CYBER SECURITY EDUCATION ON THE LABOR MARKET IN THE EUROPEAN UNION

Ghenadie CIOBANU [a*], Amelia DIACONU [b], Mihai DINU [c], Cristina DIMA[c], Alexandra Maria SÂRBU [c]

[a] National Scientific Research Institute for Labour and Social Protection, Romania
[b] Artifex University of Bucharest, Romania
[c] Bucharest University of Economic Studies, Romania

ABSTRACT

Considering the process of digital reforms in all branches of economic activity and society, the activity of public and private institutions is digitization. There is an ample process of digitization of the educational system and of the health system, an important moment belongs to the problem of Cyber Security of functioning of the digitization systems. Of course, in this process an important role belongs to the training and preparation of staff in the field of cyber security, which requires the adaptation of the specialist training in the field in the member countries of the European Union. Last but not least, the creation of new specializations in the field of cyber security and the modification of the university curriculum.

KEYWORDS: *budget process, US Congress, budget analysis*

1. INTRODUCTION

The digital revolution, the development of the digital economy and digital society both in Romania in EU member countries, but also globally (Radulescu et al., 2018). In the last decade of activity has greatly changed the applicability of information systems, the development of artificial intelligence, the development of smart industry and urban development (Smart City, Smart Village), industry development 4.0, 5.0, new applications in the development of precision agriculture (Sarbu et al., 2021).

Very dynamic, government activities have begun to be, digitized through the development of e-government platforms (Burlacu et al., 2021), and public administration services at central, regional and local levels In particular, the application of digitalization tools to society at the global level began with the global epidemiological crisis Covid - 19 which accelerated the digitalization activity at all levels and in all branches of public and private activity (Radulescu et al., 2021).

A particularly important place for the development and efficient activity of digital systems is to ensure cyber security of public and private institutions, cyber security in the activity of national governments, banking systems and computer systems of financial markets, platforms of enterprises and companies (Burlacu et al., 2019)., activity virtual educational systems and in the field of health care, platforms for the promotion of public services, the platforms of companies for the promotion of products and the development of online marketing (Orzan et al., 2020).

Therefore, we all witness and participate in the development of a new paradigm for the development of society, the economy, the involvement of man in this activity and the highlighting of the strong and weak aspects of the challenges we face (Radulescu et al., 2020).

* Corresponding author. E-mail address: *gciobanu019@gmail.com*

The pandemic crisis has radically changed the market, reduced the demand for air travel and all types of transport. The Horeca industry has suffered a lot (restaurants, hotels, tourism activity which in recent years had a development perspective) (Burlacu et al., 2021) .
But, there has been another problem and a niche that will grow more and more in the field of cyber security work that will grow more and more in the coming years . The uncertainty we face today is increasingly strengthening the Information Security industry, Cyber Security a broader term found in the literature internationally (Burlacu et al., 2020). Priority is given to education and training in this important and challenging field. Jobs in the field of cyber security were in high demand until the Covid - 19 pandemic crisis, but with the crisis in which we found of course that the demand for the development of cyber security as well as a specialist in the field labor market (Profiroiu et al., 2020). The rapid transition to remote work has created an urgent need to train cybersecurity specialists to secure networks, technologies and staff in all branches of public and private activity globally.
Of course, experts in the field are actively discussing the impact of such radical changes on the Internet, the security of Secure World, protection against cyber - attacks and privacy, the pitfalls of cyber uncertainty and the shift to online work (Radulescu et al., 2020).
All branches of activity urgently need a specialist in the field of cyber security, software with a high level of protection and cyber security, computers and networks with a high level of security to ensure efficient operation of economic agents, strategic institutions, public and private and ensuring the national cyber security of states.
For these reasons, we set out to prepare an article in this field that would highlight the priorities, problems and opportunities for the development of a special segment of the labor market for the training of specialists in the field of cyber security.

2. MANUSCRIPT

2.1 Bibliographic study of the problem

The author Melé (2021) consider: “ Much of the Industrial Revolution (FIR) study focuses on efficiency, productivity and economic progress, but very few have taken, its ethical aspects into account. This article aims to help complement this important aspect by providing an address for ethical risks in the workplace. Based on Catholic social education (CST) - addressed to all people of good faith and approach, it analyzes the ethical issues proposed at work by FIR, especially Industry 4.0, which is the core of the revolution. CST Catholic social education highlights the dignity of the worker, the need for progress and development in the workplace. Robots, artificial intelligence, all interconnected technologies are instrumental; the real subject of work is the worker”.
That activity directs a special light on the ethical issues analyzed, but also the impact on employment, wages and consequently inequality, the treatment of human quality, relationship issues, safety and health, employee supervision and work significant. John Gorman (2008). Treatment of human quality, relationship issues, safety and health, employee supervision and meaningful work. John Gorman (2008). Do you know where their employees go when they are, given access to the Internet and the World Wide Web? Should he know? Is it a violation of privacy? Exploring this sensitive area a former consultant for a software company, who is completing his MBA at London Business School. Richard Kissel, Mark Wilson (2009) is of the opinion: “Cyber security, educational training and awareness programs (ETA) is the “Critical Component” of the cyber security program. It is that "educational and informational vehicle" for the dissemination of cyber security information, which is necessary and useful for that group of employees in the field, including managers, which will support them to fulfill their objectives and tasks at a much higher quality. . Regarding the total security solution, the importance of the workforce in achieving the cyber security objectives, the importance of learning as a “countermeasure” cannot be, exaggerated.
Both the establishment, maintenance and development of a relevant ETA program, as a component part of the global cybersecurity program, is the main conduit for providing the workforce with the information and tools needed to ensure the protection of an organization's vital information resources.

These programs will ensure that staff at all levels of the organization fully understand the responsibilities of "cyber security" in order to use and protect the information and resources that have been, entrusted.

The authors Wendzel, S., Tonejc,J., Kaur,J., Kobekova,A.,(2017) addressed the issue of relevant communication protocols. The authors wanted to explain the basics of a smart building, with the technical components, a brief analysis of their historical developments, presented the role of smart buildings in smart cities, known cases of attacks on smart buildings. The authors explained the communication protocols of smart buildings and their security features.

They also covered the technical aspects of the attacks on the intelligent building infrastructure and their implications, respectively the attacks and the reasons for the unsafe buildings. After analyzing these problems, they discussed the solutions for the protection of automatic buildings. They therefore reflected recent trends in intelligent building security research.

Authors Scarfone, Benigni and Grance (2009) focused on cybersecurity, standards for improving the security of systems, networks and critical information technology (IT) infrastructures. The cyber security standard defines the functional requirements, the security requirements within an IT product environment, system, process or technology. Well-developed "cyber security" standards in terms of mathematical, computer, technological and technical assurance allow software and hardware developers and serve as a reliable method for purchasing security products. Cyber security standards cover a wide range of details, from the mathematical definition of a cryptographic algorithm to the specification of security features in a web browser and are usually independent of implementation. A standard must meet the needs of users, which must be, designed with costs and technological limitations considered in the construction of products to meet the standard. The requirements of a standard need to be, verified, so that users can evaluate the safety even when the products are, tested according to the standard.

Hwang & Kwon (2016) studied the development of unmanned aerial vehicle (UAS) applications that are becoming an integral part of many applications, and that ensure the security of those systems against harmful cyber threats, which is a growing concern big.

Regarding the rules for addressing this issue, it is very important to investigate the various interactions between cyber and physical components within UAS. Both feasible cyber threats, associated vulnerabilities, and other such phenomena analyzed for different security properties. Although traditional security for computers, software, computer networks is the necessary approach in the UAS cyber layer, that method alone is not sufficient to diagnose the general risk, because the dynamics of UAS behavior is not, considered.

Respectively, a fairly, comprehensive framework for cybersecurity analysis is introduced from a systems perspective. UAS cyber processes must include the basic elements of physical behavior: an approach that allows a UAS with security not only, in terms of software, but also whose physical operations are fundamentally, inspected and have security guarantees, complementing the UAS security architecture existence.

Given the process of digital reforms in all branches of economic activity and society, the activity of public and private institutions is digitalization, which includes: (1) The process of efficient digitization of the education system; (2) The process of efficient digitization of the health care system. Therefore, we would like to mention that there is an extensive process of digitization of the education system and the health care system, respectively, an important moment belongs to the problem of cyber security of the operation of digitization systems.

Of course, an important role in this process lies in the training and education of staff in the field of cyber security, which requires the adaptation of specialized training in the field in the member countries of the European Union. Last but not least, the creation of new specializations in the field of cyber security and the modification of the university curriculum.

(3) Creating new specializations in the field of cyber security. With the accelerated development of the Internet, especially in the midst of the 2020 pandemic crisis, transaction traffic has reached an unprecedented level. The number of fraudulent business and activities has increased. So the question

is what do we do and how do we fight cybercrime? Improving skills and training in cybersecurity, recruiting new employees, needed today in this confrontation, we want to mention that the development of appropriate programs and systems is fragmented and inadequate.
There is an acute shortage of qualified experts in this field worldwide. Why is it happening? Technology is constantly changing, which makes it difficult to keep up with the industry and requires specialized knowledge that takes time to develop. The European Cyber Security Agency (ENISA), manufacturers and other organizations using solutions for Industry 4.0 and IoT often fail to properly train, their staff before things change again, exposing them to potential risks. Moreover, the training available to them often does not correspond to the real facts and / or is extremely expensive.
In recent years, cyber - attacks have become more frequent, which has led organizations to rush to hire qualified professionals, which makes it extremely difficult to find professionals in this field in the labor market. The need for and urgency to take action is exacerbated by the COVID-19 pandemic and the call for a sharp increase in the number of cyber-attacks that have been successful for criminals. Education and training in cybersecurity have not, been trained in the need to train skilled workers. The reasons for this deficiency are very diverse and many in number. The level of formal education (university or college), the number of cybersecurity professionals have increased steadily in the last decade and a half, but the number of graduates is still below the level required by industry.
It takes a long time to educate and train, highly qualified specialists and it takes even more time for them to gain practical work experience. At the same time, investments in cybersecurity training are extremely limited, as budgets for expenditure not directly related to profit and revenue have been, significantly reduced. What does this mean for our future if nothing else done?

2.2. Study method for implementation to develop the labor market in the field of cyber security
The lack of highly qualified professional cybersecurity specialists not only in Romania and other EU countries, but worldwide has a direct, important impact on organizations and their ability to defend against cyber threats. It poses a threat to the overall economic well-being of countries, regions and the well-being of society. This issue covers at least three areas of particular interest: (1) Availability of highly qualified specialists in information security management, administration and assistance of organizational operations (2) Availability of qualified cyber engineers to develop security systems, software and security tools. (3) General awareness of cyber security at every organizational level. Every employee should have a basic knowledge of threats, cyber and specific risks in the context of each job function. If the global talent shortage in cybersecurity continues, it will be more difficult for organizations to ensure cybersecurity. An increase in the number of cyber - attacks can expected, with serious financial losses, major disruptions in operations, disruptions in the provision of services and supply chains, breaches of privacy and public security and other consequences. To try to encourage talented cyber professionals to fill the growing gap in knowledge and skills.
ENISA represents the dissemination of multifunctional knowledge in the field of IT and OT security, as well as the continuation of training and advanced training courses. The organization has selected capacity building as a key objective of its new strategy and is now conducting numerous consumer awareness activities to promote safer online behavior. Promoting and analyzing cybersecurity education to address the lack of cybersecurity professionals, which is a challenge for the country's economic development and national security.
In some countries, specialized programs have been developed and implemented to ensure that this problem solved. These programs include - national cyber security awareness campaigns; encourages universities, colleges (high schools), middle and vocational schools; of training institutions, to promote cyber security as a field of learning. For example, in Canada and the United Kingdom, "cyber education" introduced into the school curricula of children from the age of eight.
This is encouraging, because we need to create future generations of talented cyber specialists. It is necessary to draw up a technical report on cybersecurity education and training. When this document published, it will highlight why, what and how to do cybersecurity education and training to help improve the current situation.

This report will provide information on why cybersecurity education and training are essential and how it needed to create a well-trained and competent workforce that protects businesses and society large. The new standard could provide insight into why cybersecurity education should be a strategic priority in the development of the workforce in organizations and government in all business sectors. What can organizations do to protect themselves? Full understanding of the risks they face, the application of mitigation controls. Application of ISO / IEC 27002 - Information Technology - Security Technologies - Code of Practice for Information Security Control, provides a set of controls that are based on industry best practices; meets the need for organizations to create opportunities to defeat cybercriminals, while better understanding them.

The series of ISO / IEC 27000 standards ensures the information security of institutions and organizations. The implementation of the standard set, in carrying out the operations of an institution, will ensure the security of data, for example: financial information, intellectual property, information about employees or information provided by third parties.

ISO / IEC 27001 is one of the best - known standards in this series, meeting the requirements of information - security management systems (ISMS).

WHAT IS ISMS? ISMS is a systematic approach to managing confidential information in a company in a secure way. This system includes personnel, production processes and IT systems, united by the implementation of risk management processes. The mechanism can help small, medium and large enterprises to maintain information security.

The cyber security of the industry in the era of total digitalization. Technological advances have affected many areas of our lives. Experts talk about two trends that set the vector for the evolution of society, business and industrial production: the digital transformation and the fourth industrial revolution. Digitization of production not only increases the capacity and basic comfort. The dynamic development and maintenance of leadership positions - depends on the security of the information environment and automated control systems.

What modern cyber threats industrial enterprises exposed? How real and dangerous are hacker attacks? It must said that there are wrong actions and that there are real situations of cyber- attacks. These are, special harmful actions that increase daily, although they try not to reveal information about incidents (attacks on electricity networks, disconnections of networks in some significant objects; scanning ports for access to classified financial information; industrial espionage or theft of design documents is also, a great danger. Remote access can lead to the risks of taking control of equipment and much more. What are the characteristics of ensuring the cyber security of enterprises in the mining and metallurgical industries?

- First of all, these industrial enterprises are objects of critical information infrastructure. These, are companies that form cities, whose closure can lead, to social damage and an ecological disaster. Second, they are important technological facilities, with expensive equipment and production. Third, companies that often have a geographically distributed network with different information network architectures.

Consequently, the main principle of protecting industrial networks is "do no harm".

If in the business Segment, the emphasis is on ensuring confidentiality, in the industrial networks (ICS) the emphasis is on accessibility: the main thing is that everything should work flawlessly. In addition, most equipment and technology manufacturers do not include in their solutions the possibility of additional installation of antivirus cyber protection products should not complicate the work of the utility network.

Recently, more and more companies are trying to coordinate the production process with information security issues. The main issue: to strike a balance between the principle of sufficient rationality and those legislative requirements in the field of critical information infrastructure protection. The lack of skills in cyber security (CSSS), in that document refers to the lack of qualifications of the professions in cyber security on the labor market, which today is a problem for economic development, for national security, for the rapid digitalization of the global economy. Represents threats with high impact on data, information technology systems and computer networks that is

essential for modern societies. This shortcoming can be, further analyzed in two competing issues: one quantitative and one qualitative. The problem of providing information on the global deficit, is important and has subsequently reduced it to the situation in the EU, where granular data are still lacking compared to other countries. For example - Australia, the United Kingdom and the United States. We would like to mention "the way in which employers (public or private) recruit and appreciate cybersecurity professionals". Experienced professionals, internationally recognized certificates, diplomas are sought. Those people are hard to find in the extremely limited labor market. Respectively, employers need to increase salaries in order to attract specialists in this sector, to provide adequate training, which is still, rarely done.

There are two reasons why the education and training system could be responsible for this blockage in this segment of the labor market: it does not stimulate enough students to adhere to relevant diplomas in cybersecurity and it seems unable to equip with adequate knowledge, skills of the security system. Which could provide a better chance of becoming a cybersecurity professional one day.

Most issues affecting cybersecurity education, low cybersecurity courses in IT and related IT programs, poor alignment between educational offerings, labor market demands, emphasis on multidisciplinary knowledge, the prominence of theory-based education, and less on training practice - revolves around the need to redefine educational and training pathways to provide the unified standard for knowledge, skills needed by pupils and students. The way to achieve this is to bring stakeholders to discuss and define ways that can contribute to the education of students in the field of cybersecurity, after graduation and before entering the labor market.

To carry out this project, four states - Australia, France, the United Kingdom and the United States have established certification procedures that confirm the diplomas in the field of cybersecurity, comply with quality standards agreed by national expert groups. A certified diploma in higher education, in cybersecurity should have: (1) sufficient specific appropriations for cybersecurity courses and activities; (2) a structured curriculum, which includes a practical component of training, or specific types of examinations and activities, such as cyber security competitions; (3) high quality teaching faculty, which includes industry professors; (4) broad multi/interdisciplinary emphasis; (5) awareness-raising activities and measures, collaborations with the cyber security ecosystem; (6) information on academic results and employment.

In terms of recommendations: Recommendations are based on evidence generated, they are informed about the reflections of the government, industry stakeholders, on this evidence in the recommendation workshop. Changing attitudes and behavior: *Recommendation 1:* The existing guide to communicating cyber security risks with an impact on board members should be reviewed, updated and promoted to ensure that discussions in terms of commercial risk help to achieve the cyber framework. *Recommendation 2:* There should be additional guidance (eg on awareness-raising and training activities), access to good practice, Cyber Security solutions, lead to the functioning of change and the maintenance of staff behavior outside Cyber Security teams.

Recommendation 3: The ability to positively influence organizational behavior and culture, which should be included as a general competency requirement for any licensed cyber professional. These competencies must be included in the qualifications developed, included by the UK Cyber Security Council. What are career paths and transitions ?: *Recommendation 4:* Work in progress on mapping careers in cybersecurity should include the development of examples, job descriptions and minimum qualification requirements to encourage employers in Cyber Security to develop more job advertisements, realistic.

Recommendation 5: The future career framework for cyber security should include sets of training pathways, other innovative solutions that allow staff quickly from a wide range of IT roles, acquired cyber security skills, the transition forward in the general framework. Recruitment and diversity of the workforce: Recommendation 6: Small businesses in the cybernetic sector should be encouraged and supported to build collaborative relationships with educational institutions (schools, colleges and universities), in order to carry out internships, through an IT platform, page web. It should allow them to hire more core cyber employees and recruit many more.

Recommendation 7: It is welcome to have written guidance, training manual, on cyber security of small organizations, especially without Human Resource Support, respective information on basic actions, which includes: NCSC Board Toolkit, home guidance, s.a.
Recommendation 8: Recruitment agencies and human resources staff should play a greater role in educating cybernetics, leading to good practices for realistic and impartial recruitment. This can This may include, for example, events or workshops at cybersecurity conferences led by recruiters or human resources professionals.
Recommendation 9: Further work should be, done to understand the reasons behind the lack of diversity of senior roles in cyber firms - an issue that potentially extends to senior cyber roles outside the sector - and steps that would improve career progress in these superior roles for diverse group.
This may include events, workshops at cybersecurity conferences, led by recruiters or human resources professionals. Recommendation 9: It is welcome to make further efforts to understand the reasons behind the lack of diversity of senior roles in cyber firms: an issue that extends to the role of higher cyber security outside the sector, steps that will improve career progress for managers and experts superiors from various groups and fields of activity.
Recruiting and maintaining the validated number of cyber security professionals at work is a permanent struggle, not only for the technical problem of Cyber Security, but also for the area with a view to non-technical jobs, related to management in the cyber sector. There has been little emphasis on the human dimension of cybersecurity; the lack of cybersecurity professionals is a global problem. To overcome this, the current education systems need to be reformed and cooperation between the various stakeholders needs to be, introduced. This chapter presents and discusses actions and developments in the field of education, the concept of knowledge and skills in cybersecurity to meet the needs of the EU labor market.
The skills shortage identified in "cyber security" has had an impact on the market, which has begun to take shape in the last decade with intensive digitization. The skills in "cyber security" have become very current as the evolution and development of the digital economy and the loss of resources. The EU General Data Protection Regulation (GDPR), which entered into force in May 2018, needs to be, considered in order to give data security in each system the processing of data or information, but due to lack of skills, many organizations are not preparing for compliance. Many EU GDPR webinars in 2019 showed that 60% of companies are unprepared for the GDPR, compared to research conducted in 2020 by computerweekly.com, which accounts for 90%.
A priority issue is the development of the labor market and the European cyber education ecosystem given the need to build knowledge, skills and capabilities, according to the requirements of European employers in cybersecurity, or set up four competence centers. Two have tasks to address the development of cyber education in the EU. Another competence center (“Concordia”) develops the new education ecosystem in the field of cyber security, offers training in industry, and another Center (“Cybersecurity Europe”) focused on *EU HEI programs.*
Both approaches contribute to the development of the new cybersecurity education program in Europe, with the main aim of bridging the gap in cybersecurity skills and meeting the needs of the digital society as a whole. This can: (1) Provide education and training in cybersecurity, which shaped by the needs of the industry. A Price Waterhouse Coopers survey found that failed cybersecurity jobs reduced workforce morale and extended employment, introducing additional costs. (2) Standards, curricula appropriate to the competencies between candidates: the root cause of job failure. (3) Standards, curricula with guidelines and accreditation. A Diploma in the field of "cyber security" can cover a fairly, wide range of disciplines, depending on the area of the educational program. Many essentially different programs called "cyber security" or another similar generic name. Due to the variety of existing programs and the names of diplomas, the distinction of a cybersecurity program that uses an accreditation and certification system seems to be a very useful idea. (4) These constants indicate that cyber security comprises a very wide portfolio of fields, expertise and practical activity and cannot be, expected that a single educational program can cover all specialized skills, specific knowledge in the sector desired by each employer. There is certain knowledge, skills that are essential

for any employee in a critical role of technical work, regardless of field of activity, which includes knowledge of computer and network architecture, data, cryptography, networking, security encryption principles, operating systems as well as proficiency in working with Linux-based systems, fluency in low-level programming languages, and familiarity with common operating methods and mitigation techniques. (5) The need to build a new educational ecosystem in the EU: is this how we will eliminate the gap between skilled and skilled labor? There has long been a growing interest in cybersecurity education and skills in the EU, and there has been a policy concern since the European Commission's publication of the first EU Cyber Security Strategy in 2013, calling on Member States to step up education and training efforts in the field of network and information security (NIS), planning a "driving license" - voluntary certification program to promote ICT skills and competencies and cyber security. Another task is the general European accreditation and certification of the degree of cyber security.

SCHRÖDER & MIHAI, I.-C., p.9-19(2020) is of the opinion: “The phenomenon of cybercrime is developing, by its nature, fast, transnational and without borders. Cybercrime includes traditional crimes, content-related crimes and crimes unique to computers and information systems. In recent years, the digital and cybernetic component in most types of crime has steadily increased. "As a learning organization, the European Union Agency for Law Enforcement Training (CEPOL) approaches cybercrime training from a perspective of where the agency can best optimize its impact, partnering with relevant organizations and focusing on mainstreaming cybercrime into its overall learning and training strategy and the corresponding output. CEPOL has strengthened its cyber-training portfolio and human resources, establishing the Cybercrime Training Academy in order to support the development and delivery of training, primarily for senior police and specialized officers with a range of activities in the cybercrime divisions of cyber-attacks, non cash payment frauds, child sexual exploitation, cyber-forensics and electronic evidence. CSDP Cyber Education,” Training, Exercise and Evaluation (ETEE) Platform under the ESDC Dirk DUBOIS, Dr. Marios THOMA, Dr. Gregor SCHAFFRATH Following an update study by RAND Europe, the EU Army Committee (EUMC) agreed on a point collegial view for the creation of a cyber-defense.

Center / Platform for Education, Training, Exercise and Evaluation (ETEE) under the auspices of CESA. On 13 November 2017, the EDA Steering Committee, bringing together the 27 participating Ministers of Defense, agreed with this collegial view and decided to request ESDC to set up such a center. Taking into account the "modus operandi" of the ESDC, the idea was focused on the implementation of the Cyber ETEE platform, which should not change the main features of the ESDC being a network of training providers, led by Member States in the field of CSDP. The main purpose is to educate and train civilian personnel, military personnel of member states, EU institutions in various fields of Cyber Security and Cyber Defense, in particular, personnel designated for CSDP missions and operations.

3. CONCLUSION

The trend of increasing cyber attacks in recent years has made institutions more likely to hire cybersecurity professionals, which has made it difficult to find professionals in the field on the labor market and the lack of a segment, and a well-defined and organized platform in the field.

The need to urgently take action were and are conditioned by the COVID-19 pandemic, by the call for a sudden increase in the number of cyber attacks.

Education and training in cybersecurity have not been trained in the need for skilled workforce training, although cybersecurity courses are taught in many universities.

Lack of highly qualified cybersecurity specialists not only in Romania but also in other EU countries. Globally it has a direct impact on organizations and their ability to defend themselves against cyber threats, a threat has been created to the overall economic well-being of countries, regions and the well-being of society.

In some countries, specialized programs have been developed and implemented to ensure the solution of the problem. Those programs include: national cyber security awareness campaigns; encourages universities, high schools, middle and vocational schools; of training institutions - to promote cyber security as a field of learning.
Institutions and organizations in order to protect themselves from the point of view of cyber security must understand the risks they face, the application of mitigation controls. Application of ISO standards: ISO / IEC 27002; ISO / IEC 27000; ISO / IEC 27001.
The process of digitization of production will increase the capacity and basic comfort, and the dynamic development and maintenance of management positions depends on the security of the information environment and automated control systems.
The characteristics of ensuring the cyber security of enterprises in various industries (primarily for the mining and metallurgical industries) are: (1) Industrial enterprises are objects of critical information infrastructure. There are companies that form cities, whose closure can lead to social damage and an ecological disaster. (2) are important technological facilities, with expensive equipment and production. (3) There are companies that have a geographically distributed network, with different information network architectures.
Many of the issues affecting cybersecurity education: few cybersecurity courses in IT and related IT programs, poor alignment between educational offerings, labor market demands, focus on multidisciplinary knowledge. In the article we identified some recommendations for improving this teaching process at different levels and for educational and training institutions: (1) Development of a guide for communicating cyber security risks with impact on board members, and promoted to ensure the achievement of the framework cybernetic, discussions in terms of commercial risk. (2) Additional guidance on awareness-raising and training activities, access to good practice, Cyber Security solutions. (3) The ability to positively influence organizational behavior and culture, which should be included as a general competency requirement for licensed cyber professionals. (4) Preparation of work on career mapping in cybersecurity: include the development of examples, job descriptions, minimum qualification requirements. (5) The future framework in the cybersecurity career, to include sets of professional training, innovative solutions that allow staff to quickly train and fit in the field. (6) Small businesses in the cyber sector should be encouraged and supported to build partnerships with educational institutions. (schools, colleges and universities) for traineeships (7) Develop guidance, training manual, on cyber security of small organizations, especially without Human Resource Support, respective information on basic actions. (8) Recruitment agencies, human resources staff, must play the role of cyber education and training, the development of good practices for real and impartial recruitment. (9) Make further efforts to understand the reasons behind the lack of diversity of senior roles in cyber companies.
Develop the concept of cybersecurity knowledge and skills to meet the needs of the EU labor market. The skills shortage identified in "cyber security" has had an impact on the market, which has begun to take shape in the last decade with intensive digitization.

REFERENCES

Burlacu, S., Alpopi, C., Mitrită, M. & Popescu, M. L. (2019). Sustainable e-Governance and Human Resource Development. *European Journal of Sustainable Development*, 8(5): 16.

Burlacu, S., Diaconu, A., Balu, E. P. & Gole, I. (2021). The Economic and Social Effects of Unemployment in Romania. *Revista de Management Comparat International*, 22(1): 21-27. DOI: 10.24818/RMCI.2021.1.21.

Burlacu, S., Guţu, C., Dobrea, R.C., Bodislav, A.D. & Platagea, G.S. (2020). Approaches to the internet of things. *Competitivitatea şi inovarea în economia cunoaşterii*, 531-538.

Burlacu, S., Patarlageanu, S.R., Diaconu, A., & Ciobanu, G. (2021). E-government in the era of globalization and the health crisis caused by the covid-19 pandemic, between standards and innovation. *Les Ulis: EDP Sciences*.

EU General Data Protection Regulation (GDPR), REGULAMENTUL (UE) 2016/679 AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor).

EU HEI, (2021), *HEI Initiative Innovation Capacity Building for Higher Education Pilot Call for Proposals*, Online, available at: https://www.eit-hei.eu/assets/pdf/hei-initiative-pilot-call-for-proposals.pdf, (accessed, August 24, 2021).

Gorman, J. (2008) *Monitoring Employee Internet Usage*, First published: 28 June 2008, https://doi.org/10.1111/1467-8608.00081.

Hwang, I. & Kwon, C., (2016), *System and Cyber Security: Requirements, Modeling, and Management UAS, Integration Issues: Safety, Security, Privacy*, First published: 13 June 2016 https://doi.org/10.1002/9780470686652.eae1150.

ISO / IEC 27000 ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary.

ISO / IEC 27001 SECURITATEA INFORMATIILOR - ISO/IEC 27001, Standard de referinta, ISO/IEC 27001:2018.

ISO / IEC 27002 - Information Technology - Security Technologies ISO 27001 & ISO 27002 – CERTIFICAREA SISTEMULUI DE MANAGEMENT AL SECURITATII INFORMATIEI.

ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements.

Kissel, R. & Wilson, M., (2009) *Cyber Security Education, Training, and Awareness, Part 2. Cross-Cutting Themes and Technologies*, 4. Cyber Security, First published: 18 September 2009, https://doi.org/10.1002/9780470087923.hhs458.

Melé, D. (2021), *Ethics at the workplace in the fourth industrial revolution: A Catholic social teaching perspective*, First published: 16 July 2021, https://doi.org/10.1111/beer.12368.

Orzan, M.C., Burlacu, S., Florescu, M.S., Orzan, O.A., & Macovei, O.I. (2020). The effects of online marketing on financial performance in the textile industry. *Industria Textila*, 71(3): 288-293.

Profiroiu, M.C., Radulescu, C.V., Burlacu, S., & Guţu, C. (2020). Changes and trends in the development of the world economy. *In Competitivitatea şi inovarea în economia cunoaşterii*, 324-330.

Rădulescu, C.V., Bodislav, D.A., Bran, F., & Burlacu, S. (2020). The impact of cross-border cooperation between the Republic of Moldova and Romania on socio-economic development. *EURINT*, 7: 63-79.

Rădulescu, C.V., Burlacu, S., Bodislav, D.A., & Bran, F. (2020). Entrepreneurial Education in the Context of the Imperative Development of Sustainable Business. *European Journal of Sustainable Development*, 9(4): 93-93.

Rădulescu, C.V., Dobrea, R.C., & Burlacu, S. (2018). *The business management of distress situations*. THE 12th INTERNATIONAL MANAGEMENT CONFERENCE "Management Perspectives in the Digital Era" Novembre 1st-2nd, 2018, BUCHAREST, ROMANIA, 1: 741-747.

Radulescu, C.V. Ladaru, G.R., Burlacu, S.; Constantin, F.; Ioanăș, C. & Petre, I.L. (2021) Impact of the COVID-19 Pandemic on the Romanian Labor Market. *Sustainability*, 13: 271. https://doi.org/10.3390/su13010271.

Sarbu, R., Alpopi, C., Burlacu, S. & Diaconu, S. (2021). Sustainable urban development in the context of globalization and the health crisis caused by the covid-19 pandemic. *Les Ulis: EDP Sciences.* doi:http://dx.doi.org/10.1051/shsconf/20219201043.

Scarfone, K., Benigni, D., Grance, T., (2009) *Cyber Security Standards, Part 2. Cross-Cutting Themes and Technologies, 4. Cyber Security*, First published: 15 March 2009.

Schröder, D. & Mihai, I.C., (2020). *CEPOL - The European Union Agency for Law Enforcement Training Activities in the Field of Cybercrime*, (9-19). SECURITATEA CIBERNETICĂ -

PROVOCĂRI ȘI PERSPECTIVE ÎN EDUCAȚIE, ROMÂNIA 2020, Editura SITECH, Craiova, România.

Wendzel, S., Tonejc, J., Kaur, J. & Kobekova, A., (2017). *Cyber Security of Smart Buildings*, First published: 06 October 2017, https://doi.org/10.1002/9781119226079.ch16.