

The current investigation was divided into six sections: establish, investigate, choose, evaluate, present, and design.

Initially, an examination strategy centered on the study's theme was created, and research ideas were developed:

- Topics related to information security management in higher education;
- Literature study on security management in higher education.
- Importance of information security management in higher education.
- Recommendations for future research.

Secondly, the extent of the area, resources, and keywords were specified. The analysis was limited to higher education, information security, and computer science. In these instances, a search for records was performed using terms established during the review's preparation stage, according to the individual understanding of the research and a study of relevant works (Schatz & Bashroush, 2017). By narrowing the results to particular areas and putting the word management in the key phrase search, organizational and management difficulties were highlighted while an academic focus was spared. Small modifications have been implemented to the search phrases to account for the various possibilities for searches in datasets. Where achievable, the keywords, abstract, and title were investigated to confirm that the query's scope was consistent. To guarantee systematicity, all types of articles were initially examined regardless of sections such as publisher status, research methodology, or location.

Third, relevant studies were discovered using numerous characteristics to ensure applicability and quality (Pare et al., 2016). The initial round of removing focused on mathematical components: results were pared out by considering only published research and conference proceedings, which indicate rigorous methodology; papers in languages besides English were eliminated, as had been copies throughout records. The next phase of filtration concentrated on specific information elements: positive results were removed when, for instance, the phrases "college" or "higher education" reoccurred in the abstract merely as writers' connection information or for rights reasons (Wolfswinkel et al., 2013). The final phase of arranging focused on the most important parts: a broad study of summaries led to the elimination of documentation outside the area. A couple of articles from journals were also removed because they looked to have been mechanically transferred to English from another tongue, causing significant problems with accessibility and understanding. Finally, one manuscript was removed since it was very similar to another manuscript by the same creators, who most likely plagiarized their original material. Following this processing, a total of 18 articles were ultimately chosen.

Fourth, processing was carried out by analyzing the text of the examined literature with the research questions as guides.

Fifth, the findings of the evaluation were organized and reported.

Sixth, a paradigm of information security in higher education is suggested.

RESULTS

The initial step in the research process was to determine which subjects are most often referred to by researchers studying information security management at universities. Among the evaluated documentation, almost half of the selected literature focuses on researching risk management guidelines and regulations used in universities to assure information security control and a small part of the investigated papers addressed administration of information security systems as a key subject.

The following stage sought to establish that information security management is an area of interest at universities. The results revealed that the majority of studies gave barely any rationale for studying information security management in higher education. Some studies identified institutions as accessible, multifaceted systems with a complicated structure that could raise susceptibility to information compromises. Two publications viewed universities as knowledge-intensive organizations for whom knowledge preservation is strategically important. Half of the researchers investigated the peculiarity of information security management in higher education, demonstrating its significance according to these considerations:

- Higher education institutions offer different computer systems that promote innovation and leadership and equilibrium of cultural and technological diversity with commercial and company requirements.
- Universities must secure the anonymity, honesty, and timeliness of legal records, such as graduation certificates.
- IT innovations and a BYOD attitude are widely used at schools.
- Higher education institutions are experiencing an increase in recorded privacy violations.
- Universities are open innovation engines and institutions of society.
- Universities and colleges' internet pages have turned into a focus for criminals in response to fragile information security technologies.
- Universities have usually been considered uncertain from an IT viewpoint.
- Universities are going through developing enrollment, making them more susceptible as organizations.
- Universities keep broad amounts of hard-copy products.

Multiple researchers focused on academics as consumers of college networks, investigating networking practices, sensitivity to risky websites, and susceptibility as a measure of managing information security success.

The fourth work stage synthesized proposals for future study in the subject of information security management at institutions. Overall, the examined publications made few or no specific suggestions for further study on the topic. Within those investigations that identified topics for additional research, scientists advocated using universities as an intermediary for examining security issues in public companies or as a standard for doing so in smaller enterprises. Other sectors proposed examining an information security management system designed for college surroundings, exploring the relationship among information security policies and university employees' tactical papers, or figuring out the way a policy on appropriate use might be relevant to higher education.

Likewise, several studies called for a broader comparison of managing information security among universities. Human factor evaluation was another potential field for further study, particularly in the areas of unintentional loss of data, end-user opinions on cyber-behaviors, the function of cyber-routines in the offender-offender dynamic, along with goals to prevent malicious software while employed at the place of employment and working from their homes.

MODEL

Information security encompasses safety concerns in all types of data handling and can be thought of as a method of securing data in order to ensure accessibility, privacy, honesty, and responsibility (SIS, 2003; ISO/IEC, 2005a). The essential concepts of information security include privacy, reliability, and accessibility (Ahlfeldt et al., 2007). These are known as CIAs. Confidentiality relates to protecting records from improper use. Integrity is characterized as safeguarding from unwanted shifts, and availability involves the expected utilization of items during the stipulated time frame. It has been contended and asserted that more elements ought to be added to the concept of information protection. SIS (2003) includes obligation as an additional factor in the security of data, building on BS 7799 (2002), ISO/IEC 17799 (2005a), and ISO/IEC 27002 (2005b). Accessibility entails understanding ways to trace performed work down to a particular individual. A third party is specifically deemed responsible and held accountable for the protection of something or a collection of services. The focus here is on individuals and their own accountability. All four of these features demand combined technical and managerial safety precautions. Administration privacy refers to the administration of the safety of information, including tactics, procedures, evaluations of risks, and others. In addition, the preparation and execution in the security field necessitate an organized approach. This aspect of total security is thus structural in nature, affecting the entire firm. It is geared toward what the overall safety guidelines would be. Practical protection is concerned with the steps to be performed to meet the total criteria (Dark & Shanks, 2002). Practical security can be separated into two categories: building safety and security for information technology. Physical safeguarding, for example, covers the actual safeguarding of knowledge storage and alarms, whereas IT security relates to ensuring the safety of information in technical information systems. IT safety can subsequently be classified into two categories: security of computers and safety of communication. Information technology safety protects infrastructure and its contents, whereas security for communication protects systems as well as different devices used to convey info across machines (Bjorck & Yngstrom, 2001).

To more fully comprehend how these features and safety safeguards interact, a model of information safety was created and employed in the first research (see Figure 1). The model's goal is to concisely convey what information security entails. The model includes the concepts and descriptions provided above.

The primary notion, the safety of information, is located at the center. The four traits are arranged at the highest level and symbolize the safety of information. To accomplish the security of data, all of the organization's requirements for these qualities must be met. Fulfilling only a portion of them would be insufficient. The lower section of the model displays the various security methods in an ordered manner.

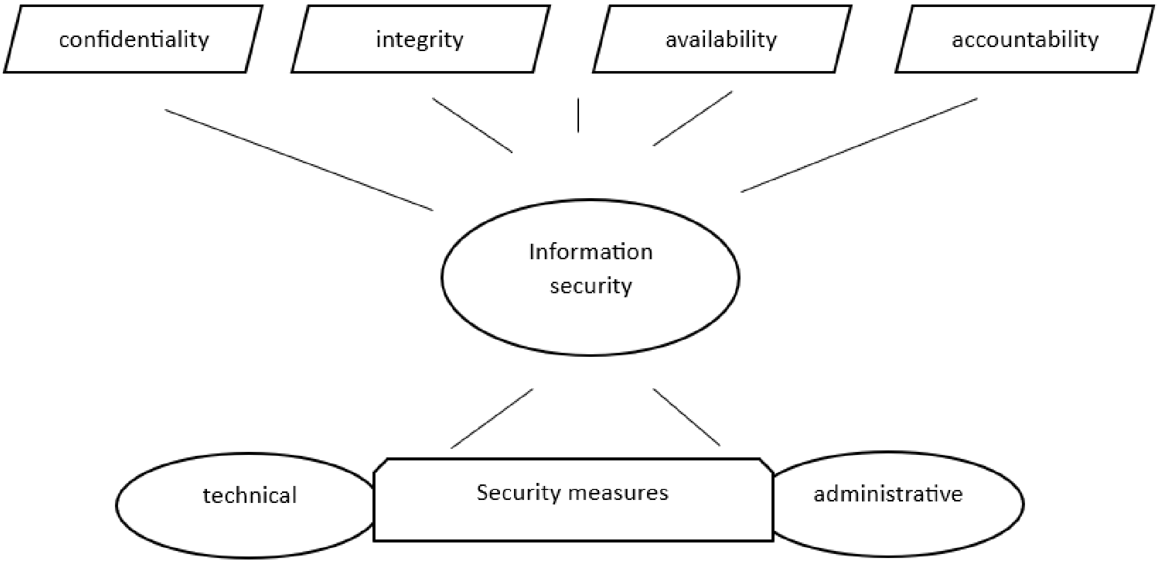


Figure 1. Information security model

The main goal of safeguarding data in higher education is to meet two critical objectives: student confidentiality and security. These phrases are well-known within the higher education sector. However, these concepts are crucial to the current study, so they have been further explained and explained. Student information is important and has to be safeguarded against misuse in order to protect students and build trust in higher education. Student safety and privacy are thus inextricably linked to student information and, by extension, the security of data. Student safety requires the correct knowledge at the right time, which includes the availability and integrity of student information. Similarly, to achieve student privacy, only the appropriate individual should have access to student information, ensuring confidentiality and responsibility. To better understand the relationship between safety and privacy regarding data security, the logic of the above was applied and integrated into the information security model (fig. 2).

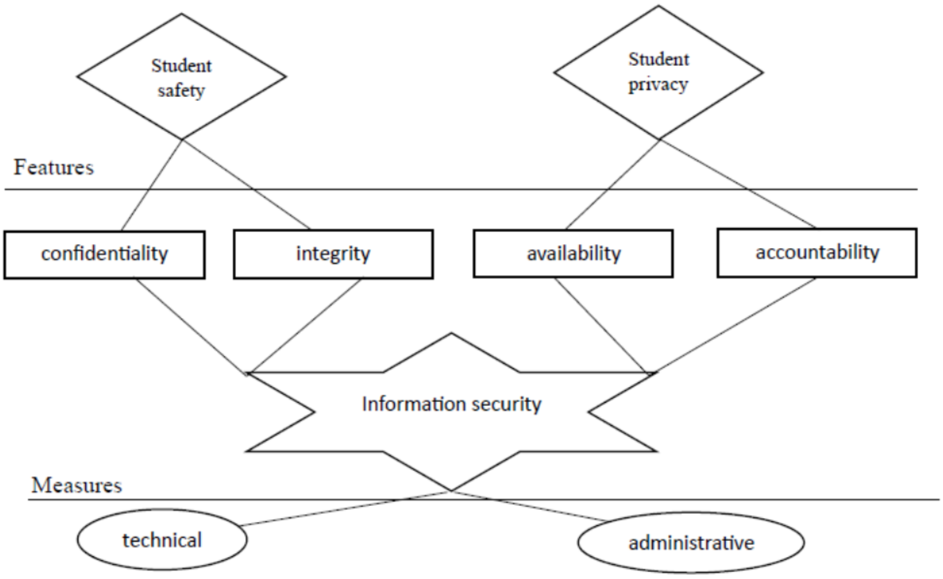


Figure 2. Model for higher education information security, adapted by (Ahlfeldt, 2008)

However, it needs to be highlighted that those connections are not unchanging, as there may be times when secrecy and transparency are required to ensure student safety, while availability and integrity are required to protect student privacy. Missing student information can jeopardize student privacy and safety, raising ethical concerns. This compromises either the student's privacy or safety. Figure 2:7 demonstrates the importance of balancing student safety and privacy in a comparable way that the information security sector has to deal with the fundamental ideas related to data security in order to reach an appropriate degree of safety for information.

CONCLUSION

The present research is an attempt to systematize the latest research findings related to the topic of information security management in higher education institutions. This research has made conceptual advances in a variety of methods by taking an analytical approach, which is based on research that used a strategy designed to improve systematicity and openness. In the first place, it has emphasized the difficulty of institutions in terms of the methods they apply when managing the security, integrity, and accessibility of the information they retain at all times. It has accomplished this by recognizing some major topics (and numerous sub-topics) covered in the literature, which include the implementation of insurance guidelines and regulations related to technology approaches to cyber-related difficulties in organizational structures executed for efficient security of data. This indicates an increasing desire and a requirement to raise the amount of research in this location; this is further demonstrated by the number of abstracts and a shortage of empirical research in the sample, as well as the fact that the majority of the articles reviewed didn't offer specific justifications for investigating information security management in colleges.

Being a late theoretical influence, the article lists themes for further research in this area, including security culture and comparisons that contrast educational institutions to other industries. Notwithstanding its mostly academic nature, a summary of research can provide useful insights, and this research is no exception. Its complete and creative technique may help both IT managers and data security teachers in schools, broadening their understanding of the present situation in managing information security work. In addition, security experts with no background in higher education may utilize the findings to obtain a grasp of the character of higher education, which includes a transparent framework, institutional structures, and a huge number of users, all of which create concerns with anonymity.

REFERENCES

1. Ahlfeldt, R-M. (2008). Information Security in Distributed Healthcare - Exploring the Needs for Achieving Patient Safety and Patient Privacy. DSV Report Series No. 08-003
2. Ahlfeldt, R-M. & Soderström E. (2007). *Information Security Problems and Needs in a Distributed Healthcare Domain – A case study*. Twelfth International Symposium on Health Information Management Research (iSHIMR 2007), Sheffield, UK, July 18 – 20, 2007, 97-108. ISBN: 0 903522 40 3.
3. Ahlfeldt, R-M., Spagnoletti, P. & Sindre, G. (2007). *Improving the Information Security Model by using TFI.* 22tn IFIP TC-11 International Information Security Conference (SEC 2007). Sandton, South Africa, May 14-16, 2007. 73-84. ISBN: 13:978-0-387- 72366-2
4. Bjorck, F. & Yngstrom, L. (2001). *IFIP World Computer Congress. IFIP TC11 WG 11.8* Second World Conference on Information Security Education, Perth, July 12-14. 209-223. Perth, Australia: International Federation for Information Processing

5. Borgman, C.L. (2018). *Open data, grey data, and stewardship: universities at the privacy frontier*. arXiv: 1802.02953
6. Chapman, J. (2019). *How safe is your data? Cyber-security in higher education. Higher Education Policy Institute,* 12. Higher Education Policy Institute, Oxford, UK, 1–6. HEPI Policy Note
7. Curry, S. (2017). *Boards should take responsibility for cybersecurity. Here's how to do it.* Harvard Business Review. Available at: https://hbr.org/2017/11/ boards- should- take- responsibility- for cybersecurity- here- how-to-do- it.
8. Dark, P. & Shanks, G., (2002). *Case Study Research, in Research methods for students, academics and professionals - Information management and systems*. Williamson K. (Ed), Second edition. Quick print
9. Doherty, N.F., Anastasakis, L., & Fulford, H. (2009). *The information security policy un- packed: a critical study of the content of university policies*. International Journal of Information Management. 29 (6), 449–457. doi: 10.1016/j.ijinfomgt.20 09.05.0 03
10. Liu, C.-W., Huang, P., & Lucas, H. (2017). *IT centralization, security outsourcing, and cybersecurity breaches: evidence from the US higher education*. International Conference on Information Systems ICIS 2017
11. Lowry, P.B., Dinev, T., & Willison, R. (2017). *Why security and privacy research lies at the centre of the information systems (IS) artefact: proposing a bold research agenda*. European Journal of Information Systems. 26 (6), 546–563. doi: 10.1057/s41303- 017- 0066-x
12. Okibo, B.W., & Ochiche, O.B. (2014). *Challenges facing information systems security management in higher learning Institutions: a case study of the catholic uni- versity of eastern Africa-Kenya*. International Journal of Management Excellence. 3 (1), 336–349
13. Pare, G., Tate, M., Johnstone, D., & Kitsiou, S. (2016). *Contextualizing the twin con- cepts of systematicity and transparency in information systems literature re- views*. European Journal of Information Systems. 25 (6), 493–508. doi: 10.1057/s4I303- 016- 0020- 3
14. Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). *The human aspects of information security questionnaire (HAIS-Q): two further validation studies*. Computer Security 66, 40–51. doi: 10.1016/j.cose.2017.01.004 .
15. Schatz, D., & Bashroush, R., (2017). *Economic valuation for information security invest- ment: a systematic literature review*. Information Systems Frontiers 19 (5), 1205–1228. doi: 10.1007/s10796-016- 9648- 8 .
16. Soomro, Z., Shah, M., & Ahmed, J. (2016). *Information security management needs more holistic approach: a literature review.* International Journal of Information Management. 36 (2), 215–225. doi: 10. 1016/j.ijinfomgt.2015.11.009 .
17. Whitson, G. (2003). *Computer security: theory, process and management*. Journal of Computing Sciences in Colleges 18 (6), 57–66.
18. Wolfswinkel, J.F., Furtmueller, E., & Wilderom, C.P.M. (2013). *Using grounded theory as a method for rigorously reviewing literature.* European Journal of Information Systems. 22 (1), 45–55. doi: 10.1057/ejis.2011.51

DIAGNOSING THE RISK EXPOSURE OF ENTERPRISES IN BULGARIA WITH ONLINE SALES

UDC: 005.334:[339.187:004.78](497.2)
DOI: https://doi.org/10.53486/tids2025.17

ZOYA IVANOVA
PH.D., Head Assist. Prof.
Tsenov Academy of Economics, Svishtov, Bulgaria
z.ivanova@uni-svishtov.bg
ORCID ID: 0000-0002-6521-2288

Abstract. In modern conditions, enterprises conducting online sales need to continuously apply new concepts, logic and mechanisms that are in line with the ongoing evolution of information and communication technologies and digital transformation. Unfortunately, Bulgarian enterprises operating in digital markets are significantly lagging behind in this direction. The main purpose of this study is to perform a thorough and multifaceted diagnostic to show the risk exposure of Bulgarian enterprises that operate online sales. The main theoretical and methodological basis of the study is the general risk theory and the private-scientific approach, as well as analytical methods such as: comparative method, analogy method. The specialized information sources of statistical data on the basis of which the research and comparative analyses are conducted are the National Statistical Institute (NSI) and Eurostat. Respondents of the survey are enterprises in Bulgaria with online sales of goods or services in the non-financial sector, which have 10 persons employed or more. Summarising the main findings of the survey suggests a relatively high-risk exposure of the enterprises surveyed.

Keywords: risk exposure, enterprises in Bulgaria, online sales, e-commerce.

JEL Classification: F14, L81, L86.

INTRODUCTION

Technological globalisation and digital transformation are revolutionising philosophy and imposing new standards and approaches to doing business. With the increasing adoption and use of digital technologies, the corporate world is rapidly entering e-commerce. The speed of digital development is so intense that modern e-commerce is prioritizing expanding the reach and efficiency of buying and selling channels and creating additional opportunities for commercial relationships. At the same time, economic actors are operating in an online environment where the safety and security of online transactions is becoming a critical factor. A number of conditions and reasons are created for the occurrence of risky situations and circumstances which increase their risk exposure.

A number of studies have shown that businesses selling online face a variety of challenges. On the one hand, they are driven by a change in the behaviour of their counterparties (Petrova, et al., 2022), (Luján-Salamanca, et al., 2025), (Hu, et al., 2025), (Zhao & Cao, 2024), (Stevenson & Rieck, 2024). At the same time, they face problematic situations as a result of wrong decisions and actions in the introduction and implementation of digital initiatives that change commercial relationships with consumers (Li & Yuan, 2025), (Pollák & Markoviˇc, 2022), (Min, 2021), (Aseri, 2021), (Henriette, et al., 2016), (Hannibal & Knight, 2018), (Saeed, et al., 2023). These challenges are highly dynamic over time and give rise to a number of bottlenecks, with relatively high degrees and intensities of impact. They occur at all stages of the exchange of goods over the internet or through digital technologies and in all directions of the market activity of businesses with online sales, increasing their risk exposure. The uncertainties of the actual commercial processes, especially for the Bulgarian online businesses, are reinforced by the challenges discussed.

The main purpose of this study is to conduct a thorough and multifaceted diagnostic to show the risk exposure of Bulgarian enterprises that sell online. In order to achieve the objective, the following research tasks are set: to track the changes in the status and risk exposure of Bulgarian enterprises with online sales in specific problematic events and situations; to interpret empirical aspects of the risk characteristics of Bulgarian enterprises with online sales and to indicate different potential for digital transactions; to formulate more important conclusions and generalizations about the weaknesses of the studied objects.

1. Materials and Methods

The commercial activity of Bulgarian enterprises operating on digital markets is invariably accompanied by the emergence of various risks and problematic situations. Identifying their manifestation during a certain period and diagnosing the risk exposure of enterprises has economic value. Risks can affect partly or wholly, singly or complexly, the state and functioning of enterprises with online sales. Thus, to a large extent, they are likely to affect the size and magnitude of their economic and financial performance, future development or survival.

In this context, different conceptual approaches, methods and tools are used to achieve the goal and realize the research tasks. The main theoretical and methodological basis of the research is the general risk theory and the private-scientific approach based on the research methods of deduction and induction, as well as the descriptive method and the method of analysis and synthesis. In this direction, analytical methods are also added, such as: comparative method, analogy method. The specialised information sources of statistical data on which the survey and comparative analyses are based are the National Statistical Institute and Eurostat. Respondents of the survey are enterprises in Bulgaria with online sales of goods or services from the non-financial sector, which have 10 persons employed or more, whose economic activity is in accordance with the Classification of Economic Activities. The target statistical population is defined on a random basis, which ensures a representative sample. The observation is sampled using one-stage cluster sampling. Technical processing and data calculations were performed by MS Excel.

In the analytical aspect, the study of the risk exposure of Bulgarian enterprises with online sales is based on quantitative and qualitative measures. In the course of the study, the relative share of enterprises in the EU countries that sell goods and services over the Internet is characterized, which results in the determination of the position and identification of the lag of Bulgarian enterprises. It compares the types of online sales (website, app sales or EDI-type sales) differentiated in Bulgaria and in the European Union. The survey focuses on enterprises in Bulgaria that own and maintain a website and the functionalities provided to online users. It takes into account the relative share of value of e-commerce sales of enterprises in the EU countries and specifically for Bulgaria. It analyses the quantitative and qualitative variables relating to the difficulties experienced by enterprises in Bulgaria, as well as the reasons that put them in problematic situations, which increase their risk exposure. On this basis, certain negative indications are identified and derived. Relevant conclusions and generalizations of theoretical and practical significance are reached.

2. Results and Discussion

The surveyed data show that the number of *enterprises in Bulgaria with e-commerce sales is still too small*. In 2024, Bulgaria ranks an unenviable 25th in this indicator compared to all member states, ahead of only Romania and Luxembourg. The relative share of enterprises selling goods and services online is 15.1%, 8.7 percentage points below the EU-27 average (23.8%) (Eurostat, 2024). Figure 1 visualises the data for all EU countries.

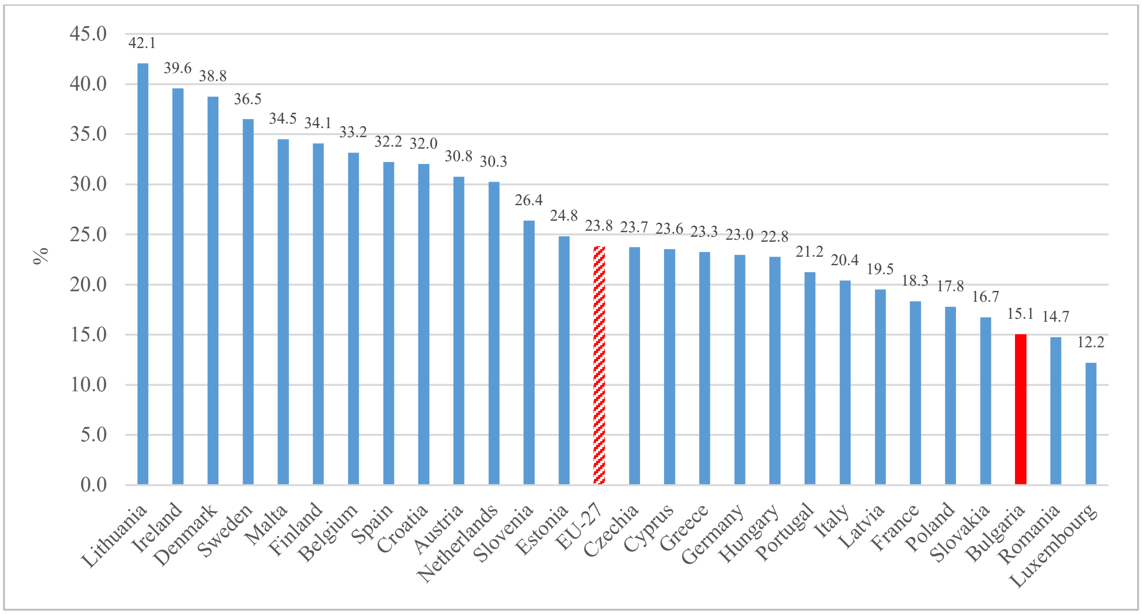


Figure 1. Relative share of e-commerce sales of enterprises in EU-27 in 2024.
Source: *Eurostat. E-commerce sales of enterprises by size class of enterprise.* *https://doi.org/10.2908/ISOC_EC_ESELS*

In 2024, only 26.3% of *large enterprises* in Bulgaria will sell online, 19.5% of *medium-sized enterprises* and 13.9% of *small enterprises*. The values by which Bulgaria is more than 2.5 times behind the leaders in the respective groups – Sweden, where 65.6% of large enterprises sell goods and services online, and Lithuania and Ireland for small and medium-sized enterprises – 39.7% and 51.2% respectively (Eurostat, 2024).

When analyzing the enterprises in Bulgaria with online sales it is necessary to take into account the way the transaction is carried out. Enterprises prefer two ways – web sales via website or apps and EDI-type sales. Essentially, web sales are made through a developed own website or apps, namely: own online store; virtual Extranet platform; apps for booking services; mobile apps; PC apps. The other option is through online platforms used by businesses to buy and sell goods and services over the internet, such as Amazon, eMag, eBay, Glovo, Takeaway, Booking.com, Alibaba, TimoCom, etc. EDI-type sales include all orders placed by enterprise users via EDI-type messages for electronic data interchange. They are in an agreed or standard format so that they are suitable for fast automated processing. Specifically, these are: EDI-type orders that are created by the user's business system; orders that are forwarded via a dedicated EDI service provider; orders that are automatically generated by the user's business system; orders that are placed directly in the enterprise ERP system.

According to the monitoring data, in 2024 the relative share of enterprises in Bulgaria selling goods and services via *web sales* is only 13.9%, and those using *EDI-type sales* – 1.9%. These values are 6.7 and 4.2 percentage points lower than the EU-27 average of 20.6% and 6.1% (Eurostat, 2024). In this context, the comparative analysis proves that there is a serious problem in the ratio of the parameters, as both indicators show an unfavourable lag behind the European average, which can hardly be compensated. A detailed breakdown of the data is presented through Figure 2.

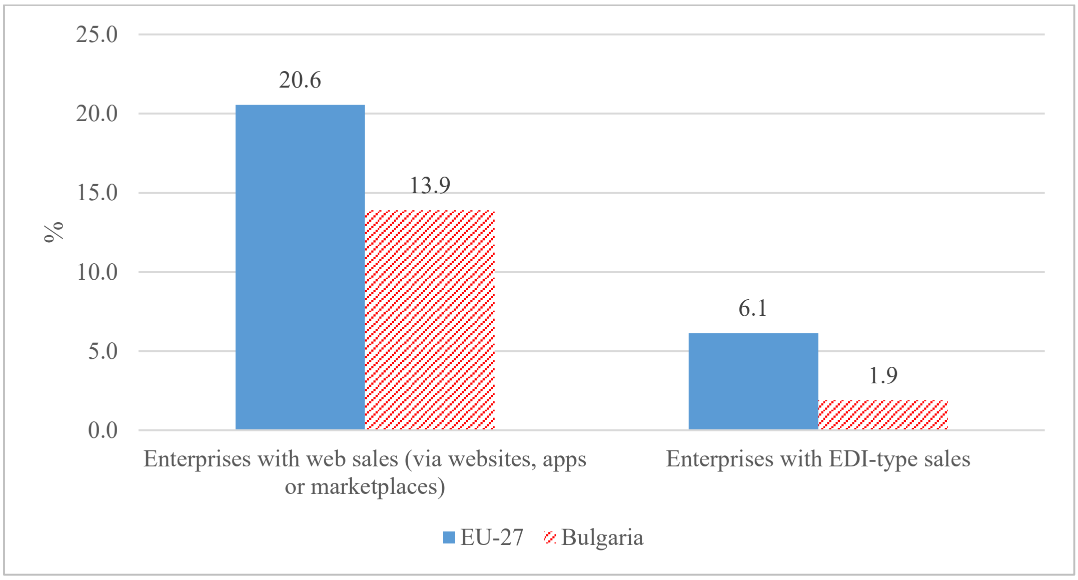


Figure 2. Relative share of e-commerce sales of enterprises in Bulgaria and EU-27 in 2024, by type of sales.

Source: *Eurostat. E-commerce sales of enterprises by size class of enterprise. https://ec.europa.eu/eurostat/databrowser/view/ISOC_EC_ESELS.*

It is also negative that in the structure of enterprises making web sales in 2024, only 11.2% are selling goods and services through their *own website or apps*, and 6.7% through *online marketplaces* (NSI, 2024). This data is largely indicative that businesses are not able to take advantage of the opportunities presented by different online sales methods.

It is important to point out that the surveyed enterprises provide functionalities on their own website that are informative rather than facilitating and accelerating the purchase of goods (services), which turns the online visitor into an active online consumer (see Figure 3).

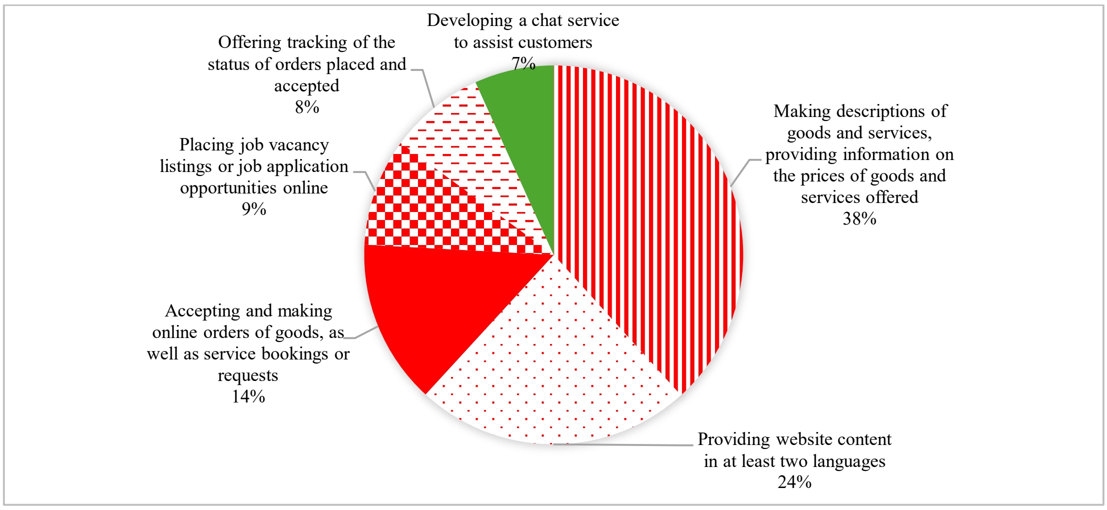


Figure 3. Features that enterprises in Bulgaria provide on their own website.

Source: *National Statistical Institute.*

The data in Figure 3 is indicative that businesses are not prioritizing their websites for sales or actively participating in online marketplaces, which limits the implementation of initiatives to streamline e-transaction operations or improve consumer relationships by offering the convenience and practicality of shopping anywhere, anytime.

Such behaviour has a negative impact on the value of e-commerce sales of Bulgarian companies. In 2024, the indicator will account for only 7.9% of total value of e-commerce sales, while the EU-27 average is 19.1% (Eurostat, 2024). On this indicator, Bulgaria ranks last among all member states (see Figure 4). This further puts businesses in Bulgaria in an unenviable position to influence consumers through their perceived online sales options. A comparative analysis of the data visualised in Figure 4 shows a poor performance of enterprises in Bulgaria with online sales.

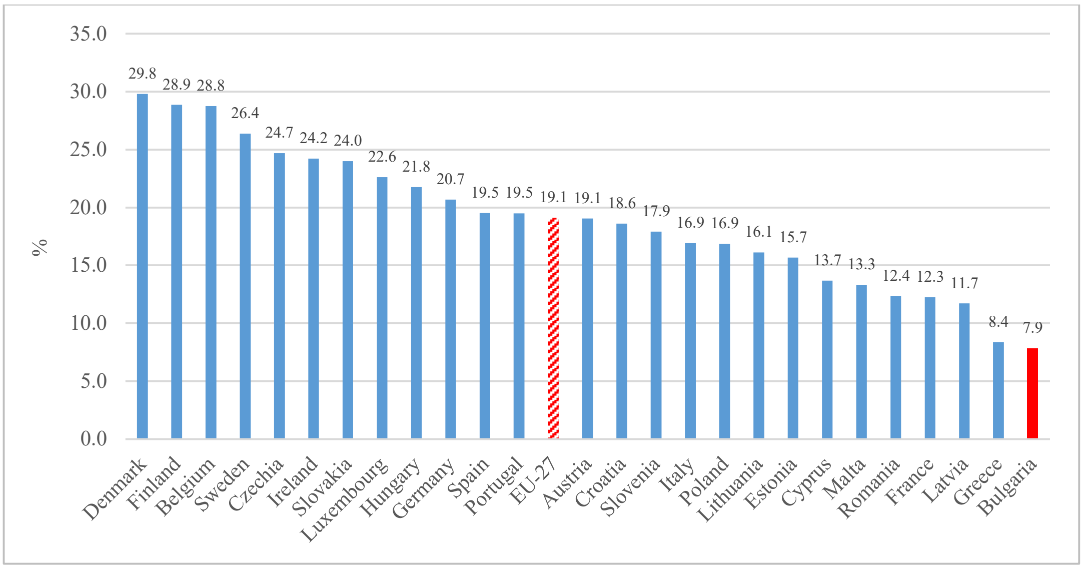


Figure 4. Relative share of value of e-commerce sales of enterprise in EU-27 in 2024.[1]
Source: *Eurostat. Value of e-commerce sales by size class of enterprise.* https://ec.europa.eu/eurostat/databrowser/product/page/ISOC_EC_EVALS.

The key benchmark of such behaviour is the fact that 13.7% of Bulgarian enterprises with web sales experience certain *difficulties, which are constantly accompanied by the emergence of diverse risks* (Eurostat, 2024). This objective circumstance should not be overlooked, as businesses are placed in specific risk situations.

In this respect, attention is focused on those explicit internal and external obstacles that have the most significant impact on the occurrence of risks. In particular for (Eurostat, 2024):

✓ 9.5% of businesses with online sales, the main problem is the *high costs of delivering or returning products*, which affects the expected results as well as their image and reputation;

✓ 4.3% – the leading issue is the difficulty in *related to resolving complaints and disputes*, causing controversy and creating uncertainty in relations with consumers;

✓ 1.8% – a real threat is the *adapting product labelling,* as well as *quality standards of products* meeting the standard requirements and parameters, according to the Regulations and Directives of the Union, which creates doubt and distrust in consumers;

[1] Data not available for the Netherlands for 2024.

✓ 2.9% – the *lack of knowledge of foreign languages* is considered as an immediate threat, which is among the parameters of primary importance, limiting market positioning and contractual relations;

✓ 1.7% – *restrictions from business partners* is a risky circumstance creating difficulties and inability to react quickly or adequately to the online market as well as to changes in the actions of market participants;

✓ 3.9% – the main obstacles are *related to the VAT system in EU countries*, especially in the calculation of the price and the emergence of unfair trade practices, which affects counter-agent behaviour.

Figure 5 visualizes the share of enterprises in Bulgaria that report obstacles for web sales according to their size.

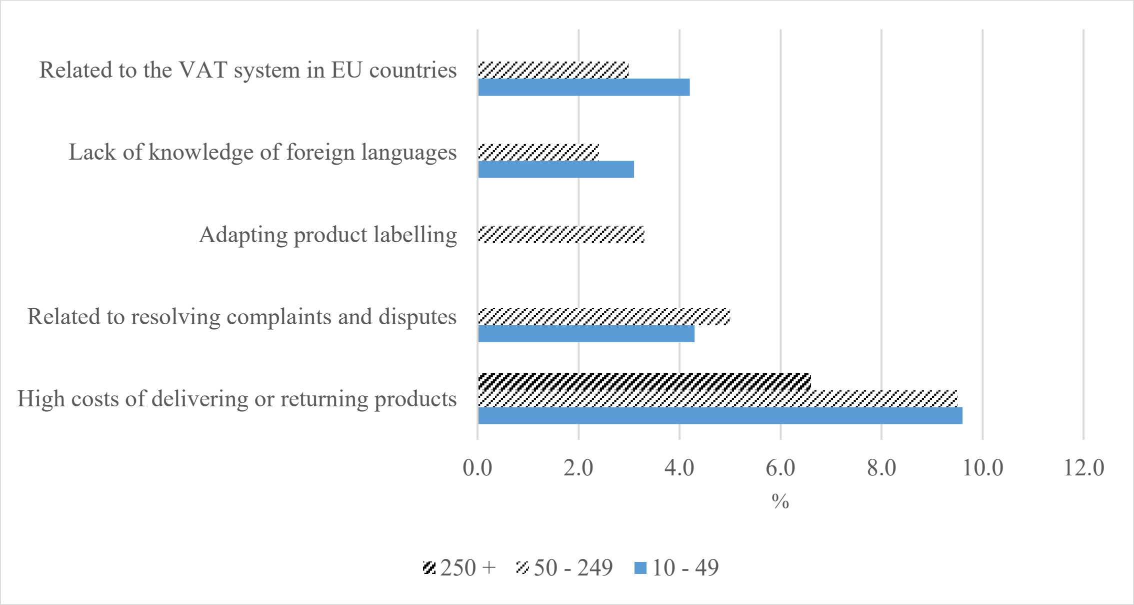


Figure 5. Relative share of enterprises in Bulgaria whit obstacles for web sales by size class of enterprise.

Source: *Eurostat. Obstacles for web sales by size class of enterprise. https://doi.org/10.2908/ISOC_EC_WSOBS.*

The data in Figure 5 shows that the highest proportion of *small enterprises* struggling to make web sales is 14.1%. *Medium-sized* enterprises came second with 12.5%, while the smallest share was 8.8% for *large enterprises* (Eurostat, 2024). This confirms the greater vulnerability of small and medium-sized enterprises in the face of challenges with a strong financial and consumer dimension that predetermine the risky nature of the online sales process.

CONCLUSIONS

On the basis of the diagnostics and the resulting findings, it can be pointed out that enterprises in Bulgaria with online sales have limited positioning. The differences between individual enterprises in terms of integration of digital tools and applications for goods exchange, as well as the degree of their actual implementation in online sales, are significant. There are a number of adverse effects and influences that increase the risk exposure of enterprises as they have a limiting impact and reflect on the emergence of serious challenges in the implementation of digital transactions.

In the light of these key findings, Bulgarian online businesses should continuously monitor and organise appropriate actions to mitigate risks and threats. They should promptly revise and reconsider the anti-risk methods and procedures that allow early identification of potential causes of their occurrence, as well as rapid mitigation of the development and change of risk parameters. Undoubtedly, in digital markets this is not an easy task, but its implementation leads to inevitable business success.

REFERENCES

1. Aseri, A. M., 2021. Security Issues For Online Shoppers. *International Journal of Scientific & Technology Research, 10(3),* pp. 112-116.
2. Eurostat, 2024. *E-commerce sales of enterprises by size class of enterprise.* Available at: https://doi.org/10.2908/ISOC_EC_ESELS [Accessed 15.05.2025].
3. Eurostat, 2024. *Obstacles for web sales by size class of enterprise.* Available at: https://ec.europa.eu/eurostat/databrowser/view/isoc_ec_wsobs__custom_10530221/default/table?lang=en [Accessed 15.05.2025].
4. Eurostat, 2024. *Value of e-commerce sales by size class of enterprise.* Available at: https://ec.europa.eu/eurostat/databrowser/product/page/ISOC_EC_EVALS [Accessed 15.05.2025].
5. Hannibal, M. & Knight, G., 2018. Additive manufacturing and the global factory: Disruptive technologies and the location of international business. *International Business Review, 27(6),* pp. 1116-1127.
6. Henriette, E., Feki, M. & Boughzala, I., 2016. *Digital Transformation Challenges.* Paphos, Cyprus, AIS Electronic Library (AISeL).
7. Hu, H., Li, M., Xiao, S. & Zhang, Z., 2025. The Strategic Adoption of Platform Schemes and Its Impacts on Traditional Distributors: A Case Study of Gree. *Mathematics, 13(10), 1591*, pp. 1-27.
8. Li, H. & Yuan, X., 2025. How Does the Manufacturer Optimize Pricing Decision and Channel Strategy Under Platform Encroachment? *Systems, 13(6), 416*, pp. 1-24.
9. Luján-Salamanca, A., Infante-Moro, A., Infante-Moro, J. C. & Gallardo-Pérez, J., 2025. Factors That Influence the Use of the Online Channel for the Purchase of Food Products in Spain. *Journal of Theoretical and Applied Electronic Commerce Research, 20 (2), 74*, pp. 1-17.
10. Min, H., 2021. Exploring Omni-Channels for Customer-Centric e-Tailing. *Logistics, 5(2), 31*, pp. 1-10.
11. NSI, 2024. *E-commerce. Enterprises with e-commerce sales.* Available at: https://www.nsi.bg/statistical-data/311/894 [Accessed 15.05.2025].
12. Petrova, S., Marinov, I. & Ivanova, Z., 2022. *Impact of Retail Business Digital Transformation on Online Purchases in the European Union.* Rome, Italy, BC GRUP INC. Publishing, pp. 52-63.
13. Pollák, F. & Markoviˇc, P., 2022. Challenges for Corporate Reputation—Online Reputation Management in Times of Global Pandemic. *Journal of Risk and Financial Management, 15(6), 250*, pp. 1-18.
14. Saeed, S. и др., 2023. Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. *Sensors,* pp. 1-20.
15. Stevenson, A. B. & Rieck, J., 2024. Investigating Returns Management across E-Commerce Sectors and Countries: Trends, Perspectives, and Future Research. *Logistics, 8(3), 82*, pp. 1-37.
16. Zhao, S. & Cao, X., 2024. Sustainable Suppliers-to-Consumers' Sales Mode Selection for Perishable Goods Considering the Blockchain-Based Tracking System. *Sustainability, 16(8), 3433*, pp. 1-29.

MODERN APPROACH OF FIREWALL IN LOCAL NETWORK

UDC: 004.056.52:004.732
DOI: https://doi.org/10.53486/tids2025.18

ANDRONATIEV VICTOR
Academy of Economic Studies of Moldova
andronatiev@ase.md
ORCID ID: 0000-0002-0294-457X

ZGUREANU AURELIU
Academy of Economic Studies of Moldova
zgureanu.aureliu@ase.md
ORCID ID: 0000-0003-3301-2457

Abstract. In modern society, computer networks are increasingly used across a wide range of activities. According to data provided by CISCO, in 2020 the number of users and devices connected to the Internet reached 50 billion. While initially computer networks were used primarily for file sharing, email, and reading news, today they serve many more purposes—such as online conferences, medical appointments, online shopping, remote learning, gaming, social media platforms like YouTube and Facebook, Wikipedia, and more. Given this widespread expansion, hundreds of billions of dollars are invested annually in computer network infrastructure. To ensure proper functionality and user convenience, a high level of security is essential. Without proper protection, users and companies risk losing money, personal data, or intellectual property, which would erode trust in these technologies.

As a result, investments in cybersecurity are critical: better security protocols are being developed, network equipment and operating systems are becoming more secure, cybersecurity experts are being trained, and users are being educated on how to interact safely in a digital environment.

One of the key protection methods in network security is the use of firewalls. Firewalls can be implemented in various ways: on servers to protect the local network from external access (and vice versa), on networking devices such as routers, or built into modern operating systems. Additionally, certain applications that require high levels of security may include their own dedicated firewalls, known as next-generation firewalls (NGFWs).

Keywords: local networks, firewall, network security, filter rules, nat.

JEL Classification: D85, L86

INTRODUCTION

As of 2023, it is estimated that there are over 2 billion personal computers in use globally (UMA Technology, 2025). This data includes desktops and laptops, highlighting the significant prevalence of personal computing devices in households and workplaces. The widespread use of computers necessitates enhanced security measures. No one would use computers if they knew their data could be stolen, falsified, or deleted. One of the first methods of data protection was the firewall. Users access the Internet through local networks, whether from home or work. Initially, firewalls were used to protect users within local networks. With the exponential growth of the Internet, firewalls evolved, and today they are used on routers, servers, operating systems, and applications that require enhanced security.

The importance and relevance of this research topic stem from the fact that billions of dollars are spent annually on security. In 2024, global end-user spending on information security is estimated at $183.9 billion. In 2025, global end-user spending on information security is projected to reach $212 billion, a 15.1% increase from 2024, according to a forecast by Gartner, Inc. (see Table 1). Additionally, enormous sums are spent on training security specialists and regular users.

Table 1. Information Security End-User Spending by Segment, Worldwide, 2023-2025 (Millions of U.S. Dollars)

Segment	2024 Spending	2024 Growth (%)	2025 Spending	2024 Growth (%)
Security Software	87,481	14.2	100,692	15.1
Security Services	74,478	13.6	86,073	15.6
Network Security	21,912	9.6	24,787	13.1
Total	**183,872**	**13.4**	**211,552**	**15.1**

Source: *Gartner (August 2024)*

The first publication related to firewalls appeared in 1988. It described a packet filtering system that operated up to the third level of the OSI model (first-generation firewall). In 1989-1990, second-generation firewalls were introduced - these operated up to Level 4 of the OSI model, taking into account connections between stations. Then, in 1994, third-generation firewalls were launched - these operated up to Level 7 of the OSI model and considered the source and destination applications of packet flows (Bolun I., Andronatiev V., 2014). In 2012, next-generation firewalls (NGFW) were introduced, offering more detailed inspection of application-level aspects of the OSI model, such as intrusion prevention systems and web application firewalls, etc.

MAIN CONTENT

1. Firewall Description

A firewall allows only packets that comply with specific rules to pass through. These firewalls can be of two types: stateful and stateless. Stateful firewalls keep track of the state of data transfer connections (such as TCP streams and UDP communications) and perform dynamic packet filtering. They allow only packets belonging to known connections to pass. When a new connection is established, it is checked against the security policy. Once approved, all packets in the current session related to that connection are accepted. Stateless firewalls, which preceded stateful firewalls, treat each packet independently of others (in isolation) without considering connections. They analyze only the packet header (Greyson C., 2025).

To examine the functionality of the firewall, we will use MikroTik networking equipment, which provides the following capabilities (Haddad M., 2023):

- Filter Rules – define filter rules;
- NAT – define NAT rules;
- Mangle – define Mangle rules;
- Service ports – define service port parameters;
- Connections – characteristics of active connections to the router;
- Address Lists – create groups of IP addresses with common rules;
- Layer7 Protocols – define Application-level rules.

When defining *firewall rules*, it must be taken into account that NAT rules are applied first and only then the others. Depending on the source address and destination address, we distinguish the following types of traffic:

- input - entering the router;
- output - leaving the router;
- forward - forwarding through the router.

When filtering packets, in addition to the type of traffic, the type of service is also used. For example, we allow web browsing, but prohibit copying files. Or, we can prohibit certain web pages with malicious content using the port number, according to the service being examined. Table 2 shows port numbers for the most commonly used services.

Table 2. Widely used port numbers and protocols

Port number	**Transport layer or Network (Internet) protocols**	**Application Layer Protocols**
20, 21	TCP	FTP
22	TCP	SSH
23	TCP	Telnet
25	TCP	SMTP
53	TCP/UDP	DNS
123	UDP	NTP
143	TCP	IMAP4
443	TCP	HTTPS, SSL
465	TCP	SMTP over SSL
989, 990	TCP	FTP over SSL
8080	TCP	Proxy
/1	ICMP	ping

Source: *Prepared by the author*

After identifying which type of traffic the packet corresponds to, we indicate which actions can be performed:

- *accept* – accept the packet;
- *add-dst-to-address-list* – add the destination address to the address list specified by the address-list parameter;
- *add-src-to-address-list* – add the source address to the address list specified by the address-list parameter;
- *drop* – drop the packet without notification;
- *jump* – move to another user-defined chain, by specifying the value of the jump-target parameter – the action is used to check the packet's compliance with a criterion from another chain;
- *log* – add a message to the system log to track the processed traffic. It is used to monitor data traffic;
- *passthrough* – ignore the current rule and move to the next one (it is useful for diagnostics, statistics);

- *reject* – reject the packet and send an ICMP reject message;
- *return* – passing control back to the point where the jump action was applied;
- *tarpit* – capturing and holding TCP connections (to the incoming TCP SYN packet, it is responded with SYN/ACK);

2. Examples of firewall rules

Filter Rules. Let's examine what traffic filtering options we can use. Firewall rules consist of two parts: a set of criteria (IF), to which the packet corresponds, and the action (THEN) that defines what to do with the given packet (RouterOS documentation, 2025).

First, let's protect the router from unauthorized access. For this, we need 2 rules. The first allows access only for the administrator's computer, the second prohibits access for everyone else. For remote connection, the Telnet and SSH protocols are used. The rules that perform these actions are specified below.

```
[admin@user1] > ip firewall filter print
Flags: X - disabled, I - invalid, D - dynamic
 0   chain=input action=accept protocol=tcp src-address=192.168.120.10
     in-interface=ether2 dst-port=22 log=no log-prefix=""
1    chain=input action=drop protocol=tcp dst-port=22,23 log=no log-prefix=""
```

As can be seen from rule number 0, access to the router is only for input traffic, port 22, i.e. SSH protocol. Since Telnet protocol, port 23 is insecure, connection through it is prohibited. In addition, the computer addresses 192.168.120.10 and the ether2 interface, i.e. local network are specified. From rule 1, it can be seen that for all other computers, from other interfaces, port 22 and 23 access is prohibited, because we have the drop action.

Another action, often used, is blocking access to certain services, for all users or some of them. For example, let's say we need to block access to web browsing, for certain users. For web browsing, the HTTP protocol, port 80, and the HTTPS protocol, port 443, are used. In order to indicate the rule for certain users, the most convenient is to use address lists. In the same way, we can block access not for users, but access from the local network to certain web pages on the Internet. Let's say we have a Deny list - a list of addresses that do not have access to web browsing and the other addresses, implicitly, have access to web browsing:

```
[admin@user1] > ip firewall address-list print
Flags: X - disabled, D - dynamic
 #  LIST        ADDRESS                            CREATION-TIME
 0  Deny         192.168.120.101-192.168.120.200     apr/21/2025 16:14:01
```

As we can see, in the 192.168.120.0/24 network, the Deny list includes computers with addresses from 192.168.120.101 to 192.168.120.200. Then, the web browsing blocking rule looks like this:

```
1    chain=forward action=drop protocol=tcp src-address-list=Deny dst-port=80,443
     log=no log-prefix=""
```

An important role in the work of the firewall is its speed of operation. Usually, the more rules we have, the more secure the network is, because we give access only to the necessary services. Services that are not needed are blocked, or access to certain services is given only to certain addresses. But, with an increase in the number of rules, the latency of the firewall increases (Artūrs C., 2024). One of the main methods of increasing the speed of the firewall is the use of connection status. In this way, connections can be classified as: new, established, related, invalid (see figure 1).

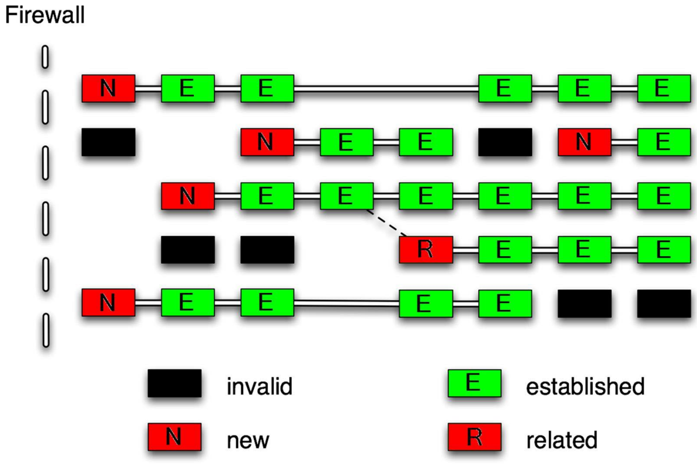


Figure 1. Classification of connections depending on their status

Source: *Mikrotik. First Time Setup. Available at: https://docs.calebsargeant.com/en/latest/networking/mikrotik.html#firewall.*

As can be seen from Figure 1, we have 5 connections, that contain packets of different types. It is recommended to check the first packets, of the *new* and *related* type. If these packets are accepted, then the other packets in the connection (*established*) can also be considered valid and *invalid* packets have been modified during transmission, so they are erroneous or malicious, and in this case, they must be rejected. Another important point is to let only new packets pass through the firewall, which means that the place of their placement is important. If they remain in the queue, then they are of no use, because new packets, anyway, pass through the entire firewall. In this case, they must be placed at the beginning of the firewall. Let's say that on average, each connection has 50 packets. Then using this method, theoretically, the speed of the firewall increases by 50 times. In this way, the mentioned rules look like this:

```
0    chain=forward action=drop connection-state=invalid log=no log-prefix=""
1    chain=forward action=accept connection-state=established, related log=no log-prefix=""
```

NAT Rules. Another type of firewall rules is *nat* rules. Network Address Translation (NAT) is necessary to transmit data from the local network to the Internet, and vice versa. Since the local network uses private addresses and the Internet uses public addresses, NAT changes the private address to a public one. This can be the external address of the router or server. When the response of the requested data comes, the reverse procedure takes place.

Depending on the number of public addresses used, NAT can be: one-to-one, one-to-many, many-to-many. One-to-one is when a single public address corresponds to a single private address. As an example, this method can be assigned to servers. Computers on the local network connect to the server via private addresses. And, computers on the outside via public addresses. One-to-many allows all computers on the local network to access the Internet via a single public address, thus saving enormous amounts of public addresses. In the case of large networks, several public addresses are used. This allows a large number of computers to access the Internet through several public addresses. This method allows computers to access the Internet at a higher speed, compared to the one-to-many method.

Depending on the purpose of using NAT rules, they can be:

- *accept* – accept the packet;
- *add-dst-to-address-list* – add the destination address to the address list specified by the address-list parameter;
- *add-src-to-address-list* – add the source address to the address list specified by the address-list parameter;
- *dst-nat* – perform the destination NAT function;
- *jump* – jump to another user-defined chain;
- *log* – add a message to the system log to track the processed traffic.
- *masquerade* – perform the source NAT function, when the public address of the external interface (Out. Interface) of the router is not known;
- *netmap* – static 1:1 mapping of a set of IP addresses to another set. It is often used to distribute public IP addresses to stations in private networks;
- *passthrough* – ignore the current rule and move on to the next one (useful for diagnostics, statistics);
- *redirect* – replacing the destination address of IP packets with one of the local addresses of the router, redirecting the packets to the router;
- *src-nat* – performing the source NAT function, when the public address of the external interface (Out. Interface) of the router is known.

Next, let's get acquainted with how some rules work:

1. As can be seen in Figure 2, the computer on the local network uses the private address, but in order to send information to the Internet, this address is changed to the public address using the src-nat rule.

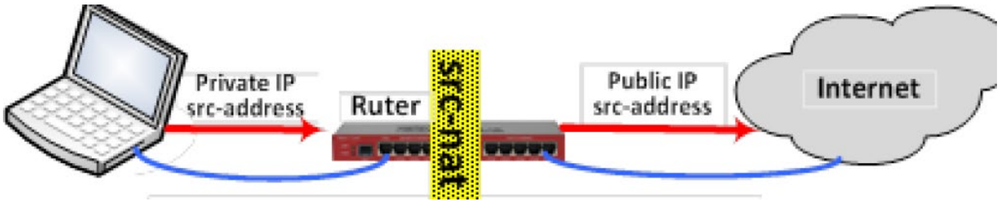


Figure 2. The src-nat rule

Source: *Bolun I., Andronatiev V., 2014. Internet şi Intranet.*

2. Another case is when someone from outside wants to connect to a server on the local network. This server can be: web server, ftp server, etc. Normally, local network users can connect without adding any rules, but users from outside the network need to add a *dst-nat rule*.

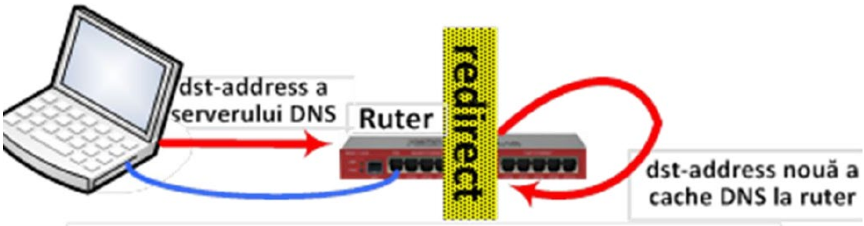


Figure 3. The redirect rule

Source: *Bolun I., Andronatiev V., 2014. Internet şi Intranet.*

3. In some cases, to save traffic or increase security, the redirect rule can be used. For example, in many cases users use the server address of Google (8.8.8.8) as a DNS server. Adding the redirect rule allows to reduce the use of external traffic, because the router instead of forwarding the DNS request outside, uses the cache on the router, (see Figure 3). This is very important when the Internet access speed is low or the network is under maximum load.

CONCLUSIONS

Nowadays, computers are used in practically all activities: at work, at home, for communication, online shopping, reading news, social networks, for tourism, weather forecasting, information search and many others. This is where the importance of securing user data comes from, because no one will use the Internet if they know that the user's sensitive data can be stolen, deleted, modified. Since the early days of the use of computer networks, one of the first means of protecting data has been firewalls.

If from the beginning the firewall worked at layer 3 of the OSI model (generation 1) and was used to protect the user's local network, with the evolution of the Internet and the exponential growth in the use of computer networks, the firewall also evolved. Today, 4th generation firewalls are used, which work within applications that require a high level of security. Even though every modern operating system has its own firewall, we see that firewalls are also widely used by applications at level 7 of the OSI model. In addition, if better security is needed, more powerful firewalls can be installed on computer, even though every operating system has its own firewall. So, we see that if initially the firewall was used only on the router, now it is used in different places: on the router, in the operating system and in applications.

In this paper, we examined what a firewall is and how it works, for this we examined Filter Rules and NAT rules. Since the firewall increases the latency of data transfer, special attention was paid to the performance of the firewall. For example, the use of address lists, connection status, redirect rule and correct programming allow to secure the transmitted information without annoying retentions.

REFERENCES

1. Bolun I., Andronatiev V., 2014. *Internet şi Intranet.* Chişinău: Editura ASEM.
2. Haddad M., 2023. *MikroTik MTCNA- Student Guide*. Independently published, ISBN-13: 979-8391913528.
3. Greyson C., 2025. *Firewall Configuration and Management: Advanced Strategies for Securing Your Network.* Kindle Edition.
4. *RouterOS documentation*, 2025. Available at: https://box.mikrotik.com/d/1a069dba20724f279e30/files/?p=%2FROS-200525-1501-900.pdf, [Accessed 07.06.2025].
5. Artūrs C., last updated by Normunds R. on Nov 29, 2024. *NAT.* https://help.mikrotik.com/docs/spaces/ROS/pages/3211299/NAT, [Accessed 07.06.2025].
6. UMA Technology, 2025. *How Many Computers Are In The World?* Available at: https://umatechnology.org/how-many-computers-are-in-the-world-up-to-date-stats/, [Accessed 04.06.2025].
7. STAMFORD, Conn., August 28, 2024. *Gartner Forecasts Global Information Security Spending to Grow 15% in 2025.* Available at: https://www.gartner.com/en/newsroom/press-releases/2024-08-28-gartner-forecasts-global-information-security-spending-to-grow-15-percent-in-2025, [Accessed 04.06.2025].
8. *Mikrotik. First Time Setup.* Available at: https://docs.calebsargeant.com/en/latest/networking/mikrotik.html#firewall, [Accessed 01.06.2025].

ASSESSING MOLDOVA'S ECONOMIC DYNAMICS USING THE COBB-DOUGLAS PRODUCTION FUNCTION: ESTIMATION, VALIDATION AND FORECASTING[1]

UDC: 330.44+338.27:338(478)
DOI: https://doi.org/10.53486/tids2025.19

ZINOVIA TOACĂ
Associate Professor
Academy of Economic Studies of Moldova
toaca@ase.md
ORCID ID: 0000-0002-8304-1961

LUCIA GUJUMAN
Associate Professor
Academy of Economic Studies of Moldova
gujuman.lucia@ase.md
ORCID ID: 0000-0001-7940-4291

IULIAN SOTROPA
Academy of Economic Studies of Moldova
sotropa.iulian@ase.md

Abstract. The study evaluates the economic dynamics of the Republic of Moldova based on the Cobb–Douglas production function, with the aim of estimating, validating and forecasting the relationships between capital, labor and output. The econometric analysis, carried out on the basis of annual data for the period 1994–2024, included testing for stationarity, normality, autocorrelation and homoscedasticity, applying the Newey–West correction. The obtained coefficients (α≈0.37, β≈0.63) confirm the hypothesis of constant returns to scale and are consistent with the results from the international literature. The model integrated Dummy variables to capture the structural shocks of 1996 (transition to a market economy) and 2022 (the war in Ukraine and the energy crisis), which had negative effects on productivity. The forecasts for 2025–2026 anticipate moderate GDP growth (2.5% and 3.6%), supported by capital intensity and labor dynamics, but limited by low total factor productivity. The results highlight the importance of investments in infrastructure, digitalization, and institutional reforms to strengthen resilience and long-term economic growth.

Keywords: Cobb-Douglas production function, economic model, economic shocks, factors of production

JEL Classification: A2, C5, E6

INTRODUCTION

The Cobb-Douglas function is significant in economics as a mathematical representation of the relationship between inputs (capital and labor) and output, the importance being expressed through the empirical estimation of production relations, its use in the theory of marginal productivity, by contributing to the establishment of the use of statistical techniques (Biddle, 2012). Currently, it is

[1] The article was developed within the framework of Subprogram 030101 "Strengthening the resilience, competitiveness, and sustainability of the economy of the Republic of Moldova in the context of the accession process to the European Union", institutional funding.

widely used both at the macroeconomic (Gamețchi & Solomon, 1998, pp. 348-355) and microeconomic levels ((Iacob & Dumitru, 2020) (Gamețchi & Solomon, 1998, pp. 191-210)). The Cobb-Douglas production function is part of complex models for analyzing the national economy at the macroeconomic level (Dobrescu, 2006). It is also used in the process of determining synthetic indicators (Havik, Karel et al., 2014), such as the potential Gross Domestic Product of the Republic of Moldova (Toacă & Tolocico, 2012).

Elements of the production function have been identified in the work of earlier economists, although widespread use of the function began with the explicit presentation by economist Paul Douglas and mathematician Charles Cobb. The first economist who formulated the production function algebraically in 1894 is considered to be Philip Wicksell. In (Velupillai , 1973) is emphasized how Wicksell formulated his production function in 1900–1901, which is identical to the Cobb–Douglas function. However, there is evidence to suggest that Johann von Thünen may have first formulated it in the 1840s (Mishra, 2007). But intensive use of these functions in economic analysis began in the 1930s, when it was first proposed by Charles Cobb and Paul Douglas in their classic work (Cobb & Douglas, 1928). They were the first to use empirical data to construct this model. It has been subjected to harsh criticism (Biddle, 2012), often unfriendly, but also to refinements, which have encouraged the academic community to continue research in this direction. Despite all the initial criticism, Cobb-Douglas regression has become a fundamental tool in economic analysis, influencing both microeconomics and macroeconomics.

The Cobb-Douglas function is significant in economics for several reasons. First of all, it is a formalized representation of economic processes (Cobb & Douglas, 1928), indicating inputs and outputs, creating possibilities for analyzing cause-effect relationships. In fact, this is a statistical tool (Biddle, 2012)that allows quantifying the contributions of inputs to production. Based on the function, the principle is determined according to which payments to production factors are determined by their marginal productivity. At the same time, the function has contributions to economic policy, because the discovery of the relationships between inputs and outputs provides quantitative tools to determine the effects of changes in labor and capital on production. A significant contribution, the Cobb-Douglas production function, had on modern econometrics, which in turn contributed to microeconomic and macroeconomic research. Thus, the Cobb-Douglas function became a cornerstone in economic modeling and empirical analysis. Cobb and Douglas were innovators in applying the LS (Least Squares) Method to economics, advancing empirical research methods.

Estimating a production function for a real economy, whether at the macroeconomic or microeconomic level, remains a challenge, determined by several moments. This has generated and continues to generate discussions. One of the challenges is the quality of statistical information, but even more so what type of information should be included in the factors involved in the function. Another major challenge concerns the theoretical foundations of the function. The most radical in this regard are the Marxist and post-Keynesian schools, arguing that it oversimplifies reality, treats capital incorrectly and ignores the social and institutional relations of production. (Shaikh, 1973) demonstrated that the empirical success of the Cobb-Douglas function is due to its mathematical properties, not its economic validity. The heated discussions regarding the production function known as the "Cambridge capital controversy" had profound implications for economic theory, especially for the use of aggregate production functions and the foundations of neoclassical economics. There are several reasons underlying this controversy, one of which is related to the major difficulties in measuring capital, since capital is heterogeneous (e.g., machines, buildings) and its aggregation into a single measure is problematic. This dispute has exposed fundamental flaws in neoclassical theory. The dispute did not lead to the abandonment of this theory, but it remains a reminder of the limits of an aggregate production function and the need for more robust theoretical foundations.

The formalization of economic processes is a tool that is useful in certain situations, but we must never forget the limits of any mathematical formulations. Socio-economic processes are too complex to be modeled even by the most sophisticated formulas. The multitude of relationships, but also the system effect, is complicated to be taken into account, even by the most complex formulas. However, mathematics (Kurakova, 2023)remains a useful tool in scientific research in the economic field. The mathematical apparatus comes, first of all, to arrange things that are obvious from an economic point of view, and their formalization allows the quantification of relationships that allow experiments to be carried out in laboratory conditions with the aim of determining the consequences of possible decisions. Although mathematics is an exact science, we cannot say the same about economics. In this context, the results of mathematical models used in modeling economic processes cannot be treated as exact, well-determined solutions. The result of a mathematical model can indicate a possible direction of evolution of events in the case of one or another decision. Often decisions, which are supported by an analysis based on formalized models, are less surprising. (Jacobs, 2023) mentions “a mathematical model should be the beginning of a dialogue, not the end”. This paper also mentions the excessive use of mathematical models in the decision-making process. The use of mathematical models requires a thorough understanding of the limitations, because a mathematical model is “a mathematical view of a phenomenon”. In conclusion, mathematical modeling (Kurakova, 2023)is an important tool in decision-making in various fields of activity, but it must be used with caution. It helps to analyze complex systems and processes, find optimal decisions and predict results. To achieve maximum efficiency, it is necessary to choose the right methods and algorithms, as well as to have a sufficient amount of data for analysis. The importance of mathematical modeling and the exchange of experience is actively discussed (Tasarib, Rosli, & Rambely, 2025). The problem is that there is increasingly a reluctance towards mathematics (Nourallah & Farzad, 2012) and one of the methods would be to learn mathematics simultaneously with mathematical modeling, which would contribute to understanding the need for its use in the real field.

The purpose of this study is both didactic and practical, aiming at the use of the Cobb-Douglas production function in the analysis of economic processes, including forecasting. In the process of estimating the function, all the stages of econometric analysis specific to trend data were covered and described. This can be useful both for students of deeper analyses in mathematical modeling disciplines, and for researchers, whose goal is economic analysis.

THE GENERAL FORM OF THE COBB-DOUGLAS PRODUCTION FUNCTION

The general form of the Cobb-Douglas production function is

$$Y = A * K^{\alpha} * L^{\beta} \tag{1}$$

To estimate this model using LS method, linearization by logarithm is required. In the specialized literature, logarithmization is done by natural logarithm. This is just a convention, in reality any other logarithm can be used, but the natural logarithm is easy to explain economically, namely the estimated coefficients are elasticity coefficients, used quite often in economic analyses. Given the uniformity in the specialized literature, after logarithmic transformation, (1) becomes:

$$\log[2](Y) = \log(A) + \alpha * \log(K) + \beta * \log(L) \tag{2}$$

In case if the hypothesis $\alpha + \beta = 1$, then the Cobb-Douglas function has the form:

$$Y = A * K^{\alpha} * L^{1-\alpha} \tag{3}$$

To estimate the parameters of this function, the following logarithmic form is used:

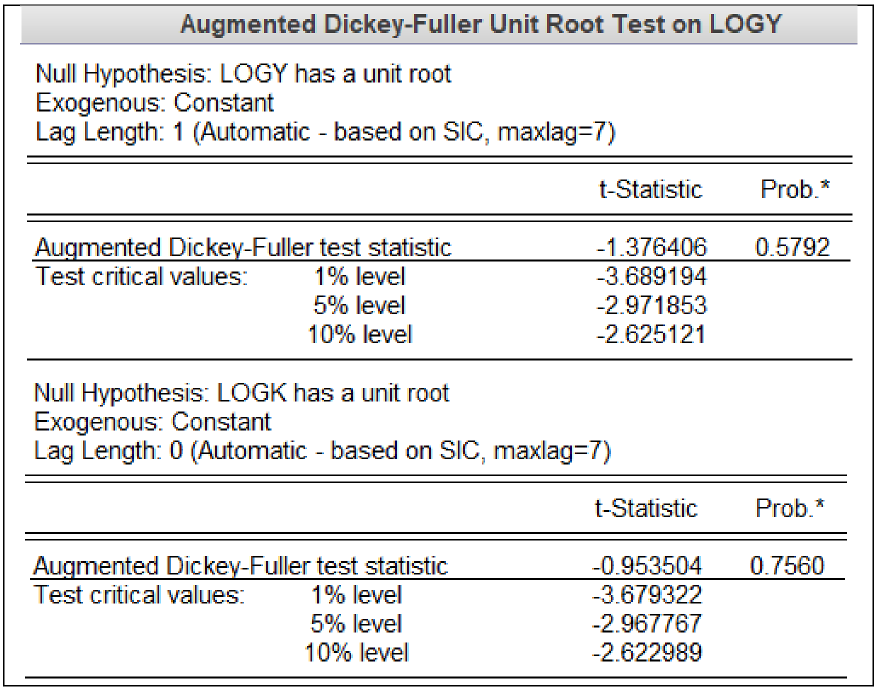
$$\log(Y/L) = \log(A) + \alpha * \log(K/L) \tag{4}$$

Next, regressions in the form of (2) or (4) are tested based on the annual statistical information of the Republic of Moldova for the period 1994-2024. The sample includes 29 observations, which allows validating the application of all statistical tests used in the estimation process. Statistical information is taken from the website statistica.md. Production values, i.e. Y is the Gross Domestic Product, K- gross fixed capital formation, and labor (L) was calculated as the average number of employees multiplied by the average wage in the economy. The factors are time trends, which implies the need to verify the stationarity of the series, in order to avoid spurious estimates and to ensure the validity of the obtained econometric relationships.

TESTING THE STATIONARITY OF SERIES

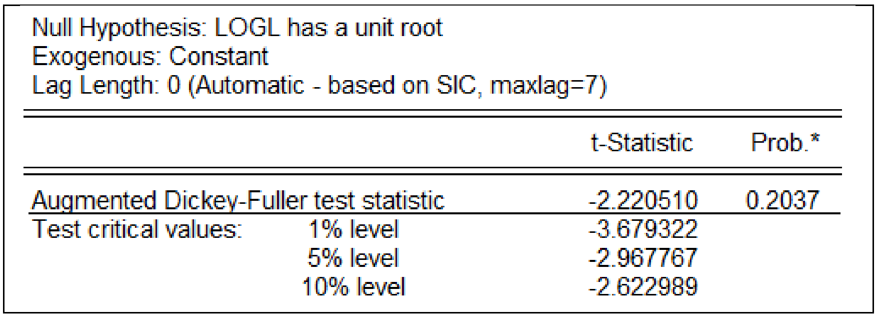
The stationarity of the data series was tested using the Phillips-Perron ((Phillips & Perron, 1988)) and Augmented Dickey-Fuller ((Dickey & Fuller, 1979), (Dickey & Fuller, 1981)) tests. The general form of the tests was presented in (Toaca , Staver , Stratan , Lopotenco , & Cociug , 2025). Stationarity tests applied to time series indicate that level series, including logarithmic ones, are not stationary (Table 1).

Table 1Stationarity testing of logarithmic series.



```
Augmented Dickey-Fuller Unit Root Test on LOGY

Null Hypothesis: LOGY has a unit root
Exogenous: Constant
Lag Length: 1 (Automatic - based on SIC, maxlag=7)

                                              t-Statistic    Prob.*

Augmented Dickey-Fuller test statistic        -1.376406     0.5792
Test critical values:        1% level         -3.689194
                             5% level         -2.971853
                            10% level         -2.625121

Null Hypothesis: LOGK has a unit root
Exogenous: Constant
Lag Length: 0 (Automatic - based on SIC, maxlag=7)

                                              t-Statistic    Prob.*

Augmented Dickey-Fuller test statistic        -0.953504     0.7560
Test critical values:        1% level         -3.679322
                             5% level         -2.967767
                            10% level         -2.622989
```

[2] The log notation was used instead of ln, since in the econometric software EViews the natural logarithm is notated in this way.

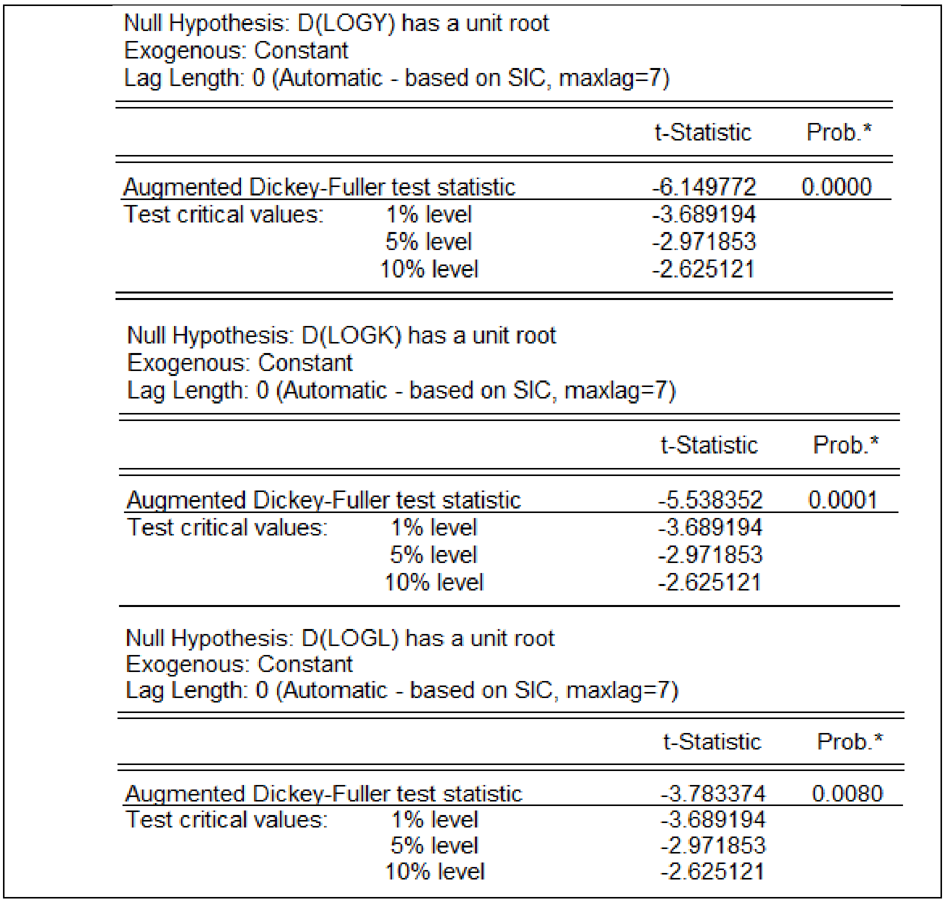


```
Null Hypothesis: LOGL has a unit root
Exogenous: Constant
Lag Length: 0 (Automatic - based on SIC, maxlag=7)

                                              t-Statistic    Prob.*

Augmented Dickey-Fuller test statistic        -2.220510      0.2037
Test critical values:        1% level         -3.679322
                             5% level         -2.967767
                             10% level        -2.622989
```

Source: *Econometric estimation results generated using EViews software.*

The differences of order 1 become stationary (Table 2), which means that the series are integrated of order 1 (I(1)).

Table 2Stationarity testing of differenced logarithmic series.



```
Null Hypothesis: D(LOGY) has a unit root
Exogenous: Constant
Lag Length: 0 (Automatic - based on SIC, maxlag=7)

                                              t-Statistic    Prob.*

Augmented Dickey-Fuller test statistic        -6.149772      0.0000
Test critical values:        1% level         -3.689194
                             5% level         -2.971853
                             10% level        -2.625121

Null Hypothesis: D(LOGK) has a unit root
Exogenous: Constant
Lag Length: 0 (Automatic - based on SIC, maxlag=7)

                                              t-Statistic    Prob.*

Augmented Dickey-Fuller test statistic        -5.538352      0.0001
Test critical values:        1% level         -3.689194
                             5% level         -2.971853
                             10% level        -2.625121

Null Hypothesis: D(LOGL) has a unit root
Exogenous: Constant
Lag Length: 0 (Automatic - based on SIC, maxlag=7)

                                              t-Statistic    Prob.*

Augmented Dickey-Fuller test statistic        -3.783374      0.0080
Test critical values:        1% level         -3.689194
                             5% level         -2.971853
                             10% level        -2.625121
```

Source: *Econometric estimation results generated using EViews software.*

REGRESSION ESTIMATION

The Cobb-Douglas function was estimated by LS method using EViews software. Obtaining a plausible regression involved several attempts with repeated verification of the tests confirming the statistical quality, respectively the compliance with the basic hypotheses. As a result, the regression presented in Figure 1 was obtained. Notations used in regression:

- *DLOG(K/L)* - first-order differences of the natural logarithm of the *Capital* to *Labor ratio;*
- *DLOG(Y/L)* - first-order differences of the natural logarithm of the *Output* to *Labor ratio;*

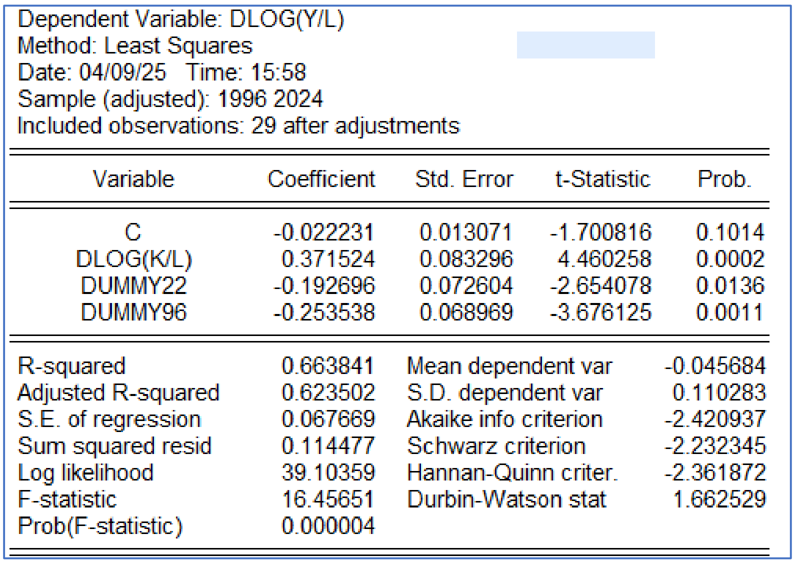
- DUMMY96 - A binary variable that will capture the shock of the transition from the Soviet to the market economy:

$$DUMMY96 = \begin{cases} 1, for\ the\ year\ 1996 \\ 0, for\ the\ other\ years \end{cases}$$

- DUMMY22 - A binary variable that will capture the shock in 2022 (war in Ukraine, energy crisis, etc.)

$$DUMMY22 = \begin{cases} 1, for\ the\ year\ 2022 \\ 0, for\ the\ other\ years \end{cases}$$

According to the student statistic, all variables are significant.



```
Dependent Variable: DLOG(Y/L)
Method: Least Squares
Date: 04/09/25   Time: 15:58
Sample (adjusted): 1996 2024
Included observations: 29 after adjustments
==========================================================================
         Variable        Coefficient    Std. Error    t-Statistic    Prob.
==========================================================================
            C             -0.022231     0.013071      -1.700816     0.1014
         DLOG(K/L)         0.371524     0.083296       4.460258     0.0002
         DUMMY22          -0.192696     0.072604      -2.654078     0.0136
         DUMMY96          -0.253538     0.068969      -3.676125     0.0011
==========================================================================
R-squared                  0.663841    Mean dependent var       -0.045684
Adjusted R-squared         0.623502    S.D. dependent var        0.110283
S.E. of regression         0.067669    Akaike info criterion    -2.420937
Sum squared resid          0.114477    Schwarz criterion        -2.232345
Log likelihood             39.10359    Hannan-Quinn criter.     -2.361872
F-statistic                16.45651    Durbin-Watson stat        1.662529
Prob(F-statistic)          0.000004
==========================================================================
```

Figure 1. Estimated model.

Source: *Econometric estimation results generated using EViews software.*

Multiple linear regression looks like this:

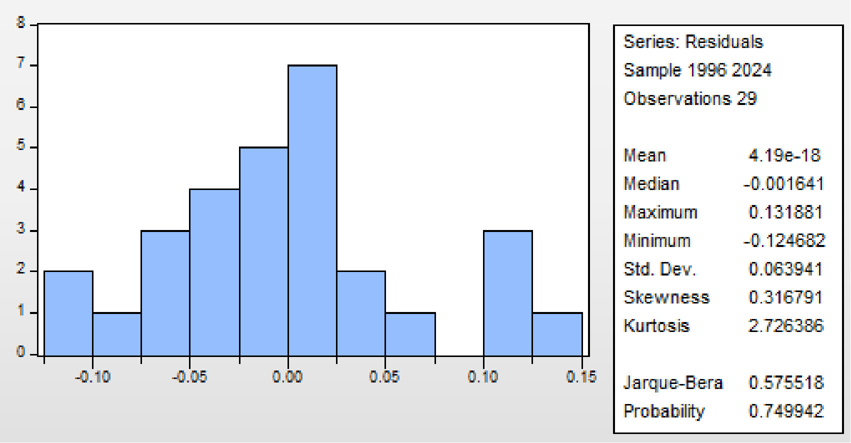
$$\mathrm{DLOG}\left(\frac{Y}{L}\right) = -0{,}022 + 0{,}37\ DLOG\ \left(\frac{K}{L}\right) - 0{,}19\ DUMMY22 - 0{,}25DUMMY96 \qquad (2)$$

The obtained regression confirms the hypothesis α+β=1, where α=0.37, β=0.63. The obtained results are reasonable and correspond to the research carried out in this direction. If in the classical model values of approximately (Cobb & Douglas, 1928) α=0.25, β=0.75 were obtained, then in subsequent research they vary: the coefficient α between 0.20 and 0.40, and the coefficient β between 0.60 and 0.80. In the methodology of the European Commission ((Havik, Karel et al., 2014), (Streicher, 2022)) for the calculation of potential GDP, the values α=0.35, β=0.65 are proposed. For OECD countries (Organization for Economic Cooperation and Development) whose members are high-income states, (Charles, 2003) it is documented that the share of capital is in the range of 0.3-0.4. Many economic models assume that the share of labor must be constant in time and space. Time series data are consistent with this notion, while analysis of international cross-sectional data (Douglas, 2002)demonstrates that the labor share varies between 0.60 and 0.80.

If the sum of the coefficients is 1, the function is considered to have constant returns to scale, in other words, if we multiply all the factors of production, then the output multiplies by exactly the same proportion. The economic meaning of the variables included in the model: the dependent variable is Y/L - labor productivity, which depends on K/L - capital per worker (capital intensity). The capital-labor ratio (K/L) measures capital intensity. Typically, over time, firms tend to have a higher capital-labor ratio, as they try to obtain productivity improvements from capital investments and automation of the production process.

Testing fundamental statistical hypotheses.

Normality of the residuals. The distribution of the residuals is bell-shaped, centered on zero, with no strongly deviated values.



Series: Residuals
Sample 1996 2024
Observations 29

Mean	4.19e-18
Median	-0.001641
Maximum	0.131881
Minimum	-0.124682
Std. Dev.	0.063941
Skewness	0.316791
Kurtosis	2.726386
Jarque-Bera	0.575518
Probability	0.749942

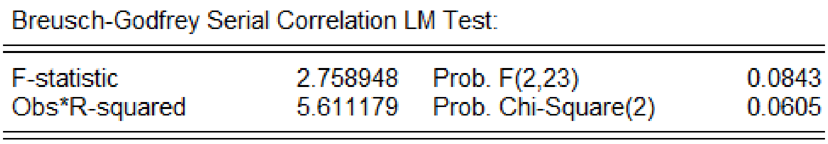
Figure 2. Testing the normality of the residuals.

Source: *Econometric estimation results generated using EViews software.*

Based on the information in Figure 2 we obtain:

- Average – $4{,}19 * 10^{-18}$, close to zero, largest residual – 0,13; smallest – $(-0{,}12)$.
- Negative skewness (slight leftward skew)
- Kurtosis – 2.72 – close to 3, demonstrates an almost normal distribution.
- The Jarque-Bera index of 0.575 and the probabilityof 0.7499 suggest that there is no significant evidence to reject the hypothesis of normality of the residuals. A probability greater than 0.05 indicates that the residuals are normally distributed, which confirms the validity of the regression model assumptions.

Autocorrelation of Errors. The Breusch-Godfrey Serial Correlation LM test checks whether the regression residuals are autocorrelated (a key assumption for valid LS method inference). We cannot reject the null hypothesis of no serial correlation at 10%, but there is slight evidence of autocorrelation at 5%.



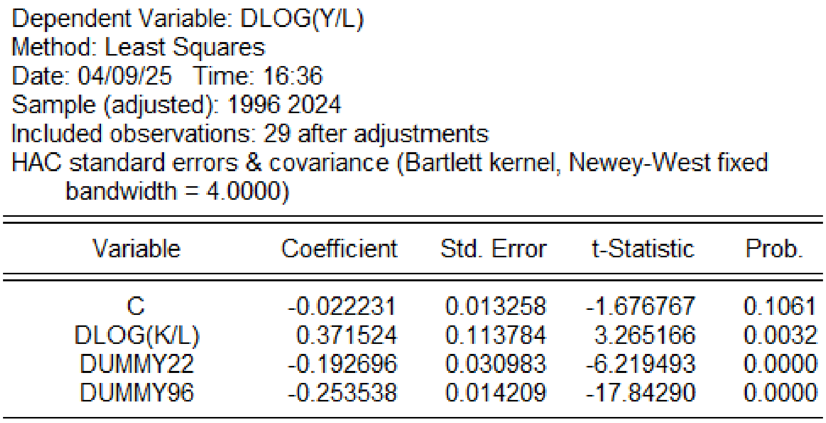
Breusch-Godfrey Serial Correlation LM Test:

F-statistic	2.758948	Prob. F(2,23)	0.0843
Obs*R-squared	5.611179	Prob. Chi-Square(2)	0.0605

Figure 3. for error autocorrelation using the Breush-Godfrey test.

Source: *Econometric estimation results generated using EViews software.*

Autocorrelation correction can be performed by recalculating standard errors using the HAC (Heteroskedasticity and Autocorrelation Consistent) method. For this purpose (Figure 4), the Newey-West method was used.

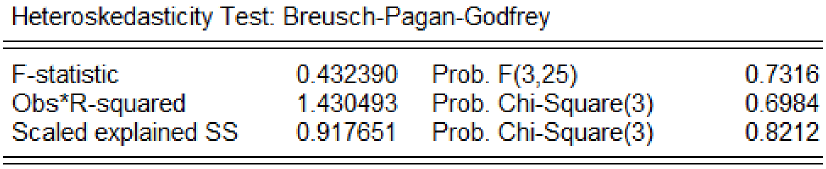


```
Dependent Variable: DLOG(Y/L)
Method: Least Squares
Date: 04/09/25   Time: 16:36
Sample (adjusted): 1996 2024
Included observations: 29 after adjustments
HAC standard errors & covariance (Bartlett kernel, Newey-West fixed
        bandwidth = 4.0000)

      Variable        Coefficient    Std. Error    t-Statistic     Prob.

         C            -0.022231      0.013258     -1.676767      0.1061
      DLOG(K/L)        0.371524      0.113784      3.265166      0.0032
      DUMMY22         -0.192696      0.030983     -6.219493      0.0000
      DUMMY96         -0.253538      0.014209     -17.84290      0.0000
```

Figure 4. Re-estimation of the regression in which the standard errors were corrected by the Newey–West method.
Source: *Econometric estimation results generated using EViews software.*

The presence of autocorrelation of errors may affect the significance of exogenous factors. However, re-estimation of the regression demonstrated the significant influence of the factors included in the model on labor productivity (Figure 4).

Homoscedasticity of errors. The Breusch-Pagan-Godfrey test for heteroscedasticity shows that the hypothesis of the presence of heteroscedasticity can be rejected, having F-statistic – 0.43, p – 0.7316.



```
Heteroskedasticity Test: Breusch-Pagan-Godfrey

F-statistic            0.432390    Prob. F(3,25)            0.7316
Obs*R-squared          1.430493    Prob. Chi-Square(3)      0.6984
Scaled explained SS    0.917651    Prob. Chi-Square(3)      0.8212
```

Figure 5. Testing for homoscedasticity of errors using the Breush-Pagan-Godfrey test.
Source: *Econometric estimation results generated using EViews software.*

Finally:

- Capital intensity per worker significantly improves productivity;
- Structural shocks (1996, 2022) are captured and are significant;
- The model is homoscedastic;
- The residuals are well distributed (normality is maintained);
- Autocorrelation was corrected by HAC.

Interpretation of the results obtained:

1) Consistent economic theory: The obtained model is based on the logic of the Cobb-Douglas production function, for the case when α+β=1.

2) The coefficient DLOG(K/L) (~0.37) is reasonable (Figure 1) and consistent with theory and estimates from other countries.

3) The dummy variables capture the institutional and geopolitical shocks that Moldova faced in 1996 and 2022.

4) The model explains 66.38% of the production variation ($R^2 = 0.6638$), which confirms the correct specification of the model.

5) The F-statistic value is 16.45 with a probability of 0.0000, confirming that the model is significant overall.

ANALYSIS OF THE EVOLUTION OF THE NATIONAL ECONOMY BASED ON THE OBTAINED MODEL

Productivity increases mainly through capital intensity. An one percent increase in capital intensity per worker is associated with a 0.37% increase in labor productivity. This finding confirms the importance of investments in infrastructure, machinery, and technology for increasing productivity. Total factor productivity (TPF) growth (c=-0.022) is low, indicating the need for institutional and structural reforms. The estimated average TPF growth is slightly negative over the period, suggesting structural inefficiencies unrelated to capital or labor accumulation. This highlights the need for institutional reforms, technological adoption, and alignment of the education system with labor market needs.

Moldova's economy remains sensitive to shocks – energy and regional risk mitigation are essential:

1) 1996: Productivity fell by ~25%, reflecting deep disruptions during the post-Soviet economic transition.

2) 2022: There was a ~19% drop in productivity, likely caused by the war in Ukraine, the energy crisis, and supply chain disruptions.

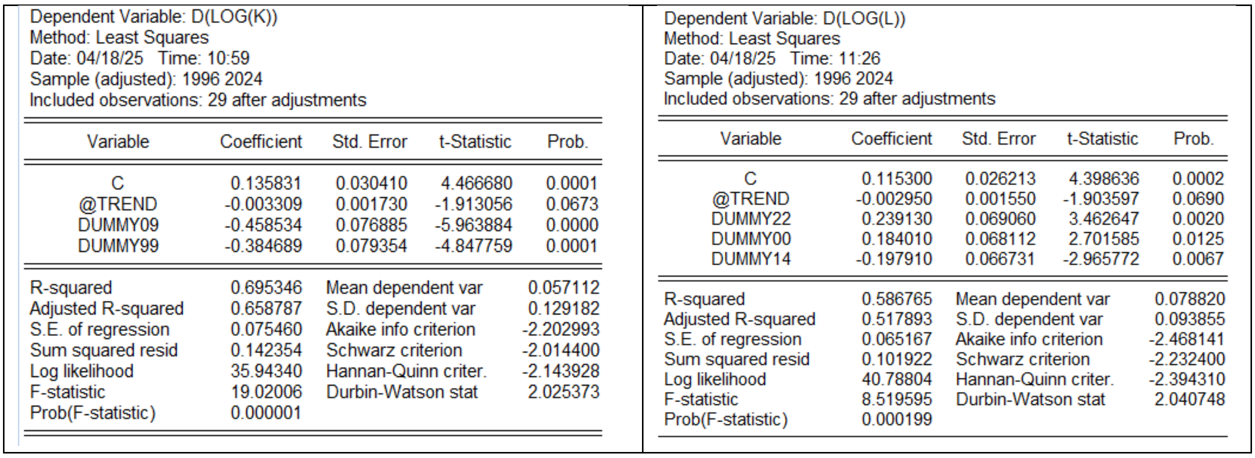
Based on the obtained model, political implications can be proposed for improving the economic situation of the Republic of Moldova. In fact, the proposals made are known and are largely the main objectives of the current leadership. It can be noted that some of them are on the way to being realized. One of the proposals is to support and expand public and private investments to maintain the deepening of capital. This is the direction in which we need to work, but it is necessary to mention that geopolitical conditions continue to be an obstacle in this direction.

Another problem is the increase in TFP. Improving education and vocational training further is one of the factors through which TFP growth can be achieved. Dual education can be a support in this direction. The Government of the Republic of Moldova creates conditions for the opening of new SMEs (Small and Medium Enterprises). SMEs implement new technologies and digitize the production process by accessing projects. The public sector has a special importance in this direction. It is necessary to improve the efficiency of the public sector and institutional quality.

Another direction is to strengthen economic resilience to shocks, which can be achieved by diversifying trade and energy sources. These are actions successfully implemented by the Moldovan government, the benefits of which will be visible in the long term.

ECONOMIC FORECAST

The estimated model can be used for the forecast of the GDP of the Republic of Moldova. As an initial stage in this process, it is necessary to estimate the dynamics of capital and labor. The forecast was carried out based on the trends (Figure 6) of the 1st order differences of the logarithmic series, which were found to be stationary series.



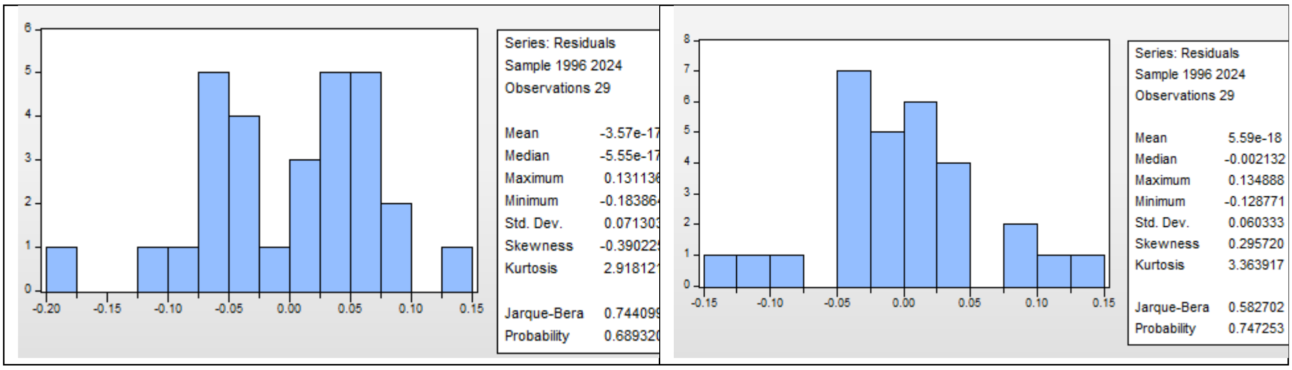
```
Dependent Variable: D(LOG(K))
Method: Least Squares
Date: 04/18/25   Time: 10:59
Sample (adjusted): 1996 2024
Included observations: 29 after adjustments

    Variable        Coefficient   Std. Error   t-Statistic    Prob.

       C             0.135831     0.030410     4.466680      0.0001
    @TREND          -0.003309     0.001730    -1.913056      0.0673
    DUMMY09         -0.458534     0.076885    -5.963884      0.0000
    DUMMY99         -0.384689     0.079354    -4.847759      0.0001

R-squared            0.695346    Mean dependent var      0.057112
Adjusted R-squared   0.658787    S.D. dependent var      0.129182
S.E. of regression   0.075460    Akaike info criterion  -2.202993
Sum squared resid    0.142354    Schwarz criterion      -2.014400
Log likelihood       35.94340    Hannan-Quinn criter.   -2.143928
F-statistic          19.02006    Durbin-Watson stat      2.025373
Prob(F-statistic)    0.000001
```

```
Dependent Variable: D(LOG(L))
Method: Least Squares
Date: 04/18/25   Time: 11:26
Sample (adjusted): 1996 2024
Included observations: 29 after adjustments

    Variable        Coefficient   Std. Error   t-Statistic    Prob.

       C             0.115300     0.026213     4.398636      0.0002
    @TREND          -0.002950     0.001550    -1.903597      0.0690
    DUMMY22          0.239130     0.069060     3.462647      0.0020
    DUMMY00          0.184010     0.068112     2.701585      0.0125
    DUMMY14         -0.197910     0.066731    -2.965772      0.0067

R-squared            0.586765    Mean dependent var      0.078820
Adjusted R-squared   0.517893    S.D. dependent var      0.093855
S.E. of regression   0.065167    Akaike info criterion  -2.468141
Sum squared resid    0.101922    Schwarz criterion      -2.232400
Log likelihood       40.78804    Hannan-Quinn criter.   -2.394310
F-statistic          8.519595    Durbin-Watson stat      2.040748
Prob(F-statistic)    0.000199
```

Figure 6. Trends for the time series D(LOG(K)) and D(LOG(L)).

Source: *Econometric estimation results generated using EViews software.*

The definition of the Dummy variables is analogous to the definition in regression (3). The factors included in the trend, according to *the Student statistic*, are significant. The residuals have an almost normal distribution, without visible outliers or strong asymmetries (Figure 7).



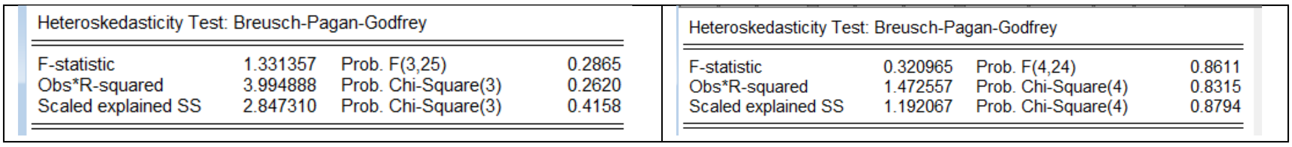
```
Series: Residuals
Sample 1996 2024
Observations 29

Mean         -3.57e-17
Median       -5.55e-17
Maximum       0.131136
Minimum      -0.183864
Std. Dev.     0.071303
Skewness     -0.390225
Kurtosis      2.918121

Jarque-Bera   0.744099
Probability   0.689320
```

```
Series: Residuals
Sample 1996 2024
Observations 29

Mean          5.59e-18
Median       -0.002132
Maximum       0.134888
Minimum      -0.128771
Std. Dev.     0.060333
Skewness      0.295720
Kurtosis      3.363917

Jarque-Bera   0.582702
Probability   0.747253
```

Figure 7. Checking the normality of the residuals for the trend a) D(LOG(K)) and b) D(LOG(L)) respectively.

Source: *Econometric estimation results generated using EViews software.*

Homoscedasticity of the residuals There is no evidence of heteroscedasticity in the developed models ($p > 0.05$ in all tests). The residuals have constant variance, it follows that the hypothesis of homoscedasticity cannot be rejected.



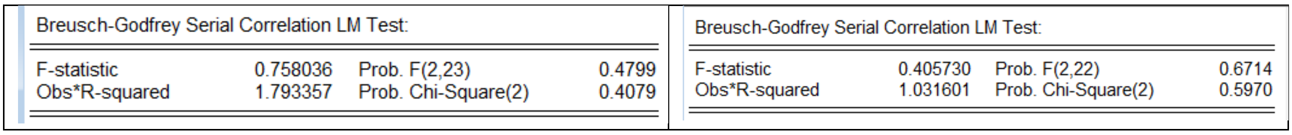
```
Heteroskedasticity Test: Breusch-Pagan-Godfrey

F-statistic           1.331357    Prob. F(3,25)          0.2865
Obs*R-squared         3.994888    Prob. Chi-Square(3)    0.2620
Scaled explained SS   2.847310    Prob. Chi-Square(3)    0.4158
```

```
Heteroskedasticity Test: Breusch-Pagan-Godfrey

F-statistic           0.320965    Prob. F(4,24)          0.8611
Obs*R-squared         1.472557    Prob. Chi-Square(4)    0.8315
Scaled explained SS   1.192067    Prob. Chi-Square(4)    0.8794
```

Figure 8. Testing the homoscedasticity of errors in the developed models using the Breush-Pagan-Godfrey test.

Source: *Econometric estimation results generated using EViews software.*

Autocorrelation of errors. There is no autocorrelation of the residuals up to lag 2 and the model without AR terms can be retained, and the estimates are statistically valid.



```
Breusch-Godfrey Serial Correlation LM Test:

F-statistic          0.758036    Prob. F(2,23)            0.4799
Obs*R-squared        1.793357    Prob. Chi-Square(2)      0.4079
```

```
Breusch-Godfrey Serial Correlation LM Test:

F-statistic          0.405730    Prob. F(2,22)            0.6714
Obs*R-squared        1.031601    Prob. Chi-Square(2)      0.5970
```

Figure 9. Testing the normality of residuals.

Source: *Econometric estimation results generated using EViews software.*

The macroeconomic forecast for the period 2025–2026 outlines a moderate recovery trajectory for the Republic of Moldova's economy. According to the developed scenario, gross domestic product is expected to register an annual growth of 2.5% in 2025 and 3.6% in 2026, signaling a gradual consolidation of economic activity. At the same time, the labor force is estimated to continue expanding, with rates of 2.7% and 2.4% in the same period, after a significant acceleration in previous years. The capital stock, an essential indicator for supporting investments and productivity, returns to a positive trend, with an estimated growth of 3.7% in 2025 and 3.4% in 2026. These dynamic highlights the importance of maintaining productive investments and implementing structural reforms, in order to improve the efficiency of the use of production factors and consolidate economic growth in the medium and long term.

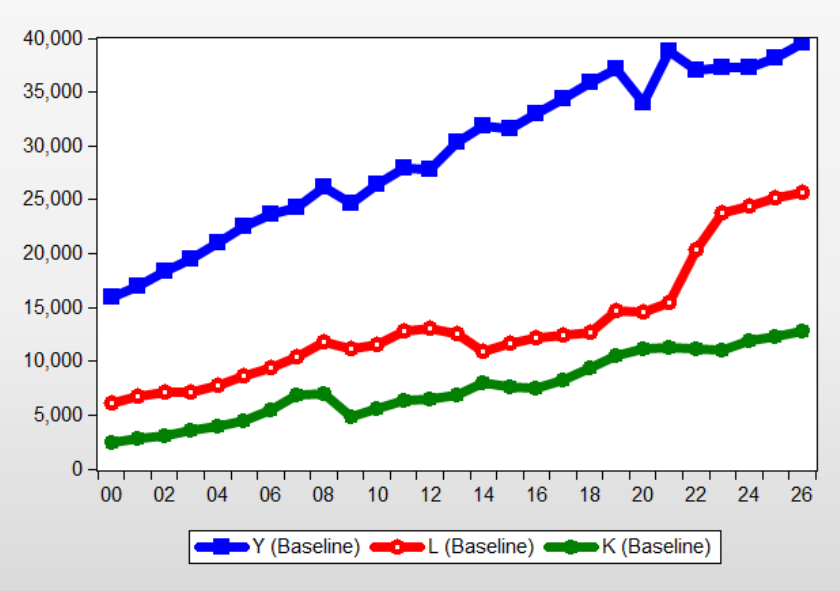


Figure 10. Evolution of Capital, Labor and Production.

Source: *Econometric estimation results generated using EViews software.*

Figure 11 showing the evolution of labor productivity (Y/L) and capital intensity (K/L) in the Republic of Moldova over the period 1996–2026 highlights fundamental economic relationships. After a sharp decline in productivity during the post-Soviet transition years, Y/L has stabilized, but at a low level and vulnerable to external shocks, such as the pandemic crisis and the war in Ukraine.

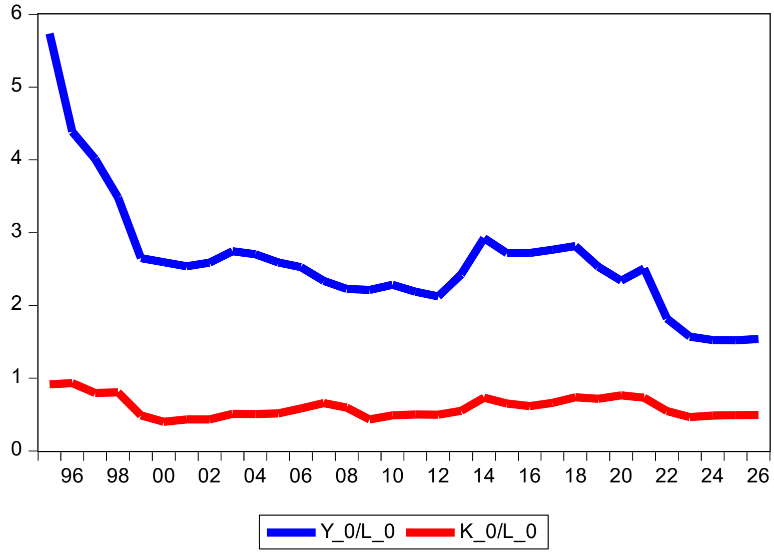


Figure 11. Evolution of labor productivity and capital intensity.
Source: *Econometric estimation results generated using EViews software.*

In parallel, K/L has recorded a relatively flat evolution, with slight increases between 2010 and 2018, followed by stagnation. This dynamic suggests an insufficient deepening of capital, which limits the potential for labor productivity growth. The relatively close correlation between the two series after 2010 confirms the significant role of capital in determining labor productivity in Moldova, and the stagnation of both indicates the need for structural reforms to stimulate investment and increase economic efficiency.

CONCLUSION

The research conducted confirms the validity of using the Cobb-Douglas production function in analyzing the evolution of the national economy. The econometric results obtained confirm the hypothesis of equality of the sum of the regression coefficients to one, which means that the economy has constant returns to scale. The estimated coefficient (0.37) is coherent with international literature and economic theory. By including Dummy variables, it was possible to capture the external shocks to which the national economy was subjected. The shocks led to a decrease in productivity, which confirms the vulnerability of the RM economy. This result once again indicates the need for policies that will strengthen the resilience of the national economy. The economic evolution of the Republic of Moldova depends particularly on capital accumulation and reforms that support productivity growth. The reforms needed in this direction are new technologies, digitalization of the national economy, development of human capital through education, vocational training and lifelong learning. This model provides a solid empirical basis for planning long-term growth policy.

REFERENCES

1. Biddle, J. (2012). Retrospectives: The Introduction of the Cobb–Douglas Regression. *Journal of Economic Perspectives, 26* , 223-236. Retrieved from https://pubs.aeaweb.org/doi/pdfplus/10.1257/jep.26.2.223
2. Charles, I. (2003). *Growth, Capital Shares, and a New Perspective on Production Functions.* Department of Economics, UC Berkeley and NBER. Retrieved from https://web.stanford.edu/~chadj/alpha100.pdf

3. Cobb, C., & Douglas, P. (1928). A Theory of Production. *The American Economic Review, 1* (Supplement, Papers and Proceedings of the Fortieth Annual Meeting of the American Economic Association), 139-165. Retrieved from http://digamo.free.fr/cobbdoug28.pdf
4. Dickey, D., & Fuller, W. (1979). Distribution of estimators for autoregressive time series with a unit root., . *Journal of the American Statistical Association 74 (366a)* , 427–431. doi:https://doi.org/10.1080/01621459.1979.10482531
5. Dickey, D., & Fuller, W. (1981). Likelihood ratio statistics for autoregressive time series with a unit root.. *Econometrica, 49(4),* , 1057-1072. doi: https://doi.org/10.2307/1912517
6. Dobrescu, E. (2006). *Macromodels of the Romanian Market Economy.* Bucharest: ed. Economica.
7. Douglas, G. (2002). Getting Income Shares Right. *Journal of Political Economy, University of Chicago Press, vol 110(2),* , 458-474.
8. Gamețchi, A., & Solomon, D. (1998). *Mathematical Modeling of Economic Processes.* Chisinau: Evrica.
9. Havik, Karel et al. (2014). *The Production Function Methodology for Calculating Potential Growth Rates & Output Gaps* (Vol. Economic Papers 535). Brussels, Belgium: European Commission.
10. Iacob, Ș. V., & Dumitru, D. (2020). The production function used in microeconomic analysis studies. *Romanian Statistical Review* , pg. 136-149. Retrieved from /www.revistadestatistica.ro/supliment/wp-content/uploads/2020/07/rrss_07_2020_a5_ro.pdf
11. Jacobs, M. (2023). The importance of applying mathematical models in decision making: a plea for dialogue and common sense. Retrieved from https://medium.com/@marc.jacobs012/the-importance-of-applying-mathematical-models-in-decision-making-a-plea-for-dialogue-and-common-45d714cd7515
12. Kurakova, O. (2023). Methodological aspects of applying. *E3S Web of Conferences 389, 03111* . doi:https://doi.org/10.1051/e3sconf/202338903111
13. Mishra, S. (2007). A Brief History of Production Functions. *MPR Munich Personal RePEc Archive* . Retrieved from https://mpra.ub.uni-muenchen.de/5254/1/MPRA_paper_5254.pdf
14. Nourallah, N., & Farzad, B. (2012). Mathematical modeling in university, advantages and challenges. *Journal of Mathematical Modeling and Application* , 34-49. Retrieved from https://scispace.com/pdf/mathematical-modelling-in-university-advantages-and-37yxwe0f60.pdf
15. Phillips, P., & Perron, P. (1988). Testing for a Unit Root in Time Series Regression. *Biometrika, 75(2)* , 335-346. doi:https://doi.org/10.1093/biomet/75.2.335
16. Shaikh, A. (1973). Laws of Production and Laws of Algebra—Humbug II. *Growth, Profits and Property (ed.) Nell. EJ, Cambridge Univ. Press, Cambridge* . Retrieved from e http://homepage.newschool.edu/~AShaikh/humbug.pdf
17. Streicher, S. (2022). *RGAP: Output Gap Estimation in R.* (KS Institute, Ed.) Zurich: KOF Working Papers 503.
18. Tasarib, A., Rosli, R., & Rambely, AS (2025). Impacts and challenges of mathematical modeling activities on students' learning development: A systematic literature review. *Modestum, EURASIA Journal of Mathematics, Science and Technology Education* . doi:https://doi.org/10.29333/ejmste/16398
19. Toaca, Z., Staver, L., Stratan, A., Lopotenco, V., & Cociug, V. (2025). Forecasting Moldova's monthly exports using autoregressive models with seasonal dummies. . *Cogent Business & Management* . doi:10.1080/23311975.2025.2519988.
20. Toacă, Z., & Tolocico, L. (2012). Estimating the potential Gross Domestic Product of the national economy of the Republic of Moldova. *Competitiveness and innovation in the knowledge economy* (pp. 23-28). Chisinau: ASEM.
21. Velupillai, K. (1973). The Cobb-Douglas or the Wicksell Function? - A Comment,. *Economy and History* , 111-113.

THE ROLE OF AI IN CREATING FALSE REALITIES TO MANIPULATE THE MASSES

UDC: [004.8+004.932]:32.019.5(478)
DOI: https://doi.org/10.53486/tids2025.20

VICTORIA LOZAN
PhD, Associate Professor
Academy of Economics Studies of Moldova
lozan.victoria@ase.md
ORCID ID: 0000-0002-5869-8515

ION COSTIN
IT Engineer
Vocational School from Soroca, Republic of Moldova
ioncostyn1@gmail.com
ORCID ID: 0009-0008-4540-3256

Abstract. Recently, products based on Artificial Intelligence (AI) technology have been used to create photo and video content aimed at influencing public opinion, especially during election periods. Alongside healthy use for enhancing creativity in the film industry, advertising, or journalism, offering new possibilities for artistic expression, and creating personalized content tailored to the specific needs of different audiences, AI platforms are also being used to generate content designed to influence public opinion. This is an extremely relevant and complex issue that raises numerous ethical, social, and political questions. Content creation platforms are being used to spread conspiracy theories, damage people's reputations, or manipulate electoral outcomes. In some cases, the falsified content is difficult to detect. Deep fakes can create scenes or false statements that appear authentic, which can lead to the spread of misinformation. AI-generated content can be used to amplify certain messages or ideologies, reinforcing social and political divisions. It is essential that the public is informed about the existence of these technologies and educated on critically evaluating the content they consume. Scientists and tech companies are working on developing algorithms capable of detecting AI-generated fake content. Dedicated tools, relying on complex algorithms, are used to create deep fakes. As the technology for generating fake content becomes more advanced, it becomes increasingly difficult for the public to distinguish between reality and fiction. Another dilemma is accessibility; as AI technology becomes more accessible, the costs of generating fake content will decrease, and the ability to produce such materials will become available to an ever-growing number of individuals. The purpose of this paper is to analyze AI-generated content (wefaceswap.com) and determine the aspects that define the fictitious nature of the material. While AI offers enormous opportunities for innovation and creativity, it also comes with significant risks related to misinformation, manipulation, and the erosion of trust in the media.

Keywords: Artificial Intelligence, deepfake, content, fiction, reality, manipulation, polarization.

JEL Classification: C80, C88, C92, O33, O36.

INTRODUCTION

The rapid development, over the last decade, of technology based on artificial intelligence and its implementation in various fields has substantially facilitated human activity. The use of modern technologies reduces the time required to complete certain activities, improving the final result. Technologies based on artificial intelligence are used in transport management (Abirami, *et al.*, 2024), enabling traffic flow forecasting, enabling congestion management and intelligent routing, increasing efficiency in various facets of modern transportation systems. Due to its potential to improve functionality, decision-making, and efficiency, AI is used in Internet of Things systems (Khadam, *et al.*, 2024). The technology also makes a considerable contribution to software-based industrial networks, smart manufacturing, logistics, supply chains, construction and 5G/6G networks (Rojas, *et al.*, 2024). AI-based methods are implemented for software development and testing (Amalfitino, et al., 2023) and in engineering (Martínez-Fernández, Bogner and Franch). AI-based methodologies, algorithms, data sources, results, diagnoses are also applied in the medical field (Martinez-Millana, et al., 2022). AI-based technologies are also being implemented in self-driving vehicles, multimedia recognition, cybersecurity, space exploration, genetics, climate change, agriculture (Goel, *et al.*, 2023). AI is also being implemented in wireless drone networks for trajectory optimization, radio resource management, routing and topology control, edge and cache calculation, and improved security and privacy. (Zhou, *et al.*, 2024).

A valuable use of artificial intelligence technology is seen in the creative industry, where it enables content generation, information analysis, optimization of materials and post-production workflows, as well as efficient data extraction, enhancement and compression (Anantrasirichai & Bull, 2022).

This paper analyzes existing platforms for creating deepfakes, the way such content is created, and the impact of the spread of these products.

DEEPFAKE PRODUCTS AND MASS MANIPULATION

1. Deepfake generation applications

Deepfake technologies allow users to create convincing images and videos, generated by artificial intelligence, that mimic the appearance, sound, and mannerisms of real people. Currently, there is a wide range of platforms that allow the creation of deepfakes and any user is able to use them to create different projects, even to generate fake video or audio content. No advanced knowledge is required, just select the required platform, subscription type and device hardware configuration to ensure efficient running of the web application. Of course, desktop applications are also available. A description of the most popular platforms for creating deepfake can be found on (Taylor, 2025). The paper will analyze the possibilities of creating deepfakes using the (Wefaceswap, 2025) platform which offers a *Creator package* for $19.99/month (80 credits: 80 swapped images or 120 seconds of swapped video can be made) and the Microsoft Clipchamp app.

Deepfake is a type of synthetic media in which AI, specifically deep learning algorithms, are used to manipulate or generate visual and audio content that closely resembles real people, making it appear authentic. Some apps work by swapping the subject's face with existing media, others can create new images and video avatars from scratch.

Experts estimate that over 500,000 deepfake videos and voice recordings were shared on social media by the end of 2023 (Kaur, *et al.*, 2024).

Deepfake apps offer valuable tools for innovation and effective content creation. For example, applications are used in entertainment to enhance film production, creating special effects or “reducing the aging” of actors; in marketing, deepfakes personalize advertisements and attract customers with realistic avatars; in education and training, by simulating real-life scenarios for improved learning; for language translation, by synchronizing lip movements with translated audio for more localized content; in content creation, thanks to technology for rapidly producing personalized media content.

2. The process of creating deepfakes and ethical considerations

The deepfake creation process goes through several stages. The first stage involves collecting high-quality images and videos of people whose faces are to be changed. This data must cover a wide range of facial expressions and positions to ensure a successful deepfake. The second stage consists of using computer vision techniques to detect and isolate faces from the collected images and videos. Accurate face detection ensures precise results for the next steps. The third stage involves aligning the detected faces so that they have a similar position and orientation. Correct alignment is important for achieving a realistic deepfake, as it ensures that machine learning algorithms accurately analyze and reproduce facial features and expressions. In the fourth stage, facial features and expressions are encoded into a mathematical representation, important for training machine learning algorithms. The fifth stage consists of training machine learning algorithms. Depending on the complexity of the product and the capacity of the dataset, this process can take several hours or days to complete. The creation of the deepfake is completed by swapping faces in the video, using the encoded facial data to manipulate the video and produce a realistic deepfake.

The creation of a deepfake must be accompanied by a clear statement that the image or video was generated using a deepfake application or an Artificial Intelligence system. Transparency is important in the process of creating and distributing deepfakes. Maintaining an ethical framework in the process of using technology allows avoiding misleading the public. As long as deepfakes are not used to manipulate, defame, deceive, or violate the rights of others, they can be considered legal.

In the case of using photos, videos or voice recordings belonging to other people in the creation process, it is necessary to obtain their explicit consent. Lack of consent may lead to a violation of copyright, image rights or privacy, thus attracting legal consequences. Social platforms, such as Facebook/Meta, have begun to impose clear rules on labeling AI-generated content to combat misinformation and abuse.

With the implementation of AI technologies, companies face various technological, organizational and cultural challenges (Ångström, *et al.*, 2023).

3. Deepfakes detection

Depending on the platform and resources used, the quality of deepfakes varies. To identify a deepfake, an analysis of unnatural facial movements, awkward or infrequent blinking, and inconsistent expressions is required. Inaccurate lighting or shadows and blurry areas, especially around the face, can also indicate manipulation. Lip sync issues, where the mouth doesn't match the speech, are also an indication of manipulation. Another aspect would be unnatural reflections in the eyes or excessively smooth skin textures. Additionally, audio mismatches, such as voices not aligning with lip movements, can be a clear indication. These visual and audio inconsistencies are key indicators of a fake video created using deepfake technology.

In parallel with the evolution of tools for creating deepfakes, methods and techniques for their detection are being researched and identified. In the case of complex and qualitative deepfakes, the analysis of the above aspects in detecting manipulation will not be successful. An important direction is to evaluate the performance of learning-based deepfake detectors in more realistic contexts, quantitatively measuring their robustness against different processing operations (Lu & Ebrahimi, 2024). An in-depth analysis of state-of-the-art techniques and tools for identifying deepfakes, encompassing image-based, video, and audio content can be found in (Sunil, *et al.*, 2025). Fundamental technologies, such as deep learning models, are explored and their effectiveness in differentiating real from manipulated environments is evaluated. Additionally, new detection methods are being explored that use sophisticated machine learning, computer vision, and audio analysis techniques.

The integration of Vision Transformers with a DenseNet-based neural feature extractor is presented in (Siddiqui, *et al.*, 2025). The authors claim that "the approach produces results equivalent to the latest Vision Transformer techniques, without relying on complex tactics such as distillation or ensemble methods. Furthermore, the inference technique is simple yet effective, which uses a voting mechanism to identify numerous faces in a single video frame."

Deepfake detection can be achieved through a multi-scale interactive dual-stream network (MSIDSnet). The network is divided into spatial and frequency domain streams and uses a multi-scale fusion module to capture both the facial features of images that have been manipulated in the spatial domain under different circumstances and the fine-grained information about the high-frequency noise of the falsified images. The network fully integrates the features of the streams in the spatial and frequency domains through a dual-stream interactive module and uses the vision transformer (ViT) to further learn the global information of the faked facial features for classification (Cheng, *et al.*, 2024).

Another direction in detection is the examination of spatial and temporal properties. Fake videos disrupt statistical regularity in original videos. Therefore, the generalization of deepfake detection is stimulated by distinguishing regularity disruption that does not appear in real videos. Perturbing a real video with a Pseudo-Fake Generator creates a wide range of pseudo-fake videos for training. Such a practice allows for deepfake detection without using fake videos and improves generalization ability in a simple and efficient way. To capture spatial and temporal perturbations together, a spatiotemporal enhancement block is proposed to learn regularity perturbation in space and time on self-generated videos (Guan, *et al.*, 2023).

There are other detection techniques that are researched in specialized articles, such as the approach to datasets, algorithmic techniques and challenges, useful for an overall analysis; methods based on large models and biometrics; classification of machine learning and deep learning methods, and hybrid ones; adversarial robustness, real-time processing and evaluation metrics.

4. Manipulation of public perception

The evolution of deepfake creation technology comes with both positive and negative aspects, the resulting products can directly influence collective perception and behavior. Advances in generative technologies allow the production of hyper realistic audio-visual content, which can mislead the audience by creating artificial realities that are difficult to distinguish from authentic ones. This content has the ability to simulate the voice, facial expressions and behavior of real people, thus becoming a potentially dangerous tool for information manipulation.

Recent research (Ranka, *et al.*, 2024; Jungherr, *et al.*, 2024) indicates that the use of AI in the generation of false information can have a significant impact on democratic processes, including elections, where the manipulation of public perception can be decisive. In addition, the AI integration in areas such as digital journalism, social media, online education and political campaigns facilitates the amplified distribution of falsified narratives, often difficult to identify even by specialists. Experiments with real subjects show that audio deepfakes are harder to detect than video ones and that human discernment depends on the environment in which they are presented (Groh, *et al.*, 2024).

In this context, rigorous analysis of the technical and socio-cognitive mechanisms through which AI can contribute to the creation and dissemination of false realities is necessary (Tugarev, 2023). It is also important to assess the impact of these technologies on social cohesion, public trust and the democratic functioning of society. This study aims to investigate how artificial intelligence is used to generate and distribute misleading content, to identify how disinformation through deepfakes can polarize public opinion in electoral campaigns and diminish final scores.

Deepfakes are no more disinformation than regular fake news, but they can affect public perception and contribute to polarization, especially among the less digitally literate. Nationally, the website https://stopfals.md is a portal that publishes and exposes forgeries appearing in the digital environment. The independent press from the Republic of Moldova also informs citizens about the deepfakes circulating on the Internet. Next, we will analyze the impact of the deepfake that appeared on October 16-17, 2024, which has President Maia Sandu as its main actor, on the eve of the presidential elections and the Constitutional Referendum in the Republic of Moldova. The video is currently not available to the public, so reference will be made to Detector Media, which translated the Romanian audio track used in the fake video (Koldomasov & Pylypenko, 2024), where the message of the President of the Republic of Moldova is contained, who *"repents"* for her position, campaigns against herself and calls for a *"no"* vote in the referendum: *"The Republic of Moldova will not be accepted into the EU even in 30 years. I know for sure that once the war in Ukraine ends, we will be next. If I remain president, I will have to ban all independent media and open criminal cases against opposition politicians. Vote for any candidate, just don't vote for me or for this fake Euro-referendum. My defeat is the only chance to save the life of the Republic of Moldova and your children."* This deepfake appeared and was distributed simultaneously on several local pro-Russian Telegram channels ("Republica Gagauza", "Prydnestrovets" and "112.md — Moldovan News 24/7"), disguised as campaign material for Maia Sandu.

Watchdog, between August 20-23, 2024, conducted a survey on a sample of 1011 people aged 18 and over. The respondents were asked the question: *"But if you had to choose in a referendum between the accession of the Republic of Moldova to the European Union (EU) and the accession of the Republic of Moldova to the Eurasian Economic Union (EEU), what would you choose?"*. The results are shown in Figure 1.

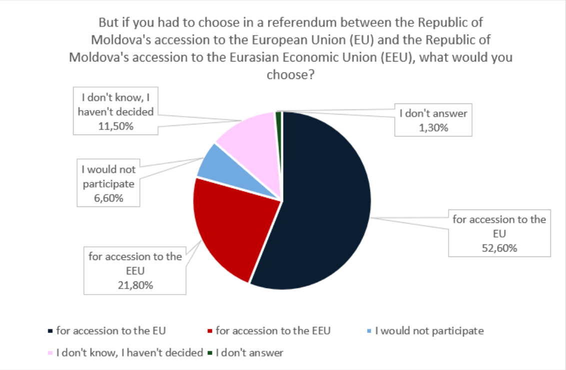


Figure 1. Watchdog survey results.

Source: *https://watchdog.md/news/208261/creste-impactul-campaniilor-de-dezinformare-si-influentare-a-opiniei-publice-in-republica-moldova/*

In early October, the Institute for Public Policy (IPP) conducted a survey on a sample of 1,100 people, in which respondents were asked to express their opinions on the foreign policy options of the Republic of Moldova. When asked whether they would support the accession of the Republic of Moldova to the European Union, 54.5% declared that they would vote in favor. The results of the survey are presented in Figure 2.

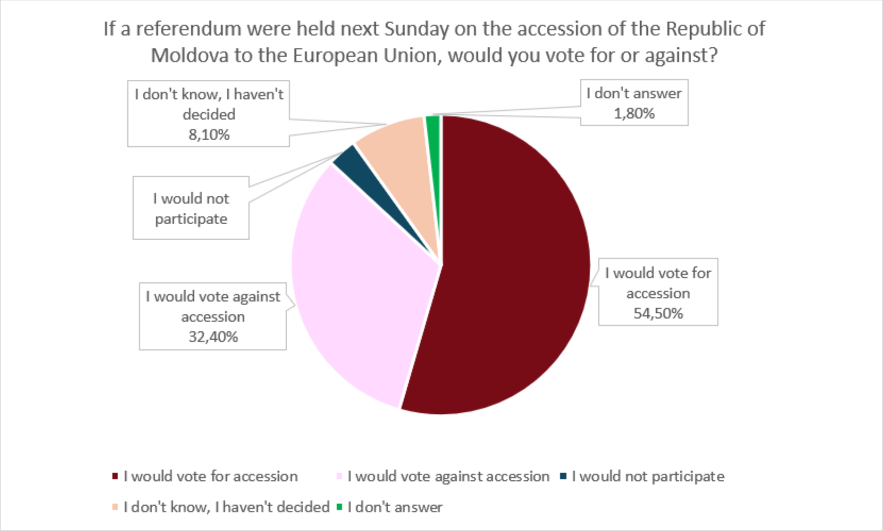


Figure 2. Results of the survey conducted by the Institute for Public Policy.
Source: *http://bop.ipp.md/ (Accessed: 5.9.2025)*

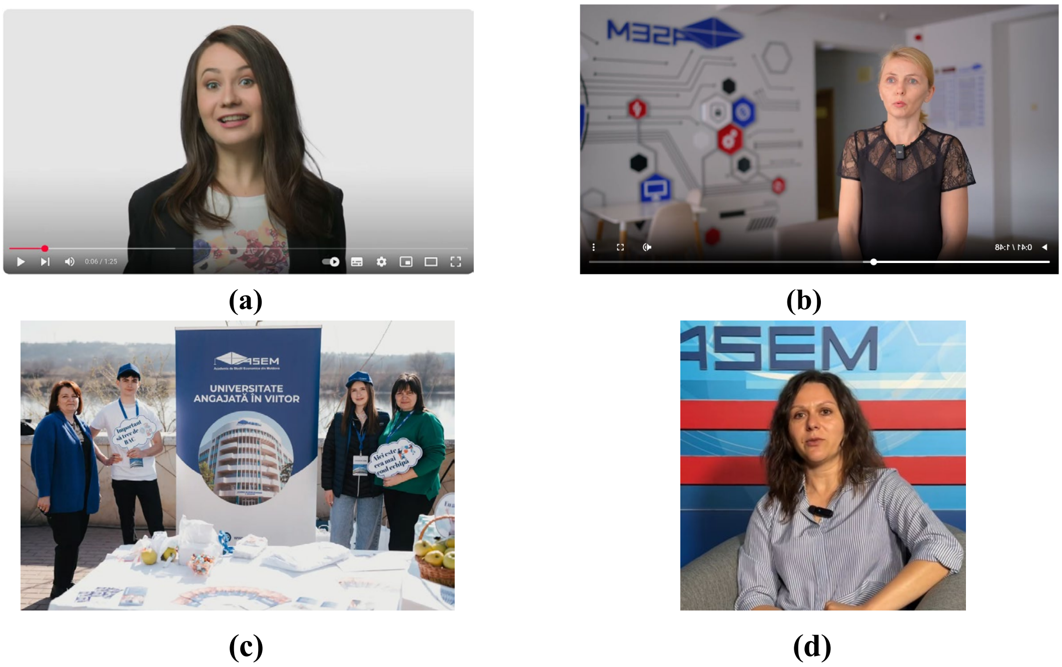
The results of the Republican Constitutional Referendum of October 20, 2024 on supporting the amendment of the Constitution in view of the accession of the Republic of Moldova to the European Union are available on (CEC, 2024), 50.35% of voters voted for and 49.65% - against. If the votes from the diaspora are excluded, then internally there are 45.38% - for and 54.62% - against. A very large gap compared to the results of the survey conducted in early October 2024 by IPP, about 9.12%.

The conclusion may be subjective without concrete evidence, but the polarization of public opinion and the numbers of the Referendum results can be seen. Directly or indirectly, it is a consequence of the deepfake that appeared on the eve of the elections.

Analysis of surveys conducted by (IPP, 2024) attests to a significant increase in 2024 in the use of social networks as a source of information for the population of the Republic of Moldova. The most popular are Facebook, Instagram, Telegram, TikTok, YouTube, odnoklasniki.ru, Viber, Vkontakte. Each person, thanks to the implementation of AI-based algorithms, is provided with certain content depending on their interests. Algorithms analyze browsing history and place individuals in an information bubble specific to their preferences. This process is done subtly by algorithms without the subject's awareness.

5. Making deepfakes with Wefaceswap

To better understand the generation process and analyze the result obtained, deepfake images and videos will be created using the Wefaceswap platform and the Microsoft Clipchamp application. The images and videos available on the website https://ase.md/ and the institution's Facebook page will be used as data sources. Another source is the video promoting Vocational Technical Education in the Dual System available on the official Youtube channel. Figure 3 presents the sources used.



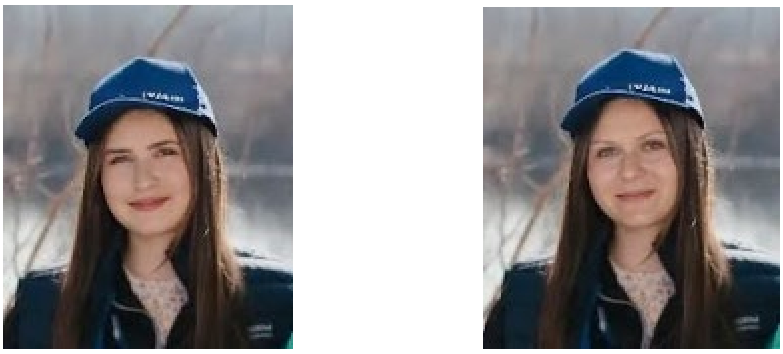
(a) (b)

(c) (d)

Figure 3. Data sources for generating deepfakes.

***Source:* (a)** *https://www.youtube.com/watch?v=Nm4QBGQ2cHc*
(b) *https://ase.md/la-asem-a-fost-deschis-un-laborator-pentru-studierea-sistemului-informational-geografic/*
(c) *https://ase.md/asem-la-targurile-educationale-regionale-din-causeni-si-soroca/*
(d) *https://www.facebook.com/reel/767532952118987?locale=ro_RO*

The first deepfake will be created, replacing the face of the student in figure 3.c with the face in figure 3.d. The result is shown in figure 4.



Original Deepfake

Figure 4. Deepfake of changing face in an image.

Source: *Made by the author on the Wefaceswap platform based on the sources in figure 3.c and figure 3.d.*

As can be seen in Figure 4, the deepfake image appears authentic, although if the original images are examined, a difference in age is observed.

The second deepfake will replace the face in the video in figure 3.a with the face in figure 3.d. As a result, the resulting product can be considered successful, if there were no obvious synchronization errors where the face in the video remains the original one. Figure 5 shows some screenshots from the deepfake made.

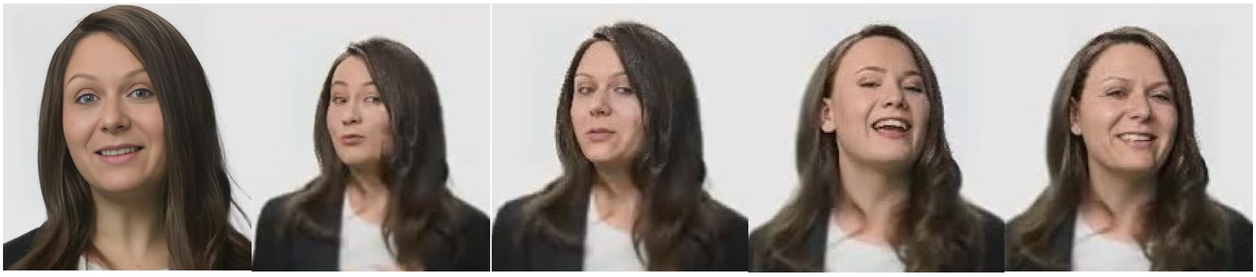


Figure 5. Screenshots from the Deepfake video Promoting Dual Education.
Source: *Made by the author on the Wefaceswap platform based on the sources in figure 3.a and figure 3.d.*

In this case, due to the rapid movements of the person in the original video, accurate face identification is not possible. To achieve a successful and high-quality deepfake, more powerful platforms and a larger dataset for the person in figure 3.d are needed.

The following deepfake consists of modifying the face in figure 3.b with the face in figure 3.d. Screenshots of the obtained deepfake are presented in figure 6.

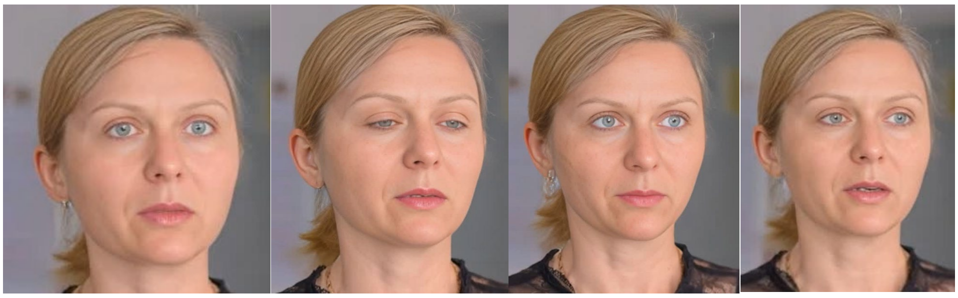


Figure 6. Screenshots from the Deepfake video Launch of the GIS Lab.
Source: *Made by the author on the Wefaceswap platform based on the sources in figure 3.b and figure 3.d.*

As can be seen from Figure 6, the face in the deepfake does not correspond to the one in Figure 3.d. A new person was obtained that has features specific to the subject in the original video and is additionally assigned facial features corresponding to the subject in Figure 3.d. Due to the slow movements in the original video, no obvious manipulations can be detected, although in the close-up frames, vibrations are observed in the face – an indication of manipulation.

From the deepfakes made, it can be concluded that to obtain a qualitative result, a platform that performs complex manipulations is needed. As data sources, it is necessary to use people of the same age, stature and appearance. It would be advisable for the original videos, the inertia of the subjects who will be subjected to manipulation.

CONCLUSIONS

The development of AI-based technologies has seen a remarkable rise in recent times, especially deepfake platforms. The products made are becoming more and more authentic and difficult to detect. Therefore, there is a need to establish methods for detecting deepfake. In some cases, detecting manipulation is simple and can be done through detailed analysis of the deepfake video, in other cases dedicated applications are needed.

Deepfakes can influence public opinion based on misleading information, thus undermining trust in the political system, mass media, etc. In case the accessed content arouses suspicions, it is necessary to investigate its source and the channels on which it is distributed. It should not be ignored that deepfake products also have positive aspects, streamlining content creation for marketing, the film industry, education, social media, etc.

Anyone can create a deepfake, without any deep IT knowledge. It is important to indicate this fact when creating a material using a deepfake application or artificial intelligence. If a person's photos are used to create a deepfake, their permission is required, otherwise legal problems may arise.

REFERENCES

1. Abirami, S., Pethuraj, M., Uthayakumar, M. & Chitra, P., 2024. A systematic survey on big data and artificial intelligence algorithms for intelligent transportation system. *Case Studies on Transport Policy,* Volume 17, article 101247.
2. Amalfitino, D. et al., 2023. Artificial Intelligence Applied to Software Testing: A Tertiary Study. *ACM Computing Surveys,* 56(3), pp. 1-38.
3. Anantrasirichai, N. & Bull, D., 2022. Artifcial intelligence in the creative industries: a review. *Artificial Intelligence Review,* Volume 55, pp. 589-656.
4. Ångström, R. et al., 2023. Getting AI Implementation Right: Insights from a Global Survey. *California Management Review,* 66(1), pp. 5-22.
5. CEC, 2024. *Comisia Electorală Centrală a Republicii Moldova.* [Online] Available at: https://pvt12024.cec.md/cec-template-referendum-results.html [Accessed 9 5 2025].
6. Cheng, Z., Wang, Y., Wan, Y. & Jiang, C., 2024. DeepFake detection method based on multi-scale interactive dual-stream network. *Journal of Visual Communication and Image Representation,* Volume 104, article 104263.
7. Goel, S., Guha, A., Kuppusamy, U. & Shanmugam, T., 2023. Survey on Artificial Intelligence and Its Applications. In: *Selvaraj, H., Chmaj, G., Zydek, D. (eds) Advances in Systems Engineering. ICSEng 2023. Lecture Notes in Networks and Systems.* vol 761: Springer, Cham, pp. 512-522.
8. Groh, M. et al., 2024. *Human Detection of Political Speech Deepfakes across Transcripts, Audio, and Video.* [Online] Available at: https://arxiv.org/pdf/2202.12883 [Accessed 10 5 2025].
9. Guan, J. et al., 2023. *Detecting Deepfake by Creating Spatio-Temporal Regularity Disruption.* [Online] Available at: https://arxiv.org/pdf/2207.10402 [Accessed 10 4 2025].
10. IPP, 2024. *Barametrul Opiniei Publice Republica Moldova.* [Online] Available at: http://bop.ipp.md/ [Accessed 9 5 2025].
11. Jungherr, A., Rauchfleisch, A. & Wuttke, A., 2024. *Deceptive uses of Artificial Intelligence in elections strengthen support for AI ban.* [Online] Available at: https://arxiv.org/pdf/2408.12613v1 [Accessed 5 2 2025].
12. Kaur, A., Noori Hoshyar, A., Saikrishna, V. & al., e., 2024. Deepfake video detection: challenges and opportunities. *Artificial Intelligence Review,* Volume 57, article 159.
13. Khadam, U., Davidsson, P. & Spalazzese, R., 2024. Exploring the Role of Artificial Intelligence in Internet of Things Systems: A Systematic Mapping Study. *Sensors,* 24(20), article 6511.
14. Koldomasov, A. & Pylypenko, A., 2024. *"Europe stole Moldova": Russian propaganda about the elections in Moldova.* [Online] Available at: https://en.detector.media/post/europe-stole-moldova-russian-propaganda-about-the-elections-in-moldova?utm_source=chatgpt.com [Accessed 6 5 2025].
15. Lu, Y. & Ebrahimi, T., 2024. Assessment framework for deepfake detection in real-world situations. *EURASIP Journal on Image and Video Processing,* Volume 6.
16. Martínez-Fernández, S. et al., 2022. Software Engineering for AI-Based Systems: A Survey. *ACM Transactions on Software Engineering and Methodology,* 31(2), pp. 1-59.
17. Martinez-Millana, A. et al., 2022. Artificial intelligence and its impact on the domains of universal health coverage, health emergencies and health promotion: An overview of systematic reviews. *International Journal of Medical Informatics,* Volume 166, article 104855.

18. Ranka, H. et al., 2024. *Examining the Implications of Deepfakes for Election Integrity.* [Online] Available at: https://arxiv.org/pdf/2406.14290 [Accessed 13 5 2025].
19. Rojas, E. et al., 2024. A Survey on AI-Empowered Softwarized Industrial IoT Networks. *Electronics 2024,* 13(10), article 1979.
20. Siddiqui, F., Yang, J., Xiao, S. & Fahad, M., 2025. Enhanced deepfake detection with DenseNet and Cross-ViT. *Expert Systems with Applications,* Volume 267, article 126150.
21. Sunil, R. et al., 2025. Exploring autonomous methods for deepfake detection: A detailed survey on techniques and evaluation. *Heliyon,* 11(3), article e42273.
22. Taylor, M., 2025. *12 Best Deepfake Apps for Realistic Face Swaps.* [Online] Available at: https://akool.com/blog-posts/5-best-deepfake-apps-for-realistic-faceswaps [Accessed 8 05 2025].
23. Tugarev, L., 2023. Deepfake - manufacturing the reality with the aid of the Artificial Intelligence. *Moldoscopie,* 1(98), pp. 182-187.
24. Wefaceswap, 2025. *WEFACESWAP.* [Online] Available at: https://www.wefaceswap.com/ro [Accessed 12 4 2025].
25. Zhou, L. et al., 2024. A Comprehensive Survey of Artificial Intelligence Applications in UAV-Enabled Wireless Networks. *Digital Communications and Networks*.

INNOVATIVE IT TECHNOLOGIES IN EDUCATIONAL ACTIVITIES AND ENSURING DIGITAL SECURITY

UDC: [004.056+004.78+004.8]:37.018.43
DOI: https://doi.org/10.53486/tids2025.21

OLGA PUGACHEVA
Francysk Skaryna Gomel State University
OPugacheva@gsu.by
ORCID ID: 0000-0003-4554-0038

Abstract. The article deals with the topical issues of using innovative information technologies in education to improve the quality of education, optimize the management of educational processes, increase the efficiency of teachers and staff of educational institutions.

The research is devoted to analyzing the possibilities of using information technologies in educational activities and the main methods of ensuring digital security in this sphere.

The main directions of research include consideration of the possibilities of using information technologies in educational activities, analysis of the used information systems in education, analysis of the directions and experience of using artificial intelligence in education, the main methods of ensuring information security in educational systems.

The use of information technologies in the following directions of educational activity is considered: automation of administrative processes, organization of the educational process, interactive learning, transparency of management in an educational institution.

The article analyzes the capabilities of such frequently used information systems in education as the system “1C: Education” for the management of educational activities and accounting of students' progress, the platform “Directum” - for electronic document management, Moodle - e-learning system.

The following directions of using artificial intelligence in education are also considered: adaptive learning platforms, individual assistance to the participants of the educational process, automation of evaluation, prediction of future success and identification of the risk of failure in learning activities, creation of innovative educational materials. In analyzing the experience of using artificial intelligence in education, examples are given, each of which demonstrates the potential of neural networks to improve learning, feedback and management in education.

The article explores areas of digital security such as data encryption, multi-factor authentication, the need for regular software updates, educating and raising cybersecurity awareness among students and staff, establishing strict policies for accessing data and systems, using backup and anti-virus programs, collaborating with security experts, and others. This helps create a multi-layered defense strategy, keeping both data and users safe in an educational environment.

Keywords: information technology, information systems, artificial intelligence, digital transformation, digital security, educational sphere.

JEL Classification: C88, D83, I2, M15, O3

INTRODUCTION

In the context of digital transformation, educational institutions are using innovative information technologies (IT) to improve the quality of education, optimize the management of educational processes, and enhance the effectiveness of teaching staff. IT opens up new opportunities for automating educational processes, personalizing educational interactions, and increasing access to knowledge.

The relevance of this research topic stems from the growing role of information technology in the education system. The introduction of digital tools enables solutions for document automation, student performance monitoring, distance learning, and other aspects that are becoming an integral part of the educational process. These changes require the development of approaches to improving information systems and methods for their application in educational institutions, as well as ensuring the security of the educational environment.

The purpose of this study is to analyze the potential for using information technology in educational activities and develop key areas for ensuring digital security in this area.

To achieve this goal, the following objectives are addressed:

– study the potential for using information technology in educational activities;

– analysis of information systems used in education;

– analysis of trends and experiences in using artificial intelligence in education;

– review of key methods for ensuring information security in educational systems.

Modern educational institutions face challenges that require optimizing the educational process and increasing the efficiency of administrative management. In response to these challenges, innovative IT is being actively introduced into educational activities, opening up new opportunities for automation, data management, and personalization of learning. IT enables the educational process to be organized using digital systems that ensure effective interaction between teachers and students, as well as support administrative activities (Pugacheva, 2021).

Automation of processes in the educational sector allows for more efficient management of large volumes of data and rapid response to changing conditions. The implementation of automated systems helps reduce the labor intensity of routine administrative processes, such as attendance tracking, grading, reporting, and other tasks that require significant time and human resources. Automation allows such processes to be completed more quickly and at a lower cost (Pugacheva, 2021).

ANALYSIS OF THE USE OF IT TECHNOLOGY IN EDUCATION AND METHODS OF ENSURING DIGITAL SECURITY

1. Study of the possibilities of using information technology in education

Let's consider the possibilities of using information technology in educational activities.

Information technology in education is aimed at solving the following problems (Pugacheva, 2019):

1. Automation of administrative processes.

This includes managing class schedules, tracking student progress, processing attendance data, and document management. These tasks traditionally take up a significant amount of staff time, but automation can significantly reduce labor and time costs.

2. Organization of the educational process.

IT tools make it possible to create and manage digital educational resources, conduct remote classes, and organize blended learning. For example, platforms such as Moodle, Microsoft Teams, and Google Workspace are becoming standard in the modern educational process.

3. Interactive learning.

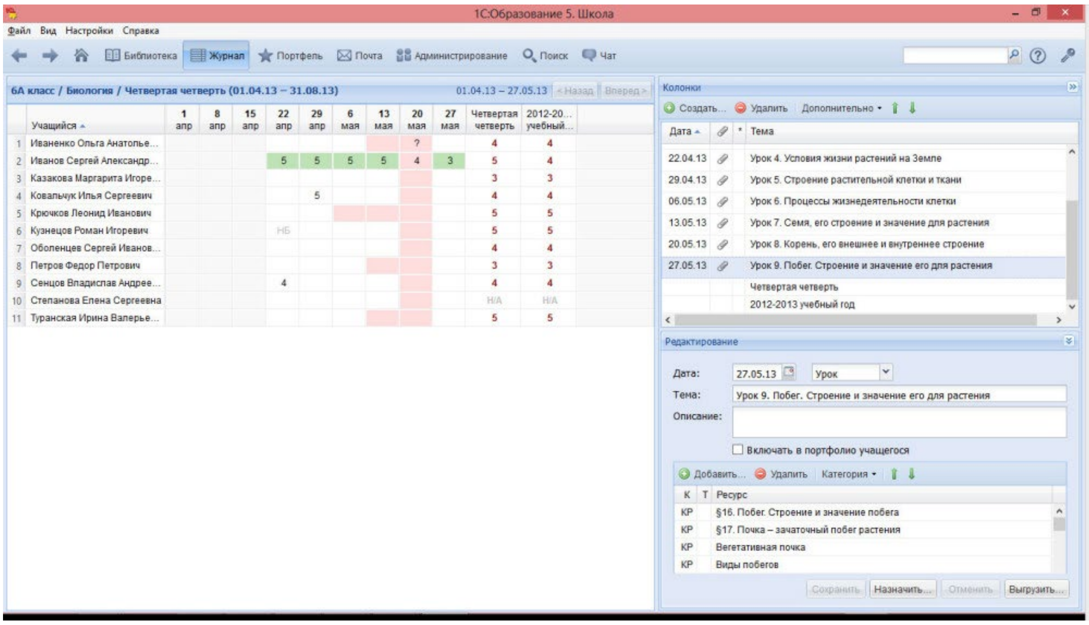
Software including electronic textbooks, virtual reality (VR) and augmented reality (AR) systems, and simulators helps diversify the learning process and increase student engagement.

4. Increased management transparency.

Electronic diary and journal systems provide parents and students with real-time access to academic results. This promotes greater transparency and builds trust in the educational organization.

2. Analysis of information systems used in education

One of the most popular automation solutions is the 1C: Education system, which is widely used in educational institutions to manage learning activities and track student achievement. Its interface is shown in Figure 1.



6А класс / Биология / Четвертая четверть (01.04.13 – 31.08.13) 01.04.13 – 27.05.13

	Учащийся	1 апр	8 апр	15 апр	22 апр	29 апр	6 мая	13 мая	20 мая	27 мая	Четвертая четверть	2012-20... учебный...
1	Иваненко Ольга Анатолье...								?		4	4
2	Иванов Сергей Александр...				5	5	5	5	4	3	5	4
3	Казакова Маргарита Игоре...										3	3
4	Ковальчук Илья Сергеевич					5					4	4
5	Крючков Леонид Иванович										5	5
6	Кузнецов Роман Игоревич				НБ						5	5
7	Оболенцев Сергей Иванов...										4	4
8	Петров Федор Петрович										3	3
9	Сенцов Владислав Андрее...				4						4	4
10	Степанова Елена Сергеевна										Н/А	Н/А
11	Туранская Ирина Валерье...										5	5

Дата		*	Тема
22.04.13			Урок 4. Условия жизни растений на Земле
29.04.13			Урок 5. Строение растительной клетки и ткани
06.05.13			Урок 6. Процессы жизнедеятельности клетки
13.05.13			Урок 7. Семя, его строение и значение для растения
20.05.13			Урок 8. Корень, его внешнее и внутреннее строение
27.05.13			Урок 9. Побег. Строение и значение его для растения
			Четвертая четверть
			2012-2013 учебный год

Дата: 27.05.13 Урок

Тема: Урок 9. Побег. Строение и значение его для растения

Описание:

☐ Включать в портфолио учащегося

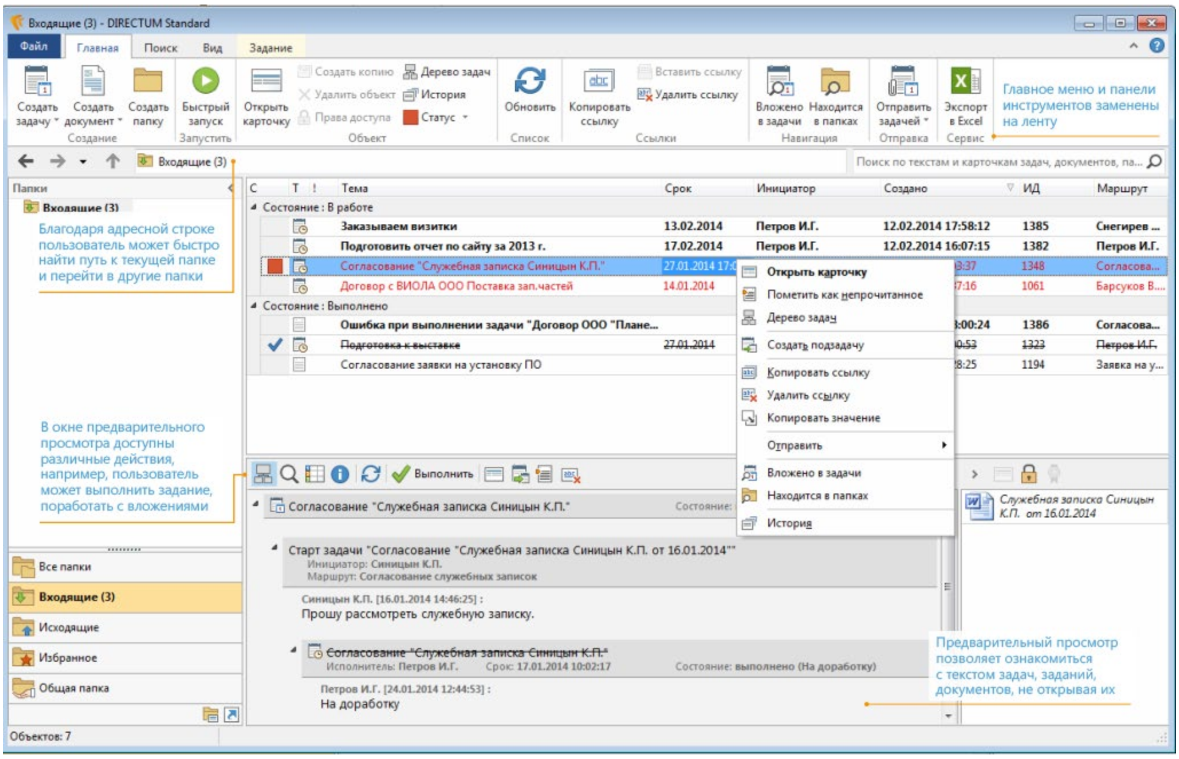
К	Т	Ресурс
КР		§16. Побег. Строение и значение побега
КР		§17. Почка – зачаточный побег растения
КР		Вегетативная почка
КР		Виды побегов

Figure 1. 1C: Education system.
Source: *1C: Education. Digital educational solutions*.

This system offers a wide range of functionality, including creating and maintaining academic performance reports, automated scheduling, attendance tracking, and other operations related to the educational process.

The 1C system allows teachers and administrators to easily access data and reports, making it a useful tool for management decision-making. By implementing this system, educational institution leaders can quickly evaluate the effectiveness of various educational programs and adjust the learning process based on current results.

Another important component of automation is the use of electronic document management platforms, such as Directum, the interface of which is shown in Figure 2.



Главное меню и панели инструментов заменены на ленту

Благодаря адресной строке пользователь может быстро найти путь к текущей папке и перейти в другие папки

С	Т	!	Тема	Срок	Инициатор	Создано	ИД	Маршрут
Состояние : В работе								
			Заказываем визитки	13.02.2014	Петров И.Г.	12.02.2014 17:58:12	1385	Снегирев ...
			Подготовить отчет по сайту за 2013 г.	17.02.2014	Петров И.Г.	12.02.2014 16:07:15	1382	Петров И.Г.
🟥			Согласование "Служебная записка Синицын К.П."	27.01.2014 17:0		3:37	1348	Согласова...
			Договор с ВИОЛА ООО Поставка зап.частей	14.01.2014		7:16	1061	Барсуков В....
Состояние : Выполнено								
			Ошибка при выполнении задачи "Договор ООО "Плане...			3:00:24	1386	Согласова...
✓			~~Подготовка к выставке~~	~~27.01.2014~~		~~0:53~~	~~1323~~	~~Петров И.Г.~~
			Согласование заявки на установку ПО			8:25	1194	Заявка на у...

В окне предварительного просмотра доступны различные действия, например, пользователь может выполнить задание, поработать с вложениями

Согласование "Служебная записка Синицын К.П." Состояние:

Старт задачи "Согласование "Служебная записка Синицын К.П. от 16.01.2014""
Инициатор: Синицын К.П.
Маршрут: Согласование служебных записок

Синицын К.П. [16.01.2014 14:46:25] :
Прошу рассмотреть служебную записку.

~~Согласование "Служебная записка Синицын К.П."~~
Исполнитель: Петров И.Г. Срок: 17.01.2014 10:02:17 Состояние: выполнено (На доработку)

Петров И.Г. [24.01.2014 12:44:53] :
На доработку

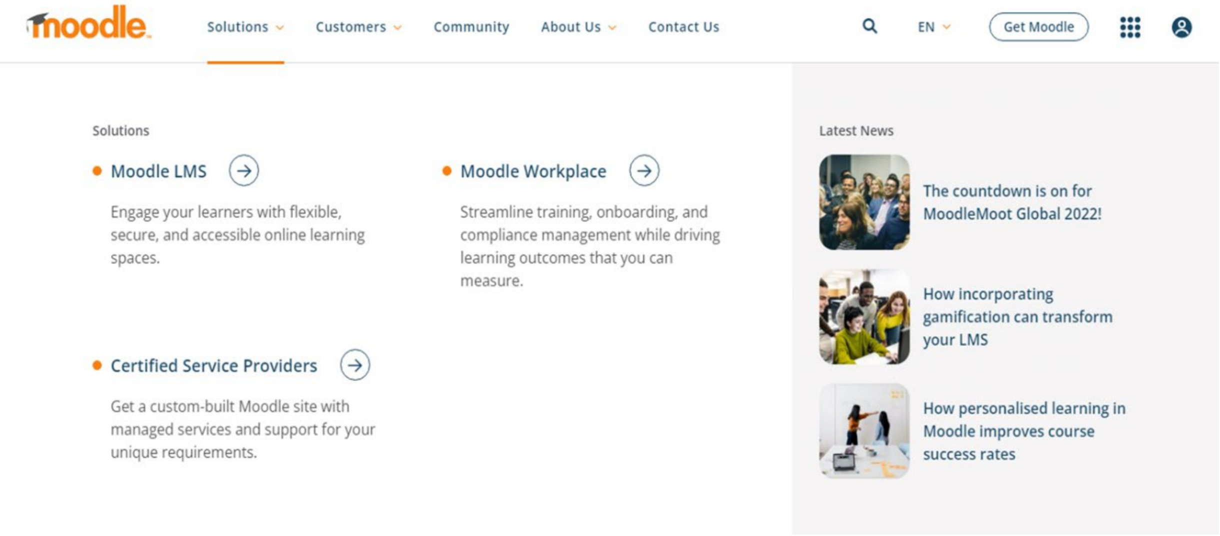
Служебная записка Синицын К.П. от 16.01.2014

Предварительный просмотр позволяет ознакомиться с текстом задач, заданий, документов, не открывая их

Figure 2. Directum platform.
Source: *Directum*: *An intelligent ECM system for large companies.*

This system optimizes document flow, improving organizational document management and ensuring task control. Directum supports the creation, storage, and transmission of electronic documents, reducing paper costs and simplifying the work of educational institution employees.

Moodle is one of the most well-known e-learning systems (Figure 3). It has been translated into more than 100 languages.



Solutions

- Moodle LMS

Engage your learners with flexible, secure, and accessible online learning spaces.

- Moodle Workplace

Streamline training, onboarding, and compliance management while driving learning outcomes that you can measure.

- Certified Service Providers

Get a custom-built Moodle site with managed services and support for your unique requirements.

Latest News

The countdown is on for MoodleMoot Global 2022!

How incorporating gamification can transform your LMS

How personalised learning in Moodle improves course success rates

Figure 3. Moodle – a distance learning system.
Source*:* *Moodle LMS 5.0.*

Moodle (Modular Object-Oriented Dynamic Learning Environment) is a popular distance learning system (DLS). It is successfully used by major universities worldwide, schools, and private companies. Its open source code allows for flexible customization of the platform to meet any needs.

The Moodle platform is versatile and highly customizable. This distance learning system was developed for schools and universities, but is also well suited for corporate environments and private use. Thanks to the collaboration of developers and a large user community worldwide, Moodle is constantly evolving, adding new tools, extensions, and modules. The DLS supports integration with other services, including video conferencing, analytics, payment systems, and uniqueness verification services.

The Moodle LMS solves the following tasks:

1. Conducting training courses. In Moodle, training materials (text documents, presentations, and videos) can be combined into a single training course, accessible to all students or a specific group.

2. Conducting tests during training. For this purpose, the Moodle LMS has a built-in test editor. It initially offers 15 assignment formats, from choosing the right answer to moving objects. To prevent course participants from peeking during the test, you can limit the time and attempt count. Moodle automatically checks user responses, displays their errors, and displays the final score.

3. Feedback to the course administrator. The learning system includes forums and comments for this purpose. If participants need to contact the instructor/course administrator to ask a question or discuss the material, they can leave comments or use the built-in forum.

4. Knowledge base creation. The Moodle system allows for the creation of an archive of materials accessible to all users at any time. In the knowledge base, students can find the lecture or video lesson they need.

5. Mobile learning capabilities. The system has an official Moodle mobile app (from Moodle Pty Ltd.), which allows you to take courses and tests from your smartphone or tablet, but this can also be done using a mobile browser. Using a mobile device, you can not only access learning materials but also administer the course. The app is available on Google Play and the App Store.

6. Learning statistics. The Moodle system tracks student performance and monitors their progress, generating reports for teachers/administrators. The reports show the time it took participants to complete the course and any errors made.

7. Blended learning. This format is currently very popular: students' complete theory remotely using Moodle courses, while practical classes are conducted offline. The system flexibly adapts to the current educational environment and global circumstances.

8. Student surveys and feedback. The system allows for assessment, feedback, and participant opinions on specific topics through surveys and polls. Both forms are integrated into Moodle. Surveys are compiled with pre-defined questions, while polls are prepared by the administrator.

9. Analytics. Moodle's integrated system generates reports that show the activity level of users on the platform's courses: how many people viewed the course and what comments they left.

Thus, Moodle can help reduce the financial and time costs of launching a training course and distance learning in general.

3. Analysis of the directions and experience of using Artificial Intelligence in education

Artificial intelligence (AI) and neural networks offer a number of opportunities for improving education. The main areas of their application in this area may be the following (Pugacheva, 2024):

– adaptive learning platforms. AI can be used to create learning platforms that can adapt to the learning needs of each individual learner. Based on training data and feedback, AI can suggest personalized materials and exercises.

– individualized assistance. Neural networks can be used to automatically analyze learners' performance to provide personalized feedback and recommendations for improving the learning process.

– automated assessment. AI can be used to automatically grade assignments, tests, and quizzes, helping teachers save time on marking and focus on more important educational tasks.

– predicting success. Based on training data and student assessments, AI can help predict their future success and even identify the risk of failure in learning.

– creating innovative educational materials. AI and neural networks can be used to create interactive educational materials, such as virtual labs, educational games, and interactive textbooks.

Let's consider the potential uses of certain neural networks in education (Pugacheva, 2024):

1. Teacherbot. To help teachers develop materials for their classes, Teacherbot provides quick answers to questions about what content they want to create. Teachers can use the service to generate assignments, exercises, and create teaching materials.

2. Gradescope. Gradescope is a web application that simplifies the process of administering and grading tests for teachers. It helps reduce the time spent on the entire educational process, assigning grades, and provides a more accurate picture of student progress.

3. Fobizz Tools. Fobizz Tools is a collection of educational apps. The platform offers a variety of resources, including online courses, live webinars, teaching materials, and tools for effective personalized education. It features AI assistants for text, images, and speech. With these tools, you can create worksheets, multimedia boards, surveys, websites, video and audio recordings, screen recordings, shortened links, shared files, and QR codes.

4. EssayGrader.ai. To help instructors quickly and accurately grade student work, EssayGrader.ai can be used. It features feedback, error, and summary reports, as well as an artificial intelligence detector. With it, instructors can determine whether the entire work was written by a neural network or only part of it.

During their studies at the university, students in the Faculty of Economics explore the following areas of neural network use: text writing, video creation, image generation, audio processing, photo processing, brand naming and logo creation, code writing, text translation into other languages, document and presentation creation, website and design creation, and more. Students primarily use ChatGPT 3.5 or GPT-4o, and for image generation, they utilize tools such as DALL-E, Kandinsky 2.2, Leonardo.ai, Stable Diffusion, GigaChat, Yandex Shedevroom, and other neural networks.

The introduction of artificial intelligence technologies into the educational process requires a rethinking of traditional approaches to assessing learning outcomes. Modern neural networks can generate texts by simulating statistical patterns in language, which can reduce the effort students expend on written assignments. This can reduce the quality of education and students' critical thinking.

Overall, the use of neural networks in education can transform the role of the teacher from a traditional performer to a personal mentor and data analyst. However, it is important to note that the human aspect of education remains essential, and teachers will always play a key role in the educational process, regardless of the technology used.

4. Key methods of ensuring digital security in education

Digital security in the education sector is ensured through various methods and practices aimed at protecting information, systems, and users.

The key methods of ensuring digital security are as follows (Pugacheva, 2021):

1. Data encryption. Using encryption to protect confidential information, both in transit and at rest. This helps prevent unauthorized access to data.

2. Multifactor authentication (MFA). Implementing additional layers of verification when logging into systems (e.g., passwords + SMS codes or biometric data) to enhance account security.

3. Regular updates and patches. Keeping software and operating systems up to date to eliminate vulnerabilities that could be exploited by attackers.

4. Training and awareness. Conduct cybersecurity training for students and employees to ensure they are aware of the risks and can recognize potential threats, such as phishing.

5. Access policies. Establish strict data and system access policies, including the principle of least privilege, to ensure users have access only to the information they need.

6. Monitoring and auditing. Regularly monitor systems for suspicious activity and conduct security audits to identify vulnerabilities and evaluate the effectiveness of existing measures.

7. Data backup. Create regular backups of critical information to protect against data loss due to cyberattacks or technical failures.

8. Firewalls and antivirus software. Use software to protect networks and devices from malware attacks and viruses.

9. Network segmentation. Separate the network into different segments to restrict access between them and reduce the risk of threat propagation.

10. Incident management. Having a clear incident response plan that includes actions to identify, analyze, and mitigate the consequences of cyberattacks.

11. Collaborating with security experts. Engaging external specialists to conduct security assessments and implement best practices.

These methods help create a multi-layered security strategy, ensuring the security of both data and users in the educational environment.

CONCLUSIONS

Thus, information technology is a key tool for modernizing the educational process, ensuring automation, efficiency, and precision of management. Its use streamlines administrative tasks, improves interaction between participants, and creates conditions for effective learning and decision-making.

Improving the automation of educational activities through the use of IT is not simply a technical upgrade but also a strategic objective that contributes to the modernization of the educational process. The implementation of systems that automate processes such as scheduling, managing educational materials, and tracking academic performance makes educational institutions more flexible, efficient, and responsive to the needs of modern society.

Artificial intelligence and neural networks can transform education, making it more accessible, personalized, and effective for learners.

With the increasing digitalization of educational processes, the need to protect student, faculty, and administrative data from leaks and cyberattacks is growing. This requires the implementation of appropriate protocols and security systems. Digital security in the educational sector is a complex process that requires attention to various aspects of protecting the information and technologies used in the educational process.

REFERENCES

1. Directum: An intelligent ECM system for large companies. – URL: https://www.directum.ru/products/document-management-system [Accessed: 24.03.2025].
2. 1C: Education. Digital educational solutions. – URL: https://obrazovanie.1c.ru/ [Accessed: 28.04.2025].
3. Moodle LMS 5.0: More control, less complexity. – URL: https://moodle.org/ [Accessed: 25.04.2025].
4. Pugacheva, O., 2021. *Application of information technologies in the economy and education on of the Republic of Belarus: condition, problems and prospects*. Business management, D. A. Tsenov Academy of Economics, Svishtov (Stopansk Academy «Dimitar A. Tsenov» – Svishtov), №1. pp. 22-37.
5. Pugacheva, O.V., 2019. *Digital transformation of the national education system. Modern education: succession and continuity of the educational system "school - university - enterprise":* XII International Scientific and Methodological Conference (Gomel, February 14-15, 2019): [materials]. / Ministry of Education of the Republic of Belarus, Francysk Skaryna Gomel State University, Main Department of Education of the Gomel Regional Executive Committee; editorial board: I.V. Semchenko (editor-in-chief) [and others]. - Gomel: Francysk Skaryna Gomel State University. pp. 682-685.
6. Pugacheva, O.V., 2024. *Directions and experience of using artificial intelligence in education. Actual issues of scientific-methodical and educational-organizational work: traditional values and innovative technologies in education as a factor in the progressive development of society*: collection of materials of the Republican scientific-methodical conference (Gomel, February 22-23, 2024) / Ministry of Education of the Republic of Belarus, Francysk Skaryna Gomel State University; editorial board: Yu. V. Nikityuk (editor-in-chief) [et al.]. – Gomel: Francysk Skaryna Gomel State University pp. 328-330.
7. Pugacheva, O.V., 2024. *Use of Artificial Intelligence in the Economy and Society: directions, problems, and regulation.* Proceedings of Francisk Skorina Gomel State University, No. 5 (146). pp. 136-141.
8. Pugacheva, O.V., 2021. *Innovative security in the context of the formation of the digital economy of the Republic of Belarus.* National SecurityY Studies Journal of Ressearch and Practice Nr. 3 (1). pp. 95-112.

DATA SECURITY AND ACCESS MANAGEMENT IN MICROSOFT TOOLS: EXCEL, POWER QUERY AND POWER BI

UDC: [004.056.52+004.056.53+004.4]:005.334
DOI: https://doi.org/10.53486/tids2025.22

MARIA MORARU
Academy of Economic Studies of Moldova
morarumaria924@gmail.com
ORCID ID: 0009-0008-2499-8588

VARVARA ŢAPCOV
Academy of Economic Studies of Moldova
varvara.tapcov@gmail.com
ORCID ID: 0009-0005-1775-3740

VALENTINA CAPAŢINA
Academy of Economic Studies of Moldova
vcapatina@yahoo.com
ORCID ID: 0009-0007-9767-7243

Abstract. In the era of accelerated digitalization and the large volume of information generated by the internet, social networks, financial transactions, etc., the exponential growth of data requires it to be processed, analyzed, reported and secured. These processes are fundamental to transform raw data into valuable information that supports strategic decisions, operations and innovations in an increasingly digitalized world. Protecting data and information is an important issue in the context where the large volume of information is exposed to cybersecurity risks, data theft, unauthorized access and other threats.

The main objectives of this research are to identify and describe some methods and strategies for securing and managing data access in the application environment: Microsoft Excel, Power Query, Power BI, in order to evaluate their effectiveness in the development of information processing.

This study adopts a mixed-methods approach, with a focus on integrating solutions with Azure Active Directory and applying best practices in information protection.

Applying security measures helps protect the confidentiality and integrity of data, ensuring business continuity and the trust of customers and partners. Data must be protected not only during storage, but also during processing and transmission between various organizations, systems and applications. In this context, in MS Excel there are techniques such as: file encryption, password protection of spreadsheets, data access control, access auditing and monitoring, encryption of connections in Power Query, deletion of sensitive data, password protection for connecting to the external data source, file sharing with protection, backup and restore, data validation and integrity rules, source access control (SQL, APIs, etc.).

Keywords: Encryption, Power Query, Power Pivot, Validation.

JEL Classification: D8, O3, L8, M1, G2.

INTRODUCTION

The process of ensuring information security requires attention, involvement, and alignment with the needs of organizations of all sizes.

Currently, Microsoft Excel is one of the most popular and widely used spreadsheet programs in the world. According to recent estimates, there are over 1 billion users of Microsoft Excel worldwide. This number includes individuals, companies, and organizations that use Excel not only in business, but also in education, public administration, and government due to its versatility and integration with other Microsoft tools, such as Power BI and Microsoft 365.

In our opinion, information security should be viewed as a path (process) and not as a ultimate goal, as cyber threats and risks are constantly changing and evolving. It is essential to view information security as an ongoing process, involving constant learning, adaptation and implementation of new measures as technologies and attack methods become increasingly sophisticated.

The steps of this process are:

- *identifying valuable information resources* of organizations;
- *knowledge of the threats and dangers* to which information resources have been or may be exposed;
- *classifying information resources* from the perspective of the need to ensure their confidentiality, integrity and accessibility;
- *applying improved or newly introduced security measures* in the latest operating system version produced by Microsoft;
- *using data validation and consolidation operations,* creating pivot tables and interactive graphical representations, sheet and workbook level protection in MS Excel;
- *securing the use of networks* at the individual and organizational level.

MAIN CONTENT

In this research, we analyzed official sources regarding security and access control mechanisms implemented in Excel, Power Query, and Power BI, and reviewed the security functionalities offered by these three tools. A comparative analysis was also conducted between the security mechanisms available in Excel, Power Query, and Power BI, using practical test scenarios to validate permission settings, data encryption, and user-level access control.

For the case study, we used Microsoft Excel version 2021, Power Query, and Power BI Desktop.

In the use of information resources, there must be security measures that protect data and systems from external threats (viruses, hacking, phishing, etc.) and internal (human errors, unauthorized access). These measures may include the use of strong passwords, data encryption, regular software updates, and the implementation of cybersecurity solutions.

Today, many economists and professionals use Excel and other tools as complementary tools in data analysis. The most popular alternatives and complements to MS Excel, which are frequently used in the field of economics and financial analysis, are: Power Query, Power Pivot and Power BI. Each of these tools adds additional functionality and improves the analysis and reporting process. Therefore, it is important to know how information can be secured both in Excel and with each of the complementary tools.

Each of the MS Excel, Power Query, Power Pivot, and Power BI tools has its own features and methods for securing data and offers options for protecting it.

Below we will present some ways in which information can be protected in each of these tools.

MS Excel offers several security methods (levels) that allow access control to information:

- marking as final;

- password encryption;
- worksheet level protection;
- protecting the registry structure;
- data access control;
- adding digital signatures.

All of these levels of protection are not mutually exclusive, but rather complement each other. Each security method adds an additional layer of protection, and together they make the file more difficult for unauthorized people to modify or access. Some methods can be used together.

Mark as final security mode (Mark as Final) makes the file read-only and prevents accidental modification. If the file is marked as final, users will receive a message telling them that the file is final and should not be modified. *Marking as final* does not encrypt the file or completely prevent editing, but it adds a visual protection to indicate that the file is final. *Marking as final* is applied when the Excel file is open, by accessing the File > Info > Protect menu. Workbook > Mark as Final.

Password encryption security mode. If a stronger level of security is needed, there is the option of *encryption with a password.* (Encrypt with Password), where a password will be added that will prevent access or modification of the file by other users. Encrypting Excel files is one of the most effective methods of data protection. When files are encrypted, access to them is allowed only to those who have the appropriate password. Encryption can be applied from the File > Info > Protect menu. Workbook > Encrypt with Password. This method is essential for securing sensitive data (financial information, personal data, confidential company details, etc.) and preventing unauthorized access. With this security option, you can:

- Prevent unauthorized access,
- Preserved data integrity,
- Protect the file on shared devices or sent via email.

Preventing unauthorized access prevents unauthorized persons from accessing the file, even if they have access to the physical or online file.

Maintaining data integrity means preventing unauthorized changes and avoiding accidental changes. The password protects the file not only from viewing, but also from unauthorized changes. If the file is password protected, users who do not know the password will not be able to edit, add, or delete data from the file.

Protecting files when shared or emailed adds an extra security measure so that even if the file is intercepted during transfer, it will not be accessible without a password.

Worksheet-level protection is an additional measure to prevent unauthorized changes to the contents of a specific data set or specific cells in a spreadsheet. This method prevents users from changing locked cells in the worksheet. Spreadsheet password protection can be set only for specific pages if we select Protect from the Review tab > Sheet.

Registry Structure Protection is another method to prevent accidental or intentional changes to the underlying file structure and is essential in the context of a collaborative work environment or when managing important files. By enabling registry structure protection: File > Info > Protect Workbook > Protect Workbook Structure The entire file is protected so that worksheets cannot be added, moved, hidden, or deleted. This applies to all sheets in the file and cannot be enabled on specific sheets.

The way to securing *Control data access,* is another one data security method in THE Excel program and application complementary Power Query which involves DEFINITION SOME PERMISSION to control who can access or amend data, especially when When files are shared on internal networks or via the cloud (OneDrive, SharePoint, etc.). For this method, in Excel can be applied so techniques such as: hiding COLUMN or rows, creating controls for validation data, auditing changes (Review, Allow Edit Ranges).

In SharePoint, you can configure read permissions or editing for Excel files. Configuration read permissions or editing is done through the file 's permission settings, like this received the ability to control who has access to the file and What actions maybe effect if follow this algorithm: SharePoint > click on the name file > click on (...) > Details > Permissions > Permissions for this document > Stop Inheriting Permissions > Grant Permissions > add USERS or the groups DESIRED > choose permission level: View – only view, Edit – editing permission > Share.

Query and Power BI companion applications, data access control can be achieved through the following methods:

1. Row-Level Security Security - RLS)

- *Define roles.* In Power BI, you can define roles that restrict users' access to data in models based on certain criteria. For example, a user can only access data that is relevant to them, such as data from a specific region or department.
- *Configuring filters.* You can use DAX language commands to create measures and filters that define what data is visible for each role. These filters can be applied in the Power BI interface or in the Power Query editor using the UserName () method to reference the logged- in user.

2. Use of credentials and secure connections

- *Secure Connections.* When connecting to data sources, we need to ensure that secure authentication methods are used. For example, using Windows authentication, token -based authentication depending on the data source.
- *Creating credentials.* Power Query allows you to save credentials for the data sources you connect to, which helps restrict unauthorized access.

3. Data protection in storage locations

- *Data persistence.* It is necessary to ensure that sensitive data is stored in secure locations, such as SQL servers with limited access or cloud services that offer advanced security options.
- *Securing export files.* When exporting data from Power Query, we need to ensure that the files are encrypted or password protected, especially if they are sent via email or stored in unsecured environments.

4. Audit and Monitoring

- *Data access monitoring.* In Power BI services, you can enable audit logs to monitor who has accessed what data. This includes the history of interactions with reports and dashboards.
- *Usage reporting.* Internal reports are created to track data usage across projects so you can assess who has access to what information.

5. Using parameters in Power Query

- *Parameters for filtering data.* You can use parameters in Power Query to control which datasets are loaded into the model. For example, we could have a user-based filtering parameter that determines what data is retrieved based on the user's context.

6. Formatting report files

- *Limit data visibility.* When creating a report in Power BI or Excel, you can control which views are available to end users so that they cannot access sensitive data.

Security method *Adding a digital signature* to an Excel file is an important security method because it ensures the authenticity and integrity of the file. A digital signature confirms that the document has not been modified after it was signed and that it comes from a trusted source. To add a digital signature, you need a digital certificate. This can be obtained from a certificate service provider. The algorithm for adding a digital signature to an Excel file (File > Info > Protect Workbook > Add a Digital Signature > select the digital certificate from the available list > you can add a message, for example, “Signed by [Name]” which will appear with the signature > Sign) is the first part of this security level. Next, save the file.

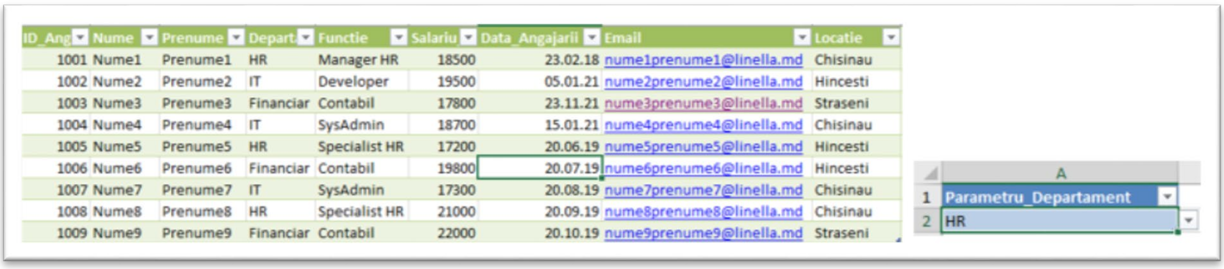
If the file was digitally signed and someone modified something, the digital signature will become invalid, and when opening the file, a message will be displayed saying that the file has been modified after signing. Information about the data modification can be found in the File > Info tab. Under the Sign section, the signature details will be displayed and its validity can be verified.

The digital signature can be verified. When another user opens the signed file, the first user will be able to verify the digital signature to ensure that the file has not been modified. To do this, open the signed Excel file, File tab, Info option, Under the Sign section, you will see the details of the signature and can verify its validity.

In the Power Query application, information security is also provided because data is imported from external sources. These sources can be:

- *Files* (Excel Workbook, -. xlsx,. xls, CSV / Text,-. csv,. txt, XML, JSON, Folder,- it imports all files from a folder, PDF, - available in Power BI and recent versions of Excel)
- *Databases* (SQL Server, Access, Oracle, MySQL, PostgreSQL, IBM DB2, Teradata, SAP HANA, Azure SQL Database and others)
- *Online services / Cloud* (SharePoint Folder / List, OneDrive, Google Sheets, - via web connector, Salesforce, Microsoft Exchange, Dynamics 365, Facebook, Azure Blob Storage, Azure Data Lake Storage)
- *Web / API sources* (Web Page, - scraping or extracting tables from a web page, REST APIs, - using the *Web connector* + authentication). Scraping means automatically extracting information from a web page, such as bringing a table with exchange rates that can then be updated whenever necessary without having to Copy / Paste each time. In Excel, data sources are imported using Data > Get Data and in Power BI we connect via Home > Get data.

Case study 1: Suppose a company that has employee salary data in an Excel file wants department managers to be able to manage and view only the employee data in their own department, without having access to the other information. The Excel file consists of 2 sheets. The “ Employees ” sheet with a table full of fictitious data containing *information about employee salaries, divided by departments (Finance, HR, IT) and the "Parameter" sheet with a single cell where you can enter a department (ex: HR, IT, etc.), which will be used as a dynamic parameter in Power Query for filtering*

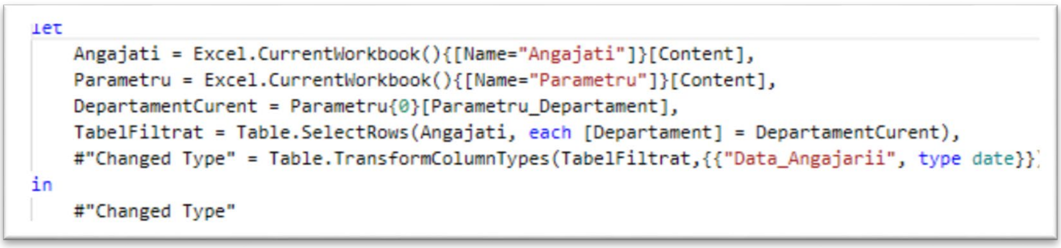


ID_Ang	Nume	Prenume	Depart	Functie	Salariu	Data_Angajarii	Email	Locatie
1001	Nume1	Prenume1	HR	Manager HR	18500	23.02.18	nume1prenume1@linella.md	Chisinau
1002	Nume2	Prenume2	IT	Developer	19500	05.01.21	nume2prenume2@linella.md	Hincesti
1003	Nume3	Prenume3	Financiar	Contabil	17800	23.11.21	nume3prenume3@linella.md	Straseni
1004	Nume4	Prenume4	IT	SysAdmin	18700	15.01.21	nume4prenume4@linella.md	Chisinau
1005	Nume5	Prenume5	HR	Specialist HR	17200	20.06.19	nume5prenume5@linella.md	Hincesti
1006	Nume6	Prenume6	Financiar	Contabil	19800	20.07.19	nume6prenume6@linella.md	Hincesti
1007	Nume7	Prenume7	IT	SysAdmin	17300	20.08.19	nume7prenume7@linella.md	Chisinau
1008	Nume8	Prenume8	HR	Specialist HR	21000	20.09.19	nume8prenume8@linella.md	Chisinau
1009	Nume9	Prenume9	Financiar	Contabil	22000	20.10.19	nume9prenume9@linella.md	Straseni

	A
1	Parametru_Departament
2	HR

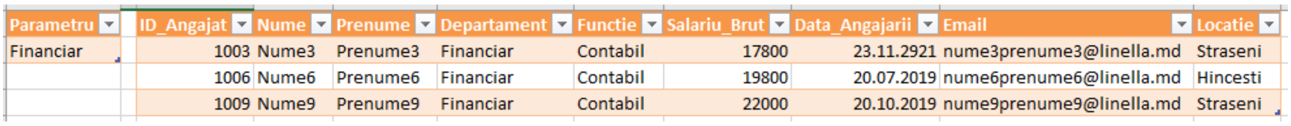
Figure 1. Preparing data from both pages.
Source: *Own research.*

The algorithm for solving this case consists of several steps: preparing the data from both sheets, figure 1, importing these tables into Power Query and creating a parameter by writing code in the M language, figure 2, exporting to Excel and creating a validated source for selecting the department, figure 3.



```
let
    Angajati = Excel.CurrentWorkbook(){[Name="Angajati"]}[Content],
    Parametru = Excel.CurrentWorkbook(){[Name="Parametru"]}[Content],
    DepartamentCurent = Parametru{0}[Parametru_Departament],
    TabelFiltrat = Table.SelectRows(Angajati, each [Departament] = DepartamentCurent),
    #"Changed Type" = Table.TransformColumnTypes(TabelFiltrat,{{"Data_Angajarii", type date}})
in
    #"Changed Type"
```

Figure 2. A Power Query parameter with M language.
Source: *Own research.*

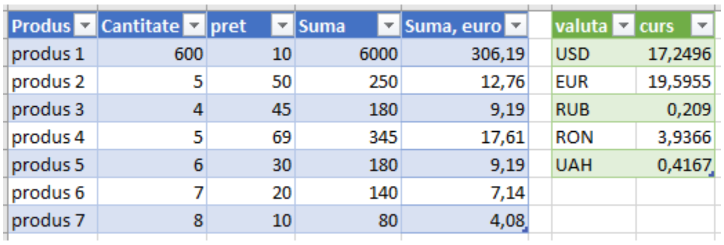


Parametru	ID_Angajat	Nume	Prenume	Departament	Functie	Salariu_Brut	Data_Angajarii	Email	Locatie
Financiar	1003	Nume3	Prenume3	Financiar	Contabil	17800	23.11.2921	nume3prenume3@linella.md	Straseni
	1006	Nume6	Prenume6	Financiar	Contabil	19800	20.07.2019	nume6prenume6@linella.md	Hincesti
	1009	Nume9	Prenume9	Financiar	Contabil	22000	20.10.2019	nume9prenume9@linella.md	Straseni

Figure 3. **A single department in the filter list.**
Source: *Own research.*

Case study 2: A company, whose activity consists of purchasing and selling various products, uses data on the official exchange rate in calculations and for this purpose aims to automate the process of taking over the official exchange rate from the NBM website with the creation of a history of changes during the activity. Also, to protect the data and prevent information leaks, the company wants to establish a level of confidentiality so that only people inside the company have access.

To solve this case study, it is necessary to import the exchange rate table into Excel or Power BI without copying it with copy -paste, by entering the website URL in the From Web option.



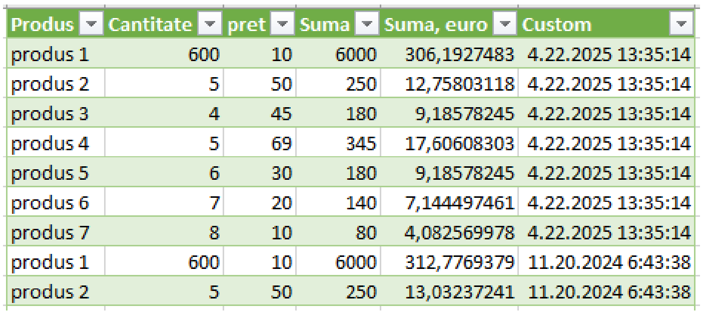
Produs	Cantitate	pret	Suma	Suma, euro
produs 1	600	10	6000	306,19
produs 2	5	50	250	12,76
produs 3	4	45	180	9,19
produs 4	5	69	345	17,61
produs 5	6	30	180	9,19
produs 6	7	20	140	7,14
produs 7	8	10	80	4,08

valuta	curs
USD	17,2496
EUR	19,5955
RUB	0,209
RON	3,9366
UAH	0,4167

Figure 4. Product data and official exchange rate.
Source: *Own research.*

Select the required table, import it into the Excel or Power BI editor, perform the necessary transformations, define the confidentiality level and export it to Excel or Power BI, for use in calculations, figure 4. Next, whenever it is necessary to update the exchange rate data, Refresh is performed, figure 5.

To protect data and prevent information leaks between data sources, Power Query implements a three-level privacy system: *public, organizational and private.*



Produs	Cantitate	pret	Suma	Suma, euro	Custom
produs 1	600	10	6000	306,1927483	4.22.2025 13:35:14
produs 2	5	50	250	12,75803118	4.22.2025 13:35:14
produs 3	4	45	180	9,18578245	4.22.2025 13:35:14
produs 4	5	69	345	17,60608303	4.22.2025 13:35:14
produs 5	6	30	180	9,18578245	4.22.2025 13:35:14
produs 6	7	20	140	7,144497461	4.22.2025 13:35:14
produs 7	8	10	80	4,082569978	4.22.2025 13:35:14
produs 1	600	10	6000	312,7769379	11.20.2024 6:43:38
produs 2	5	50	250	13,03237241	11.20.2024 6:43:38

Figure 5. Updated data and change history.
Source: *Own research.*

To configure privacy levels in Power Query, the user must assign one of the levels to each data source.

These levels are designed to prevent information leaks, especially in scenarios where data from multiple sources is combined, such as internal databases and external or public files.

For example, if a data source is labeled as “Private”, Power Query will avoid any interaction with “Public” or “Organizational” sources that may contain less sensitive information. This protects the integrity and confidentiality of the data, preventing combinations that could accidentally expose certain information.

This method of privacy management also helps organizations meet legal requirements and data protection regulations, such as GDPR (General Data Protection Regulation), while protecting customer and employee data.

In Excel, after accessing the data source and opening the editor Power Query, privacy levels is activated from the tab File > Options and Settings > Data Source Settings > Edit Permissions and select one of the options *public, organizational or private.*

In Power BI desktop, after opening, activate the Transform tab, Power Query, File, Options and settings, Query Options, Privacy section.

Setting the privacy level *to Public* means that the data sources do not contain sensitive information and are accessible to the general public.

Organizational privacy level will make the data sources internal to the organization and not accessible to the general public.

Private privacy level is required for data sources containing sensitive or confidential information that needs to be protected.

To avoid data leaks, if data from multiple sources is to be combined, it is necessary that the confidentiality levels are set correctly for all of them. For example, do not combine *Private sources* with *Public sources.*

CONCLUSIONS

It is very important that users know how data security is achieved.

In the digital age, data security and access management are essential to protect sensitive information and ensure a safe work environment. Microsoft tools, such as Excel, Power Query, and Power BI, offer a powerful set of functionalities that allow users to manipulate and analyze data effectively.

By using built-in security features such as encryption, permissions management, and authentication, organizations can control access to sensitive data, protecting it from unauthorized access. Also, the auditing and monitoring options available in these tools allow companies to follow compliance guidelines and improve transparency in data management.

Integrating good access management and data security practices into daily workflows not only supports information protection, but also helps increase trust and collaboration.

By adopting effective data security and access management measures, organizations can benefit from the analytical power of data without compromising its integrity and confidentiality. All of this supports the creation of an organizational culture oriented towards security and accountability.

REFERENCES

1. Airinei, D., Grama, A., Fotache, D., Georgescu, M., Munteanu, A., Dospinescu, O., Popescul, D., Păvăloaia, D. *Information technologies applied in organizations*. Iaşi: Alexandru Ioan Cuza University, 2017.
2. Ionescu, A., Popa, D. *Securitate și confidențialitate în instrumentele BI bazate pe cloud*. Revista: Management Informațional, Vol. 18(2), pp. 112–128, 2022
3. Georgescu, M. *Guvernanța datelor în mediile Business Intelligence self-service.* Revista: Sisteme Informaționale, Vol. 16(4), pp. 85–101, 2022
4. *Security in Excel*. Available at: https://learn.microsoft.com/en-us/office/troubleshoot/excel/security-in-excel [Accessed 21.04.2025]
5. *Power BI security*. Available at: https://learn.microsoft.com/en-us/power-bi/enterprise/service-security [Accessed 1.05.2025]
6. *Row-level security (RLS) in Power BI.* Available at: https://learn.microsoft.com/en-us/power-bi/enterprise/service-security-row-level-security [Accessed 8.05.2025]

THE EFFECTS AND CHALLENGES OF COVID-19 ON DIGITAL TRANSFORMATION IN THE DEMOGRAPHIC AND ECONOMIC SECTOR

UDC: 616-036.22:[004.7:338.05](478)
DOI: https://doi.org/10.53486/tids2025.23

ION PÂRȚACHI
Academy of Economic Studies of Moldova
ipartachi@ase.md
ORCID ID: 0000-0002-8042-983X

SIMION MIJA
Academy of Economic Studies of Moldova
mija.simion@ase.md
ORCID ID: 0009-0000-0814-5982

CLAUDIU HERȚELIU
Bucharest University of Economic Studies
hertzi@ase.ro
ORCID ID: 0000-0001-8860-9547

Abstract. The digital transformation, in the demographic and economic sectors, has been accelerated by the COVID-19 pandemic, and has led to the rapid adoption of digital technologies, which have increased productivity and operational resilience. The COVID-19 pandemic has highlighted significant digital divergences, driven by age, education, income and location-based gaps, affecting access to remote work and digital services. Workers in digital area or with digital roles have been relatively protected, while employees in the traditional sector have faced increased vulnerability. In addition, the shift to remote work has raised challenges in terms of workforce management, cybersecurity and infrastructure. While digital technology adoption has increased, ***evidence of lasting structural changes in labor demand remains limited, indicating that the pandemic has acted more as a catalyst than a transformer.*** Addressing the digital differences and investing in skills and infrastructure are essential to ensure an inclusive and sustainable economic recovery.

Keywords: Covid-19, digital transformation, digital services, statistical analysis.

JEL Classification: C10, C46, C51.

INTRODUCTION

The COVID-19 pandemic has had a propound impact on societies and economies around the world, accelerating the already underway process of digitalization and all the proceses connected eith, and requiring sharply adaptation in numerous areas. In the case of the Republic of Moldova, a country on the way to be aligning with European standards, the health crisis has represented a major test for its digital capabilities and level of strategic preparedness. This research examines the multifaceted effects and challenges of COVID-19 on digital transformation within Moldova's demographic and economic sectors, analyzing how the crisis accelerated the journey towards a comprehensive digital future.

Digital transformation is understood as a fundamental process involving the adoption and integration of digital technologies to create new or modify existing products, services, and operations by translating business processes into a digital format. Digital transformation is not limited to digitizing existing functions but involves a profound rethinking of the way how the organizations interact with their customers, employees and partners. This leads to the development of new business models and a more efficient use of internal resources. The change is driven by advanced technologies that allow for the optimization of the processes, the analyses of data in the way to obtain relevant insights and delivery of innovative products and services. However, all these developments crucially depend on reliable and equitable access to the internet — the basic infrastructure that connects people, devices and systems. Without widespread connectivity, the benefits of digitalization remain inaccessible to a large part of the population, increasing digital disparities and hindering inclusive economic and social progress. In this context, ensuring universal access to the internet is not only a technological challenge, but also an essential condition for equity in the digital age, facilitating innovation, education and sustainable development at a global level.

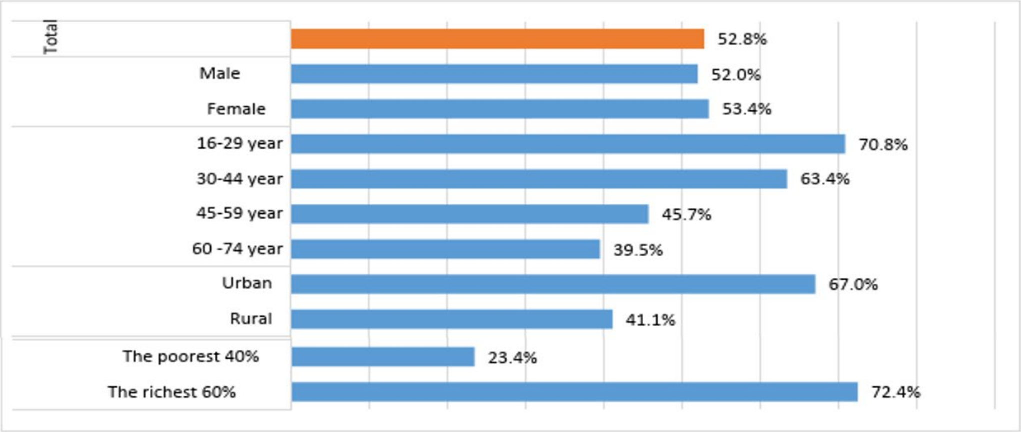


Figure 1. Household computer ownership rate.

Source: *E-governance Agency, World Bank.*

Digital transformation opens up vast prospects for economic development and social progress, influencing all areas – from health and education to energy and agriculture. This comprehensive approach highlights that digitalization is not limited to technological updates but involves a profound reconfiguration of economic and social structures. In this context, the success of the transformation process does not depend exclusively on the technical infrastructure, but also on the existence of sound public policies, the capacity of organizations to adapt, widespread digital skills and an effective governance system.

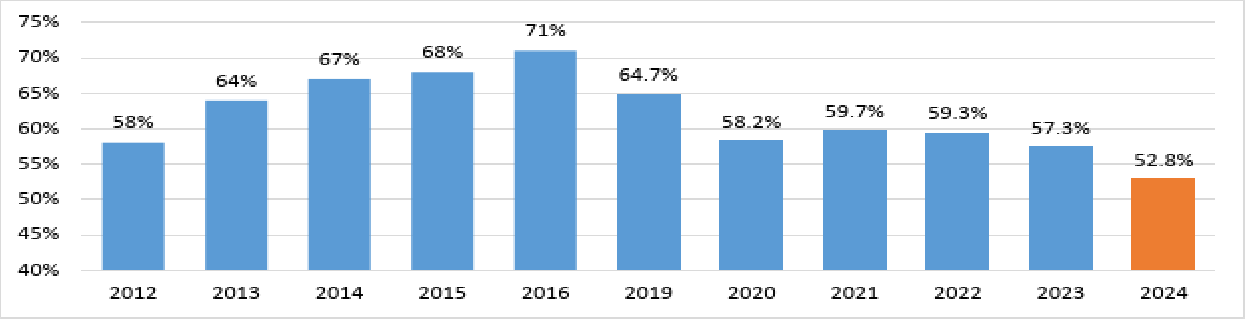


Figure 2. Trends in household computer ownership.

Source: *E-governance Agency, World Bank.*

In Republic of Moldova, according to the National Survey 2024 of *"The perception, adoption, and support of e-Government and the modernization of government services by the population"*, in recent decades, has been a rapid process of computerization of households, along with an increase in internet access levels. At the same time, other processes have unfolded that have further driven digitalization. Over time, the previously rising trend of computerization shifted to a decline, influenced by the widespread availability of smartphones among the population. The internet has taken on an increasingly important role as a source of information, surpassing television, which has traditionally represented the main means of information for decades.

Over half of households in the Republic of Moldova (52.8%) have a computer at home (Figure 1). However, the indicator of computer ownership has registered a constant downward trend during the COVID-19 pandemic and in the post-crisis period: 52.8% in 2024, compared to 57.3% in 2023, 59.3% in 2022, 59.7% in 2021 and 58.2% in 2020. This decrease is significant compared to the maximum level of 71% reached in 2016 (Figure 2).

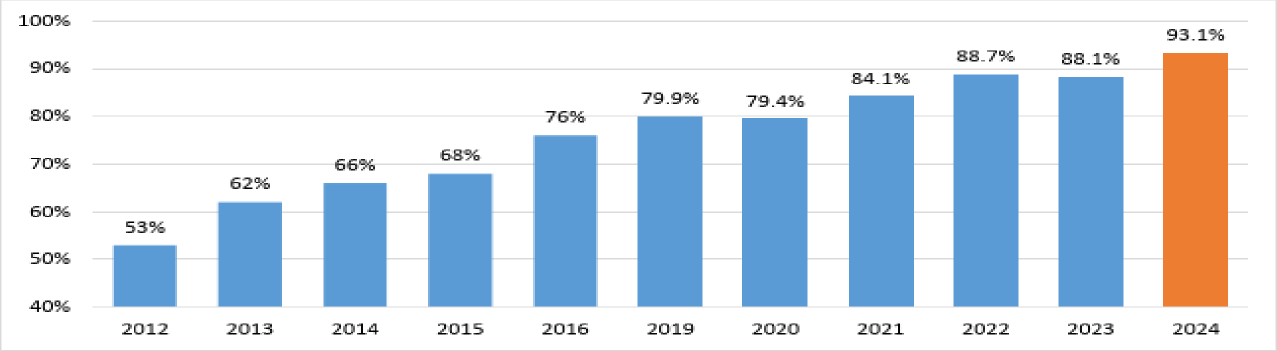


Figure 3. Trends in household internet access.
Source: *E-governance Agency, World Bank.*

This trend can be explained by changing preferences in terms of ways of accessing the internet – an increasing number of people use other types of devices, especially mobile phones. This change is supported by data from the same study, which shows that the majority of households without a computer (85.8%) are nevertheless connected to the internet. In fact, the overall rate of internet connection (93.1%) significantly exceeds the rate of computer ownership (Figure 3).

COVID-19 as a Catalyst for Digital Acceleration. The COVID-19 pandemic has undeniably accelerated the digital transformation process, both globally and in the Republic of Moldova. Mobility restrictions and the urgent need for remote access to services in all areas of life have driven a rapid transition to digital solutions. Areas such as online education, e-commerce and e-health services have seen rapid and significant growth in demand. This crisis has clearly highlighted the need for enhanced support and substantial investments in digital transformation, as well as the importance of effective digital governance – essential for ensuring the continuity of basic public services and strengthening the resilience of the private sector (Figure 4).

In recent years, the internet has increasingly become the main source of information for the population. According to the 2024 study *"Perception, Adoption and Support of e-Government and the Modernization of Government Services by the Population"*, three quarters of respondents (75%) consider the internet to be the most important channel for accessing information. This trend reflects the changing way people consume news and information, increasingly turning to the digital environment at the expense of traditional sources.

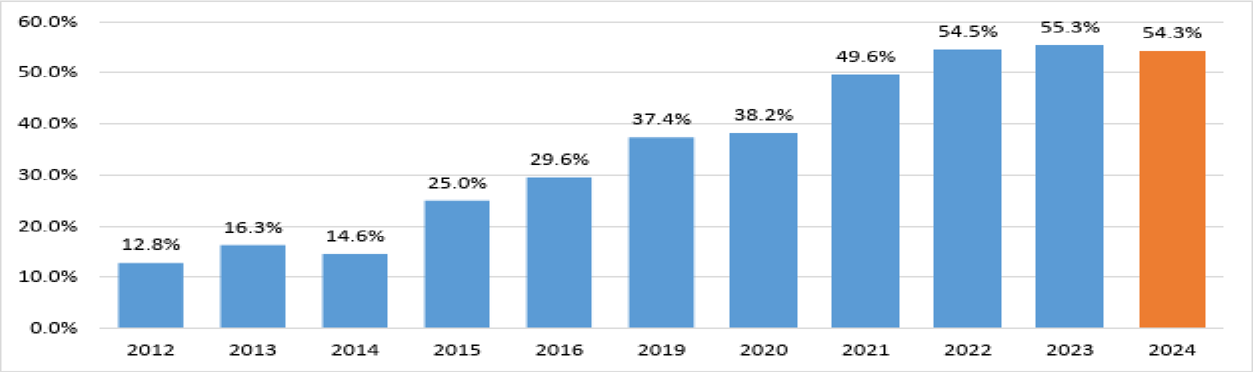


Figure 4. Access of the electronic public services over the past 12 months.
Source: *E-governance Agency, World Bank.*

The COVID-19 pandemic period has shown that the adoption of digital technologies was initially carried out in a reactive manner, driven by immediate needs rather than long-term strategic planning. While the crisis undoubtedly accelerated the rapid use of digital solutions, it also highlighted systemic vulnerabilities that, in a more gradual and well-structured process, could have been addressed more effectively and comprehensively. In the context of an immediate emergency, the priorities were survival and ensuring the continuity of services, which led to the rapid implementation of already existing digital tools. Thus, the challenge for the Republic of Moldova in the post-pandemic period is to transform this accelerated and temporary reaction into a strategic, sustainable and coherent digital transformation process that integrates the solutions adopted in the emergency into a solid and long-term national digital agenda.

EFFECTS ON THE DEMOGRAPHIC SECTOR

The COVID-19 crisis has had a profound impact on the demographic sector in the Republic of Moldova, highlighting and, in many cases, exacerbating existing inequalities related to access to technology and digital skills. At the same time, this situation has spurred initiatives to reduce these disparities by accelerating the digitalization of public services and the education system.

1. Exacerbation and Bridging of the Digital Divide (Urban-Rural, Age, Income)

Although the pandemic has accelerated internet use in the Republic of Moldova, it has simultaneously accentuated the already existing digital gaps between various segments of the population. (Figure 5) In the Republic of Moldova, **significant disparities persist in access to connectivity between urban and rural areas**, and socio-economic inequalities are evident in the ownership of digital equipment, with rates of 60-70% recorded for the wealthiest households, compared to only 20-35% for the most financially vulnerable. *This disparity meant that access to essential digital tools was largely a function of economic status.*

Older populations, particularly people aged 60 and above, faced substantial difficulties due to a pervasive lack of digital skills and limited internet access. This technological barrier led to increased social isolation and considerable struggles in accessing online social services (Goharik, 2024).

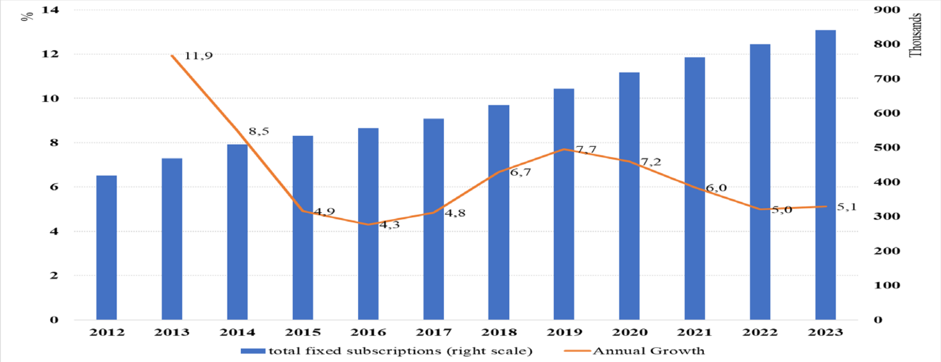


Figure 5. Moldova - Fixed Broadband Internet Subscribers.
Source: *World Bank.*

For example, in July 2020, at the peak of COVID-19 infections, many older adults who lacked access to online social services were forced to queue in person at the National Social Insurance House to request pension recalculations. Often without adequate personal protective equipment, they faced significant exposure to health risks. This situation clearly illustrates how the crisis, by forcing a digital shift, disproportionately benefited those already digitally capable or resourced, effectively widening the gap for vulnerable and underserved populations, *Bringing generations together for change. Case study: Moldova*, (2022). The crisis-driven demand for digital services, without sufficient pre-existing digital literacy and equitable access mechanisms, directly led to the increased isolation and exclusion of these vulnerable groups, amplifying pre-existing inequalities.

In response to these challenges, concerted efforts were made to bridge these divides. Initiatives and programs that connected youth with seniors, provided mobile phones and comprehensive training in basic digital skills, including the use of communication and messaging apps, social networks, and online payments.

These efforts were specifically designed to combat the isolation experienced by older people and improve their access to essential services, simultaneously fostering intergenerational dialogue and understanding. Furthermore, the authorities, mostly with international support, have assisted educational institutions by equipping schools across the country with modern technology such as computers, smartboards, projectors, aiming to narrow the digital gap in education (Botezatu, 2021).

2. Digitalization of Public and Social Services: Continuity and Challenges

The COVID-19 pandemic has exposed Moldova's major vulnerabilities, stemming from its traditional reliance on offline and paper-based government processes, which have severely disrupted the continuity of public services and exposed government employees to increased risks of contamination. In response, the authorities have significantly stepped-up efforts to implement digital governance, focusing on the digital inclusion of vulnerable groups and stimulating the development of participatory digital solutions, achieved through innovative collaborations with the private sector.

Significant progress has been made in the digitalization of public services. By 2024, 54% of public services were digitalized, and an impressive 86.1% of government-to-business service requests were conducted online. The variations in the indicator regarding access to electronic public services across socio-demographic categories are very pronounced. Young people aged 18–29 have used electronic services nearly six times more often than individuals aged 60–74 (Figure 6).

The discrepancy among population categories from different residential environments is nearly 30%. There is a huge difference in the same indicator when comparing individuals with incomplete secondary education to those with higher education. Household internet connection is a variable that significantly influences access to electronic public services, increasing the likelihood by 2-3 times.

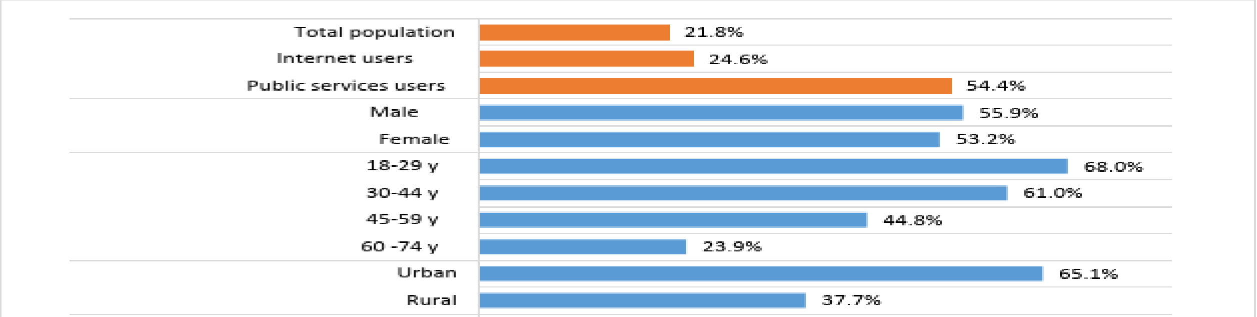


Figure 6. The profile of electronic service users.
Source: *E-governance Agency, World Bank.*

3. Shifts in Social Interactions, Digital Skills and Literacy Gaps: A Critical Barrier

The COVID-19 pandemic, with its stringent mobility restrictions, significantly increased the demand for digital services, implicitly driving a notable shift in social interactions from physical to online spaces. This forced transition, however, also led to heightened isolation for those segments of the population lacking adequate digital access and skills, particularly the elderly. For instance, older individuals, already prone to isolation, found their limited social contact further constrained by the inability to communicate with family and friends through digital means.

Conversely, the crisis also spurred governmental and organizational shifts towards leveraging data for better understanding and managing population behavior, *Socio-economic impact assessment of COVID-19 in the Republic of Moldova* (2020).

Despite the overall acceleration in internet use during the COVID-19 pandemic, Moldova faced significant and pervasive digital literacy gaps across various societal segments, including the general population, government officials, and Small and Medium-sized Enterprises (SMEs). A notable absence of systematic assessments of digital skills further compounded this issue, making it challenging to precisely identify and address specific deficiencies.

This situation underscores that while Moldova possessed a decent digital infrastructure, its human capital, in terms of digital skills and literacy, lagged significantly. This gap became a major impediment to the effective and equitable adoption of digital transformation across critical sectors. The digital divide is not merely a singular problem of “access” but a complex interplay of infrastructure availability, affordability, equipment ownership, and, crucially, digital literacy and trust. Addressing one component in isolation, such as merely expanding infrastructure, will not resolve the overall challenge of digital exclusion. The pre-existing lack of systematic digital skills assessment and targeted training directly resulted in widespread digital literacy gaps, which in turn limited the effective adoption of digital services during the pandemic, particularly for vulnerable groups and in essential sectors like education and public services. Therefore, policies must adopt a multi-pronged approach, simultaneously targeting infrastructure expansion, affordability, provision of devices, and comprehensive, tailored digital skills training programs that build confidence and address specific user needs and fears related to online payments and government services.

EFFECTS ON THE ECONOMIC SECTOR

The economic landscape of the Republic of Moldova underwent significant changes due to the pandemic, with digital transformation playing a dual role as both a driver of adaptation and a source of new disparities.

Business Adaptation, E-commerce Growth, and Digital Adoption Patterns. The COVID-19 pandemic compelled local businesses to rapidly adapt their operational models, with approximately one-third initiating or significantly increasing their online business activities. Notably, firms that had a pre-existing history of innovation demonstrated greater resilience in sustaining the economic shock induced by the crisis. This surge highlighted the critical need for developing online payment and banking systems. The government has since responded by developing a national digitalization roadmap specifically focused on e-commerce development, the promotion of online stores, attracting international e-commerce actors, and facilitating cashless payments.

However, while the pandemic undeniably accelerated digital adoption in the private sector, this acceleration was not uniform across all businesses. Evidence suggests that the digital divide among firms increased, with substantial gaps persisting between small and large enterprises, and across different sectors, particularly concerning new investments in digital solutions. Many small and medium-sized enterprises (SMEs) were notably unprepared for the sudden shift to online sales, leading to the cessation of their activities and contributing to an overall economic downturn, with Moldova’s GDP decreasing by 8.3% in 2020. The sudden shift to digital channels during the pandemic, coupled with pre-existing disparities in digital readiness and access to resources, directly led to an increased digital divide among firms and a concentration of online sales supported by the online transactions with payment cards (Figure 7).

1. Labor Market Dynamics: Remote Work, Employment, and Skills Demand

The COVID-19 pandemic instigated a rapid and widespread adoption of remote work practices in Moldova. In response to this shift, the Moldovan parliament swiftly adopted regulations concerning telework in May 2020, just two months after the declaration of a national state of emergency. By 2020, an estimated 24,500 individuals were working from home or remotely (NBS, 2021). This transition, while offering significant benefits such as increased flexibility for employees and potential cost savings for businesses (e.g., optimized office spaces and reduced maintenance costs), also introduced a new set of challenges (Cebotari, 2022). These included maintaining employee engagement, ensuring effective communication, and helping individuals achieve a healthy work-life balance amidst the blurring lines between professional and personal spheres.

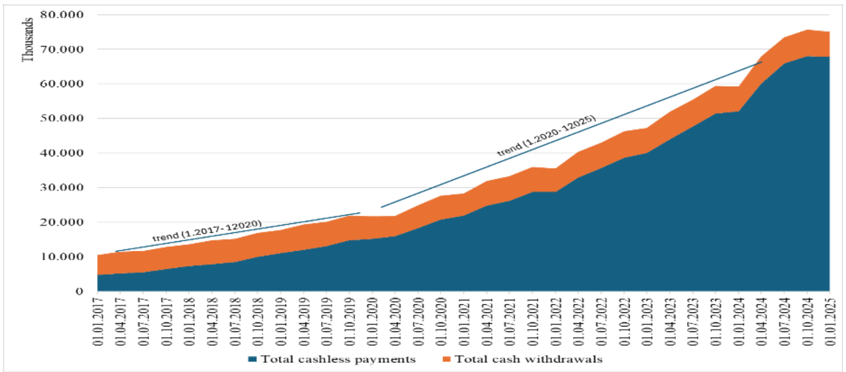


Figure 7. The number of transactions with payment cards issued in the Republic of Moldova.

Source: *National Bank of Moldova.*

The advance of digitalization of the economy has generated a growing demand for specialists with advanced technical skills. However, the persistent skills shortage within the Moldovan workforce risks slowing down the pace and limiting the large-scale impact of the digitalization process. The COVID-19 pandemic has accelerated a profound transformation of the labor market, consecrating remote work as an increasingly common practice. This evolution has highlighted the need to develop not only classic technical digital skills, but also an expanded set of essential digital skills, such as self-management, virtual collaboration and digital communication ethics. The forced adoption of remote work has amplified the demand for such skills, but has also revealed significant gaps in the current training of employees, accentuating the gap between available skills and market requirements, especially in areas that go beyond strictly technical aspects. Consequently, preparing the workforce for the future requires the implementation of continuous improvement and retraining programs, which include the development of both technical expertise and indispensable non-technical digital skills.

upply chain digitization and digital transformation of SMEs

The COVID-19 pandemic has sent a strong signal globally about the crucial importance of supply chain resilience, accelerating the adoption of digital technologies in their management. Digitalization has been shown to significantly contribute to increasing the integration and efficiency of supply chains. In the Republic of Moldova, companies are increasingly active in exploring and implementing logistics innovations, adopting modern technologies and methods aimed at reducing costs, optimizing operations, improving service quality and strengthening their competitive position in the market.

The COVID-19 pandemic has deeply affected SMEs in the Republic of Moldova, which have faced significant difficulties on both the demand and supply sides. The impact has been particularly severe given that SMEs represent approximately 98% of all enterprises, and around 75% of them are micro-enterprises, often lacking the necessary resources — including knowledge and financing — to respond quickly to new market challenges.

At the same time, recent data indicate that less than 17% of SMEs have managed to integrate digital technologies into their activities, highlighting both a considerable untapped potential and a pressing need to accelerate the digitalization process in this sector.

CONCLUSIONS

The COVID-19 pandemic served as a stark and undeniable reminder of the critical importance of digital transformation for national resilience and continuity in the Republic of Moldova. The crisis significantly accelerated the adoption of digital technologies across public services, education, and the economy, compelling rapid shifts that might otherwise have taken years. However, this accelerated shift simultaneously highlighted and exacerbated deep-seated digital divides across various demographic groups and between firms, exposing critical gaps in digital literacy, cybersecurity preparedness, and the “soft infrastructure” of institutional coordination and leadership.

The digitalization during the pandemic simultaneously enabled continued interaction for some while deepening social isolation for others, particularly vulnerable groups. This creates a paradox where technology can both connect and disconnect, depending on equitable access and digital literacy.

In this context, future digital transformation strategies must explicitly integrate the objective of social cohesion, ensuring that the digital solutions developed do not contribute to the involuntary marginalization of certain segments of the population, but on the contrary – facilitate active inclusion, equal participation and intergenerational connectivity. Initiatives such as the "Digital Skills Connect Generations" project, which provides training to seniors in the use of smartphones and social networks, represent concrete steps in this direction, helping them to maintain their social connections and access essential information in the digital environment.

ACKNOWLEDGEMENTS: *Ion Pârțachi, Simion Mija and Claudiu Herțeliu are partially supported by a project "Analysis of the impact of Covid-19 on the main demographic indicators in Romania and the Republic of Moldova by using econometric modeling" code PN-IV-P8-8.3-ROMD-2023-0208 funded by the Romanian Ministry of Research, Innovation and Digitalization (MCID) through UEFISCDI.*

REFERENCES

1. Botezatu, S., UNDP Report, 2021 Digital Transformation of Moldova: there is no way back. October 4. Available at: https://www.undp.org/moldova/blog/digital-transformation-moldova-there-no-way-back [Accessed 20.04.2025]
2. Cebotari M., 2022. Telework in the Republic of Moldova. International Lawyers assisting workers network, Available at: https://www.ilawnetwork.com/wp-content/uploads/2022/12/Moldova-Telework-FINAL.pdf [Accessed 20.04.2025]
3. EU4Digital Report, 2025. More for Moldovans: digital development with EU4Digital. March 12. Available at: https://eufordigital.eu/more-for-moldovans-digital-development-with-eu4digital/ [Accessed 20.04.2025]
4. Goharik, T., 2024. Bridging the digital divide in education: Lessons from Armenia, Moldova and Ukraine. GC Human Rights Preparedness, September 26 Available at: https://gchumanrights.org/gc-preparedness/preparedness-economic-social-and-cultural-rights/article-detail/bridging-the-digital-divide-in-education-lessons-from-armenia-moldova-and-ukraine.html [Accessed 20.04.2025]
5. HelpAge International Report, 2022. Bringing generations together for change. Case study: Moldova. Available at: https://www.helpage.org/what-we-do/society-for-all-ages/bringing-generations-together-for-change/ [Accessed 20.04.2025]
6. National Bureau of Statistics of the Republic of Moldova [NBS], 2021. Labour Force in the Republic of Moldova: Employment and Unemployment. Available at: https://statistica.gov.md/en/statistic_indicator_details/1 [Accessed 20.04.2025]
7. National Survey, 2024. The perception, adoption, and support of e-Government and the modernization of government services by the population. Available at: https://egov.md/ro/node/40721 [Accessed 20.04.2025]
8. UNDP Report, 2020. Socio-economic impact assessment of COVID-19 in the Republic of Moldova. November 25. Available at: https://www.undp.org/moldova/publications/social-and-economic-impact-assessment-covid-19-republic-moldova [Accessed 20.04.2025]

LEADING TECHNOLOGICAL INNOVATIONS IN DIGITAL SECURITY

UDC: 005.334:[004.056:330.341.1]
DOI: https://doi.org/10.53486/tids2025.24

ZORAN ČEKEREVAC
Independent Researcher, Belgrade, Serbia
zoran@cekerevac.eu
ORCID ID: 0000-0003-2972-2472

LYUDMILA PRIGODA
Maykop State Technological University, Maykop, Russian Federation
lv_prigoda@mail.ru
ORCID ID: 0000-0002-4762-3892

Petar Čekerevac
Independent Researcher, Belgrade, Serbia
petar.cekerevac@gmail.com
ORCID ID: 0000-0001-6100-5938

Abstract: Digital security holds critical importance in the era of global digitalization, which increasingly shapes daily life and business practices. Cyber threats such as ransomware, hacking, and data breaches demand continuous improvement of protective strategies to safeguard the integrity, confidentiality, and availability of information. Implementing advanced technologies has become essential for risk mitigation and enhanced system resilience. Innovations such as zero-trust architecture ensure access control and the elimination of implicit trust, while multi-factor authentication (MFA) significantly enhances system security. Artificial intelligence (AI) and machine learning (ML) enable real-time threat detection and response. At the same time, advanced cryptography, including post-quantum algorithms and homomorphic encryption, provides future-proof resilience against emerging threats. Technologies like blockchain and cloud security reduce administrative costs and enhance transparency, while specific protective measures for IoT devices and mobile platforms address their inherent vulnerabilities. Automation and *Security Orchestration, Automation*, and *R*esponse *(*SOAR*)* platforms optimize the efficiency of security teams, enabling faster incident responses. Efficient digital security requires a combination of cutting-edge technologies, user education, and continuous adaptation to the evolving threat landscape. A focus on the contextual needs of users ensures the successful implementation of protective measures. This paper the authors prepared using research methods typical of review articles, including the systematic processes of searching, selecting, analyzing, and synthesizing existing literature. The findings highlight that integrating AI, IoT, and blockchain technologies significantly fortifies digital security within the finance sector. Key benefits include enhanced fraud detection, automated threat response mechanisms, and improved data integrity. Recommended measures for bolstering security encompass advanced encryption protocols, robust authentication techniques, regular software updates, cryptographic validation of transactions, and the automation of smart contracts. Collectively, these technological advancements minimize vulnerabilities, deter malicious actors, and foster greater trust among users.

Keywords: Zero Trust Authentication, Blockchain, IoT, Post-Quantum Cryptography, Homomorphic Encryption, Ransomware.

JEL Classification: C88, D83, K24, L86, M15, O33

INTRODUCTION

Global digitalization has permeated every aspect of modern life, positioning digital security as critically important. With the increasing prevalence of cyber threats such as cyberattacks, hacking, and ransomware, protecting data has become essential for individuals, organizations, and governments. As digital services grow and remote work becomes the norm, new vulnerabilities have emerged, offering cybercriminals opportunities to exploit them and underscoring the critical role of security risk management.

Furthermore, digital security is essential for ensuring compliance with data protection laws, such as the GDPR (2024). Companies now bear significant responsibility for safeguarding their users' data, as trust and reputation are often directly tied to their ability to prevent security incidents.

In an era where the boundaries between the physical and digital realms are increasingly blurred, security impacts everyday life—from online transactions and communications to critical infrastructure, such as energy, healthcare, and finance. Digital security is no longer merely a technical challenge; it is vital for maintaining the stability and safety of society.

1. Methodology

This study employs research methods typical of review articles, including systematic literature searches, selection, analysis, and synthesis. Sources identified were from academic sources like Google Scholar, IEEE Xplore, SpringerLink, and MDPI, alongside reputable websites focusing on information system security. Keywords such as Zero Trust Authentication, Blockchain, IoT, and Post-Quantum Cryptography guided the search.

The selection focused on relevance, quality, and recent publications, complemented by the inclusion of the authors' prior works on related topics. The authors thoroughly evaluated the papers, assessing their validity, reliability, and significance. Through thematic analysis, they uncovered key patterns, which led to the development of a conceptual framework that integrates existing knowledge while highlighting gaps. Bullet points ensured a concise and clear presentation of findings.

This methodology provides insights into digital security advancements while proposing directions for future research.

2. Research Question and Hypotheses

The authors conducted the research based on the following research question and hypotheses:

- *Research Question:* How does integrating advanced technologies such as AI, IoT, blockchain, post-quantum cryptography, and SOAR platforms influence digital security in the financial sector?
- *Null Hypothesis (H_0):* The advanced technologies (AI, IoT, blockchain, post-quantum cryptography, SOAR platforms) integration does not significantly enhance digital security in the financial sector.
- *Alternative Hypothesis (H_1):* The advanced technologies (AI, IoT, blockchain, post-quantum cryptography, SOAR platforms) integration significantly enhances digital security in the financial sector by improving fraud detection, automating threat responses, and ensuring data integrity.

KEY TECHNOLOGICAL INNOVATIONS

Organizations must ensure the security of their networks but also the confidentiality and integrity of their data, especially when dealing with sensitive information. Given attackers' ability to execute diverse and sophisticated attacks, the defense of digital systems requires advanced security measures. These measures must continually evolve as attackers also improve their methods daily. Security innovations are numerous, but they can be grouped and prioritized as follows (Authors, based on (Čekerevac & Radonjić, 2013; Cekerevac, et al., 2025; Brooks, 2010; Wong, et al., 2023; Jore, 2019)):

- Zero Trust architecture - fundamental security approach.
- Multi-factor authentication (MFA) - wide application.
- Artificial intelligence and machine learning - prevention.
- Advanced cryptography - resilience against future threats.
- Blockchain technology - data security.
- Cloud security - growth of cloud-based data).
- Security Information and Event Management (SIEM) - real-time monitoring.
- Mobile Device Management (MDM) platforms - mobile device protection.
- Security orchestration and automation - operational efficiency.

3. Zero Trust Authentication

Using the principle of "never trust by default, always verify", Zero Trust architecture represents a fundamental approach to digital security (Jena, 2023). The core idea behind this model is that access to resources is never automatically granted—even within an organization's network—requiring continuous verification of the identity and authority of every user and device.

The main components of the Zero Trust model include (Authors, based on (Dhiman, et al., 2024; Gambo & Almulhem, 2025; Hartl & Brack, 2024; Cekerevac, et al., 2025)):

- Micro-segmentation: Dividing the network into smaller zones to restrict potential attacker movements.
- Multi-factor authentication (MFA) - multi-layered user identity verification using additional factors such as mobile codes, biometrics, or token devices.
- Continuous monitoring, that is, the user and device activities constantly tracking to detect anomalies and unauthorized access attempts.
- Least privilege principle: Granting users only the minimum level of access required to complete their tasks, thereby reducing potential damage in case of compromise.
- The Zero Trust model is applied across various industries, ranging from healthcare institutions that protect sensitive patient data to airports, where ensuring infrastructure and operational security is critical**.**

4. Multi-factor Authentication

Multi-factor authentication (MFA) is a security process that requires users to verify their identity using two or more authentication factors, significantly enhancing protection levels. That means that, in addition to username and password, users must provide additional verification to access an account or service.

Authentication factors can include (Authors, based on (Abhishek, et al., 2013; Ometov, et al., 2018)):

1. Something the user knows: Information such as passwords, PINs, or answers to security questions.
2. Something the user has: Physical devices or resources the user possesses, such as:
   - A mobile phone (used to receive codes via SMS, authentication apps, or email).
   - A token device (hardware that generates one-time codes).
   - Smart cards.
3. Something the user is: This refers to biometric characteristics, such as:
   - Fingerprints.
   - Iris or facial scans.
   - Voice recognition.
4. Somewhere the user is / Someone the user knows. When attempting to log in:
   - The user enters their username and password.
   - The system requires an additional factor, such as a one-time code sent via SMS or a fingerprint scan.
   - Upon entering the additional factor, the user gains access.

For example, even if an attacker gains knowledge of a user's password, they cannot access the account because they lack the second factor, such as the user's phone or biometric data.

MFA is vital because it ensures:

- Enhanced security: Prevents unauthorized access, even if the password is compromised.
- Protection of sensitive data: Essential for banking and business systems, where confidential documentation is stored.
- Phishing resistance: Even if an attacker deceives a user into revealing their password, the second factor, typically, remains inaccessible.

5. Artificial Intelligence and Machine Learning

Artificial intelligence (AI) and machine learning (ML) are utilized for identifying patterns and anomalies in data, aiding in threat prevention and detection. AI plays a pivotal role in enhancing digital security, particularly in banks and government institutions, but it simultaneously serves as a tool for malicious actors.

On the positive side, AI in security offers several advantages (White, 2025; Malatji & Tolah, 2024). Among these is the ability to rapidly analyze large volumes of data in real time and identify suspicious activities, such as unauthorized access or unusual usage patterns. AI can also detect anomalies in network traffic that may indicate hacking attempts. By employing ML, AI can identify and block malware before it causes damage (Antić, 2024). Precise identity management and access control strengthen security, especially concerning sensitive information. Additionally, AI automates security checks and incident responses, reducing reaction time and increasing the efficiency of security teams.

However, from a user perspective, AI introduces certain risks. Malicious actors can leverage AI to develop sophisticated attack methods, such as phishing campaigns, adaptive malware, and deepfake technologies. Data analysis powered by AI can pose risks to privacy and security, especially when sufficient protective measures are lacking. Beyond technical challenges, ethical considerations arise, such as transparency and accountability in AI-driven decision-making.

Analyzing the potential applications of AI must always consider worst-case scenarios. Offensive AI attacks reveal their complex and dynamic nature, necessitating adaptive defensive mechanisms that AI can support. Every AI-driven attack has multidimensional implications, strategies, motivations, and societal consequences, significantly complicating protection and underscoring the need for even more advanced defensive methods.

Defensive AI employs AI techniques to safeguard computer systems and networks against attacks (e.g., anti-malware systems, intrusion detection systems—IDS). Offensive AI utilizes AI techniques to attack computer systems (e.g., developing new cyber-attacks, and automating the exploitation of existing vulnerabilities). Adversarial AI is maliciously used to exploit AI/ML systems and data, including poisoning training data and manipulating input data (Malatji & Tolah, 2024).

6. Advanced Cryptography

Advanced cryptography encompasses sophisticated techniques and algorithms to protect data and communications in modern digital systems. These methods address increasingly complex threats and ensure security in various scenarios, including financial transactions, government secrets, and personal data. Advanced cryptographic techniques, such as quantum cryptography, enhance data security, making it more challenging for unauthorized parties to gain access.

One key aspect of advanced cryptography is the application of asymmetric algorithms, such as RSA (Rivest-Shamir-Adleman) and ECC (Elliptic Curve Cryptography), which use a pair of keys—a public key and a private key—for encryption and decryption. These algorithms rely on mathematical problems, such as the factorization of large numbers or discrete logarithms, which are extremely difficult to solve without the appropriate keys. (Ahmed & Ahmed, 2022)

Post-quantum cryptography is becoming increasingly important with the development of algorithms designed to resist quantum computer attacks. These algorithms, including lattice-based and code-based methods, ensure the long-term security of data, even in the era of quantum computing.

Hash functions are another critical component of advanced cryptography. They are used to verify data integrity and create digital signatures. Hash functions, such as SHA-256, generate unique data summaries crucial for authentication and detecting unauthorized changes (Mironov, 2005).

Advanced cryptography encompasses techniques such as homomorphic encryption, enabling the processing of encrypted data without decryption, and zero-knowledge proofs, allowing claims to be verified without revealing any additional information.

These methods find application in areas such as blockchain technology, IoT device security, and cloud security.

7. Blockchain Technology

Blockchain technology enables decentralized and transparent data protection, ensuring its integrity and authenticity. It is ideal for securely storing and verifying transactions, reducing the risk of fraud and data manipulation (Cekerevac, et al., 2018).

In finance, blockchain plays a significant role by enabling transactions without time constraints, independent of banks and governments. Advances in hardware and communications accelerate transactions while increasing market capitalization stabilizes cryptocurrency values. Additionally, blockchain reduces transaction costs by eliminating intermediaries and reducing administrative requirements (Cekerevac & Cekerevac, 2022).

Blockchain technology is resistant to many attacks, including MITM attacks, but connected IoT devices may be compromised if they are not adequately secured (Cekerevac, et al., 2017). That can endanger blockchain, for example, through compromised data, manipulation of smart contracts, DDoS attacks, device identity theft, or ransomware attacks. Mitigating these risks requires the implementation of strong security measures for IoT devices and networks, along with ensuring the integrity of blockchain systems.

Preventing attacks requires secure communication between IoT devices and the blockchain network, encryption, authentication, secure system boot processes, and regular software updates. IoT device identification involves unique recognition through serial numbers and MAC addresses, while authentication utilizes certificates, digital signatures, or cryptographic methods to verify authenticity. Data verification includes checking sensor readings, software versions, and security configurations.

When a device with the appropriate certificate accesses the blockchain network, verification includes initial checks, continuous monitoring, cryptographic methods for transaction verification, and automated smart contract processes. Strong security measures help reduce risks and protect IoT devices and blockchain networks.

8. Cloud Security

An increasing volume of data is migrating to the cloud. Innovations in cloud security include improved access management, data encryption, and activity monitoring within the cloud. Key cloud security innovations encompass the Zero Trust approach, AI and machine learning, data encryption at rest and in transit, specific measures for container protection, security automation, post-quantum cryptography, and Secure Access Service Edge (SASE). SASE integrates network functions and security services into a unified platform, enabling safer cloud access from any location (Chen, et al., 2023).

A fundamental element of cloud security is multi-factor authentication (MFA), which facilitates multi-layered verification of user identities.

9. Security Information and Event Management (SIEM)

Security Information and Event Management (SIEM) platforms are vital for real-time monitoring, analysis, and response to cyber threats, empowering organizations to act swiftly and decisively. Advanced technologies, such as artificial intelligence (AI) and machine learning (ML), enable the analysis of large data volumes, anomaly detection, and prediction of potential attacks. These capabilities contribute to automated responses and a reduction in reaction times. (González-Granadillo, et al., 2021)

The Zero Trust model increasingly contributes to ensuring controlled access to resources, while post-quantum cryptography and advanced encryption algorithms provide resilience against future quantum threats. These innovations make SIEM platforms more scalable, robust, and efficient in addressing modern cyber challenges.

10. Mobile Device Management (MDM) Platforms

Mobile Device Management (MDM) platforms allow organizations to manage and secure mobile devices that access corporate data. MDM requires cutting-edge technological advancements to fully protect data and devices in an increasingly complex digital environment. Key innovations include (Authors, based on (Glowinski, et al., 2020; Barthwal, 2016; Howell, et al., 2023)):

- Biometric authentication: Technologies such as facial recognition, fingerprint scanning, and voice analysis provide reliable user identity verification, reducing the risk of unauthorized access.
- Zero Trust model: Applied to mobile devices through continuous verification of user identity and authority, ensuring security even in environments with multiple access points.
- AI and machine learning: Artificial intelligence aids in the real-time detection of anomalies and threats, enabling rapid responses to potential attacks.
- Data encryption: Advanced encryption algorithms secure data during transmission and storage, mitigating the risk of information theft.
- Application management: MDM platforms employ technologies to control the installation and use of applications, preventing the spread of malware and unauthorized programs.
- Automated security checks: Automated processes allow for the rapid identification of mobile device vulnerabilities and the application of patches, reducing response times to incidents.

These innovations enhance MDM platforms' resilience against threats and improve their efficiency in protecting mobile devices and data.

11. Automation and Orchestration (SOAR)

Security Orchestration, Automation, and Response (SOAR) is an advanced framework designed to streamline and enhance cybersecurity operations. It integrates diverse security tools and systems into a unified platform, centralizing management and coordination. By automating routine tasks, such as threat analysis and incident response, SOAR accelerates reaction times and reduces the burden on security teams, enabling them to focus on complex challenges. Additionally, SOAR leverages artificial intelligence and machine learning to analyze large datasets, detect anomalies, and predict potential cyber threats. These capabilities significantly improve the efficiency and precision of responses to incidents. Often operating in tandem with Security Information and Event Management (SIEM) platforms, SOAR uses collected and analyzed data to orchestrate and automate robust defense mechanisms. Its adoption is particularly beneficial for large organizations with intricate security environments, ensuring rapid and effective management of evolving threats. (Mir & Ramachandran, 2021; Bartwal, et al., 2022)

12. Priorities by User Groups

The innovations discussed play a vital role in strengthening digital security and protecting against increasingly sophisticated threats. An analysis of the security needs of organizations and individuals reveals varying priorities across user groups, depending on their size, industry, and exposure to threats:

1. Large Companies and Corporations:
    - Zero Trust architecture, in combination with SIEM systems, secures complex networks against internal and external threats, providing granular access control and real-time monitoring, which is critical for large organizations.
    - Automation and security orchestration are essential for companies aiming for rapid incident response while reducing manual effort.
2. SaaS Providers:
    - The Zero Trust model ensures secure cloud access for SaaS providers and protects data from unauthorized access.

- AI and machine learning are crucial in real-time anomaly detection and threat identification.
- Post-quantum cryptography ensures resilience against quantum computer attacks.
- Secure Access Service Edge (SASE) technology integrates network functions and security services into a unified platform, enabling safer cloud access.
- Security automation reduces incident response time.
- Data encryption guarantees protection during transmission and storage.
- Container security is crucial for protecting applications and data in dynamic environments.

3. Organizations Handling Sensitive Data:
    - Advanced cryptography, such as quantum cryptography or homomorphic encryption, is vital for banking, healthcare, and government.
    - Blockchain technology can secure transactions and ensure data integrity, especially in the financial sector.
4. Small Businesses and Individuals:
    - MFA offers a simple and effective solution for account protection.
    - Mobile Device Management (MDM) platforms help smaller firms protect employees' mobile phones and other devices.
5. Research and Advanced Centers:
    - Post-quantum cryptography and other cryptographic innovations are essential for institutes and organizations preparing for future threats, such as quantum computer attacks. This field of cryptography focuses on developing algorithms that are more resistant to attacks from quantum computers.

POST-QUANTUM CRYPTOGRAPHY

With the development of quantum computers, the demand for new cryptographic techniques resistant to quantum attacks is becoming increasingly urgent. Due to their ability to solve specific mathematical problems much faster than classical computers, quantum computers are a potential threat to current cryptographic systems, particularly those based on public keys, such as RSA, ElGamal, and ECC.

Core Concepts of Post-Quantum Cryptography (Bernstein, et al., 2009; Dekkaki, et al., 2024):

a. *Resilience to Quantum Attacks*. Post-quantum algorithms aim to withstand threats from powerful quantum computers, ensuring security. For example, Shor's algorithm, utilized by quantum computers, can efficiently factorize large numbers, thereby compromising RSA encryption.

b. *Mathematical Approaches*. Post-quantum cryptography leverages mathematical problems that are challenging to solve, even for quantum computers, such as:
    - Lattice-based cryptography: This approach uses mathematical structures known as lattices, arrays of points in multidimensional space. The foundation of security lies in the complexity of solving problems such as:
        - Shortest Vector Problem (SVP): Finding the shortest vector in a lattice.
        - Closest Vector Problem (CVP): Finding the closest vector to a target within a lattice. These problems pose significant challenges, remaining incredibly difficult to solve

even for quantum computers. Lattice-based methods offer practical versatility, supporting encryption, digital signatures, and key exchange.

- Code-based cryptography: This method relies on error-correcting codes, primarily used for reliable data transmission. The security is based on the difficulty of decoding randomly generated codes. A well-known example, the McEliece algorithm, uses coding systems to create public and private keys. Advantages include resistance to quantum attacks and a high level of security, though key sizes can be significantly longer compared to other methods.
- Multivariate polynomial cryptography: This technique utilizes systems of multivariate polynomials as the foundation for encryption. The robustness of security relies on the intricate complexity of solving these systems, especially when numerous unknowns and parameters are involved. Multivariate polynomials are fast and energy-efficient, making them suitable for applications in resource-constrained environments, like IoT devices.

c. *Symmetric Encryption.* Symmetric algorithms, such as AES, remain relatively secure but require longer keys to maintain resilience against quantum attacks.

Each of these methods has its advantages and challenges, but they share a common goal: to provide resistance to attacks from quantum computers.

Post-quantum cryptography is essential because, once quantum computers become sufficiently advanced, they could undermine current cryptographic standards. That would have far-reaching implications for data security across financial, healthcare, and governmental sectors. Post-quantum cryptography is critical for ensuring future system resilience.

IoT SECURITY

IoT security is crucial due to the vulnerabilities and widespread adoption of IoT devices. These devices are often targets of attacks because of weaker security measures and the large number of connected sensors. They can also be exposed to Man-in-the-Middle (MITM) attacks (Cekerevac, et al., 2017). Specific measures to enhance the security of Internet of Things (IoT) devices include:

1. *Strong authentication*: Multi-factor authentication (MFA) enhances security by ensuring controlled access to IoT devices, thereby reducing the risk of unauthorized entry. Default device passwords, which are commonly exploited in attacks, are intentionally avoided.
2. *Regular software updates*: Manufacturers frequently issue security patches for IoT devices. Regularly updated software reduces the risk of exploiting known vulnerabilities.
3. *Data encryption*: IoT devices and servers use encryption to secure transmitted data and prevent information interception.
4. *Network segmentation*: IoT devices should be separated from the core network, for example, by using a dedicated Wi-Fi network for IoT devices to reduce the risk of attack propagation (Baligodugula, et al., 2024).
5. *Anomaly monitoring and detection*: Tools monitor the activities of IoT devices to find any unusual behavior that might suggest a possible attack.
6. *Security protocols*: Protocols, like Transport Layer Security (TLS), are implemented for secure data transmission. VPNs provide additional protection for device communication. Moving away from VPNs exposes users to heightened security risks (Prigoda, et al., 2014).

7. *Physical security*: Physical protection of IoT devices is essential to prevent unauthorized access, particularly in industrial or public environments.
8. *Vulnerability testing*: IoT devices are regularly tested for security flaws using penetration testing tools or by engaging cybersecurity experts.

These measures reduce the risk of attacks and ensure the reliability of IoT devices.

HOMOMORPHIC ENCRYPTION

Homomorphic encryption is an advanced cryptographic technique that allows data to be processed and manipulated while still encrypted. This technology addresses a significant security challenge by enabling operations on data without decrypting it, thereby avoiding exposure to potential attackers.

The basic concept is as follows (Armknecht, et al., 2016; Gaid & Salloum, 2021):

- Despite encryption, data remains usable: Conventional methods require decryption, which can compromise security. Homomorphic encryption allows mathematical operations to be performed directly on encrypted data.
- The result remains encrypted: Once the operation is complete, the result remains encrypted, allowing the end user to decrypt it with a private key only when necessary.

Types of homomorphic encryption include (Sen, 2013; Buchanan, 2021; Pereira, 2016):

1. Partial homomorphic encryption:
   - Allows only specific types of operations (e.g., addition or multiplication) on encrypted data.
   - Example: RSA encryption supports multiplicative homomorphism.
2. Leveled homomorphic encryption:
   - Supports multiple types of operations but with a limited number of computational steps (calculation depth).
   - Used in scenarios where the number of operations needed is predetermined.
3. Full homomorphic encryption (FHE):
   - Allows any operation (addition, multiplication, etc.) on encrypted data without limitations.
   - This technology is exceptionally effective but computationally intensive and still under development for broader applications.

Homomorphic encryption has immense potential in areas where data privacy is critical, such as:

- Healthcare: Doctors can analyze encrypted medical data without accessing patients' private information.
- Finance: Banks can process encrypted transactions without revealing sensitive data.
- Cloud services: Users can store encrypted data in the cloud and perform computations, ensuring the data remains fully protected.

However, there are limitations. Homomorphic encryption is resource-intensive in terms of processing power and time, but research and innovation in this field are advancing rapidly.

RANSOMWARE

Behavioral Analytics: Technologies that identify irregularities in user or system behavior to enable early threat detection. That is increasingly significant when combined with AI technologies. Ransomware protection consists of tools and strategies designed to detect and stop ransomware attacks.

Security programs recognize ransomware through a combination of techniques, including behavioral analysis, activity patterns, and real-time protection. The protection operates as follows (Guvçi & Şenol, 2023; Turaev, n.d.; Rehman, et al., 2024):

1. Behavioral Analysis:
   - Ransomware exhibits distinct behavior patterns, such as:
   - Encrypting large numbers of files within a short time frame.
   - Changing file extensions (e.g., .docx → .locked).
   - Creating "ransom notes."
   - Security software monitors these activities and utilizes heuristic methods to identify potential threats.
2. Threat Databases:
   - Antivirus programs use databases containing signatures of known ransomware types. When a file or process matches a known signature, the program blocks it immediately.
   - Regular updates to threat databases ensure recognition of new ransomware versions.
3. Machine Learning and AI:
   - Advanced security programs employ artificial intelligence (AI) to detect unknown threats. AI analyzes large datasets to learn how to identify suspicious behavior patterns.
   - For example, AI can detect new ransomware employing unconventional encryption methods.
4. Network Traffic Analysis:
   - Ransomware often communicates with command-and-control (C&C) servers to transmit encryption keys or receive commands.
   - Security tools analyze network traffic and block suspicious connections.
5. System Monitoring:
   - Programs monitor key directories and files for unexpected changes.
   - If unauthorized file modifications (such as encryption) are detected, the process can be stopped automatically.
6. Sandboxing (Isolation):
   - When a suspicious file is executed, some security tools first run it in a "sandbox" environment (a virtual space) to analyze its behavior before allowing it access to the real system.

These protection functions also have a preventive aspect. Many security programs use proactive strategies, including:

- Blocking email attachments that may contain ransomware.
- Identifying fake URLs attempting to deceive users.

Ransomware protection is essential for preventing attacks that lock or encrypt user data until a ransom is paid. Key preventive measures include:

1. Regular backups. Periodically saving copies of important data on external devices or in the cloud to ensure data recovery without paying a ransom.
2. Software updates. Regular installation of security patches for operating systems and applications to eliminate known vulnerabilities.
3. Antivirus and anti-ransomware tools. Employing reliable security programs that can detect and block ransomware threats before any damage occurs.
4. User training. Comprehensive training tailored to participants' needs should cover:

- Basics of advanced technologies: Training should include foundational principles of technologies like the Zero Trust model, AI and machine learning, post-quantum cryptography, data encryption, and Secure Access Service Edge (SASE).
- Practical application: Focus on real-world examples and simulations to teach participants how to apply technologies, such as configuring Zero Trust architecture or managing SIEM platforms.
- Threat recognition and response: Methods for identifying cyber threats, such as anomaly detection through AI algorithms, and procedures for reacting to various types of attacks.
- Data protection: Educating participants on proper encryption techniques, key management, and the use of post-quantum algorithms to safeguard data during transmission and storage.
- Cloud infrastructure security: Addressing challenges and solutions for securing hybrid and multi-cloud environments, including integrating network functions and protecting containers.
- Ethics and regulations: Educating participants on the legal and ethical dimensions of digital security technologies, with a focus on privacy and transparency issues.
- Incident management skills: Covering tools for automation (SOAR), coordinating security systems, and creating strategies for rapid incident response.

This training supports the understanding and application of cutting-edge innovations in digital security, empowering participants to improve risk management and data protection efficiency. However, the depth of each topic depends on individual needs and their specific areas of work.

5. Network segmentation is crucial for enhancing digital security, as it divides IT infrastructure into smaller, controlled segments or zones. This approach improves system protection against cyber threats and minimizes the potential impact of attacks. Key aspects include:
   - Limiting attack spread: In segmented networks, potential attacks are localized within one zone, preventing attackers from accessing the entire infrastructure. For example, if one server is compromised, other parts of the network remain secure.
   - Precise access control: Segmentation enables specific access rules for each zone, enhancing the protection of sensitive infrastructure against unauthorized users or systems.
   - Simplified anomaly detection: Monitoring and analyzing traffic within segmented network areas facilitates the identification of suspicious activities and quick responses to incidents.
   - Compliance with regulatory requirements: Network segmentation aids organizations in meeting data protection standards and regulations by isolating sensitive data and systems from the rest of the network.
   - Performance optimization: Dividing the network into smaller zones improves traffic management and reduces load, enhancing overall efficiency.

Segmented networks are particularly beneficial in environments with complex IT structures, such as large organizations or financial institutions, where security and data control are priorities.

6. Access control. Access control is a fundamental pillar of digital security, ensuring that only authorized users and devices can access resources, applications, and data. Its primary role is to protect sensitive information from unauthorized access and potential misuse. Access control contributes to security through:

- Restricting access: It facilitates system segmentation, determining who can access specific data or functions. For example, employees in different departments have distinct access rights, reducing the risk of accidental or intentional breaches. Applying the principle of least privilege limits access to only necessary resources for tasks, minimizing damage if ransomware compromises a user.
- Identity verification: Multi-factor authentication (MFA) provides multi-layered user identity verification, significantly reducing the risk of unauthorized access and data breaches. MFA enables secure system entry and limits damage in case of user data compromise. This approach, combined with the adaptive features of the Zero Trust model, strengthens the overall security architecture, shielding organizations from ransomware and other threats. MFA is particularly critical in environments with sensitive data, including banking, healthcare, and cloud infrastructure.
- Activity monitoring: Access control systems log and monitor login attempts and other activities, enabling rapid responses to suspicious actions or security incidents.
- Protection against cyber threats: Prevents unauthorized access by attackers attempting to exploit stolen passwords, identities, or system vulnerabilities.
- Compliance with legal regulations: Helps organizations align with privacy and data protection standards, such as GDPR or HIPAA.
- Dynamic adaptation: Modern access control systems utilize Zero Trust models and adaptive approaches, which assess user behavior in real time and adjust access levels based on risk analysis.

Access control is not merely a technical measure but also a strategic tool for managing security risks in organizations of all sizes.

Implementing these measures can significantly reduce ransomware attack risks and help protect data. These innovations enable organizations to secure their cloud data and infrastructure against increasingly sophisticated threats.

CONCLUSION

Digital security plays a crucial role in preserving the integrity, confidentiality, and availability of data in an era of growing digitalization. A combination of traditional methods and modern technological innovations has become essential for effectively protecting individuals, organizations, and governments from increasingly sophisticated cyber threats.

Zero Trust architecture is a fundamental principle that eliminates implicit trust and ensures continuous verification of every access to resources. This model, together with multi-factor authentication (MFA), enhances security in environments encompassing mobile devices, cloud infrastructure, and sensitive data. Post-quantum cryptography and homomorphic encryption are becoming key for resilience against future quantum computer threats, enabling secure data processing.

Blockchain technology and cloud security contribute significantly to decentralized protection and cost optimization, while IoT devices, due to their vulnerabilities, require specific measures such as network segmentation and regular software updates. Security Information and Event Management (SIEM) platforms, combined with security orchestration and automation (SOAR), enable faster threat response and reduce manual workload.

The analysis highlights differences in user priorities by category. For instance, MFA and MDM platforms play a vital role for small businesses and individuals, while advanced technologies such as Zero Trust architecture, SIEM systems, and post-quantum cryptography are indispensable for large corporations, SaaS providers, and research centers.

Nevertheless, advanced systems do not diminish the importance of fundamental security practices. User training, regular data backups, and software updates remain essential for attack prevention. Digital security requires an integrated approach that combines cutting-edge technologies with practical strategies, adapting continuously to the evolution of threats.

The conclusion emphasizes the need for education and ongoing improvement to prepare individuals and organizations for future challenges. A balance between innovation and fundamental security measures ensures protection that is not only effective but also sustainable in an ever-changing world.

Based on the research and analysis, there is sufficient evidence to reject the null hypothesis. The findings support the alternative hypothesis, which states that integrating advanced technologies (AI, IoT, blockchain, post-quantum cryptography, SOAR platforms) significantly enhances digital security in the financial sector by improving fraud detection, automating threat responses, and ensuring data integrity.

REFERENCES

1. Abhishek, K., Roshan, S., Kumar, P. & Ranjan, R., 2013. *A Comprehensive Study on Multifactor Authentication Schemes.* Berlin, Springer, pp. 561-568.
2. Ahmed, S. & Ahmed, T., 2022. Comparative Analysis of Cryptographic Algorithms in Context of Communication: A Systematic Review. *International Journal of Scientific and Research Publications,* 12(7), pp. 161-173.
3. Antić, M., 2024. *Digitalizacija donosi napredak, ali i nove izazove.* [Online] Available at: https://banke-biznis.com/mirko-antic-digitalizacija-donosi-napredak-ali-i-nove-izazove/
4. Armknecht, F. et al., 2016. *A Guide to Fully Homomorphic Encryption.* [Online] Available at: https://eprint.iacr.org/2015/1192.pdf [Accessed 02 04 2025].
5. Baligodugula, V. V., Ghimire, A. & Amsaad, F., 2024. An Overview of Secure Network Segmentation in Connected IIoT Environments. *Computing & AI Connect,* Issue 1, p. Article ID: 0004).
6. Barthwal, D., 2016. *Mobile Device Management (MDM) in Organizations.* [Online] Available at: https://www.researchgate.net/publication/305380830_Mobile_Device_Management_MDM_in_Organizations [Accessed 03 04 2025].
7. Bartwal, U., Mukhopadhyay, S., Negi, R. & Shukla, S., 2022. *Security Orchestration, Automation, and Response Engine for Deployment of Behavioural Honeypots.* s.l., arXiv:2201.05326 [cs.CR], p. 8.
8. Bernstein, D. J., Buchmann, J. & Dahmen, E., 2009. *Post-Quantum Cryptography.* Berlin Heidelberg: Springer.
9. Brooks, D. J., 2010. What is security: Definition through knowledge categorization. *Security Journal,* Volume 23, pp. 225-239.
10. Buchanan, B., 2021. *On Global Encryption Day: A Practical Guide to Homomorphic Encryption.* [Online] Available at: https://asecuritysite.com/blog/2021-10-22_On-Global-Encryption-Day--A-Practical-Guide-to-Homomorphic-Encryption-be5670240900.html [Accessed 01 04 2025].
11. Cekerevac, Z. & Cekerevac, P., 2022. Blockchain and the application of blockchain technology. *MEST Journal,* 15 07, 10(2), pp. 14-25.
12. Cekerevac, Z., Cekerevac, P., Prigoda, L. & Naima, F. A., 2025. Security Risks from the Modern Man-In-The-Middle Attacks. *MEST Journal,* 15 01, 13(1), pp. 34-51.

13. Cekerevac, Z., Dvorak, Z., Prigoda, L. & Cekerevac, P., 2017. Internet of things and the Man-In-The-Middle attacks – Security and economic risks. *MEST Journal,* 5(2), pp. 15-25.
14. Cekerevac, Z., Prigoda, L. & Cekerevac, P., 2025. *Enhancing Digital Security in the Financial Sector With AI, IoT, and Blockchain.* Chisinau, Moldova, s.n.
15. Cekerevac, Z., Prigoda, L. & Maletic, J., 2018. Blockchain Technology and Industrial Internet of Things in the Supply Chains. *MEST Journal,* 15 July, 6(2), pp. 39-47.
16. Chen, R. et al., 2023. *Overview of the Development of Secure Access Service Edge.* Singapore, s.n.
17. Čekerevac, Z. & Radonjić, S., 2013. *Some SMEs data safety and security issues in the in-house and in the cloud computing.* Žilina, Slovakia, s.n.
18. Dekkaki, K. C., Tasic, I. & Cano, M.-D., 2024. Exploring Post-Quantum Cryptography: Review and Directions for the Transition Process. *Technologies,* 12(12), p. 242.
19. Dhiman, P. et al., 2024. A Review and Comparative Analysis of Relevant Approaches of Zero Trust Network Model. *Sensors,* 24(4), p. 1328.
20. Gaid, M. L. & Salloum, S. A., 2021. *Homomorphic Encryption.* Settat, Morocco, s.n., pp. 634-642.
21. Gambo, M. L. & Almulhem, A., 2025. *Zero Trust Architecture: A Systematic Literature Review.* [Online] Available at: https://arxiv.org/abs/2503.11659 [Accessed 03 04 2025].
22. GDPR, 2024. *General Data Protection Regulation (GDPR).* [Online] Available at: https://gdpr-info.eu/ [Accessed 03 04 2025].
23. Glowinski, K., Gossmann, C. & Strümpf, D., 2020. Analysis of a cloud-based mobile device management solution on android phones: technological and organizational aspects. *SN Appl. Sci.,* 2(42).
24. González-Granadillo, G., González-Zarzosa, S. & Diaz, R., 2021. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. *Sensors,* 21(14), p. 4759.
25. Guvçi, F. & Şenol, A., 2023. An Improved Protection Approach for Protecting from Ransomware Attacks. *Journal of Data Applications,* 02 08, 0(1), pp. 69-82.
26. Hartl, K. & Brack, F., 2024. *What is Zero Trust Architecture (ZTA)?.* [Online] Available at: https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture
27. Howell, G. et al., 2023. *Guidelines for Managing the Security of Mobile Devices in the Enterprise.* Gaithersburg, MD: NIST Special Publication SP 800-124r2.
28. Jena, K., 2023. Zero-Trust Security Models Overview. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology,* 9(6), pp. 70-76.
29. Jore, S., 2019. The Conceptual and Scientific Demarcation of Security in Contrast to Safety. *Eur J Secur Res,* Issue 4, p. 157–174.
30. Malatji, M. & Tolah, A., 2024. Artificial intelligence (AI) cybersecurity dimensions: a comprehensive framework for understanding adversarial and offensive AI. *AI Ethics,* 15 02.
31. Mir, A. W. & Ramachandran, R. K., 2021. *Implementation of Security Orchestration, Automation and Response (SOAR) in Smart Grid-Based SCADA Systems.* Singapore, Springer, pp. 157-169.
32. Mironov, I., 2005. *Hash functions: Theory, attacks, and applications,* Mountain View, CA: Microsoft Research, Technical Report.
33. Ometov, A. et al., 2018. Multi-Factor Authentication: A Survey. *Cryptography,* 2(1), p. 1.
34. Pereira, H. V. L., 2016. *Difference between leveled FHE and normal FHE scheme.* [Online] Available at: https://crypto.stackexchange.com/questions/15794/difference-between-leveled-fhe-and-normal-fhe-scheme [Accessed 01 04 2025].
35. Prigoda, L., Cekerevac, Z., Dvorak, Z. & Cekerevac, P., 2014. One Look at the Modern Information Security. *Sustainable Development of Mountain Territories,* 4(22), pp. 99-103.
36. Rehman, M., Akbar, R., Omar, M. & Gilal, A., 2024. *A Systematic Literature Review of Ransomware Detection Methods and Tools for Mitigating Potential Attacks.* Singapore, s.n.
37. Sen, J., 2013. *Homomorphic encryption-theory and application.* Rijeka, Croatia: IntechOpen.

38. Turaev, H., n.d.. *Literature Review on Ransomware and Approaches to Its Mitigation.* [Online] Available at: https://www.academia.edu/32167535/Literature_Review_on_Ransomware_and_Approaches_to_Its_Mitigation [Accessed 01 04 2025].
39. White, M., 2025. *AI arms race: How AI will be used by cyber-attackers (and defenders).* [Online] Available at: https://specopssoft.com/blog/ai-in-cybersecurity-arms-race-attackers-defenders/
40. Wong, R., Morris, K. & Masys, A. J., 2023. Safety and Security Science and Technology. In: *Safety and Security Science and Technology: Perspectives from Practice.* s.l.:Springer, Cham, pp. 127-139.

DIGITAL TRANSFORMATIONS IN THE PUBLIC SECTOR OF RUSSIAN REGIONS AND CHALLENGES TO ENSURING SOCIAL JUSTICE

UDC: 004-048.35:[338.465:351](470+571)
DOI: https://doi.org/10.53486/tids2025.25

ELENA BAZHENOVA
Southern Federal University, Russia
eubazhenova@sfedu.ru
ORCID ID: 0000-0001-8253-5073

SERGEY BAZHENOV
Science Horizons Foundation, Russia
sbazhenov@mail.ru
ORCID ID: 0000-0001-7593-0526

Abstract. The article presents a comprehensive analysis of the impact of digital transformation in the public sector across Russian regions on ensuring social justice. Through examining regulatory and strategic documents (Government Directive No. 2998-r, Spatial Development Strategy), implementation practices of digital platforms (Unified Public Services Portal "Gosuslugi", Interagency Electronic Interaction Systems, Regional Situation Centers), and scholarly research, the dual nature of digitalization is revealed. On one hand, its potential to enhance service accessibility, governance transparency, and corruption reduction – particularly for remote territories and vulnerable groups – is demonstrated. On the other hand, the study systematically analyzes key challenges: deepening digital inequality (infrastructure limitations, digital literacy deficits, territorial disparities), risks of social exclusion among elderly and low-income populations, alongside issues of algorithmic discrimination and the erosion of the "human dimension". The authors substantiate the necessity of transitioning to an inclusive digitalization model, proposing concrete mechanisms: (1) Eliminating the digital divide through ICT infrastructure development and digital literacy programs; (2) Guaranteeing multi-channel access (preserving Multifunctional Public Service Centers, simplifying interfaces); (3) Adapting public administration to data-driven approaches; (4) Providing differentiated support for lagging regions. Social justice in the digital era necessitates prioritizing inclusivity over technological determinism.

Keywords: public sector, Russian regions, social justice, digital divide, inclusive digitalization

JEL Classification: H83, R58, O35, I38

INTRODUCTION

The relevance of the research is determined by the rapid digitalization of the public sector of the Russian Federation, initiated within the framework of national projects and digital economy development strategies. This process, objectively aimed at increasing the efficiency of public administration and the accessibility of public services, acquires particular significance in the context of the country's significant regional differentiation. Differences in the level of socio-economic development, the state of infrastructure, and human potential between the subjects of the Russian Federation create serious risks of exacerbating existing social inequality. The implementation of digital platforms and services, such as the Unified Public Services Portal (EPGU) and regional digital ecosystems, potentially can both reduce access barriers for remote and socially vulnerable population groups and generate new forms of digital exclusion. In this regard, the analysis of the impact of the digital transformation of regional authorities on the realization of the principle of social justice, implying equal opportunities and protection for citizens regardless of their place of residence or social status, appears critically important.

MAIN CONTENT

The goal of this study is a comprehensive analysis of the relationship between the processes of digital transformation in the public sector of the subjects of the Russian Federation and ensuring social justice, followed by the identification of key challenges and the development of conceptual foundations for balanced development.

To achieve this goal, the following tasks are proposed:

- To characterize the key vectors and scale of digital transformations in the system of regional public administration and provision of public services in the Russian Federation, highlighting the specifics of different groups of regions (leaders, outsiders).
- To systematize the potential positive effects of digitalization for expanding service accessibility, increasing management transparency, and reducing corruption risks, which contribute to strengthening social justice.
- To identify and classify the main challenges and risks associated with the deepening of digital inequality (Digital Divide) by territorial, infrastructural, and competence characteristics, as well as with the potential marginalization of vulnerable population groups (elderly citizens,

low-income individuals, residents of depressed territories).

- To develop scientifically based principles and recommendations for the formation of an inclusive model of digital transformation of the public sector in Russian regions, ensuring the priority of social justice and minimizing exclusionary effects.

The digital transformation of the public sector of the economy in the Russian Federation is a complex, multi-level process associated with achieving the national development goal of Russia "*Digital Transformation of State and Municipal Administration, Economy, and Social Sphere*" (Government of the Russian Federation, 2021). Digital transformation correlates with the national strategy for spatial development of the Russian Federation for the period up to 2030 with a forecast until 2036 (Government of the Russian Federation, 2024.). It takes place within the framework of the national project "Data Economy and Digital Transformation of the State" (Ministry of Digital Development of Russia, no date a) through relevant federal projects: "Ц1. Infrastructure for Access to the Information and Telecommunication Network 'Internet'", "Ц2. Digital Platforms in Social Sectors", "Ц4. Digital Public Administration" and "Ц8. Personnel for Digital Transformation".

The implementation of the national project is carried out with significant variability at the level of the subjects of the federation. State policy in this area is formed by the Ministry of Digital Development of Russia. The key driver of change is the desire to increase the efficiency of public administration, the speed and accessibility of providing services to the population and businesses. Currently, several interrelated vectors of development of the digital landscape in the regional public sector of the Russian Federation can be distinguished.

Electronic government infrastructure ensures the interaction of state bodies, local self-government, and organizations in the provision of state and municipal services in electronic form. *The main directions of digitalization* concentrate, first of all, around the creation and development of national integrated digital platforms, such as the FGIS "Federal Situation Center of Electronic Government" (Ministry of Digital Development of Russia, no date b) and the FGIS "Unified

Information Platform of the National Data Management System" (Ministry of Digital Development of Russia (no date c)).

The central place among them is occupied by the *Unified Portal of State Services* (EPGU, "Gosuslugi") (Rostelecom (operator), no date), acting as the main virtual "window" of interaction between Russian citizens and the state. In parallel, *Regional Portals of State Services (RPGU)* are developing, designed to adapt national services to local specifics and provide services under the jurisdiction of the subjects of the Russian Federation and municipalities. The network of *Multifunctional Centers for State and Municipal Services (MFCs, "My Documents" centers of the Russian Federation)* plays a significant role in ensuring accessibility, especially for overcoming the digital divide, which integrate digital technologies into their processes, becoming points of "live" support and access.

An equally significant direction is the formation of *digital management platforms and interagency interaction*. Systems of interagency electronic interaction (SMEV) (Ministry of Digital Development of Russia, no date d) provide the necessary data exchange between authorities of different levels. Regions are actively developing their own data platforms (for example, "Geoportal of the Moscow Region") (Government of the Moscow Region, no date) and regional situation management centers (TsUR) (Ministry of Digital Development of Russia, no date e), allowing for monitoring of the socio-economic situation, managing municipal services ("smart cities"), and making decisions based on the analysis of large volumes of information (Data-Driven Governance). Initiatives in the field of *open data* are also gaining momentum, contributing to increased transparency and citizen involvement in governance processes.

Digitalization of the social sphere represents a separate, critically important segment of transformations. In healthcare, this is manifested in the implementation and development of the *Unified Medical Information and Analytical System (EMIAS) of Moscow*, providing electronic appointment scheduling and telemedicine consultations. In the field of education, *digital educational platforms* (analogues of the "Moscow Electronic School" (MES), the platform for online learning "Modern Digital Educational Environment" (SDES) (Ministry of Science and Higher Education of Russia, no date), developed by the Ministry of Science and Higher Education of the Russian Federation, are actively used. Social protection of the population is also transitioning to electronic services, including the assignment and payment of benefits, maintaining social registries in digital format.

Regional specifics determine the landscape of digital transformations. *Significant differentiation* in the pace, depth, and success of the implementation of digital solutions between the subjects of the Russian Federation is observed. Conventionally, a group of *"leaders" of digitalization* can be distinguished (traditionally including Moscow, the Republic of Tatarstan, the Khanty-Mansi Autonomous Okrug, the Nizhny Novgorod Region, and a number of others), demonstrating a comprehensive approach, developed infrastructure, and a high level of penetration of digital services. They are opposed by *"outsiders"* – often economically depressed, sparsely populated, remote regions (a number of subjects of the North Caucasus, Siberia, the Urals, and the Far East), facing chronic underfunding, weak ICT infrastructure, and a shortage of qualified personnel.

This *disproportion* is due to a combination of factors:

1. *Financial resources:* The capabilities of regional budgets to invest in expensive ICT infrastructure, purchase equipment, and develop software are extremely unequal.
2. *State of ICT infrastructure:* The level of development of broadband Internet access (especially in rural areas), mobile coverage, and computing power varies widely.

3. *Personnel potential:* The presence in the region of IT specialists capable of developing and maintaining complex systems, as well as the level of digital competence of the regional civil servants themselves.
4. *Digital culture of the population:* The readiness and ability of the region's residents to actively use digital services, which affects the demand for initiatives.
5. *Managerial will and competence of regional elites:* The presence of a clear strategy for digital transformation and effective mechanisms for its implementation at the level of the leadership of the subject of the Russian Federation.

Thus, the landscape of digital transformations in Russian regions is characterized by the dynamic development of key areas (digital services, management platforms, digital social sphere) against the backdrop of deep and persistent regional differentiation. This heterogeneity, caused by objective factors, creates a significant context for analyzing the impact of digitalization on social justice, since the basic conditions for access to the digital benefits of the state are initially not equal for all citizens of the country depending on their place of residence.

The potential of digitalization for increasing social justice. Despite the identified disparities in the development of digital infrastructure and services between regions, digital transformation of the public sector itself has significant, though not always fully realized, potential for strengthening the principles of social justice in the Russian Federation. This potential lies in overcoming traditional barriers that limit citizens' access to public services and opportunities, and in forming a more transparent and accountable management system.

The key positive effect is *increased accessibility of state and municipal services*. Digital platforms, such as the "Gosuslugi" portal and regional analogues (RPGU), combined with a developed network of multifunctional centers (MFCs), provide channels for remote interaction. This is critically important for residents of remote and hard-to-reach territories, as well as for citizens with disabilities or reduced mobility (for example, elderly people or parents with young children), for whom physically visiting departments was associated with significant difficulties and costs. Thus, digitalization contributes to the equalization of opportunities by territorial and physical characteristics.

A significant contribution to ensuring justice is *increased transparency and reduced corruption risks*. The automation of administrative procedures, the introduction of electronic document management and the System of Interagency Electronic Interaction (SMEV) (Ministry of Digital Development of Russia / Gosuslugi Portal, no date) minimize the need for personal contacts between citizens and officials at the stage of service provision (Ministry of Digital Development of Russia, no date d). Standardized regulations published on portals and the ability to track the status of an application online limit the scope for arbitrariness and informal practices. Equal rules of access to services, formalized in the digital environment, and open data on the activities of government bodies (budgets, public procurement, regulations) *strengthen public control* and contribute to the creation of equal conditions for all categories of the population.

The optimization of administrative processes through digitalization leads *to a reduction in citizens' transaction costs*. Simplifying application procedures (through pre-filled forms, digital electronic signatures), eliminating duplication of document requests between departments thanks to SMEV, and a significant *reduction in service delivery times* – all this reduces bureaucratic burden, saves time and resources of citizens, especially valuable for socially vulnerable groups. Eliminating the "administrative runaround" between institutions is in itself a step towards greater justice, reducing the disproportionate burden that traditional procedures placed on the least protected.

Personalization of public services based on data analysis represents another important aspect of digitalization's potential. The integration of information systems allows authorities to get a more complete picture of the needs of a particular citizen or family (for example, in the field of social support, healthcare, education). This creates the basis for *more targeted and timely assistance*, better meeting individual needs and, in the future, for a transition from universal to fairer, needs-based models of social security.

Finally, *data-driven governance* potentially contributes to *fairer resource allocation and decision-making*. Analysis of large volumes of information about citizens' requests, service quality, and socio-economic indicators of territories allows identifying real problems and disparities, assessing the effectiveness of support measures, and adjusting regional policy towards greater balance and consideration of the interests of different population groups.

Thus, the digital transformation of the public sector in Russian regions contains *significant opportunities for promoting social justice* through ensuring greater accessibility, transparency, efficiency, and targeting of public services, as well as through creating the foundation for more objective and balanced governance. The realization of this potential, however, directly depends on the successful overcoming of challenges related to digital inequality and inclusivity, which will be discussed further.

Key challenges of digital transformation for social justice. Despite the significant potential of digitalization for strengthening social justice, its implementation in the context of Russian regions is associated with a complex of serious challenges that can not only negate the expected positive effects but also exacerbate existing social inequality. The main threat lies in the risk of *systemic digital exclusion* (Plotichkina, 2020) of vulnerable population groups and entire territories, which contradicts the principles of equal access to public goods (Tertyshnikova and Pavlova, 2022.).

The central and most significant challenge is *digital inequality* (Digital Divide), manifested at several interconnected levels:

1. *Inequality in access to infrastructure:* Significant territories, especially in rural areas, remote and economically depressed regions (for example, a number of districts in Siberia, the Far East, the North Caucasus), suffer from the lack of quality broadband internet or stable mobile coverage. Even if a network is available, the cost of connection and necessary devices (computers, smartphones) may be prohibitive for low-income families and pensioners, forming the phenomenon of "*digital poverty*".
2. *Inequality of digital competencies* (Digital Literacy Gap): A deep gap in the level of skills for effectively using digital services exists between generations (elderly citizens), between urban and rural residents, and between different socio-economic groups. *Functional digital illiteracy* means the inability of citizens, even with access, to correctly complete registration procedures on EPGU (for example, identity verification), fill out complex electronic forms, ensure the security of their data, or understand the essence of the digital service provided.
3. *Inequality in use* (Usage Gap): Certain population groups may consciously avoid digital channels due to *distrust* in the security of systems, *fears* about the confidentiality of personal data, psychological discomfort, or a simple preference for traditional forms of interaction

(so-called "human communication"). This barrier is often underestimated, but it is significant, especially among the older generation.

The risk of marginalization of vulnerable groups directly stems from the digital divide. The accelerated transfer of services to a predominantly electronic format without ensuring guaranteed alternative channels or adequate support *de facto* deprives access to critically important social, medical, and administrative services:

– *Elderly citizens*, for whom digital interfaces may be insurmountably complex.
– *Persons with disabilities*, if digital platforms do not comply with accessibility standards (WCAG) (W3C Web Accessibility Initiative, no date).
– *Residents of remote settlements* with underdeveloped communication infrastructure.
– *Low-income segments of the population* who lack the means for devices and internet.
– *Persons without permanent registration or documents*, facing difficulties with electronic identification.

Usability issues and "digital bureaucratism" represent a significant barrier. Poorly designed, complex navigation interfaces of official state portals (EPGU, RPGU), confusing electronic authentication procedures (for example, requirements for a qualified electronic signature for some services), technical failures, and lack of prompt technical support create new, digital forms of *administrative barriers*. This not only reduces satisfaction but also discriminates against less technologically advanced users, reproducing "*digital injustice*" in a new form.

Threats to data privacy and security undermine trust in the state's digital tools. Citizens' concerns about possible *leaks of personal data* (including sensitive information about health, income, family), *unauthorized use of data* by state or commercial structures, as well as risks of "*algorithmic discrimination*" (making decisions based on biased or unrepresentative data) (Falletti, 2023) are a serious deterrent to using digital services and generate new forms of social vulnerability.

Intra-departmental challenges also significantly impact justice:

– *Insufficient digital competence of civil servants* at the local level hinders the effective implementation and support of digital services, as well as assistance to citizens;
– *Conservatism and resistance to change* in the bureaucratic environment can slow down implementation or lead to formal, rather than substantive, use of digital tools;
– *Lack of flexibility and adaptability* in standardized digital processes makes it difficult to account for individual circumstances of citizens, especially in complex, non-standard situations, which can lead to unfair denials or delays.

Territorial differentiation in service quality exacerbates regional inequality. Differences in functionality, stability, and level of technical support of regional digital platforms and integrated systems (for example, the "Unified Centralized Digital Platform in the Social Sphere") between advanced and lagging regions create *unequal conditions for access and quality of services* for citizens depending on their place of residence.

Erosion of the "human dimension" in service provision is a less obvious but important risk (Sivirinov, 2025). Excessive reliance on automation can lead to the loss of an important element of empathy, the ability to consider individual nuances of a situation and provide psychological support, especially in sensitive areas (social protection, healthcare). Standardized algorithms are not always able to replace human judgment in complex social contexts.

Digital transformation, designed to increase the efficiency and accessibility of public services, carries a paradoxical risk of deepening social disparities and creating new forms of injustice.

Overcoming these challenges requires not just technical solutions, but a targeted policy of inclusivity at all stages of designing and implementing digital solutions in the regional public sector.

Ways to overcome challenges and ensure inclusive digitalization. Overcoming the identified challenges of digital transformation to social justice requires not fragmented measures, but a comprehensive, targeted policy of *inclusive digitalization* (Grokhotov, 2025), where technological development is inextricably linked to ensuring equal opportunities for all citizens, regardless of their social status, age, place of residence, or level of digital competence. Implementing this approach involves the implementation of the following strategic directions:

Adopting inclusivity as a fundamental principle of digital policy: The formation and implementation of regional digitalization programs must be based on the priority of minimizing exclusionary effects. This means mandatory *social risk assessment* (Social Impact Assessment) for new digital projects, consideration of the needs of vulnerable groups at the service design stage (the "Design for All" principle), and the establishment of clear accessibility criteria.

Eliminating the infrastructural and economic digital divide: (1) *Accelerated development of ICT infrastructure:* Priority provision of quality broadband internet and mobile communications to remote, rural, and depressed territories within the framework of national projects (such as "Eliminating Digital Inequality") with enhanced monitoring of their implementation in lagging regions; (2) *Device accessibility programs:* Development and implementation of targeted programs (subsidies, preferential loans, provision of devices through social services, libraries, MFCs) to provide vulnerable groups (low-income, pensioners, large families) with necessary gadgets.

Large-scale development of population digital literacy: (1) *Systemic educational programs:* Creation of a network of free, accessible, and adapted (including for the elderly and persons with disabilities) digital literacy courses based in libraries, MFCs, social service centers, community centers, educational institutions; (2) *Local support:* Introduction of the institution of *digital curators/volunteers* (including social workers, MFC employees, active citizens) to provide personal assistance in mastering digital services, especially in rural areas and among the elderly population; (3) *Integration into educational standards:* Strengthening the component of digital literacy and safe use of public services in school and vocational education programs.

Guaranteed multi-channel access to services: (1) *Preservation and modernization of offline channels:* Preventing the forced transfer of services *exclusively* to electronic format, developing the MFC network as centers of comprehensive service and digital assistance. Telephone support lines must remain accessible and effective; (2) *"Human accompaniment":* Ensuring sufficient numbers of competent employees in MFCs and social institutions capable of helping with complex or non-standard requests, especially for citizens experiencing difficulties with digital services; (3) *Universal design and usability:* Strict adherence to accessibility standards for digital interfaces (WCAG) for persons with disabilities. Continuous work to simplify navigation, clarity of forms and instructions on portals (EPGU, RPGU), minimizing steps to receive services.

Strengthening trust and ensuring data security: (1) *Transparency and control:* Full information for citizens about what their data is collected, how it is used and protected. Development of mechanisms for public control over the use of state information systems; (2) *Enhancing protection levels:* Continuous improvement of technical and organizational measures to protect personal data in state information systems, prompt response to threats; (3) *Countering algorithmic discrimination:*

Development of methodologies for auditing algorithms used for decision-making (especially in the social sphere) for bias and fairness.

Digital transformation of the state apparatus and management processes: (1) *Training and retraining of civil servants:* Systematic improvement of the digital competencies of officials at all levels, including skills in working with data, managing digital projects, and interacting with applicants under new conditions; (2) *Implementation of flexible methodologies:* Application of Agile approaches in the development and implementation of digital services for greater adaptability to user needs; (3) *Development of a digital management culture:* Formation of an environment within authorities that encourages innovation, feedback, readiness for change, and a focus on citizen needs.

Monitoring, evaluation, and adaptation: (1) *Regular research.* Conducting sociological surveys and focus groups to assess the real accessibility, convenience, and satisfaction with digital services among different socio-demographic and territorial groups. (2) *System of inclusivity indicators:* Development and tracking of indicators reflecting the level of digital inclusion of vulnerable groups and territories (infrastructure coverage, service usage activity, literacy level, satisfaction); (3) *Flexible policy adjustment:* Using monitoring data for prompt problem identification and adaptation of digital transformation strategies in the regions.

Interregional cooperation and replication of best practices: Creating effective platforms for experience exchange between regions (leaders and outsiders). Development and promotion of standard, adaptable solutions (especially for lagging regions) in the field of inclusive digital services, infrastructure projects, and training programs.

CONCLUSIONS

The digital transformation of the public sector in Russian regions is an irreversible and objectively necessary process with significant potential for increasing management efficiency, quality, and accessibility of public services. As the analysis has shown, it can become a powerful tool for strengthening social justice by overcoming geographical and physical barriers, increasing transparency, reducing corruption risks, and creating prerequisites for more targeted social policy. However, the realization of this positive scenario is by no means guaranteed.

The main conclusion of the study is that *technological progress in itself does not eliminate, and often exacerbates, existing social disparities if not accompanied by a targeted policy of inclusivity*. Profound digital inequality, manifested in the infrastructural limitations of lagging regions, the lack of digital skills among a significant part of the population (especially the elderly and rural residents), as well as the risks of marginalization of vulnerable groups, is a key threat to the principles of social justice in the digital age. Problems of "digital bureaucratism," threats to data confidentiality, and persistent territorial differentiation in service quality only intensify this challenge.

Successfully overcoming these risks requires rethinking the very paradigm of digital transformation in the public sector. *Inclusive digitalization* should become not a secondary addition, but a *central imperative* of state policy at the federal and regional levels. This implies systemic investments in eliminating the digital divide (infrastructure, devices, literacy), unconditional guarantee of multi-channel access to services, designing services considering user diversity, building trust through security and transparency, as well as a deep digital transformation of the state apparatus itself.

Particular importance in the context of modern Russia has the *regional context*. Inclusive digitalization policy must provide for *differentiated approaches and targeted support for lagging subjects of the Russian Federation*, where the challenges of digital inequality and social exclusion are most acute. Mechanisms of interregional cooperation and replication of best practices are critically important here.

Ultimately, ensuring social justice in the process of digital transformation of the public sector is not a technical task, but a *complex socio-political problem*. Its solution depends on recognizing the priority of social goals over technological ones, readiness for systemic investments in human capital and infrastructure, and, above all, on consistent political will aimed at ensuring that the digital benefits of the state become truly accessible and useful to every citizen, regardless of their circumstances and place on the map of Russia. Only under these conditions can digitalization realize its potential as a force contributing to greater justice, rather than deepening existing divides.

REFERENCES

1. Government of the Russian Federation. (2021). *Распоряжение от 22 октября 2021 г. N 2998-р [Directive No. 2998-r of October 22, 2021 "On Approval of the Strategic Direction for Digital Transformation of Public Administration"]*. https://www.garant.ru/products/ipo/prime/doc/402867092 (Accessed: 25.05.2025).
2. Government of the Russian Federation. (2024). *Распоряжение от 28 декабря 2024 г. № 4146-р [Directive No. 4146-r of December 28, 2024 "On Approval of the Spatial Development Strategy of the Russian Federation for the Period until 2030 with a Forecast to 2036"]*. https://www.consultant.ru/law/hotdocs/87971.html (Accessed: 25.05.2025).
3. Ministry of Digital Development of Russia (n.d. a). Национальный проект "Экономика данных и цифровая трансформация государства" [National Project "Data Economy and Digital Transformation of the State"]. https://digital.gov.ru/target/naczionalnyj-proekt-ekonomika-dannyh-i-czifrovaya-transformacziya-
4. gosudarstva (Accessed: 25.05.2025).
5. Ministry of Digital Development of Russia (n.d. b). Федеральный ситуационный центр электронного правительства [Federal E-Government Situation Center]. https://digital.gov.ru/activity/czifrovizacziya-gosudarstva/infrastruktura-elektronnogo-pravitelstva/federalnyj-situaczionnyj-czentr-elektronnogo-pravitelstva (Accessed: 25.05.2025).
6. Ministry of Digital Development of Russia (n.d. c). Единая информационная платформа национальной системы управления данными [Unified Information Platform of the National Data Management System]. https://digital.gov.ru/activity/czifrovizacziya-gosudarstva/infrastruktura-elektronnogo-
7. pravitelstva/federalnaya-gosudarstvennaya-informaczionnaya-sistema-edinaya-informaczionnaya-platforma- naczionalnoj-sistemy-upravleniya-dannymi (Accessed: 25.05.2025).
8. Rostelecom (Operator) (n.d.). Единый портал государственных и муниципальных услуг (функций) [Unified Portal of State and Municipal Services (Functions)]. https://www.gosuslugi.ru/ (Accessed: 25.05.2025).
9. Ministry of Digital Development of Russia (n.d. d). Система межведомственного электронного взаимодействия [System of Interagency Electronic Interaction]. https://digital.gov.ru/activity/czifrovizacziya-gosudarstva/infrastruktura-elektronnogo-pravitelstva/sistema- mezhvedomstvennogo-elektronnogo-vzaimodejstviya (Accessed: 25.05.2025).
10. Government of Moscow Region (n.d.). Региональная геоинформационная система Московской области [Regional Geographic Information System of Moscow Region]. rgis.mosreg.ru (Accessed: 25.05.2025).
11. Ministry of Digital Development of Russia (n.d. e). Центры управления регионов [Regional Situation Centers]. https://digital.gov.ru/activity/czifrovizacziya-gosudarstva/czentry-upravleniya-regionami (Accessed: 25.05.2025).

12. Ministry of Science and Higher Education of Russia (n.d.). Портал «Современная цифровая образовательная среда в РФ» [Portal "Modern Digital Educational Environment in the Russian Federation"]. https://online.edu.ru/public/promo (Accessed: 25.05.2025).
13. Ministry of Digital Development of Russia / Gosuslugi Portal (n.d.). Что такое СМЭВ? [What is SMEV?]. https://info.gosuslugi.ru/articles/Что_такое_СМЭВ/ (Accessed: 25.05.2025).
14. Falletti, E. (2023). Algorithmic Discrimination and Privacy Protection. Journal of Digital Technologies and Law, 1(2). doi:10.21202/jdtl.2023.16.
15. W3C Web Accessibility Initiative (n.d.). Web Content Accessibility Guidelines (WCAG) Overview. https://www.wcag.com/ (Accessed: 25.05.2025).
16. Grokhotov, D.O. (2025). Цифровая трансформация государственных служб: современные решения и вызовы [Digital Transformation of Public Services: Modern Solutions and Challenges]. Bulletin of Science, 2(5(86)), 492–497.
17. Plotichkina, N.V. (2020). Цифровая инклюзия: теоретическая рефлексия и публичная политика [Digital Inclusion: Theoretical Reflection and Public Policy]. Tomsk State University Journal of Philosophy, Sociology, and Political Science, (58), 216–226.
18. Sivirinov, B.S. (2025). Будущее – человеческое измерение и позитивное переосмысление трансгуманитарного проекта [The Future: The Human Dimension and Positive Rethinking of the Transhumanitarian Project]. Theory and Practice of Social Development, (4), 49–55. doi:10.24158/tipor.2025.4.4.
19. Tertyshnikova, A.G., & Pavlova, U.O. (2022). Социальная эксклюзия как негативное последствие цифровизации [Social Exclusion as a Negative Consequence of Digitalization]. Theory and Practice of Social Development, (12), 106–110. doi:10.24158/tipor.2022.12.15.

DIGITAL TRANSFORMATION OF THE KRASNODAR KRAI: ANALYSIS OF PROGRAM AND REGULATORY SUPPORT

UDC: 004-048.35:332.146(470.620)
DOI: https://doi.org/10.53486/tids2025.26

SERGEY BAZHENOV
Science Horizons Foundation, Russia
sbazhenov@mail.ru
ORCID ID: 0000-0001-7593-0526

ELENA BAZHENOVA
Southern Federal University, Russia
eubazhenova@sfedu.ru
ORCID ID: 0000-0001-8253-5073

DMITRY ABROSIMOV
Southern Federal University, Russia
dabrosimov@sfedu.ru
ORCID ID: 0000-0002-5278-6581

Abstract. This article presents a comprehensive analysis of the programmatic and regulatory framework for digital transformation processes in the Krasnodar Krai region of Russia. Based on a content analysis of key regional strategic, programmatic, and regulatory documents, the study identifies core goals, priorities, and implementation mechanisms, while also establishing strengths, systemic issues, and regulatory gaps. The findings reveal a developed programmatic base focused on digitalizing key economic and social sectors. However, they also highlight a lag in the regulatory framework compared to the pace of technological change, fragmented regulation of emerging areas (AI, big data), and insufficient coordination between programmatic objectives and the legal instruments for achieving them. The study formulates practical recommendations for enhancing the programmatic and regulatory framework, including updating documents, addressing gaps, harmonizing legislation, and strengthening implementation monitoring.

Keywords: digitalization, Internet, digital economy, information, Krasnodar Krai.

JEL Classification: R58, O38, H70, O18

INTRODUCTION

The dynamics of technological progress dictate the necessity for fundamental changes in socio-economic systems. Digital transformation (DT) has ceased to be solely a technological trend, becoming a key factor of competitiveness and sustainable development for both national economies as a whole and individual regions. In the Russian Federation, DT is recognized as a strategic priority, enshrined in national programs and projects. In this context, Krasnodar Krai, as one of the most dynamically developing and strategically important subjects of the Russian Federation with a developed multi-sectoral economy (agro-industrial complex, tourism, transport, construction) and a large population, represents a relevant object for researching regional aspects of digitalization. The effectiveness of DT at the regional level is largely determined by the quality of its programmatic and regulatory support – the system of strategic guidelines, action plans, and legal frameworks that create conditions for innovation adoption and change management.

The *relevance* of this research is driven by the necessity for scientific understanding and assessment of existing regulatory mechanisms for DT in a major Russian region, identifying bottlenecks, and developing recommendations for overcoming them. Despite the existence of a significant body of programmatic and regulatory documents, their comprehensive analysis from the perspective of consistency, completeness, coherence, and alignment with contemporary challenges remains insufficiently represented in the scientific literature.

The *purpose of the article* is to conduct a comprehensive analysis of the system of programmatic and regulatory support for digital transformation processes in Krasnodar Krai.

To achieve this goal, the following *tasks* are addressed:

1. Identification and systematization of key federal and regional-level programmatic and regulatory documents relevant for the DT of Krasnodar Krai.
2. Analysis of the goals, objectives, priority directions, and implementation mechanisms of digital transformation, as established in the Krai's programmatic documents.
3. Analysis of the content and assessment of the completeness, relevance, and consistency of the regulatory legal framework governing DT aspects in the Krai.
4. Identification of strengths, gaps, contradictions, and potential risks within the existing system of programmatic and regulatory support.
5. Formulation of scientifically grounded recommendations for improving the programmatic and regulatory framework for digital transformation in the region.

The *object of the research* is the process of digital transformation of the socio-economic sphere of Krasnodar Krai. The *subject of the research* is the set of programmatic (strategies, concepts, state programs, roadmaps) and regulatory legal acts (Krai laws, decrees and orders of the Governor and Krai Government) that form the basis for implementing DT in the region.

MAIN CONTENT

Theoretical and Methodological Foundations and Research Context. Before proceeding to the analysis of specific regional practice, it is necessary to clarify key concepts and outline the general context.

Digital transformation in the context of this research is understood as a profound, strategically directed restructuring of business processes, activity models, products and services, and the management system based on the integration of digital technologies, aimed at achieving fundamentally new results in enhancing efficiency, creating additional value, and improving quality of life. This is a process that extends far beyond simple automation or data digitization.

Programmatic support for DT encompasses a set of strategic and tactical planning documents defining the vision, goals, objectives, priority directions, key projects, performance indicators, resource provision, and management mechanisms for the digitalization process. These include strategies, concepts, state (municipal) programs, federal and regional projects, and roadmaps.

Regulatory support for DT represents the totality of regulatory legal acts of various levels that establish the legal foundations governing relations arising in connection with the creation and use of digital technologies, data, services, and also define the rights, obligations, responsibilities of entities, and implementation mechanisms for policy in this sphere. These are laws, by-laws, administrative regulations, standards, and methodological guidelines.

The *federal context* for DT in Russia is primarily defined by the National Development Goals of the Russian Federation for the Period until 2030 and the Long-Term Perspective until 2036, the state program "Information Society", the national project "Data Economy and Digital Transformation of the State", as well as associated federal projects (*C1. Infrastructure for Access to the Internet Information and Telecommunication Network, C2. Digital Platforms in Social Sphere Industries, C3. Artificial Intelligence, C4. Digital Public Administration, C5. Domestic Solutions, C6. Applied Research and Advanced Developments, C7. Cybersecurity Infrastructure, C8. Personnel for Digital Transformation, C9. State Statistics*), state programs and strategies (Strategy for the Development of the Information Society, Strategy for Scientific and Technological Development). These documents define general goals, objectives, target indicators, directions, and principles of DT for the entire country, creating the framework within which regions operate.

Krasnodar Krai possesses a number of *specific characteristics* influencing the trajectory and priorities of its digital transformation:

1. The most populous region in Southern Russia: High demand for effective digital state and municipal services.
2. Multi-sectoral economy: Leading positions in the agro-industrial complex, a powerful resort and tourism complex, developed transport and logistics infrastructure, and a construction sector. DT must cover all key industries.
3. High investment attractiveness: Need to create digital infrastructure and a favorable regulatory climate for IT business and innovation.
4. Geopolitical position: Importance of developing digital services in logistics and ensuring cybersecurity.
5. Significant proportion of rural territories: Relevance of addressing the problem of the digital divide.

These specificities should be reflected in the regional programmatic and regulatory support for DT.

Analysis of the Programmatic Support for Digital Transformation of Krasnodar Krai. The programmatic base for DT in Krasnodar Krai is formed at several levels and includes documents of varying degrees of generality and detail.

The *Strategic level* is set by the "Strategy for the Socio-Economic Development of Krasnodar Krai for the Period until 2030". This document defines DT as one of the key drivers of regional development. It formulates overarching goals:

- Improving the quality of life of the population through the introduction of modern digital services.
- Ensuring the global competitiveness of the Krai's key economic sectors based on digital technologies.
- Forming an effective system of digital public administration.
- Creating modern digital infrastructure as a foundation for development.

Priority directions identified include: *"smart" agriculture, digital tourism, "smart" cities, digital healthcare and education, development of telecommunications infrastructure (including eliminating the "digital divide"), and training IT personnel.*

The *Tactical level of implementation* of these strategic guidelines is represented primarily by the state programs of Krasnodar Krai, which integrate digital components:

The *State Program "Information Society"* is the core program for DT. It focuses on developing communications infrastructure (including the "Information Infrastructure" project), providing state and municipal services electronically (MFCs, "Gosuslugi" portal), developing regional information systems, ensuring information security for government bodies, and promoting digital literacy among the population.

Sectoral Programs. Digitalization is a cross-cutting element of programs such as: ("Development of Agriculture and Regulation of Agricultural Markets", "Development of Resorts and Tourism", "Development of Healthcare", "Development of Transport", "Housing and Communal Services and Energy").

Specialized DT documents. The Krai has developed and adopted documents directly focusing on DT:

Strategy in the Field of Digital Transformation of Economic Sectors, Social Sphere, and Public Administration of Krasnodar Krai. This document details the goals and objectives of DT as applied to the Krai, defines specific projects and initiatives (e.g., development of platform solutions, implementation of AI technologies in public administration, creation of a regional Data Center), establishes key performance indicators and responsible executors. It serves as the main action plan.

Roadmaps for the implementation of individual DT directions. For example, a roadmap for the implementation of artificial intelligence, development of "smart" cities, ensuring information security of the region's critical information infrastructure (CII).

Analysis of the content of programmatic documents allows us to identify the following key aspects:

Goals: Primarily focused on improving public administration efficiency, quality of life for the population, business competitiveness, and creating digital infrastructure.

Priority Directions: An orientation towards sectoral digitalization (agro-industrial complex, tourism, housing and communal services, transport, healthcare, education) and the development of the digital state (electronic services, interagency interaction, data management) is evident.

Projects and Initiatives: Documents name specific projects (e.g., creation of a Unified "Smart City" Platform for municipalities, implementation of the "Digital Agronomist" system, development of the MFC network as centers for providing digital services), but details (technical solutions, budgets) often require reference to appendices or operational plans.

Indicators: Both quantitative (share of state services available online; broadband penetration rate; number of connected "smart" meters; number of people trained in digital competencies) and qualitative (level of citizen satisfaction) indicators are used. However, the link of some indicators to the ultimate effect of DT is not always obvious.

Implementation and Financing Mechanisms: Primary emphasis is on budgetary financing (Krai budget, co-financing from the federal budget), as well as public-private partnership (PPP) mechanisms. Management of implementation is assigned to relevant ministries and subordinate institutions (e.g., KRAU "Center of Information Technologies").

Evaluation of the consistency and coherence of programmatic documents reveals both strengths and problems:

Strengths: Existence of a multi-level system of documents (strategy -> state programs -> regional DT program -> roadmaps); overall alignment of the Krai's documents' goals with federal priorities (national program "Digital Economy"); coverage of key industries and spheres.

Problems: Individual sectoral programs may have weak coordination regarding their digital components; duplication of tasks in different documents is sometimes observed; success indicators do not always directly reflect the transformational effect; mechanisms for attracting private investment in DT are insufficiently developed; implementation risks (technological, personnel, organizational) are not always detailed and accounted for in plans.

Analysis of the Regulatory Support for Digital Transformation of Krasnodar Krai. The regulatory framework governing DT aspects in the Krai is formed within the framework of federal legislation and includes regional-level acts.

Overview of Key Regulatory Legal Acts (RLA) of Krasnodar Krai: Laws of Krasnodar Krai:

- On Regulating Certain Relations in the Sphere of Providing State and Municipal Services (establishes principles, procedures, including for electronic services).
- On Informatization and Information Resources of Krasnodar Krai (defines the foundations for IT management, regional information systems, data).
- On Certain Issues of Procurement of Goods, Works, Services to Meet State and Municipal Needs (regulates, in particular, procurement of IT solutions, including specifics for innovative and high-tech products).
- Official laws regulating specific spheres (healthcare, education, housing and communal services, tourism, agro-industrial complex), which contain norms concerning the application of information technologies, data processing, and provision of electronic services in these industries.

Decrees and Orders of the Governor and the Government of Krasnodar Krai. This constitutes the main body of documents directly regulating DT:

- On Approval of State Programs (including the "Information Society" program and others with digital components).
- On Approval of the Concept/Program of Digital Transformation, Roadmaps.
- On the Creation and Functioning of Regional Information Systems (RIS) (e.g., RIS Housing and Communal Services, RIS Tourism, RIS Agro-industrial Complex).
- On the Procedure for Information Interaction of Government Bodies.
- On Organizing Information Protection, Personal Data Protection, Ensuring Security of CII on the Territory of the Krai.
- On the Implementation of Specific Technologies or Services (e.g., on the application of blockchain technology in specific registries, on the development of the MFC network).
- On the Creation of Coordination or Advisory Bodies on Digitalization Issues (working groups, project offices).

Departmental Acts (orders of ministries). Administrative regulations for providing state services electronically; methodological recommendations for technology implementation; data exchange standards; regulations on regional information systems.

Analysis of the content of the regulatory framework allows for the following observations:

- *Regulation of Processes.* Issues of providing electronic services, functioning of MFCs, handling citizen appeals electronically, working with RIS, conducting IT procurements are regulated in sufficient detail. Measures have been taken to ensure information security of government bodies and protect personal data. However, regulation of new processes (big data management, AI implementation, IoT use, regulation of digital platforms) is in its infancy or absent.

- *Regulation of Relations.* General rules for interaction between government bodies and with citizens/businesses in the digital environment are established. However, norms stimulating the development of the digital economy (e.g., regulation of sandboxes for testing innovations, support for IT startups, digital contracts) are underdeveloped. Clearer definition of the rights and obligations of participants in new digital ecosystems is required.
- *Legal Conditions.* Foundations for infrastructure development have been created (e.g., issues of placing telecommunications equipment). However, norms stimulating the deployment of innovative infrastructure (data centers, 5G/IoT networks, sensor systems for "smart" cities) are clearly insufficient. The problem of the digital divide is addressed mainly through federal programs.

Assessment of completeness and relevance reveals significant problems:

- *Lagging Behind Technologies.* The regulatory framework often fails to keep pace with the speed of emergence and implementation of new technologies (AI, blockchain, big data, metaverses). Regulation is reactive, not proactive.
- *Gaps in New Spheres.* Norms regulating the use of artificial intelligence in public administration and business, management of big data (especially open data), application of the internet of things in urban services and agro-industrial complex, legal status of digital twins are absent or extremely fragmented.
- *Fragmentation and Complexity.* Regulation of digital aspects is scattered across numerous laws and by-laws pertaining to different spheres. This creates difficulties for enforcement and increases the risk of contradictions.
- *Duplication and Contradictions.* Cases of norm duplication in different acts, or worse, inconsistencies in requirements, especially in regulating interagency processes or data, are encountered.
- *Insufficient Linkage with Programmatic Goals.* Not all ambitious goals stated in programs (especially regarding innovations) are supported by the necessary legal instruments and incentives.

Assessment of Enforcement Effectiveness is difficult due to limited data openness, but indirect signs (reports of the Krai Audit Chamber, media publications, expert opinions) indicate problems with the enforcement of some norms, related to resource shortages (personnel, financial), insufficient qualifications of implementers, and sometimes the ambiguity of the legal prescriptions themselves.

Assessment of the System of Programmatic and Regulatory Support: Challenges and Opportunities. Integrating the results of the analysis of programmatic and regulatory aspects allows for a holistic assessment of the DT support system in Krasnodar Krai.

Alignment of Programs and Norms. There is a clear gap between ambitious programmatic goals for DT (especially regarding innovations, "smart" solutions) and the capabilities of the existing regulatory framework. Programs set the direction, but norms do not always provide adequate "rules of the game" for its implementation. For example, programs promote the use of AI in public administration, but legal frameworks for its ethical, safe, and effective application are absent.

Support for Basic Processes. Regarding basic digitalization (electronic services, MFCs, interagency interaction, IT infrastructure of government bodies), the programmatic and regulatory support works relatively coherently. Significant results have been achieved.

Regulation of New Spheres. It is precisely in the area of breakthrough DT directions (AI, big data, IoT, digital platforms) that the systematicity of support is minimal. Programs declare importance, but norms are either absent or fragmented and unsystematic.

Strengths of the System:

- *Existence of a Comprehensive Strategy and Programs.* DT is recognized as a priority at the highest level of regional governance, reflected in key documents.
- *Sectoral Coverage.* Programs cover the digitalization of all key sectors of the Krai's economy and social sphere.
- *Developed Base for E-Government.* A functional body of regulatory legal acts governing the provision of online state services, MFC operations, and the use of basic regional information systems has been formed.
- *Attention to Infrastructure and Security.* Programmatic and regulatory efforts are directed towards developing telecommunications and ensuring a basic level of information security.
- *Focus on Personnel.* Programs include measures for developing digital competencies among the population and civil servants.

Key Problems and Risks:

- *"Regulatory Vacuum" for Innovations.* Lack of adequate regulation for AI, big data, IoT, and digital platforms hinders their implementation, creates legal uncertainty for business and government, and increases risks (ethical, security, discrimination).
- *Fragmentation and Complexity of Regulation.* The multiplicity of acts and their dispersion across spheres makes them difficult to find, understand, and apply, especially for businesses and municipalities.
- *Lag of Norms Behind Programmatic Directives.* The regulatory framework fails to keep pace with the dynamics of programmatic documents and does not provide the necessary legal instruments for implementing innovative projects.
- *Insufficient Interagency Coordination.* Development of programs and norms is often carried out within individual agencies without proper synchronization, leading to duplication, inconsistencies, and gaps.
- *Resource Constraints.* Insufficient funding, shortage of highly qualified IT specialists and lawyers in the field of digital law within government bodies limit the possibilities for high-quality development and implementation of both programs and norms.
- *Risk of Digital Divide.* Despite programs, the regulatory framework weakly stimulates bridging the digital gap between urban and rural areas, and different social groups.
- *Cyber Risks.* Regulatory regulation of cybersecurity, especially CII, requires constant strengthening and updating due to growing threats.

Opportunities for Development:

- *Development of "Anticipatory" Regulation.* Creation of legal "sandboxes" for testing innovations, development of concepts and model acts for new directions (AI, big data).
- *Codification and Systematization.* Initiating the process of creating a Digital Code of Krasnodar Krai (or a similar consolidated act) to consolidate and harmonize norms in the field of DT.
- *Strengthening Coordination.* Creating an effective interagency body (based on an existing

project office) with authority to coordinate the development and approval of all programmatic and regulatory documents on DT.

- *Development of PPP.* Improving the regulatory framework to attract private investment in digital infrastructure and DT projects.
- *Focus on Data.* Developing a comprehensive regulatory framework for managing regional data (open data, data for AI, ensuring data quality and security).

CONCLUSIONS

The conducted analysis of the programmatic and regulatory support for the digital transformation of Krasnodar Krai allows us to draw the following main conclusions:

1. Krasnodar Krai has formed a multi-level system of programmatic documents (strategy, state programs, regional DT program, roadmaps), which defines DT as a key development priority and covers a wide range of industries and spheres of activity. The documents are generally aligned with federal guidelines.
2. The regulatory framework governing DT aspects is sufficiently developed in terms of basic e-government processes, IT infrastructure of government bodies, and ensuring information security. However, it is characterized by fragmentation, complexity, and, most importantly, a significant lag behind the dynamics of technological development and the ambitions of the programmatic documents.
3. The most critical gaps and problems were identified in the regulatory framework for new, breakthrough directions of DT: artificial intelligence, big data, internet of things, digital platforms. There is a gap between the programmatic goals of innovative development and the available legal instruments for achieving them.
4. Other significant problems include insufficient coordination between developers of programs and norms, resource constraints (finances, personnel), risks of the digital divide and cyber threats.
5. Despite the problems, the existing system of programmatic and regulatory support possesses development potential, including opportunities for anticipatory regulation, systematization of legislation, strengthening of PPP, and data management.

REFERENCES

1. President of Russia, 2021. Decree of the President of the Russian Federation dated 02.07.2021 No. 400 "On the National Security Strategy of the Russian Federation". Available at: http://www.kremlin.ru/acts/bank/47046 (Accessed: 25.05.2025).
2. President of Russia, 2024. Decree of the President of the Russian Federation dated 07.05.2024 No. 309 "On the National Development Goals of the Russian Federation for the Period until 2030 and the Long-Term Perspective until 2036". Available at: http://www.kremlin.ru/acts/bank/50542 (Accessed: 25.05.2025).
3. Government of Russia, 2014. Decree of the Government of the Russian Federation dated 15.04.2014 No. 313 (as amended on 25.12.2024) On Approval of the State Program of the Russian Federation "Information Society". Available at: https://digital.gov.ru/target/gosudarstvennaya-programma-informaczionnoe- obshhestvo (Accessed: 25.05.2025).
4. Department of Informatization and Communications of Krasnodar Krai, 2022. *Strategy in the Field of Digital Transformation of Economic Sectors, Social Sphere, and Public Administration of Krasnodar Krai dated 28.12.2022*. Available at: https://dis.krasnodar.ru/documents/strategiya-v-oblasti-tsifrovoy-transformatsii (Accessed: 25.05.2025).

5. Ministry of Economic Development of the Russian Federation, 2024. *Strategy for the Socio-Economic Development of Krasnodar Krai until 2030 dated 11.12.2018.* Available at: https://www.economy.gov.ru/material/file/e4e8b9ddede078a93f60f5e7a08fce28/krasnodar.pdf (Accessed : 25.05.2025).
6. Department of Business Development and Foreign Economic Activity of Krasnodar Krai, 2019. Passport of the Regional Project "Information Security (Krasnodar Krai)" dated 15.06.2019. Available at: https://dirmsp.krasnodar.ru/pasports/cifra/RP_Informacionnaya_bezopasnost.pdf (Accessed: 25.05.2025).
7. Gavrilov, A., 2024. Digitalization in Krasnodar Krai: How the Region's Business is Moving Towards Unified Standards. Available at: https://sochi.mk.ru/social/2024/10/08/cifrovizaciya-v-krasnodarskom-krae-kak- biznes-regiona-prikhodit-k-edinym-standartam.html (Accessed: 25.05.2025).
8. Khudov, A.M., 2022. Digital Development of Regions: Trends, Challenges, Analysis of Factors. Natural and Humanitarian Studies, 4 (42)), 300-307.
9. Bratarchuk, T.V., 2023. Current Problems of Legal Regulation of the Digital Economy in the Russian Federation. *Issues of Russian and International Law, 13* (5A). 140-147.
10. Anisimov, A.Yu., Aleksakhina, S.A., Gorshkova, A.A., and Seliverstov, S.N., 2025. Globalization of Digital Transformation Trends. *Issues of Innovation Economics, 15*(3).
11. Official Internet Portal of the Department of Informatization and Communications of Krasnodar Krai, (n.d.). Available at: https://dis.krasnodar.ru/ (Accessed: 25.05.2025).

REGULATORY ORDER IN THE CONTEXT OF STATE DIGITAL TRANSFORMATIONS

UDC: 004-048.35:[316.776:177]
DOI: https://doi.org/10.53486/tids2025.27

NATALIA CHERNOBROVKINA
Southern Federal University, Russia
nichernobrovkina@sfedu.ru
ORCID ID: 0000-0001-5385-4585

Abstract. The regulatory order in the context of digital transformations of the state is considered from the standpoint of managerial and academic approaches. According to experts representing the managerial approach, the regulatory order represents a form of social relations between individuals and social groups interacting about their standard and quality of life, therefore, the digital transformation of the state is aimed at improving them through the use of information and communication technologies. Representatives of the academic approach consider the digital transformation of the state from the standpoint of the value basis of the content of norms and regulatory mechanisms: along with legal norms and external control in the form of censorship, the regulation of the digital space is carried out by ethical control in accordance with the norms of self- organization - respect for each other network actors and the reliability of information provided.

Keywords: regulatory order, digital transformations of the state, mechanisms of social regulation, social control

JEL Classification: H83, R58, D02

INTRODUCTION

Currently, digitalization covers all spheres of society's life, which gives rise to numerous disputes among scientists and experts regarding the methods of regulatory control of this process. This is because their interpretations of the essence of the regulatory order differ.

Experts, as representatives of the political elite, believe that the regulatory order represents a form of social relations of individuals and social groups interacting about their level and quality of life as ways of realizing life opportunities. Therefore, digital transformations in the state sphere are interpreted by experts from the perspective of using information and communication technologies and artificial intelligence to improve the level and quality of life of citizens in various spheres, primarily education and medicine. The effectiveness of management also depends on these technologies, as they contribute to the rapid exchange of information, its "openness," which facilitates the monitoring of the implementation of government decisions.

Scientists offer a broader interpretation of the concept of regulatory order, which allows answering the question of why individuals and social groups obey norms and what is the basis of this obedience. According to researchers, the regulatory order is a form of social relations in which purposefully rational individuals and groups are guided by common rules and expect that their needs and interests will be satisfied within the framework of existing norms and control. Accordingly, the digital transformation of the state is considered by scientists from the standpoint of the value basis of the content of norms and mechanisms of regulatory control.

MAIN CONTENT

Thus, the different approaches of scientists and experts to the methods of digital transformation of the state are caused by differences in the interpretation of the essence of the regulatory order. These approaches can be defined as managerialist and academic. According to the managerialist approach, the regulatory order is a prescription aimed at ensuring the needs of individuals and social groups, and control over its execution. The academic approach involves considering the regulatory order from the perspective of the legalization of norms that have a value basis, due to which individuals and social groups not only submit to external control due to the threat of sanctions but recognize their significance. In this case, the regulatory order is supported not so much by prescription and prohibition as by the recognition of the significance of norms, which ensures agreement in society regarding their legalization and methods of control. Consequently, the stability of the regulatory order depends on its mechanisms—social control and legitimation, which are in a relationship of functional dependence.

The difference in the interpretation of the regulatory order, demonstrated by the managerialist and academic approaches, directly concerns the digital transformation of the state.

According to the managerialist approach, control in the digital space is carried out in relation to the information being prepared and disseminated through censorship. It is defined as "*control by official (secular or spiritual) authorities over the content, release, and distribution of printed materials, the content (performance, display) of plays and other stage works, film, video or photographic works, works of fine art, radio and television broadcasts, and sometimes private correspondence, in order to prevent or limit the dissemination of ideas and information deemed undesirable or harmful by these authorities*" (Knyazev, no date). The norms regulating censorship activities are enshrined in laws and aimed at prohibiting extremist activities, causing harm to the development and health of children, and disseminating personal data of individuals who have not given their consent.

The norms of legal control of information dissemination in the digital space are restrictive and prohibitive in nature, as demonstrated by the actions of Roskomnadzor (Russian Federal Service for Supervision of Communications, Information Technology and Mass Media), which can "*block websites at the request of the Prosecutor General's Office without a court order. Any site can be blocked in just an hour if its content is extremist in the opinion of the prosecutor's office*" (Dzyaloshinskaya, 2019, p. 44). However, these actions are recognized by experts and the public as fair "*in relation to child pornography, drugs, suicides have proven their effectiveness. This is a deterrent for owners of other Internet resources, including those with content produced by users themselves, and it is an incentive to pay closer attention to what users post and to check groups and public pages for compliance with the law*" (Bfm.ru, no date).

However, experts face a number of difficulties in the legal control of information in the digital space. On the one hand, this is caused by the specifics of the information and communication environment. In particular, its anonymity creates difficulties in identifying the subject responsible for disseminating information. Another difficulty is related to the legal status of the information disseminator if it is presented by unofficial sources: a blogger may be a subject without professional education, and their degree of responsibility is not normatively established, making it difficult to qualify. Moreover, many actions that are prohibited by law can hardly be recognized as such in the digital space. Therefore, some experts believe that legal control regarding intellectual property, privacy protection, and respect for human dignity is limited in the digital space, and due to the anonymity of disseminated information, the regulatory framework lagging behind technological development, and the procedural specifics of sanctions, such control is generally ineffective.

Consequently, an important task of legal control is the compliance of the content of norms and sanctions with the specifics of the development of the digital space, but its implementation is currently difficult.

Representatives of the academic approach emphasize the limitations of legal norms establishing responsible dependence and their control in the digital space and note that they should be supplemented by self-organization norms that define the boundaries of spontaneous decisions of subjects in the network community. Self-organization norms in the digital space are objectified in such rules as respectful attitude towards each other in the communication process and the presentation of reliable information. Their basis is values such as freedom, respect for human dignity, and inviolability of private life.

Currently, some proponents of the academic approach believe that the regulation of the digital space can be carried out through the formation of a new value system based on the values of information and knowledge. This position is related to the answer to the classical question: is the information society a new stage of social development or is it another stage of the post-industrial society caused by technological development? In answering this question, one important argument can be made: a new stage of social development is accompanied by a change in social structure, and currently this is not happening.

The contradictory nature of value attitudes, demonstrated by various subjects of the digital space, is caused by subcultural diversity, the consequence of which is various lifestyles. This occurs as a result of the constant differentiation of activities as a consequence of an increasingly complex social environment. In the digital space, network actors can only expand the boundaries of presenting their activities more quickly and increase the number of followers. However, the differentiation occurring within it leads to the restriction of spontaneous actions and adherence to self-organization norms in a situation of information freedom. A high level of consumer awareness inevitably increases competition among network actors and the quality of services they provide in the form of reliable information.

Consequently, self-organization norms, such as the respectful attitude of representatives of the network community towards each other, are formed depending on the stability of the norms of responsible dependence. According to researchers, the problem of the relationship between a high degree of freedom and the formation of norms of social responsibility is resolved when the individual themselves decides on the necessity or restriction of access to network information and the degree of their participation in the communication process. This is possible in the case of building rational relationships in the digital space based on the principle of the importance of the information received and awareness of the tasks for its use.

Currently, self-organization norms in the digital space are studied in the form of ethical principles for regulating the interaction of network actors within the framework of "*information ethics (studies moral problems arising in connection with the development and application of information technologies); computer ethics (the question of right and wrong use of information in the information society); cyberethics (the philosophical area of ethics relating to computers, covering user behavior, what computers are programmed to do, and how this affects individuals and society as a whole*" (Malkova, 2001, p. 114). The ethical principles considered by various branches of knowledge are objectified in the rules of presenting reliable information and respectful attitude towards each other by network actors, based on the values of freedom of action, respect for human dignity, and inviolability of private life.

Ethical control, as a mechanism for regulating self-organization norms in the digital space, is formed in the form of self-organization norms and social responsibility. Self-organization norms are reduced to the basic principles - respectful attitude of network actors towards each other and reliability of the information provided. They depend on the stability of the norms of responsible dependence - rational relationships based on the principles of the importance of the information received and awareness of the tasks for its use. Violation of these norms is followed by negative sanctions: exclusion of an individual from the network group as a result of condemnation of the behavior of one of its members or condemnation of actions in the form of reviews about them in chats, discussions in the same groups. They are aimed at awareness and formation of the individual's social responsibility for their behavior in the digital space and social networks.

CONCLUSIONS

Ethical control, as a mechanism for regulating self-organization norms in the digital space, is formed in the form of self-organization norms and social responsibility. Self-organization norms are reduced to the basic principles - respectful attitude of network actors towards each other and reliability of the information provided. They depend on the stability of the norms of responsible dependence - rational relationships based on the principles of the importance of the information received and awareness of the tasks for its use. Violation of these norms is followed by negative sanctions: exclusion of an individual from the network group as a result of condemnation of the behavior of one of its members or condemnation of actions in the form of reviews about them in chats, discussions in the same groups. They are aimed at awareness and formation of the individual's social responsibility for their behavior in the digital space and social networks.

REFERENCES

1. Dzyaloshinskaya, M.I., 2019. Socially Responsible Behavior on the Internet: Search for a Model. *Questions of Theory and Practice of Journalism,* *4*(1), 43-51.
2. Knyazev, A.A., (no date). *Censorship*. Encyclopedic Dictionary of Mass Media. Available at: https://smi.academic.ru/230 (Accessed: 23.06.2025)
3. Bfm.ru, (no date). *Any Site Can Be Blocked in Just an Hour.* Available at: http://www.bfm.ru/news/245757 (Accessed: 23.06.2025)
4. Malkova, E.Yu. (2001). Principles of Virtual Ethics. *Proceedings of the Scientific Conference "Religion and Morality in the Secular World", issue 20.* St. Petersburg: St. Petersburg Philosophical Society, pp.112-115.

GEOSTRATEGY OF DIGITAL THREATS

UDC: [004.056:005.21]:[32.019.5+327.8]
DOI: https://doi.org/10.53486/tids2025.28

SERGEY BAZHENOV
Science Horizons Foundation, Russia
sbazhenov@mail.ru
ORCID ID: 0000-0001-7593-0526

ELENA BAZHENOVA
Southern Federal University, Russia
eubazhenova@sfedu.ru
ORCID ID: 0000-0001-8253-5073

DMITRY ABROSIMOV
Southern Federal University, Russia
dabrosimov@sfedu.ru
ORCID ID: 0000-0002-5278-6581

Abstract. This article examines the transformation of digital threats into instruments of geostrategy, positioning cyberspace as a critical "*fifth domain*" of global power competition. Through a systematic analysis of the evolution, actors, tactics, and impacts of state-sponsored and non-state cyber operations, the study reveals how digital threats have shifted from technical disruptions to core elements of national security strategy. Key findings indicate: (1) *Geopolitical drivers*, including inter- state rivalry, technological dependency, and asymmetric advantages, fuel the weaponization of cyberspace; (2) *State and non-state actors* (e.g., cyber powers like the U.S., China, Russia; proxy groups; criminal syndicates) exploit tactics such as APTs, critical infrastructure sabotage, disinformation, and ransomware to achieve strategic goals; (3) *Systemic consequences* include the erosion of strategic stability, blurring of war/peace thresholds ("*gray zone*" conflicts), vulnerabilities in critical infrastructure, and challenges to international law and norms; (4) Regulatory fragmentation persists, with voluntary norms (UN GGE) lacking enforcement, while states prioritize national resilience, offensive cyber capabilities, and coalitional deterrence. The study concludes that digital threats now constitute a central destabilizing factor in international relations, demanding urgent multilateral cooperation to establish binding rules, foster trust, and invest in next-generation security technologies (AI, post-quantum cryptography). Without a paradigm shift toward collaborative governance, persistent cyber competition risks systemic global instability.

Keywords: geostrategy, digital threats, cybersecurity, international security, hybrid conflicts, cyber resilience, deterrence, cyberspace governance.

JEL Classification: F52, O33, H56, K24

INTRODUCTION

The modern geopolitical space is undergoing radical transformation under the influence of digitalization. Cyberspace, having evolved from a technical environment into a strategic domain, has become an arena for interstate rivalry, a tool of hybrid conflicts, and a source of existential challenges to national security. The intensification of cyberattacks on critical infrastructure (energy, transport, healthcare), large-scale disinformation campaigns, state espionage, and the activities of transnational cybercriminal groups underscore the need for a comprehensive analysis of digital threats in the context of global geostrategy. The absence of universally accepted international regulatory norms and the problem of attribution exacerbate escalation risks, making the study of their geopolitical dimension imperative for the theory and practice of international security.

The goal of this study is to identify the essence of the driving forces and strategic consequences of digital threats as a factor in contemporary geopolitics.

To achieve this goal, the following tasks are proposed:

- Define the conceptual apparatus ("*geostrategy of digital threats*", "*cybergeopolitics*").
- Analyze the evolution of digital threats from technical incidents to an instrument of state policy.
- Classify key actors (states, non-state structures) and their strategic motives.
- Investigate tactical and technical instruments for implementing geostrategies in cyberspace.
- Assess the impact of digital threats on the stability of the international system and national security.
- Analyze challenges for legal regulation and existing response strategies.

MAIN CONTENT

The evolution of digital threats in a geostrategic context. The phenomenon of digital threats has undergone a qualitative transformation: from initially sporadic acts of technical vandalism and criminal activity, they have evolved into one of the key instruments of state policy and geostrategic rivalry *(Rozhkov, 2023).* Understanding this evolution is necessary for comprehending their contemporary role in the global security system.

From technical incidents to an instrument of state policy. The origins of digital threats lie in the 1970s-1980s, when they were predominantly technical-criminal or ideological-protest in nature ("hacktivism"). The first viruses (e.g., Brain, 1986) and network worms (Morris Worm, 1988) demonstrated infrastructure vulnerabilities but lacked systematic political or strategic subtext. The 1990s saw a sharp increase in *cybercrime*, motivated by economic gain, highlighting the vulnerability of the emerging digital space to abuse. A turning point was the beginning of the 21st century, when nation-states realized the strategic potential of cyberspace:

1. *State cyber espionage.* Cyberspace became a primary field for collecting intelligence data (political, military, economic, scientific-technical). Operations such as *Titan Rain* (target – US government structures, mid-2000s) or *Aurora* (target – US corporations, 2009) demonstrated the scale and sophistication of state digital information collection programs, often attributed to China. The goal was not merely disrupting systems but long-term, covert extraction of strategically important data.
2. *Cyber operations as an instrument of power politics.* The 2007 incident in Estonia (massive DDoS attacks on government and financial institutions, linked to Russia) became one of the first examples of using digital attacks to exert *political pressure* on a sovereign state. This marked a shift toward perceiving cyberattacks as tools of *coercion and destabilization* in international relations.
3. *Sabotage of critical infrastructure.* The attack on Iranian nuclear facilities using the *Stuxnet* worm (discovered in 2010, attributed to a joint US-Israel development) became an unprecedented example of *cyber-physical impact* leading to physical destruction of industrial equipment. This proved the fundamental possibility of using cyberspace to inflict *strategic damage*

comparable to the effect of traditional weapons but with lower risk of direct confrontation and greater attribution complexity.

4. *Integration into hybrid wars.* The armed conflict in eastern Ukraine (since 2014) vividly demonstrated the model of *hybrid warfare*, where cyberattacks (on energy systems, media, government institutions – e.g., the attack on the power grid in 2015 and 2016) became an integral component alongside information campaigns, actions of irregular forces, and political pressure. Cyberspace transformed into one of the theaters of military operations.
5. *Weapons of Mass Disruption (WMD).* The 2017 *NotPetya* ransomware attack (initially targeting Ukraine but causing global collapse), attributed to Russia, went beyond military or political goals, inflicting multibillion-dollar damage to businesses worldwide. This highlighted the *transnational nature and cascading effects* of modern digital threats, their ability to paralyze global supply chains and economies.

Main driving factors of the geostrategization of digital threats. The transformation of digital threats into a geostrategic instrument is driven by a complex of interrelated factors *(Khorunov, 2025):*

1. *Intensification of geopolitical competition.* The return of "*great power rivalry*" logic (especially between the US, China, and Russia) created an environment where the pursuit of advantage and deterrence of adversaries extended to cyberspace. Digital operations became an element of *strategic deterrence, demonstration of force, and weakening of competitors* without direct military confrontation.
2. *Technological revolution and its strategic significance.* The development of key technologies sharply raised the stakes:
   - *Proliferation of the Internet of Things (IoT):* Multiple new vulnerable entry points into critical infrastructure (smart grids, industrial control systems – ICS/SCADA).
   - *Adoption of 5G:* Increased speed and reduced latency create new opportunities but also new attack vectors; the struggle for dominance in 5G standards (Huawei vs. the West) itself became a geostrategic issue.
   - *Artificial Intelligence (AI) and Machine Learning (ML):* Automation of attacks (rapid vulnerability discovery, creation of adaptive malware), enhanced capabilities for big data analysis for espionage and disinformation. The race for AI leadership is directly linked to the future military-strategic balance *(Masloboev and Tsygichko, 2025).*
   - *Quantum computing (prospectively):* Threat to break modern crypto algorithms, undermining the foundations of digital security and trust.
3. *Critical dependency of societies and economies on digital infrastructure.* Pervasive digitalization of government administration, financial systems, healthcare, transport, and energy made them *high-priority targets.* A successful attack on such infrastructure can cause damage comparable to a traditional military strike, paralyzing the functioning of an entire state.
4. *Pursuit of asymmetric advantages.* Cyberspace provides a relatively inexpensive and highly effective way for states less powerful in traditional military terms (DPRK, Iran) or non-state actors to challenge stronger opponents. *Low entry barriers* (compared to creating nuclear weapons or modern armies) and *high profitability* of attacks contribute to their proliferation.
5. *Reduced risk of direct escalation and complexity of attribution.* Relative anonymity of actions in cyberspace and technical difficulties in unambiguously identifying the source of an attack *(attribution problem)* allow states to conduct aggressive operations while remaining below the

threshold that could provoke a traditional military response. This creates an attractive *"gray zone"* for achieving strategic goals.

6. *Information-psychological dimension.* Digital platforms (social media) have become powerful tools for waging *information wars,* spreading disinformation, manipulating public opinion, interfering in elections, and destabilizing societies from within. This allows influencing political processes in other countries, undermining trust in institutions, and creating social tension as an integral part of geostrategic pressure.

Key actors and their geostrategic motives. The landscape of digital threats is characterized by a multiplicity and heterogeneity of actors, whose goals, capabilities, and strategies differ significantly *(Bazhenova, 2024).* Understanding their motivation and role in the geostrategic context is necessary for adequate risk assessment and developing effective responses. This section offers a classification of key actors based on their nature, capabilities, and predominant strategic motives.

Nation-States: Main drivers of geostrategy in cyberspace. States remain the most resource-intensive and influential actors, whose actions in cyberspace are directly linked to their global or regional strategic ambitions. They can be conditionally differentiated by capability level and priorities:

1. "Cyber Powers" (Tier-1 Cyber Powers):
   - *USA.* Possesses the most developed offensive and defensive cyber capabilities (US Cyber Command). *Motives:* Maintaining global technological and military leadership; protecting critical infrastructure and national security; deterring adversaries (concept of "Defend Forward"); economic espionage (officially denied in favor of defense/intelligence); promoting a liberal world order and norms in cyberspace. *Key document:* National Cyber Strategy (emphasizes active defense and deterrence).
   - *China.* Demonstrates rapid growth in cyber power, closely integrated with the civilian technology sector and military modernization (PLA Strategic Support Force). *Motives:* Ensuring national security and stability of the ruling regime; industrial-scale economic espionage to accelerate technological development ("military-civil fusion"); strengthening regional dominance; control over the information space ("*cyber sovereignty*"); preparation for potential future conflicts (including Taiwan scenario). *Key document:* National Security Strategy (emphasis on "network power").
   - *Russia.* Actively uses cyber operations as an element of "non-linear" and hybrid warfare, often through proxy groups. *Motives:* Strengthening regional influence and sphere of interest (post-Soviet space); destabilizing and undermining trust within Western societies and institutions; exerting political pressure on opponents; collecting intelligence; protecting the state from internal and external threats. *Key document:* Military Doctrine of the Russian Federation (cyberspace as a domain of military operations).
   - *European Union.* Focuses on cyber defense, resilience, and developing a regulatory framework. *Motives:* Protecting the single digital market and critical infrastructure; promoting a rules-based order in cyberspace; reducing dependence on non-European technologies; coordinating responses to cross-border threats (through ENISA and solidarity mechanisms). *Key document:* EU Cybersecurity Strategy.
2. *Others (Israel, United Kingdom).* Possess high offensive capabilities. *Israel's Motives:* Survival in a complex region, preemptive deterrence of threats (especially from Iran),

technological leadership. *UK's Motives:* Maintaining global influence, protecting interests within Five Eyes, countering state threats (NCSC, Offensive Cyber). "Active Players" (Tier-2/3 Cyber Powers):

- *Iran:* Significantly increased cyber capabilities, often as a tool of asymmetric response to sanctions and isolation. *Motives:* Regional deterrence (against Saudi Arabia, Israel, USA); destabilizing opponents; ideological struggle; intelligence gathering; financing (cybercrime as a source of income for proxy groups). Known for attacks on the financial sector and infrastructure (Shamoon).
- *DPRK (North Korea):* Uses cyber operations as a vital source of financing due to harsh sanctions and to demonstrate strength. *Motives:* Financing nuclear and missile programs (large-scale bank theft campaigns, cryptocurrency attacks); collecting strategic intelligence; demonstrating technological capabilities and deterrence (attacks on media, infrastructure of South Korea). Groups (Lazarus) are highly aggressive.
- *Others (India, Pakistan, Vietnam, Turkey, etc.):* Building capabilities, often in the context of regional confrontations. *Motives:* Counterintelligence, protection from neighbors, economic espionage, prestige.

Non-State Actors: Eroding the state monopoly on force. These actors operate with varying degrees of autonomy from states, complicating attribution and the threat landscape:

1. *Transnational Cybercriminal Groups:*
   - *Motive:* Exclusively financial gain (extortion, data theft, fraud, access sales). *Tactics:* Ransomware-as-a-Service (RaaS), phishing, vulnerability exploitation. *Examples:* Conti, REvil, LockBit. *Geostrategic Significance:* Inflict colossal economic damage globally; paralyze critical services (healthcare – attack on HSE Ireland, Colonial Pipeline); can be unwittingly or intentionally used by states as proxies or cover ("plausible deniability"). Growing professionalization and specialization (initial access brokers).
2. *Hacktivist Groups:*
   - *Motive:* Political protest, ideological struggle, social or environmental causes. *Tactics:* DDoS attacks, defacements, data leaks. *Examples:* Anonymous, Killnet. *Geostrategic Significance:* Can be used by states to destabilize opponents under the guise of "civilian initiative"; amplify information noise, complicating detection of state operations; create social tension. Often their impact is more symbolic than strategic.
3. *Cyber Units of Non-State Armed Groups and Terrorist Organizations:*
   - *Motive:* Propaganda, recruitment, financing, intimidation, destabilizing target states. *Tactics:* Primitive website attacks, use of social media, phishing. *Examples:* ISIS (Islamic State), cyber units of separatist groups. *Geostrategic Significance:* Currently possess limited capabilities but represent a growing threat; their actions can provoke interstate conflicts; require international law enforcement cooperation.
4. *State Proxy Groups (State-Sponsored Advanced Persistent Threat - APT Groups):*
   - *Status:* Exist in a "gray zone" – formally non-state but closely linked to state intelligence services or military (funding, cover, tool transfer). *Motives:* Performing tasks the state wants to keep in the shadows (espionage, sabotage, disinformation), ensuring "plausible deniability". *Examples:* APT28 (Fancy Bear, Russia), APT29 (Cozy Bear, Russia), APT41 (Winnti, China - mix of espionage and crime), Lazarus Group (DPRK).

Geostrategic Significance: Key tool for states to conduct operations in the "gray zone"; complicate attribution and hinder responses; lower the threshold for using cyber force.

Private Sector: Object, subject, and capability provider. The role of the private sector is multifaceted:

- *Primary target of attacks:* Corporations own and operate most critical infrastructure and store valuable data (PII, intellectual property).
- *Key technology and service provider:* Companies develop and implement technologies shaping the threat and defense landscape (cloud, IoT, AI, security systems). States depend on their products and expertise.
- *Actor shaping threats:* Technology giants possess unprecedented data volume and influence over information flows, becoming a geopolitical factor in itself (struggle for digital sovereignty, Big Tech regulation). Cybersecurity companies (sometimes with unclear ties) develop and sell tools that can be used offensively (e.g., exploits, spyware - NSO Group).
- *Public-Private Partnership (PPP):* The need for threat intelligence sharing and coordinated responses makes state-business interaction critical but often problematic due to trust, confidentiality, and liability issues.

Tactics and instruments of the geostrategy of digital threats. The implementation of geostrategic goals in cyberspace is carried out through a diverse and constantly evolving arsenal of tactics and instruments. Their choice is determined by the actor's tasks (espionage, sabotage, destabilization, coercion), their capability level, desired degree of stealth, and calculation of consequences *(Matyashova, 2023).* This section systematizes key methods used by state and non-state actors to achieve strategic effect.

Cyber Espionage: The invisible war for information. Essence: Targeted, covert collection of confidential information of a political, military, economic, scientific-technical, and diplomatic nature.

- *Tools and methods:*
  - *Advanced Persistent Threats (APT):* Long-term (months, years), targeted, and sophisticated operations, often conducted by state or proxy groups. Use zero-day vulnerability chains, targeted spear phishing, complex remote access malware (RATs).
  - *Supply Chain Compromise:* Compromising legitimate products during development or distribution to implant backdoors (example: *SolarWinds Orion (2020),* attributed to Russia, affected US government structures and corporations).
  - *Credential Theft:* Using phishing, exploits, leaked password databases to gain access to protected systems.
  - *Passive Traffic Interception:* Monitoring unencrypted or weakly encrypted communications.
- *Geostrategic Goal:* Gaining long-term competitive advantage (military plans, technologies, negotiation positions), monitoring adversary intentions, assessing vulnerabilities. The most common form of state activity in cyberspace.

Sabotage and Destruction (Cyber Sabotage/Destruction): Inflicting material damage and disruption. Essence: Physical damage or disabling of critical infrastructure, destruction of data, disruption of key systems.

- *Tools and methods:*

  - *Cyber-Physical Attacks:* Targeted impact on industrial control systems (ICS/SCADA), leading to physical consequences. Example: *Stuxnet (2010)* – destruction of centrifuges in Iran.
  - *Wiper Attacks:* Malware that irreversibly erases data and damages boot systems (example: *NotPetya (2017),* attributed to Russia, caused billion-dollar damage globally; *Shamoon,* attributed to Iran).
  - *Denial-of-Service (DDoS) Attacks:* Overloading target systems with requests, causing unavailability (often temporary but can cause severe damage, especially to financial or media resources). Scaled using botnets.
  - *Data Manipulation:* Subtly altering information (e.g., in energy grid management systems, financial reports) to covertly undermine trust or cause wrong decisions.
- *Geostrategic Goal:* Inflicting direct damage on the adversary (economic, military), demonstrating power and capabilities, deterrence, destabilizing a state or region, escalating conflict below the threshold of open military confrontation.

Destabilization and Undermining Trust: Information-Psychological Operations (IPOs). Essence: Using digital platforms to manipulate public opinion, spread disinformation (fake news), propaganda, incite social discord, and undermine trust in institutions.

- *Tools and methods:*
  - *Targeted Social Media Campaigns:* Creating fake accounts and communities ("bot farms," "trolls"), mass boosting, using micro-targeting to spread narratives. *Example:* Election interference (USA-2016, other countries).
  - *Hack-and-Leak:* Compromising and selectively publishing confidential information to discredit political figures, parties, or organizations (example: *Operation "DCLeaks," DNC Hack,* attributed to Russia).
  - *Disinformation via Fake Media and Deepfakes:* Creating and disseminating false content mimicking authoritative sources or real people.
  - *Attacks on Independent Media and Platforms:* DDoS attacks, hacks to suppress critical voices.
- *Geostrategic Goal:* Weakening political opponents from within, polarizing society, undermining the legitimacy of elections and democratic processes, creating a favorable environment for external influence, diverting attention from other operations.

Cyber Extortion (Ransomware) as a tool of coercion and financing. Essence: Encrypting data or threatening its publication to demand ransom.

- *Tools and methods:*
  - *Targeted Attacks on Critical Infrastructure:* Hospital networks (HSE Ireland, 2021), pipelines (Colonial Pipeline, 2021), municipalities, large corporations. Use sophisticated penetration methods (exploits, buying access).
  - *Ransomware-as-a-Service (RaaS) Model:* Cybercriminal groups provide platforms and malware to "*renters*" for a share of the ransom, drastically increasing the scale of the threat.
  - *Double and Triple Extortion:* Besides encrypting data, threatening its publication (double) and launching DDoS attacks against the victim (triple).

- *Geostrategic Goal (for states/proxies):*
  - *Financing:* For states under sanctions (DPRK) or proxy groups.
  - *Destabilization and Coercion:* Targeting critical infrastructure of an adversary to cause chaos and exert political pressure (often under the cover of criminal activity for "plausible deniability").
  - *Inflicting Economic Damage.*

Supply Chain Attacks: The domino effect. Essence: Compromising legitimate software, hardware, or update services during early stages of development or distribution, allowing the attacker to access all users of the compromised product.

- *Tools and methods:* Introducing vulnerabilities or backdoors into source code, compromising update servers, replacing legitimate libraries.
- *Examples: SolarWinds Orion (2020), attack on Kaseya VSA (2021, REvil), CCleaner compromise (2017).*
- *Geostrategic Goal:* Achieving widespread impact with relatively low effort; penetrating well-protected networks through trusted suppliers; inflicting mass damage on the adversary's economy and infrastructure; demonstrating penetration capabilities into global networks.

Exploitation of Zero-Day Vulnerabilities and Managed Hacking Services. Essence:

- *Zero-Day:* Using a previously unknown vulnerability in software/hardware for which there is no patch. Extremely valuable and expensive tool.
- *Managed Services:* Hiring specialized cyber contractors (commercial companies, hacker collectives) by a state or group to conduct specific operations.
- *Geostrategic Goal:* Ensuring maximum stealth and effectiveness for high-value operations (espionage, sabotage); accessing maximally protected targets; outsourcing operations to reduce risks and ensure denial.

Regulation challenges and response strategies. The complexity, cross-border nature, and rapid evolution of digital threats used for geostrategic purposes create significant difficulties for developing and implementing effective regulatory mechanisms. Response strategies of states and the international community are constantly evolving, trying to adapt to the dynamic threat but facing fundamental political, legal, and technical obstacles *(Romashkina, 2020).* This section analyzes key regulatory challenges and the spectrum of emerging responses at national and international levels.

Challenges of International Law and Diplomacy

1. *Applicability of Existing Law:*
   - *Use of Force and Self-Defense (UN Charter, Art. 2(4) and 51):* Ongoing debates about when a cyberattack reaches the threshold of "*use of force*" or "*armed attack*". States hold different positions: some (US, allies) allow Art. 51 application to large- scale destructive attacks on critical infrastructure, others (Russia, China) insist on a higher threshold, close to traditional armed attack, fearing legitimization of "*preemptive*" strikes.
   - *International Humanitarian Law (IHL):* Difficulties in applying principles of proportionality, distinction, and precaution to cyber operations during armed conflict. Defining the status of cyber combatants and civilian objects in cyberspace remains contentious.

  - *State Sovereignty and Non-Intervention:* Lack of consensus on which actions in cyberspace (espionage, DDoS, disinformation) violate the sovereignty of the target state and the principle of non-interference in internal affairs. Positions range from broad interpretation (any unauthorized interference) to narrow (only actions causing significant damage or coercion).
2. *State Responsibility:*
   - *For Actions of Non-State Actors:* To what extent is a state responsible for cyberattacks originating from its territory if it "*knew or should have known*" about them but did not take measures? The principle of "*due diligence*" is recognized by many but its practical application and evidentiary base are complex.
   - *For Actions of Proxy Groups:* The problem of establishing and proving actual state control over such groups to apply norms of international legal responsibility.
3. *Formation of Norms of Responsible Behavior:*
   - *Multilateral Efforts (UN):* Work by Groups of Governmental Experts (UNGGE) and the Open-Ended Working Group (OEWG) led to the recognition of 11 norms of responsible state behavior (UNGGE reports 2015, 2021; OEWG final report 2021). These include: commitment to cooperate, not to intentionally damage critical infrastructure, promote stability, respect human rights, combat cybercrime, report vulnerabilities, not use civilian infrastructure for attacks, not use ICT to interfere in internal affairs, respect supply chains, not damage emergency response infrastructures, protect key digital infrastructure objects.
   - *Problems:* Norms are *voluntary, non-binding*. There are no mechanisms for verifying compliance or enforcing implementation. *Deep disagreements* persist over their interpretation, especially regarding the use of force, sovereignty, human rights, and the state's role in internet governance. Uncertainty about whether specific operations (disinformation, espionage) violate these norms.
   - *Role of Regional Organizations:* OSCE (confidence-building measures), NATO (application of Art. 5 to cyberattacks – decisions 2014, 2016), ASEAN, OAS – develop regional norms and cooperation mechanisms, but their effectiveness is limited by geography and political will of participants.
4. *Bilateral Channels and Confidence-Building Measures:* Establishing "*red lines*" and hotlines between major powers (US-Russia, US-China) to prevent escalation and manage crises. However, their sustainability is subject to fluctuations in political relations (e.g., freezing of US- Russia dialogue after attacks).

National and Coalitional Response Strategies. In the absence of a reliable international legal regime, states focus on national and coalitional measures, combining defense, deterrence, and offensive capabilities:

1. *Strengthening Cyber Resilience:*
   - *Priority:* Protecting critical infrastructure (CI) through mandatory security standards (e.g., NIS2 Directive in EU, CISA initiatives in US).
   - *Measures:* Accelerated vulnerability identification and patching, network segmentation, backups, regular penetration testing (pentesting), preparation of incident response plans (IRP) and disaster recovery plans (DRP).

   - *Public-Private Partnership (PPP):* Creating Information Sharing and Analysis Centers (ISACs), joint exercises (e.g., Cyber Europe), incentivizing business security investments.
2. *Cyber Deterrence Strategies:*
   - *Deterrence by Denial:* Increasing costs for the attacker by strengthening defenses, making a successful attack unlikely or too expensive. The main focus for most states.
   - *Deterrence by Punishment:* Threat of inflicting unacceptable damage on the attacker in response. Requires:
     - *Offensive Cyber Capabilities:* Developing capabilities for conducting retaliatory or preemptive cyber operations (e.g., USCYBERCOM, NCSC Offensive Cyber, equivalents in other countries).
     - *Employment Doctrines:* Clearly defining thresholds, targets, and rules for employing offensive cyber and non-cyber means (sanctions, counterintelligence, military) in response to cyberattacks. The US "*Defend Forward*" doctrine emphasizes proactive actions outside own networks to identify and neutralize threats before they materialize.
     - *Challenges:* Attribution problems, risk of escalation, difficulty signaling intentions without compromising secrecy, ethical and legal questions.
   - *Deterrence by Engagement:* Diplomacy, norm creation, international cooperation to reduce motives for attack and increase costs for violating them.
3. *Active Defense and Response Operations:*
   - *Within National Law:* Actions to disrupt attacker infrastructures (e.g., "cleaning" botnets), returning stolen data, deactivating malware on own networks. Often requires expanding mandates of intelligence services and military.
   - *Legal and Ethical Boundaries:* Risk of violating other states' sovereignty, collateral damage, escalation.
4. *Deterrence and Coercion Diplomacy:*
   - *Public Attribution:* Publicizing evidence of state or group involvement in attacks (e.g., joint statements by Five Eyes countries, EU) to impose political costs and stigmatization.
   - *Coalition Pressure:* Coordinated sanctions (economic, diplomatic, personal) against state sponsors, hackers, and associated structures.
   - *Criminal Prosecution:* International arrest warrants (Interpol), joint law enforcement operations (e.g., against ransomware groups).
5. *Investing in the Future:*
   - *Personnel and R&D:* Mass training of cybersecurity specialists, funding research in AI for security, post-quantum cryptography, secure architectures (Zero Trust).
   - *Global Technology Regulation:* Efforts to establish security standards for IoT, critical components (chips, software), managing risks associated with AI.

Promising Directions and Enduring Challenges

1. *Role of Artificial Intelligence:* AI revolutionizes both attack (automation, adaptability, generation of targeted phishing/deepfakes) and defense (threat analysis, anomaly detection, response automation). The race in this area will be a key factor in the future balance of power *(Masloboev and Tsygichko, 2025).*
2. *Quantum Threat:* The development of quantum computing creates an existential threat to

modern cryptographic algorithms underlying digital security. Urgent investments in post-quantum cryptography (PQC) and system migration are needed *(Arrykova, Ashirov, Guvandzhov and Churiev, 2025).*

3. *Data Governance and Digital Sovereignty:* The struggle for control over data, information flows, and technological standards will intensify, generating new regulatory conflicts (GDPR, data localization laws, Big Tech regulation).
4. *"Gray Zone" and Attribution:* Will remain the main challenges. Technologies (AI, blockchain for information storage) may partially help, but political will for transparency and cooperation remains decisive.
5. *Need for Inclusive Dialogue:* Effective regulation requires involvement not only of states but also the private sector, technical community, and civil society. Multilateral platforms (UN, IGF) must become more effective.

CONCLUSIONS

The conducted analysis allows us to conclude that digital threats have evolved from technical incidents into a key instrument of contemporary geostrategy. Cyberspace has become a full-fledged "fifth domain" of global rivalry, where states and non-state actors realize their long-term goals of security, influence, and power. *Key findings:*

1. *Threat Transformation:* The geostrategic significance of digital threats is driven by intensifying geopolitical competition, the critical dependence of societies on digital infrastructure, and the pursuit of asymmetric advantages. Tactics (APT, espionage, sabotage, disinformation, ransomware, supply chain attacks) directly serve the strategic goals of actors.
2. *Systemic Challenges:* The geostrategy of digital threats generates fundamental risks:
   - *National Level:* Blurring lines between war and peace ("gray zone"), vulnerability of critical infrastructure, crisis of deterrence models, intractable dilemma of attribution and response.
   - *International Level:* Erosion of strategic stability, militarization of cyberspace, undermining of trust, maladaptation of international law, deadlock in forming effective behavioral norms.
   - *Global Level:* Colossal economic losses, threats to supply chains, undermining social cohesion and democratic processes.
3. *Regulation Deadlocks:* Lack of consensus on applying international law and the voluntary nature of UN norms limit their effectiveness. The response shifts toward national and coalitional strategies combining:
   - Strengthening cyber resilience (resilience).
   - Deterrence through denial and punishment (deterrence), including developing offensive capabilities.
   - Pressure diplomacy (sanctions, public attribution).
   - Investments in technology (AI, post-quantum cryptography) and personnel.
4. *Permanent Cyber Competition:* Despite efforts, the world is moving along a trajectory of continuous cyber competition with high risks of escalation and destabilization. Breakthrough technologies (AI, quantum computing) simultaneously amplify both threats and defense means, exacerbating the race.

Digital threats have ceased to be a peripheral challenge, becoming a central, system-forming factor in contemporary geopolitics, defining state vulnerability, the fragility of the international system, and the contours of future conflicts. Overcoming their destabilizing impact requires not only technological solutions and forceful deterrence strategies but, first and foremost, an unprecedented level of international trust, political will to overcome geopolitical differences, and the development of specific, enforceable rules of responsible behavior in cyberspace. Without this breakthrough, the world is doomed to a permanent "gray zone" of digital confrontation with unpredictable consequences for global security and stability.

REFERENCES

1. Arrykova, G.K., Ashirov, I.G., Guvandzhov A. and Churiev, M.M., 2025. Quantum Technologies in Data Security: From Theory to Reality. *Science and Worldview, 1* (45), 283-288.
2. Bazhenova, E.Yu., 2024. *Geo-economics: textbook* / E. Yu. Bazhenova, Southern Federal University. Rostov- on-Don; Taganrog: Southern Federal University Press, 344 p.
3. Masloboev, A.V. and Tsygichko, V.N, 2025. Analysis of Trends in the Influence of Artificial Intelligence on Geopolitics and Security: New Challenges and Threats of Digital Transformation. *Reliability and Quality of Complex Systems, 1* (49), 126-135. doi: 10.21685/2307-4205-2025-1-16
4. Matyashova, D.O., 2023. The Place of Digital Threats in the Modern Concept of Human Security. *Power, 31* (3), 144-150.
5. Rozhkov, E.V., 2023. Development of Digital Technologies (Opportunities and Threats) (at the Regional Level). *Forum of Young Scientists, 4* (80), 86-100.
6. Romashkina, N., 2020. The Problem of International Information Security in the UN. *World Economy and International Relations, 12(*64). 25-32.
7. Khorunov, E.K., 2025. International Cooperation in the Field of Cybersecurity. *Bulletin of Science, 3* (1 (82)), 513-524.

INTERNATIONAL EXPERIENCE OF USING COMPUTER AND GAME TECHNOLOGY TOOLS IN THE TOURISM BUSINESS

UDC: 338.48:[004.78+004.8+004.946]
DOI: https://doi.org/10.53486/tids2025.29

OLGA SHEPELEVA
PhD in Economics, Associate Professor
Department of Tourism Business and Recreation
Odesa National University of Technology, Ukraine
shepelevaolga1313@gmail.com
ORCID ID: 0000-0003-4128-2094

OLEKSANDR BOHDANOV
PhD in Economics, Senior lecturer
Department of Trade Enterprise, Merchandising and Business Management
Odesa National University of Technology, Ukraine
skream1987@gmail.com
ORCID ID: 0000-0002-8505-3675

DMYTRO TKACHENKO
Candidate of technical sciences, Senior lecturer
Department of Tourism Business and Recreation
Odesa National University of Technology, Ukraine
TkachenkoDmitry73@gmail.com
ORCID ID: 0009-0007-7406-564X

Abstract: At present, humanity is living in a technological age, when new proposals for the development of tourism appear every day. One of these proposals is to combine tourism with one of the most relevant areas of human activit - computer and information technology. The introduction of IT technologies into the tourism sector will contribute to new innovative tourism products, accompanied by an improvement in the quality of service and personalization of future tourist routes. International experience in the use of digital tools in tourism has been analyzed: online booking systems, augmented and virtual reality, virtual tours, gamified platforms, and artificial intelligence. Modern tourists are quite demanding when it comes to organizing their vacations and need to have an emotional experience even before traveling through a virtual acquaintance with the place of rest or recreation. International experience in the use of digital technologies in the development of the tourism sector clearly demonstrates an increase in the attractiveness of tourist destinations and the competitiveness of the tourism business.

Keywords: tourism, computer technologies, gamification, innovations in tourism, augmented reality, virtual reality, artificial intelligence

JEL Classification: L83, L86, O33, Z33, M31

INTRODUCTION

At present, humanity is living in a technological age, when new proposals for the development of tourism appear every day. One of these proposals is to combine tourism with one of the most relevant areas of human activity - computer and information technology. The combination of these two activities can take various forms. The creation of innovations in the tourism business, such as computer technologies, provides opportunities for the tourism industry to develop new attractive tourism products. For example, powerful accommodation booking systems, improved logistics in the tourism business, improvements in excursion and cultural and health services, the introduction of the latest technology in the field of tourism, information about the availability and accessibility of certain types of routes, the tourist potential of countries and regions – all these measures help to increase tourist interest and promote certain destinations. The combination of tourism and computer information technologies can vary, but in all cases it will contribute to improving, the efficiency of tourist services by improving the quality of service and creating personalized tourist products. In recent years, there have been significant changes in the tourism business. Modern tourists are quite demanding when it comes to organizing their vacations and need to have an emotional experience even before traveling through a virtual acquaintance with the place of vacation or recreation. This is where computer and gaming technologies come to the rescue: augmented and virtual reality, gamified applications, artificial intelligence, and interactive maps, which are now widely used as tools to attract tourists.

MAIN CONTENT

Today, computers, computer equipment, and computer technologies have become an integral part of our daily lives. It is difficult to imagine the operation of any enterprise or company without computers. Online airline ticket sales systems are particularly popular among consumers. The advantage of such a sales system is that you can make the necessary purchases, place an order, or book a ticket without leaving your home or office *(“Booking tickets online,”* accessed 10.04.2025).

Websites such as www.airbnb.com.ua/ and www.booking.com provide accommodation services for tourists to companies, i.e. owners of hotels, hostels, and apartments.

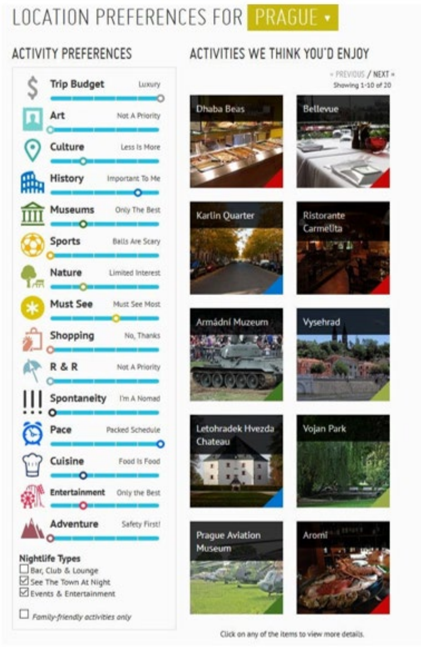
Booking.com, founded in 1996 in Amsterdam, has grown from a small Dutch startup to one of the world's digital leaders in the travel industry. Booking.com's mission is to make travel accessible to everyone. By investing in technologies that help people travel hassle-free, Booking.com offers millions of guest’s great leisure options, transportation services, and incredible accommodations, ranging from homes to hotels and beyond. As the world's largest travel platform for both well-known brands and entrepreneurs of all levels, Booking.com helps accommodation owners around the world attract guests and grow their businesses. The Booking.com platform is available in 43 languages. It offers more than 28 million listed accommodations for booking, including more than 6.2 million homes, apartments, and other unique accommodations (“*About Booking.com*,” accessed 10.04.2025).

Airbnb is an online service for finding and renting short-term accommodation around the world, operating on the paradigm of the sharing economy. The name stands for “AirBed and Breakfast.” The service helps people rent houses, apartments, rooms, or beds in more than 190 countries around the world. Airbnb founders Brian Chesky and Joe Gebbe moved from New York to San Francisco in 2007 and were unemployed for a while, unable to pay rent for an apartment. They were looking for a way to earn some money and noticed that all hotel rooms in the city were booked at the time because a local industrial design conference had attracted a large number of visitors. The young people saw this situation as an opportunity to make money (*“Airbnb: From Inflatable Mattresses to the International Market*,” accessed April 15, 2025).

Today, thanks to the development of the Internet, booking airline tickets online has become widely popular. Anyone can easily book a ticket on airline websites or on the websites of auxiliary agencies. Such bookings made using the Global Distribution System (GDS). If we analyze how booking systems work, we can conclude that these systems act as intermediaries between airline booking systems and travel agency sales systems *("Booking tickets online,"* accessed 10.04.2025).

It is also worth considering the fact that in different GDS systems, fares for the same airline and the same route, for example, Kyiv-Prague, can vary significantly. The online booking system saves consumers time. In addition, customers can always easily view all current offers and choose the best option for themselves *("Booking tickets online,"* accessed 10.04.2025).

A powerful tourism trend today at the international level is the combination of artificial intelligence with mobile applications. Below are a few examples. Utrip is a free travel planning technology that combines the best of artificial intelligence and human experience, allowing travelers to quickly create the perfect trip. A destination search and travel-planning platform combine the best of artificial intelligence and human experience to help travelers find destinations and plan trips in a unique, personalized, and enjoyable way. Utrip PRO helps increase engagement, loyalty, and conversion rates by offering the Utrip platform as a white label to hotel brands, cruise lines, landmarks, airlines, and destination marketing organizations (Utrip, accessed 15.04.2025). The service is in the process of transitioning from the old version to the new one. The most covered country in both versions is the United States. As for Europe, the new version currently covers only a few major cities (Rome, but not Milan or Venice; Barcelona, but not Madrid; Paris and London, but not Germany or Prague *("Online travel planners research. Part 5. Utrip: the two-headed monster,"* accessed 15.04.2025).



LOCATION PREFERENCES FOR PRAGUE ▾

ACTIVITY PREFERENCES

Trip Budget — Luxury
Art — Not A Priority
Culture — Less Is More
History — Important To Me
Museums — Only The Best
Sports — Balls Are Scary
Nature — Limited Interest
Must See — Must See Most
Shopping — No, Thanks
R & R — Not A Priority
Spontaneity — I'm A Nomad
Pace — Packed Schedule
Cuisine — Food Is Food
Entertainment — Only the Best
Adventure — Safety First!

Nightlife Types
☐ Bar, Club & Lounge
☑ See The Town At Night
☑ Events & Entertainment

☐ *Family-friendly activities only*

ACTIVITIES WE THINK YOU'D ENJOY

« PREVIOUS / NEXT »
Showing 1-10 of 20

Dhaba Beas
Bellevue
Karlin Quarter
Ristorante Carmelita
Armádní Muzeum
Vysehrad
Letohradek Hvezda Chateau
Vojan Park
Prague Aviation Museum
Aromi

Click on any of the items to view more details.

Figure 1. Planning a tourist route using the Utrip.

Source: *Online travel planners research. Part 5. Utrip: the two-headed monster.*

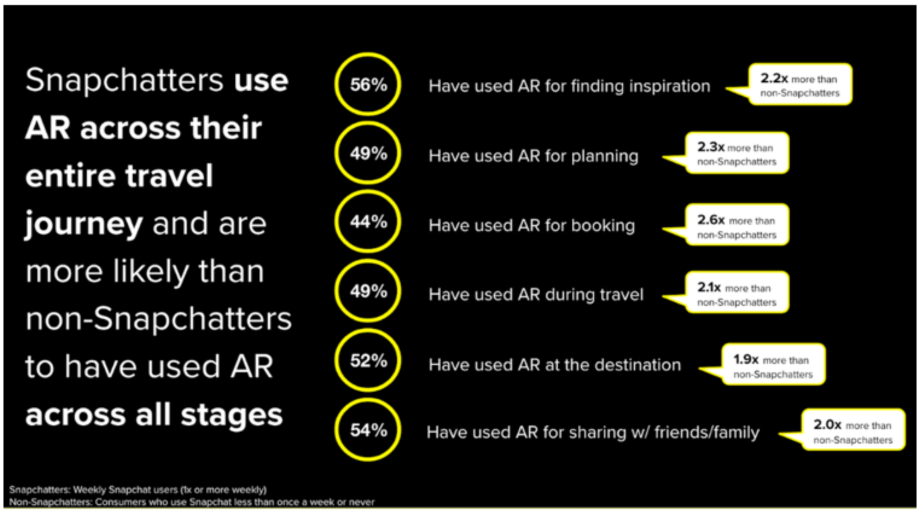
TripAdvisor is known as the largest travel review site and is a powerful tool that helps travelers decide where to stay, what to visit, where to eat, and how to fly, providing the opinions and past experiences of other travelers. The advantage of using TripAdvisor for travel planning is that it uses reviews (feedback) to facilitate the decision-making process. It combines all the necessary elements that make up a trip, namely flights, accommodation, restaurants, and attractions. Travelers can search for information and reviews on all of these elements on TripAdvisor without having to visit multiple websites to gather the necessary information. Another advantage is that TripAdvisor works with many airlines, travel agents, and booking agents to provide booking services. Travelers can book flights, tours, and accommodation. To facilitate the search, TripAdvisor uses different approaches to recommendations in different aspects (Lim Yen Yee *et al.,* 2019).

TripHobo is a travel-planning platform that helps users plan trips to destinations, restaurants, and package tours in over 90,000 cities around the world. It is an online application that functions as a one-stop shop for all travel needs, covering places of interest, route planning, package tours, and ground transportation arrangements such as accommodation and local transportation. If places are missing from the current list, users can add a place directly from Google. Users can customize their itineraries by registering as members. In addition, users can share their travel plans with others by registering through their Facebook accounts. Itineraries can also share on Google+ and Twitter. The interface is user-friendly, with drag-and-drop features, the ability to add trips to selected days, add days, and optimize routes. Although the route optimization feature may indicate that the routes for the day are almost full and the user cannot add more, it does not have the ability to group nearby places into one day of visits. TripHobo can estimate the distance and travel time from one place to another, as well as indicate the opening and closing times of each place. However, the planning does not take into account the time users spend at each location. The estimated time is the minimum for a tourist, and some tourists may find it too short and may have to use their own judgment to adjust the time accordingly (Lim Yen Yee *et al*., 2019).

The use of gamification models in tourism is not limited to tourism organizations. Gamification models are also used to promote and market tourist destinations. In particular, augmented reality (AR) and virtual reality (VR) applications are used to create a gamification model by transferring a digital environment with various animations and simulations of historical, cultural, and natural features to a destination, which can help tourists fully experience the destination. To better understand the idea, one can cite the example of the digitization of a destination, where a tourist visiting the Berlin Wall visualizes the state of the wall before its demolition on the screen of their smartphone, with instant access to information and video materials about its history outside the wall (Emrah Özkul, Emre Uygun, Selen Levent, 2020).

Digital gamification in the tourism industry makes the service interactive, allowing people to enjoy the process. The main goal of gamification is to ensure user loyalty to the business by creating the impression that they are part of a story designed to attract the user's attention with the right content and stories. Companies in the tourism industry (airlines, travel agencies, accommodation providers, etc.) have begun to transfer their booking systems to digital platforms. Mobile applications used by companies that continue to provide services on these digital platforms have allowed travel consumers to access the businesses and services offered by these companies without restrictions on time and place. Companies use gamification models to provide a more convenient and interesting way for consumers to access their services. One of the exemplary gamification models used by companies is to allow travel consumers to collect points for each flight, accommodation selection, or mobile check-in via a mobile app and earn various gifts that they can use in future transactions (Emrah Özkul, Emre Uygun, Selen Levent, 2020).

In 2021, the augmented reality market was valued at $8.6 billion, and it projected to grow at a compound annual growth rate of 38% through 2030. This growth extends beyond the technology and gaming industries, significantly affecting tourism as well. According to a Kantar study commissioned by Snapchat, up to 93% of travelers said they would use augmented reality at some point during their future travels. This rapid adoption driven by several factors: growing consumer interest in exciting adventures, the development of augmented reality technologies that make them more accessible and cheaper, and the development of solutions that simplify the integration of augmented reality for tourism organizations and tourism businesses. Companies such as Wikitude, HiVu, and Echo3D specialize in developing augmented reality models. In addition, tourist guide systems such as SmartGuide can host and publish augmented reality models for tourist destinations and attractions, simplifying the process. Even without complex augmented reality models, destinations and attractions can create immersive augmented reality experiences using authentic historical photographs that can be converted into augmented reality objects on platforms such as SmartGuide, simplifying the implementation of augmented reality *("Strategies for digitalization in tourism - Integrating digital tools in tourism management,"* accessed 20.04.2025).



Snapchatters use **AR across their entire travel journey** and are more likely than non-Snapchatters to have used AR **across all stages**

56% Have used AR for finding inspiration — **2.2x** more than non-Snapchatters

49% Have used AR for planning — **2.3x** more than non-Snapchatters

44% Have used AR for booking — **2.6x** more than non-Snapchatters

49% Have used AR during travel — **2.1x** more than non-Snapchatters

52% Have used AR at the destination — **1.9x** more than non-Snapchatters

54% Have used AR for sharing w/ friends/family — **2.0x** more than non-Snapchatters

Snapchatters: Weekly Snapchat users (1x or more weekly)
Non-Snapchatters: Consumers who use Snapchat less than once a week or never

Figure 2. Results of a Snapchat survey on the use of augmented reality by tourists.
Source: *Uncovering the Value of Augmented Reality in Travel*

Snapchat and Kantar have teamed up to better understand the role augmented reality can play for consumers on their journey to purchase for travel – from initial inspiration to sharing experiences after reaching their destination. Kantar conducted a quantitative survey of 1,004 current and future travelers in the US aged 13 to 49, and the study revealed some key findings about the role of augmented reality in travel. Snapchat is a leader in augmented reality, with an average of nearly 250 million Snapchat users interacting with augmented reality every day. The study found that augmented reality on Snapchat has a particularly strong impact on consumer travel, with 68% of Snapchat users having used augmented reality at least once during a past trip, compared to only 41% for those who do not use Snapchat *("Uncovering the Value of Augmented Reality in Travel,"* accessed 20.04. 2025).

CONCLUSIONS

Technology has always attracted attention and interest from the global community. Technologies have been improving, thereby improving human life. Information technologies have greatly facilitated human activities in many areas of life and even provided new jobs, while gaming technologies have allowed people to relax and, to some extent, replenish their moral and physical resources, similar to "recreation."

In the tourism business, information, i.e., computer technologies have greatly facilitated computing activities, customer database maintenance, interaction with tourists, advertising activities, etc. The introduction of technologies in the tourism business is relevant and even necessary now, because without automation, a company becomes uncompetitive.

International practice proves the effectiveness of introducing computer and gaming technologies in the tourism business. VR/AR technologies, gamification, interactive platforms, and AI applications contribute to increasing the competitiveness of tourism companies, creating a unique customer experience, and developing sustainable tourism.

For the Ukrainian tourism market, it is advisable to implement pilot projects using such technologies in domestic tourism, develop partnership programs with technology companies, and train personnel capable of working in the context of digital transformation.

REFERENCES

1. “Booking tickets online”. Available at: https://tourlib.net/statti_otdyh/bronirovanie2.htm [Accessed 10.04.2025].
2. “About Booking.com”. Available at: https://www.booking.com/ [Accessed 10.04.2025].
3. “Air startup: Airbnb – from inflatable mattresses to the international market. ”February, 2020. Available at: https://www.oschadbank.ua/blog/povitryaniy-startap-airbnb-vid-naduvnih-matraciv-do-mizhnarodnogo-rinku [Accessed 15.04.2025].
4. Utrip. Available at: https://www.traveltechnation.com/companies/utrip [Accessed 15.04.2025].
5. “Online travel planners research. Part 5. Utrip: the two-headed monster”. July, 2019. Available at: https://pavel-nosikov.medium.com/online-travel-planners-research-part-5-utrip-the-two-headed-monster-b73708c27b0b [Accessed 15.04.2025].
6. Lim Yen Yee, Seetha Letchumy M Belaidan, Nor Azlina Abd Rahman, Khalida Shajaratuddur Harun. Implementing K-Means Clustering Algorithm in Collaborative Trip Advisory and Planning System, July 2019. Periodicals of Engineering and Natural Sciences (PEN) 7(2):723. Available at: https://www.researchgate.net/publication/337856564_Implementing_K-Means_Clustering_Algorithm_in_Collaborative_Trip_Advisory_and_Planning_System#pf47 [Accessed 15.04.2025].
7. Emrah Özkul, Emre Uygun, Selen Levent. Digital Gamification in the Tourism Industry, October 2020. In book: Handbook of Research on Smart Technology Applications in the Tourism Industry (pp.169-204). Publisher: IGI GLOBAL. Available at: https://www.researchgate.net/publication/344831740_Digital_Gamification_in_the_Tourism_Industry [Accessed 15.04.2025].
8. “Strategies for digitalization in tourism - Integrating digital tools in tourism management”, June 2024. Available at: https://blog.smart-guide.org/en/strategies-for-digitalization-in-tourism-integrating-digital-tools-in-tourism-management [Accessed 20.04.2025].
9. “Uncovering the Value of Augmented Reality in Travel”, November, 2023. Available at: https://forbusiness.snapchat.com/blog/uncovering-the-value-of-augmented-reality-in-travel [Accessed 20.04.2025].

INFORMATION SECURITY CHALLENGES IN THE USE OF DIGITAL TOOLS FOR DATA PROCESSING AND MANAGEMENT

UDC: 004.056:[005.334+005.53]
DOI: https://doi.org/10.53486/tids2025.30

CEBAN SVETLANA
ASEM, Chisinau, MD 2005, Republic of Moldova
ceban.svetlana@ase.md
ORCID ID: 0009-0006-5957-7666

Abstract. The accelerated pace of digitalization has fundamentally transformed the way information is collected, processed, and used. This process brings significant benefits but also major vulnerabilities in the field of information security. Digital technologies – ranging from common applications and online platforms to cloud-based solutions – have become indispensable for the efficiency of educational, economic, and administrative activities. However, the increasing reliance on technology exposes organizations to increasingly complex cyber threats.

This article examines the main information security risks associated with the use of digital tools in data processing and management, drawing on theoretical approaches as well as recent practical examples. Three major categories of challenges are highlighted: technical (ransomware, phishing, software vulnerabilities, and dependence on cloud infrastructures), legal and regulatory (arising from GDPR, NIS2, and other European frameworks), and organizational and human (limited resources and the human factor as the weakest link).

The conclusions emphasize that information security is not solely a technological issue but requires an integrated approach, combining advanced technical solutions with effective organizational policies and legal compliance. Practices such as data encryption, multi-factor authentication, continuous user training, and the principle of "privacy by design" are essential for strengthening organizational resilience against present and future digital threats.

Keywords: information security, cyber threats, ransomware, phishing, cloud computing, organizational resilience.

JEL Classification: M15, O33.

INTRODUCTION

Digital transformations over the past decade have fundamentally changed the way companies, educational institutions, and organizations manage data. Modern technologies – from office software applications and online collaboration platforms to cloud services – have become essential for economic, administrative, and educational processes. These tools provide clear benefits in terms of efficiency, accessibility, and cost optimization, but at the same time they increase exposure to cyber threats and information security risks.

Alongside the benefits of digitalization, related challenges have also intensified: increasingly sophisticated cyberattacks, data breaches, and difficulties in meeting information protection requirements. Threats such as ransomware [1], phishing [1], software vulnerabilities [5], and growing dependence on cloud infrastructures [1] significantly affect both the academic and corporate sectors. In addition, strict compliance obligations under European regulations (GDPR [2], NIS2 [3]) further increase the overall level of complexity.

In this context, the present article analyzes the most significant information security challenges associated with the use of digital tools for data processing and management. It also discusses practical solutions and recommendations, emphasizing an integrated approach that combines technical, organizational, and legal dimensions to strengthen the resilience of institutions and companies against current and emerging digital threats.

INFORMATION SECURITY CHALLENGES

The transformations of today's digital environment generate a wide variety of risks that directly impact information security. These risks are not uniform but fall into several categories, depending on their nature and their effects on organizations. First, there are technical challenges, linked to cyberattacks and IT infrastructure vulnerabilities. Second, there are legal and regulatory challenges, related to compliance with strict data protection and cybersecurity requirements. Finally, organizational and human challenges must also be considered, arising from user behavior, limited resources, and an organizational culture that does not sufficiently prioritize security. Examining these three dimensions is essential for understanding the complexity of information security and for identifying solutions suited to the current context.

A. Technical Challenges

1. **Ransomware Attacks.** Ransomware is among the most widespread and dangerous forms of cyber threats [1]. Such attacks encrypt data and demand payment to restore access. Universities and companies are often targeted because their activities rely heavily on uninterrupted access to digital platforms and critical databases. Several European academic institutions have had to suspend online operations temporarily due to ransomware, disrupting education and damaging their reputation [1]. The consequences extend beyond financial losses, affecting institutional credibility and partner trust.

2. **Phishing and Social Engineering.** Unlike purely technical attacks, phishing exploits human errors such as negligence and lack of vigilance. Attackers use convincing messages to obtain sensitive data (passwords, access codes) or trick users into installing harmful software. In both academic and corporate settings, this can result in compromised email accounts, internal systems, and confidential files. The absence of regular staff training and excessive trust in seemingly safe sources make phishing a persistent cause of security breaches [1].

3. **Software Vulnerabilities.** Everyday applications – from text editors and spreadsheets to collaborative platforms and database systems – may contain hidden vulnerabilities. Failing to apply updates or using software from unreliable sources opens the door for attackers. Zero-day exploits can fully compromise IT infrastructures. Outdated, unpatched systems make institutions particularly vulnerable [5].

4. **Dependence on Cloud.** The extensive use of cloud services (Google Workspace, Microsoft 365, AWS, Dropbox) has reshaped how data is stored and shared. However, increased dependence on cloud providers brings additional risks: misconfigured sharing settings, account compromises, and legal issues related to cross-border data storage. These risks can only be reduced through strict access control and constant monitoring [1].

B. Legal and Regulatory Challenges

1. **GDPR Compliance.** The GDPR requires organizations to follow strict rules for handling personal data [2]. In practice, this is difficult, especially when data is transferred to servers outside the EU (such as Google Workspace or Microsoft 365). Many institutions lack resources for full

compliance, such as appointing a Data Protection Officer (DPO) or conducting regular audits. The threat of large fines – up to EUR 20 million or 4% of global turnover [GDPR, art. 83] – increases pressure on organizations [2].

2. **NIS2 Directive and Cybersecurity.** Adopted in 2022, NIS2 strengthens cybersecurity rules across the EU [3]. It expands to cover educational institutions, digital providers, and strategic companies. Requirements include reporting incidents within 24 hours, conducting assessments, and applying strict risk management measures. For many organizations, especially those with limited budgets, meeting these obligations requires significant investments in IT systems and specialized staff.

3. **Unregulated Emerging Technologies.** The fast development of new digital technologies creates legal and security challenges. In the absence of clear rules, responsibility for data breaches or flawed decisions remains uncertain, shifting between developers, service providers, and end users. The lack of proper regulation may also reduce transparency and fairness in critical sectors such as education, healthcare, and employment. The EU has begun drafting new frameworks, but until their full application, a regulatory gap persists [4].

C. Organizational and Human Challenges

1. The Human Factor. End users remain the weakest link in information security. Studies show that most successful cyber incidents arise more from human mistakes than technical flaws. Weak passwords, shared credentials, and careless handling of suspicious emails create major risks. In educational settings, with many users on the same platforms, the danger is even greater. Without regular training and awareness, the human factor remains a critical vulnerability (IBM Cyber Security Report, 2023) [7].

2. Limited Financial Resources. Many organizations, especially in education and the public sector, lack adequate budgets for cybersecurity [1]. This leads to reliance on outdated systems, missing updates, weak backup solutions, and a shortage of specialized staff. Such conditions make them attractive targets for advanced attacks (OECD Report on Cybersecurity, 2022).

3. Organizational Culture. In many institutions, information security is still treated as an administrative formality rather than a strategic priority [6]. The absence of clear policies and accountability results in rules being applied superficially, lowering overall protection. By contrast, organizations that view security as an investment in stability and credibility succeed in reducing their exposure to risks [6].

STATISTICAL ANALYSIS

To better understand the depth and complexity of information security risks faced by organizations, it is important to examine the evolution of ransomware attacks between 2022 and 2024. Data provided by international cybersecurity bodies, such as ENISA [1] and the Microsoft Digital Defense Reports [5], show a steady and significant rise in the number of incidents.

This upward trend reflects not only the growth of criminal activity in the digital sphere but also the ongoing weaknesses of IT infrastructures – including the lack of regular updates, configuration mistakes, and insufficient user training.

As shown in Table 1, the number of ransomware attacks increased sharply over the three-year period, with a growth rate of +26% in 2023 and +15.5% in 2024 compared to previous years.

Table 1. Evolution of Reported Ransomware Attacks Worldwide (2022–2024).

Year	Estimated Number of Reported Attacks (millions)	Annual Growth Rate (%)
2022	493	-
2023	623	+26%
2024	720	+15,5%

Furthermore, Figure 1 shows the global evolution of reported ransomware attacks, emphasizing both their continuous growth and the magnitude of the phenomenon.

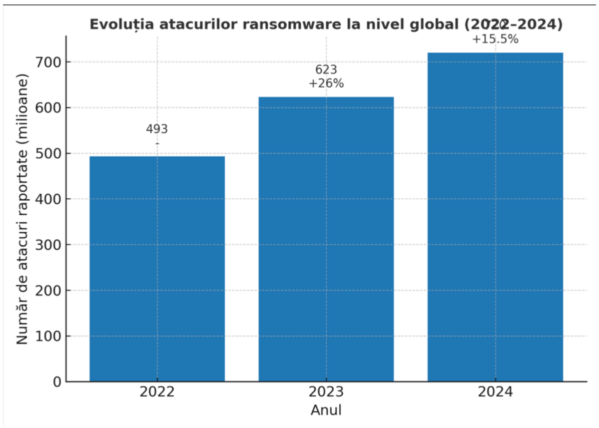


Figure 1. Evolution of Ransomware Attacks Worldwide, 2022–2024.

CASE STUDIES OF RANSOMWARE INCIDENTS

To better illustrate the figures presented in Table 1 and Figure 1, several real cases of ransomware attacks are worth mentioning.

In **December 2019**, *Maastricht University* in the Netherlands was hit by the Clop ransomware. Attackers encrypted Windows servers, including backup systems, and the university had to temporarily shut down many of its online services. The incident caused major disruption to teaching and administration, and restoration took several weeks [8].

In **March 2023**, the *Hospital Clínic de Barcelona* in Spain suffered a ransomware attack that paralyzed its IT infrastructure. Emergency rooms, laboratories, and pharmacy systems were severely affected, and thousands of medical appointments had to be canceled due to the inability to access digital records [9].

Another significant case occurred in **Andalusia, Spain**, where a ransomware attack targeted the regional health service. Internal documents and patient data were leaked, while many healthcare services were temporarily disrupted. According to ENISA, about 82% of affected medical entities reported delays in patient care as a direct consequence of the incident [10].

These examples confirm that ransomware attacks are not abstract threats but concrete realities affecting universities, hospitals, and public institutions. The impact extends beyond financial losses, directly influencing essential services, user trust, and institutional reputation.

The analysis of real incidents highlights not only the vulnerabilities of digital infrastructures but also the urgent need for proactive measures. These experiences show that effective protection requires more than reaction; it demands preventive strategies tailored to organizational realities.

SECURITY STRATEGIES AND RECOMMENDATIONS

Studying information security challenges represents only the first step in understanding the complexity of today's digital environment. To effectively counter these risks, organizations need to design and apply integrated solutions that reduce vulnerabilities and strengthen resilience. A purely technological perspective is not sufficient, since information security is by its nature multidimensional.

Therefore, a comprehensive strategy is required, combining:

- **technical measures** aimed at protecting infrastructures and data;
- **organizational measures** that engage users and promote a strong culture of security;
- **legal and compliance measures** to ensure conformity with regulations and international standards.

Only through a unified vision, adapted to the specific context of each organization, can a high level of protection against current and future digital threats be achieved.

1. **Technical Solutions.** The first line of defense is the technological component, directly focused on safeguarding systems and sensitive data. Key measures include:
   - **Data encryption** – both in transit and at rest – using strong modern standards (e.g., AES-256, TLS 1.3) to ensure confidentiality even in case of breaches.
   - **Multi-factor authentication (MFA),** which strengthens account protection by combining passwords with biometric factors or one-time codes, significantly reducing the risk of compromise.
   - **Regular application of updates and patches,** essential to eliminate vulnerabilities and prevent zero-day exploitation. Enabling automatic updates is considered best practice.
   - **Periodic backups** in offline environments or secure cloud storage, together with testing recovery procedures, to enable fast restoration after incidents such as ransomware attacks.
   - **Intrusion detection and monitoring** through IDS/IPS solutions and SIEM platforms, ensuring early detection of suspicious activity and preventing large-scale breaches.

2. **Organizational Solutions.** The second level of defense addresses human and institutional factors. No matter how advanced technology is, security remains fragile if users lack training or if internal policies are poorly defined. Essential measures include:
   - **Clear security policies,** specifying access rules, user responsibilities, and applying the "least privilege" principle (minimum necessary access).
   - **Continuous staff training,** with workshops, awareness campaigns, and guidelines to reduce exposure to phishing and social engineering.
   - **Simulations and regular testing,** such as phishing drills or incident response exercises, to measure preparedness in real scenarios.
   - **Business continuity and disaster recovery plans (BCP/DRP),** with concrete procedures for resuming operations after major incidents.
   - **Dedicated roles and resources,** including appointing a Chief Information Security Officer (CISO) or a Data Protection Officer (DPO), even in smaller organizations.

3. **Legal and Compliance Solutions.** A third essential dimension of information security is compliance with existing laws and standards. Beyond technology and organizational aspects, legal adherence is vital both for protecting data and for avoiding penalties. Important measures include:
   - **Applying GDPR principles** [2], such as "privacy by design" and "privacy by default," ensuring data protection from the earliest stages of system and application development.
   - **Meeting NIS2 Directive requirements** [3], which oblige organizations in key sectors to adopt risk management policies, report incidents within 24 hours, and perform regular security audits.
   - **Preparing for new European frameworks,** by reviewing the use of emerging digital tools and aligning internal procedures so that decisions remain transparent and accountable.
   - **Conducting internal and external compliance audits,** to detect vulnerabilities early and implement corrective actions that minimize risks of exploitation.

FINDINGS

The analysis highlights several key aspects related to information security in the context of using digital tools:

- **The evolution of ransomware attacks** confirms a steady increase during 2022–2024, showing that this type of threat continues to be one of the most critical vulnerabilities for modern organizations. The consequences extend beyond financial losses to include operational disruptions, restricted access to essential resources, and reputational damage to affected institutions.
- **The human factor** remains the weakest link in the security chain. Weak passwords, carelessness toward suspicious messages, and insufficient knowledge of security practices directly facilitate the success of cyberattacks. The absence of continuous training and the lack of a security-oriented culture within organizations amplify these risks.
- **Educational institutions** are among the most exposed, due to limited budgets and the large number of users sharing the same platforms. This makes them highly vulnerable to phishing, social engineering, and ransomware attacks, with significant effects on both teaching and administrative processes.
- **Compliance with European regulations** – such as GDPR [2] and NIS2 [3] – represents an additional burden for organizations. Adapting to these requirements requires substantial investment in IT infrastructure, regular audits, and specialized staff, along with constant alignment to an evolving legislative environment.
- **Information security** should not be viewed solely as a set of technical measures but as a multidimensional process. It integrates technological, legal, and organizational components, underlining the importance of a comprehensive and collaborative strategy to reduce risks and strengthen resilience.

The findings summarized above confirm that information security is a challenge that goes beyond technology. They emphasize the importance of integrating technical solutions with legal frameworks and organizational culture, setting the stage for the conclusions drawn in this study.

CONCLUSIONS

The analysis carried out in this article has shown that, in the context of using digital tools for data management and processing, information security is a complex and multidimensional issue. The main risks identified fall into three major categories: technical risks, resulting from cyberattacks and IT infrastructure vulnerabilities; legal and regulatory risks, linked to the requirements of the European framework and the lack of clear standards for new technologies; and organizational and human risks, where limited resources and user-related factors play a critical role.

The conclusions underline that these challenges cannot be solved in isolation but require an integrated strategy that brings together advanced technological measures, effective organizational policies, and legal compliance [1–7]. Practices such as data encryption, multi-factor authentication, regular user training, and the application of "privacy by design" principles show that information security extends beyond the technological domain, also involving managerial, educational, and legal dimensions.

Looking forward, strengthening organizational resilience against digital threats will depend not only on implementing current best practices but also on the ability to adapt continuously to new risks driven by technological innovation and the growing use of cloud services. Only a proactive and holistic approach can transform information security from a source of vulnerability into a factor of stability and credibility for modern organizations.

In the future, the effectiveness of information security will also depend on the capacity of organizations to collaborate at both national and international levels. Sharing knowledge, best practices, and incident reports can significantly improve preparedness against large-scale attacks. At the same time, investments in digital education and awareness programs are essential, ensuring that users at every level, from students to managers, understand their role in protecting data. Strengthening cooperation between institutions, governments, and the private sector can transform information security from a reactive response into a proactive shield, able to support long-term stability and trust in the digital environment.

REFERENCES

1. ENISA. (2023). *ENISA Threat Landscape 2023*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023
2. European Parliament & Council of the European Union. (2016). *Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR). Official Journal of the European Union*. https://eur-lex.europa.eu/eli/reg/2016/679/oj
3. European Parliament & Council of the European Union. (2022). *Directive (EU) 2022/2555 (NIS2 Directive). Official Journal of the European Union*. https://eur-lex.europa.eu/eli/dir/2022/2555/oj
4. European Commission. (2021). *Proposal for Regulation on Emerging Digital Technologies*. COM (2021) 206 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206
5. Microsoft. (2023). *Microsoft Digital Defense Report 2023*. Microsoft Corporation. https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report
6. Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004
7. IBM Security. (2023). *Cost of a Data Breach Report 2023*. IBM Corporation. https://www.ibm.com/reports/data-breach
8. GEANT (2020). *Case Study: What Maastricht University Learned from the Ransomware Attack*. GEANT. https://security.geant.org/case-study-what-maastricht-university-um-learned-from-the-ransomware-attack-part-2/
9. AP News (2023). *Ransomware attack on Barcelona hospital cancels thousands of appointments*. https://apnews.com/article/37e0fee33798c56459e63866ca8b449f
10. ENISA (2023). *ENISA Threat Landscape for the Health Sector*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/sites/default/files/publications/Health%20Threat%20Landscape.pdf

Bun de tipar 12.11.2025
Coli editoriale 18,65.Coli de autor 18,55. Coli de tipar 32,0.
Comanda nr. 60.

Serviciul Editorial-Poligrafic
al Academiei de Studii Economice din Moldova
Chişinău, MD-2005, str.Bănulescu-Bodoni 59.
Tel.: 022-402-910
www.ase.md