Information security and the cybernetic approach: a model for training information security specialists in the era of digitalization

TURCAN Aurelia,
PhD in Economics, Associate Professor,
Academy of Economic Studies of Moldova
E-mail address: cce.turcan@gmail.com,

GUJUMAN Lucia,
PhD in Economics, Associate Professor,
Academy of Economic Studies of Moldova
E-mail address: gujuman.lucia@ase.md,

Abstract
This study focuses on the training of information security specialists from the perspective of a cybernetic approach, taking into account the challenges posed by the rapid process of digital transformation. The analysis begins with the premise that information security cannot be viewed merely as a matter of following technical rules; rather, it requires systemic, adaptive, and multidisciplinary thinking, which is what makes the cybernetic approach relevant. Taking this idea into consideration, the paper proposes an innovative training model for information security specialists, comprising three types of skills (technical, analytical, and decision-making/ethical). Traditional training techniques will be used alongside cybernetic exercises and simulations, as well as case studies based on real-life incidents. Thus, it is concluded that there is a significant shortcoming in current educational programs in terms of artificially separating technical and strategic approaches. The conclusions will provide a number of suggestions for improving existing academic programs to better align with job requirements in the Republic of Moldova.

Keywords: information security, cybernetic approach, training of specialists, digital age, educational model

Introduction
The rapid development of digitalization in modern societies has resulted in a new system of functioning of institutions, companies, and administrations. Digitalization, transition of data into the virtual space and global connectivity have provided many advantages regarding effectiveness, fast communication, and information accessibility. However, this process has also caused a new threat which consists in the vulnerability of the information systems because of advanced cyber threats [1].

In these circumstances, information security has been gaining increasing significance as a crucial part of functioning of every modern institution irrespective of its sphere of operations. In the contemporary world, information security is no longer just about technical challenges and solutions as they are linked directly to economic competitiveness and national security [4].

Among the major issues in information security in the present-day world, there can be identified the shortage of professionals in this domain. Labor market demand is greatly outweighed by the number of students trained in information security, and they are insufficiently ready for constantly changing conditions [3]. Another issue that causes much

concern is that even when information security training courses exist, they do not provide a well-balanced education since they focus too much on technical aspects [2].

The current research begins with the idea that the classical training framework for information security professionals has become obsolete. A pure technical approach, aimed at gaining practical skills related to the use of tools and techniques of protection, has become inadequate. The problem of information security demands a systemic, adaptable, and multi-disciplinary approach, involving the possession of technical skills, analysis of complex risks, decision-making under conditions of uncertainty, and ethics of actions carried out [5]. As for the research focus, it should be emphasized that the current analysis is carried out within the boundaries of the Republic of Moldova, studying the educational market and finding deficiencies between current educational programs and employer requirements [3][6].

Theoretical Foundation. The Cybernetic Approach in Information Security

Premise: Information Security Is Not Just a Technical Issue

So far, information security has been regarded exclusively as a technical issue to be solved by developing software, applying hardware systems, and imposing restrictive access policies. It became a routine thing to regard any security breach as a result of an unattended technical flaw or the activity of an intelligent hacker. However, this point of view turned out to be inadequate in modern conditions.

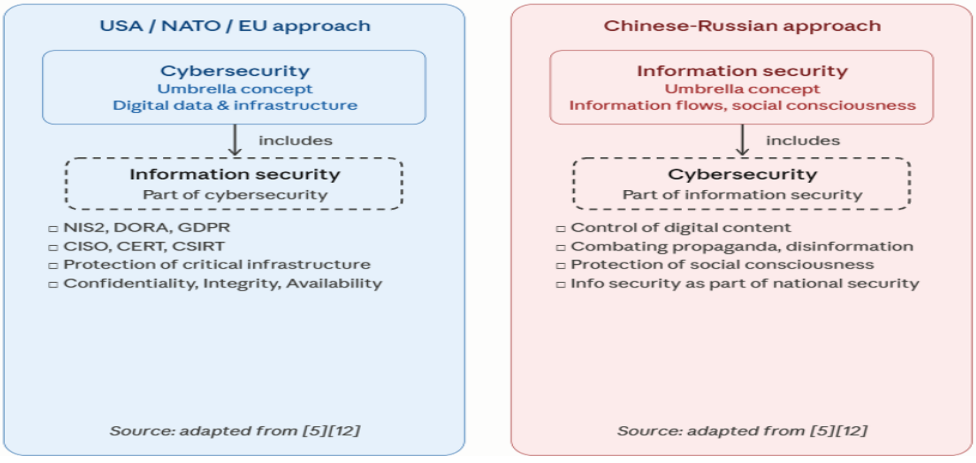
Global Cybersecurity Outlook 2025 published by World Economic Forum warns about increasing complexity of cyber threats due to growing interdependence between supply chains and global digital ecosystems and notes that joint countermeasures should always be effective and coherent [1]. Researches carried out in the Republic of Moldova also prove this thesis: according to LMPI survey (2017), the main challenges of businesses are not related to the technical aspect, but rather to the human factor, company culture, and decision making [3, p. 15].

Conceptual Clarifications: Information Security vs. Cybersecurity. International Approaches

To create a solid theoretical basis for the suggested training program, it is important to explain the relationship between information security and cybersecurity because different definitions are used by different countries depending on their geopolitical and strategic interests.

As stated by Bartsch and Frey [12], there are two major approaches to this issue. The first one assumes that cybersecurity is an overarching concept, and information security is its sub-domain. It is characteristic for the USA, NATO, and European Union. The second approach is typical for China and Russia, as it views cybersecurity as a constituent element of information security [12].

Schema 1. International approaches: information security vs cybersecurity



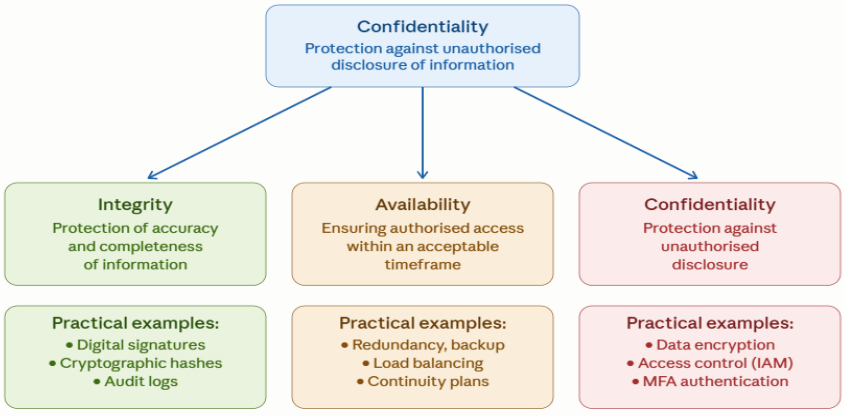
It is important to note that one of the latest approaches to defining the term cybersecurity belongs to the Canadian government, with the document acknowledged as an example of Cyber Security Strategy by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) [13]. In accordance with the Canadian definition, cybersecurity denotes the protection of digital information and the infrastructure within which it exists, seeking to provide the opportunities associated with digital life through addressing the issues of cyberspace [14].

When comparing the approaches presented above, it can be stated that the use of the term information security in the context of countries facing hybrid threats implies the wider meaning of information security as a set of government-regulated activities concerning information flows towards the society, aimed at securing the population from propaganda and other negative factors.

It is important to realize that information security is an entire system of measures ensuring the protection of confidential information in economic activities and the like in teaching students economics. It is necessary to have the following objectives to achieve the purpose of such information protection: (1) protection of the integrity of the system of managing the information resources; (2) prevention of the unauthorized use of the information resources; (3) restoration of the integrity and compensation of economic losses.

Additionally, the authors highlight the confidentiality-integrity-availability (CIA) triad, which is at the core of information security training programs [9].

Schema 2. The fundamental triad of information security (CIA)



Source: adapted from [9]

Approach of the European Union and the Republic of Moldova

The European Union takes an approach towards the issue that primarily focuses on operational and internal market issues. The key element here is cybersecurity, defined as the protection of networks, information systems, and data from threats in the digital world. The mentioned strategy finds itself materialized in the NIS Directive (2016) and its revised variant called NIS2 (2023). The latter covers an expanded scope, introduces mandatory supply chain security, sets common requirements regarding the incident reporting, and establishes managers' liability for the breach of security measures [1]. One of the key problems is the existence of diverse regulations across countries, viewed as a compliance issue by more than two-thirds of CISOs [1].

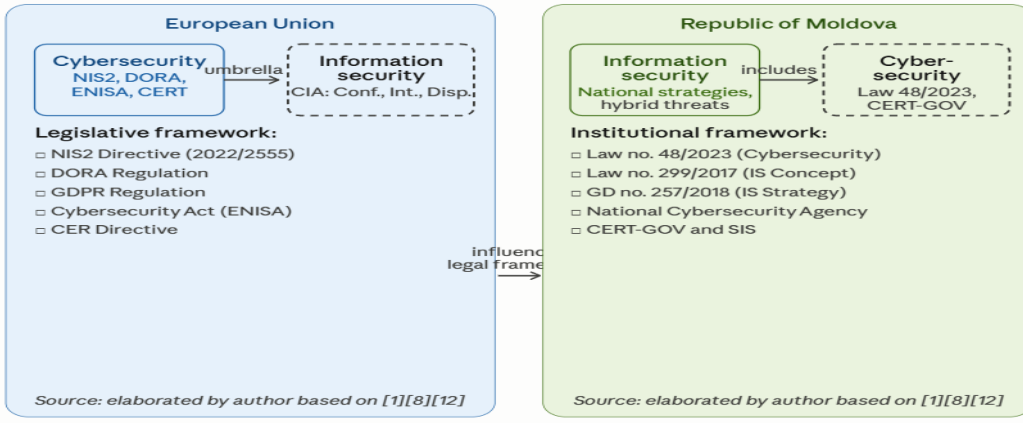
The Republic of Moldova employs a dualistic strategy of looking at the issue, driven not only by the need to harmonize regulation with EU standards but also by the hybrid nature of the threats faced today, including disinformation and coordinated cyber-attacks [5].

While cybersecurity (technical aspects) is governed by Law no. 48/2023 on cybersecurity, which reflects, to a large extent, the provisions of the NIS2 Directive, its objectives involve the development of a national cyber security management system, critical infrastructures' identification, and incident reporting obligations. In this respect, the main relevant entities include the National Cybersecurity Agency (as the body responsible for regulation), as well as the Computer Emergency Response Team of the Government of the Republic of Bulgaria (CERT-GOV) (as an incident management organization) [8].

In turn, information security (strategic aspect) is provided for in Law no. 299/2017 on the Conception of Information Security and Parliamentary Decision no. 257/2018 for the Information Security Strategy 2019-2024. As for its purposes, they are more extensive than those related to the technical aspect since the information security strategy itself is viewed as one of the elements of the national security system, aimed at defending state, societal, and personal interests against propaganda, misinformation, or any attacks on people's social

consciousness. In this regard, the main coordinating body in this area remains the Information and Security Service (SIS) [8].

Schema 3. Conceptual and legislative framework: EU vs Republic of Moldova



A fundamental distinction made in the model of the Republic of Moldova between cybersecurity (a technical problem related to protecting systems) and information security (strategic protection of the state from negative impacts) is its key difference that should be known to specialists specializing in the field and used in practical implementation.

A cybernetic approach can provide the theoretical and methodological basis for the development of information security solutions in the new information reality. Being science studying directions, communication and control in complex systems, cybernetics provides the key concepts for information security specialist training.

In particular, the *concept of feedback* lies at the core of cybernetic paradigm. Specialist with cybernetic approach not only performs certain actions related to information security but develops control system that provides him/her with information about its effectivity. Positive feedback – alarm, system log, report – initiates a corrective response. The information security activity becomes a repetitive sequence of action-feedback-correction.

The *principle of adaptability,* in its turn, is a logical continuation of the previous point. The idea of the cybernetic system implies the capability to adapt in response to any changes in the surrounding environment and to the new data that becomes available. As far as a specialist in cybersecurity is concerned, this requires him or her to constantly review and modify security strategies, architectures, and learn lessons from each new threat.

As far as the proposed training model is concerned, *the principle of interdisciplinarity* stands out as the most important. Indeed, cybernetics combines knowledge from mathematics, engineering, psychology, sociology, economy, and even law. Thus, when approaching a problem of cybersecurity from a cybernetic perspective, a specialist will regard it as an interdisciplinary issue. This implies that, along with technical means of

solving the problem, he or she will consider psychological (social engineering), legal (NIS2, DORA, and GDPR), and managerial aspects of it.

The Urgent Need for Training Specialists in Information Security

Information security is now a crucial part of state security and competitive advantage in the Republic of Moldova. According to the Global Cybersecurity Outlook 2025 report produced by the World Economic Forum, cyber-threats have grown increasingly complicated and effective defenses must remain constantly strong and coherent [1].

The present stage of the development of society features the growing effectiveness and widespread distribution of information technologies, along with the growing importance of the information field, encompassing telecommunication systems and entities that gather, process, distribute, and apply information [7]. The information field plays an active role in the social, economic, and national security aspects of any modern society [7].

For the Republic of Moldova, digital transformation of the economy has become an important strategic direction. Based on the adoption of the Conception of Information Security on December 21, 2017, the Parliament by Decision no. 257 dated November 22, 2018 adopted the Information Security Strategy of the Republic of Moldova for the period of 2019–2024 and the corresponding action plan [8]. Thus, two main objectives have been identified as follows: (1) formation of the training system for specialists in the area of information security; (2) formation of the culture of information security in society [8].

As was mentioned by Ohrimenco and Sklifos [9], within the process of training specialists in economics, information security needs to be considered as a triad consisting of three aspects: (a) information and informational resource protection goals – what needs to be protected; (b) protection influencing factors – from whom we need to protect; (c) information security tools – how we should be protected [9]. As was already mentioned above, such a triad approach is necessary while training specialists in economics, because they participate directly in the processes of information collection, processing, recording, storage, and analysis [9].

It should be emphasized that the results of the survey carried out in the Republic of Moldova as part of the European Erasmus+ LMPI project (2017), which was conducted among 199 respondents from 711 enterprises, show that the most pressing needs for specialists in terms of the lack of qualified employees are associated with: banking; enterprises of the IT sector; telecom companies; IT services; consulting companies; public administration; and large enterprises [3, p. 14]. However, the problems of enterprises are not limited to technical issues, since insufficient competence of staff and management, poor development of risk management strategies, and inability to implement security strategies depend on the human factor [3, p. 15].

Study Programs in Information Security in the Republic of Moldova

With the rapid progress of technology and increased danger in terms of cyber threats, information security becomes an urgent issue in the modern world. The Republic of

Moldova is one of those countries that are actively developing training programs in this area.

Main educational institutions for information security. The two prominent educational institutions that provide education in the field of information security within the local context are the **Technical University of Moldova (TUM)** and the **Academy of Economic Studies of Moldova (AESM).**

Technical University of Moldova - leading provider of specialist technical education
At TUM, within the faculties of Computers, Informatics and Microelectronics (FCIM) and the faculty of Electronics and Telecommunications (FET), students can choose among the broadest set of courses provided in cybersecurity.

The provision of first-cycle education in the form of specialist training (bachelor degree) includes:

- Information Security specialization (within FCIM, full-time); provides expertise in securing computer information systems;
- Security of Electronic Communications specialization (within FET, full-time and part-time);

This program specializes in securing electronic networks and transmissions.

Master Programs at TUM include advanced degrees, involving international cooperation:

- Information Security – double degree program in cooperation with the University of West Attica (Greece);
- Information Security in Communication Systems and Networks - double degree program, conducted jointly with the Polytechnic University of Bucharest and "Ștefan cel Mare" University of Suceava.

Such international cooperation provides for graduates mobility and European recognition of their studies.

Academy of Economic Studies of Moldova – information system security expertise
The AESM university enhances the educational profile through a specific focus on the economic and managerial side of information systems security issues.

Bachelor's programs (first cycle): As it happens in all universities of Moldova, the AESM university no longer provides separate specialization courses in information security. Such information security training is integrated only in terms of discipline courses into the bachelor degree programs in the field of information technologies, namely: Information Technology, Cybernetics and Economic Informatics, and Applied Informatics.

Master Programs (second cycle) at the AESM include advanced courses in information security from an economical and managerial perspective, namely: Information

Management (with specialization Information Security) and Information Systems Security [11].

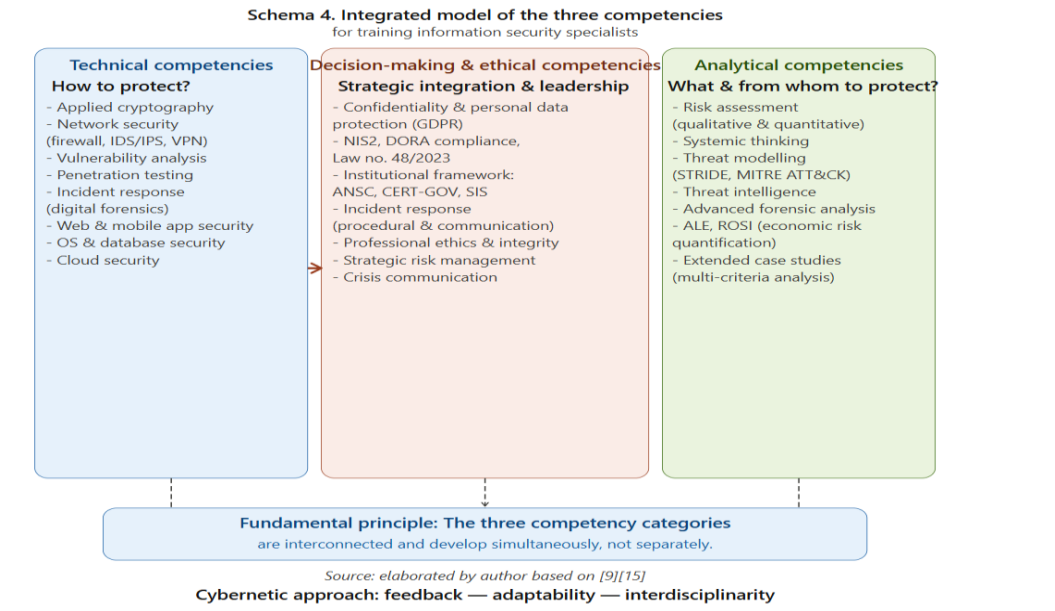
The peculiarities of the AESM course programs include economic and management capabilities of graduates, allowing integration of information security into a broader corporate strategy, along with effective information risk management from the perspective of economics [10][11].

There are many competitive educational courses in information security provided in the Republic of Moldova. On one hand, TUM provides high-quality technical courses and excellent international links at both bachelor and master levels, on the other, AESM makes a unique addition to the range due to its economic-managerial approach in the area, especially at master level and through interdisciplinary studies.

These programs are characterized by an advanced educational approach, where the focus of studies changes from mere transmission of secondary information into construction of research problems that encourage analytical and critical thinking.

In order to remain up-to-date in accordance with the changes of the modern cybersecurity landscape and prepare the next generation of professionals, it will be important to maintain constant curriculum renewal and collaboration with the private sector, providing the required competencies for facing new challenges. Another important aspect might be the launch of a new separate program in information security at bachelor level in AESM

Taking all this into account and considering the above deficiencies, mainly the artificial separation into technical and strategic areas, the author uses the theory, taking into consideration the principles of cybernetics and the triad (what should be protected, against whom, and how), proposes a new approach to the preparation of information security specialists. Such an approach presupposes a system of development of three different kinds of competences that are mutually supportive and inseparable [9].



Source: elaborated by author based on [9][15]

Cybernetic approach: feedback — adaptability — interdisciplinarity

Technical competencies

Technical competencies include information regarding tools, technologies, and techniques employed for cybersecurity, corresponding to the question how to protect? [9]. The proposed framework includes: applied cryptography (symmetric and asymmetric cryptography, digital signatures, PKI), network security (firewalls, IDS/IPS, VPNs), vulnerabilities analysis, incident response (computer forensics), web/mobile applications security, and operating systems/databases security.

Analytical Competencies

Analytical competencies convert a good technician into a real information security specialist, which is an answer to the questions of what should be protected and from whom? [9]. It is the purpose of the proposed model to provide development in the following areas: risk assessment (identification, qualitative and quantitative analysis, ALE and ROSI methods), systemic thinking (interrelations between the components of information systems), threat modeling (STRIDE, attack trees, MITRE ATT&CK), forensics and threat intelligence.

Decision-making and Ethical Competencies

It is important to overcome the artificial separation between the technical and strategic approaches to security management [2]. In the proposed model, these competencies include: data confidentiality and protection of personal data (GDPR), compliance with European (NIS2, DORA) and national laws (Law no. 48/2023), knowledge about the institutional environment (Cyber Security Agency of Romania, CERT-GOV, SIS), incident response from procedural and communicative perspectives, crisis communication, and issues related to professional ethics and integrity. *An ideal specialist must be able to*

evaluate threat sources (anthropogenic, technogenic, and natural) as well as existing vulnerabilities (objective, subjective, and accidental) [9].

Defects of Current Education Programs

An analysis was done, and it was found that current education programs have some critical flaws, which are, first of all, an artificially imposed dichotomy between technical and strategic approaches. Courses related to information security are currently included in educational programs of universities; however, the problem is not in the lack of such disciplines but rather in the way these disciplines are taught, isolated and technically-oriented without including analytical and decision-making aspects and without any connection to European regulations and demands of finance [2][9].

Educational programs must ensure that there is inclusion of the newly added sections in the theory lessons and practice labs, where information security basics and their application to banking and management information systems are covered [9].

Schema 5. Main deficiencies of current educational programmes in the field of information security

1	**Artificial separation between technical and strategic approaches** Technical disciplines (cryptography, network security) are taught in isolation from analytical and decision-making ones, producing specialists with unbalanced competencies, unable to integrate perspectives in complex situations.
2	**Exclusive focus on technical competencies** Programmes neglect analytical competencies (risk assessment, threat intelligence) and decision-making ones (ethics, compliance, crisis communication), which are essential for a well-rounded specialist.
3	**Lack of simulations and extended case studies** Teaching methods remain predominantly theoretical; case studies, where they exist, illustrate specific technical concepts without multi-criteria analysis of causes and consequences.
4	**Insufficient alignment with European regulations** The NIS2, DORA, and GDPR frameworks, as well as national legislation (Law no. 48/2023), are insufficiently integrated into curricula, leaving graduates unprepared for the current compliance environment.
5	**Gap between academic programmes and employer requirements** The LMPI survey (2017), with 199 respondents from 711 companies, found that the main problems faced by employees are not technical, but relate to organisational culture and strategic decision-making [3, p. 15].

Source: elaborated by author based on [2][3][9]

Recommendations for Improving Academic Programs

Taking into account the results of the analysis, the following recommendations for improving academic programs in the sphere of information security can be made:

- Redesigning of the curriculum taking into account the three competences' dimensions;
- Theoretical foundations based on the cybernetics principles and the confidentiality, integrity, availability triad;
- Implementation of modules related to NIS2, DORA, GDPR, and the legislation at the national level (Law no. 48/2023);
- Combining both quantitative (ALE, ROSI) and qualitative risk assessment methods;

- ❖ Putting forward the use of the extended case study (multicriteria analysis) methodology;
- ❖ Diversity in assessment techniques taking into consideration all three competences' dimensions;
- ❖ Trying to continuously train teachers in terms of European laws, financial safety, hybrid threats.

All recommendations mentioned above completely correspond to the viewpoint of the authors [18] who argue that "digital transformation in education requires much more than just implementing technology. It involves a reevaluation of pedagogy, assessments, and how education institutions engage with the labor force market."

Conclusions

Thus, this research has shown that training in information security specialists cannot be limited to purely technical matters. The cybernetic approach, uniting technical, analytical, and decision-making/ethical competences, is the only approach suitable to address the issues created by digital acceleration.

The analysis of educational programs in the Republic of Moldova, combined with the results of the LMPI study (2017) – reflecting the needs of 199 out of 711 contacted firms – and conclusions from the Global Cybersecurity Outlook 2025 report, proves the presence of a structural weakness: the artificial gap between technical and strategic skills [1][2][3].

The model proposed in this paper, divided into three categories of competences – technical, analytical, and decision-making/ethical – creates a framework consistent with the specifics of the Republic of Moldova, which attempts to adapt to European standards but also is exposed to hybrid threats. Its implementation necessitates strong institutional willingness and cooperation with stakeholders.

Recommendations for future research could include further elaboration on the comparative analysis using programs of the EU member states, examination of the actual effect that the provisions of NIS2 and DORA have on competency demand, and development of means to estimate the effectiveness of the proposed model.

References

[1] World Economic Forum. Global Cybersecurity Outlook 2025. Available: https://www.weforum.org/publications/global-cybersecurity-outlook-2025/

[2] BOGDANOVA, Violeta. Methodology of studying information protection and security technologies in higher education. PhD thesis in educational sciences. Chișinău: Tiraspol State University, 2022. 187 p.

[3] Erasmus+ LMPI Project. Enquête d'identification des métiers cibles et des besoins de formation en sécurité informatique – Moldova. 2017. 19 p. Available: https://www.lmpi-erasmus.net/Allegati/14/CommonFiles/Meetings/default/0/0/2.4_MD_Bilan%20de%20l'enquete.pdf

[4] CHERNEY, G.A., LYAKHU, F.S., OHRIMENKO, S.A. Bezopasnost avtomatizirovannykh informatsionnykh system. Chișinău: Ruxanda, 1996. 186 p.

[5] TSARUK, Oleksandr and KORNIIETS, Maria. Hybrid nature of modern threats for cybersecurity and information security. In: Smart Cities and Regional Development (SCRD) Journal. 2020, vol. 4, no. 1, pp. 57–78. DOI: https://doi.org/10.25019/scrd.v4i1.63

[6] Academy of Economic Studies of Moldova. Faculty of Information Technologies and Economic Statistics (TISE). Available: https://admitere.ase.md/tise/
[7] ZGUREANU, Aureliu and MITITELU, Vitalie. Preparing of the Specialists in Information Security of University and Master Degree Levels at Free International University of Moldova. In: International Scientific Conference. ULIM, 2012. https://ibn.idsi.md/sites/default/files/imag_file/360-365.pdf
[8] Decision of the Parliament of the Republic of Moldova regarding the approval of the Information Security Strategy of the Republic of Moldova for the period 2019–2024 and the Action Plan for its implementation: no. 257 of November 22, 2018. In: Official Gazette of the Republic of Moldova, 2019, no. 13-21, p. 80.
[9] OHRIMENCO, S.A. and SKLIFOS, K.F. Information security for economists. Chișinău: Information Security Laboratory, ASEM. security.ase.md/publ/ru/pubru106/o_s.html
[10] Academy of Economic Studies of Moldova. "Information Security" study program, first cycle Bachelor's. Available: https://admitere.ase.md/tise/securitatea-informationala/
[11] Academy of Economic Studies of Moldova. Master's programs in the field of information security. Available: https://admitere.ase.md/tise/
[12] BARTSCH, Michael and FREY, Stefanie. Cybersecurity Best Practices: Solutions To Increase Cyber Resilience For Businesses And Government. Springer-Verlag, 2018.
[13] CCDCOE. Cyber Security Strategy Documents. 2019. Available: https://ccdcoe.org/cyber-security-strategy-documents.html
[14] Government of Canada. Security And Prosperity In The Digital Age: Consulting On Canada's Approach To Cyber Security. 2019. Available: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2016-scrty-prsprty/index-en.aspx
[15] Forbes, "How Generative AI Will Change The Jobs Of Teachers," 2024. [Online]. Available: https://www.forbes.com/sites/bernardmarr/2024/02/09/how-generative-ai-will-change-the-jobs-of-teachers/. [Accessed 2026].
[16] WIENER, Norbert. Cybernetics: Or Control and Communication in the Animal and the Machine. 2nd ed. MIT Press, 1965.
[17] VRABIE, C. 2025. Artificial intelligence and education. *All in on Tech (AIoT)*. 1, (Dec. 2025). Available: https://www.scrd.eu/index.php/aiot/article/view/680/818
[18] TURCAN Aurelia; GUJUMAN, Lucia; COLESNICOV, Tatiana. Digital transformation in education: ASEM case study and the integration of modern technologies in the learning process. In: *Smart Cities International Conference (SCIC)*, 2024, București. In: *Smart Cities and Regional Development (SCRD) Journal*, 2025, vol. 9, nr. 3, pp. 67-80. https://www.scrd.eu/index.php/scrd/article/view/630