Proceedings of the Informing Science + Information Technology Education Conference

An Official Publication of the Informing Science Institute
InformingScience.org

InformingScience.org/Publications

Online July 5 – 6, 2023

CYBERSECURITY ISSUES IN THE SECONDARY AND HIGHER EDUCATION SYSTEMS' CURRICULA

Svetlana Syarova*	University of Library Studies and Information Technologies, Sofia, Bulgaria	s.syarova@unibit.bg
Stefka Toleva-Stoimenova	University of Library Studies and Information Technologies, Sofia, Bulgaria	s.toleva@unibit.bg

* Corresponding author

ABSTRACT

Aim/Purpose	This paper examines the Bulgarian educational policy in the field of information technology and cybersecurity in particular.
Background	The massive penetration of technology into daily life and the economy is transforming the possibilities for work, learning, communication, access to information, and spending free time. The result is a global electronic environment that provides new opportunities for communication and interaction with individuals and communities worldwide. New strategies, policies, and measures have been constantly reviewed and developed to meet the new demands for high-quality digital education.
Methodology	For each of the major research domains (secondary and higher education systems in Bulgaria) considered for this study, the cybersecurity issues in the curricula have been explored, collected, and analyzed. The study combines empirical research and statistical analysis.
Contribution	This paper contributes to the body of knowledge by providing evidence that in the curricula of non-IT majors, information security does not occupy its important place assigned to it by the current reality of an ever-increasing threat of cyber-attacks.
Findings	Sharing authors' experience acquired in examining educational policy related to students' digital literacy and cybersecurity literacy will contribute to the transition of secondary and higher education in a way to address 21st-century challenges.

Accepted by Editor Michael Jones | Received: March 13, 2023 | Revised: May 4, 2023 | Accepted: May 5, 2023.

Cite as: Syarova, S., Toleva-Stoimenova. S.. (2023). Cybersecurity issues in the secondary and higher education systems' curricula. In M. Jones (Ed.), *Proceedings of InSITE 2023: Informing Science and Information Technology Education Conference*, Article 3. Informing Science Institute. https://doi.org/10.28945/5114

Recommendations for Practitioners	Considering the findings of this study, schools and universities need to include cybersecurity issues and concerns in curricula to raise awareness of their graduates in this field.
Recommendations for Researchers	Conducting research on IT and cybersecurity literacy acquired at the level of secondary and higher education in Bulgaria could identify some gaps and improve the curricula.
Impact on Society	Rapid technological progress radically changes and redefines conventional teaching and learning processes in education to meet current challenges.
Future Research	Future studies can also consider comparative studies in different countries.
Keywords	training programs, educational policy, information technology, cybersecurity

INTRODUCTION

The systematic monitoring, planning, and application of information and communication technologies (ICT) in school education marks its beginning in the last decade of the last century. It is carried out within the framework of the Program for International Student Assessment (PISA) and Progress in International Reading Literacy Study (PIRLS) - students' achievement assessment programs of the Organisation for Economic Co-operation and Development (OECD) using data from national statistical institutes and Eurostat. In 2001, a systematic study of the Eurydice for their application in educational systems was also published. With the establishment of the European Union (EU) and the adoption of the Lisbon Strategy, the application of ICT in school education is a major indicator for tracking progress. This provides a better understanding of the nature and scope of national initiatives in this area. Programs are being developed to implement the measures identified in the strategies (Eurydice, 2001). The "Minerva" Sectoral Programme within the Socrates Programme (2000-2006), Lifelong Learning Horizontal Activities (2007-2013), Erasmus+ Programme (2014-2020), the priority axes and measures of the EU Structural Funds support initiatives and projects that contain clear potential and expected results in the field of ICT implementation, open access methods and resources, and distance learning in different contexts and at different levels of education.

At the current stage, ICT priorities are outlined in the EU Strategy for smart, sustainable, and inclusive growth and more specifically in the Digital Agenda for Europe 2020 and the Digital Single Market Strategy (European Commission, 2020a; 2020b; 2020e) The priorities in the field of education are presented in the Strategic Framework for European Cooperation in Education and Training (ESET 2020) and the plans for its implementation.

In November 2017, a special action plan on digital education was announced at the Gothenburg Summit. In this regard, the European Commission is taking new initiatives to improve key competencies and digital skills of European citizens. The new European Skills Agenda proposes a revised European Reference Framework for Key Competences for Lifelong Learning, which sets out the knowledge, skills, and attitudes people need in their lives, including digital competencies. The Digital Education Action (DEA) Plan (European Commission, 2020d) describes how education can make better use of innovation and support the development of relevant digital competencies for living and working in today's information society. The action plan sets out three priority directions: (1) better use of digital technologies for teaching and learning; (2) developing the digital competencies and skills necessary for life and work in an age of digital transformation; and (3) improving education through better data analysis and prediction. Initiatives include helping schools with high-speed broadband connections, wider use of self-assessment tools on the use of technology for teaching and learning in schools, and a public awareness campaign on online safety, media literacy, and cybersecurity. Three European frames have been developed that aim to provide a common basis for discussions and analyses at national, regional, and local levels. They offer a consistent set of tools for self-

reflection and monitoring aimed at citizens and learners DigComp (Ferrari, 2014; Vuorikari et al., 2022), teachers DigCompEdu (Redecker, 2017), and schools DigCompOrg (Kampylis, 2015).

According to the Digital Europe Progress Report, Bulgaria ranks last in the European Commission's Digital Economy and Society Index (European Commission, 2020c), although its overall score has risen to 36.4%, the share of people with at least basic digital skills is around 29%, while the EU average is 58%, as shown in Figure 1. This indicator has maintained its values since 2017. Only 11% of people have skills above basic, which is less than a third of the EU average. A similar trend is seen among young people: 54% of 16-24 year-olds have at least basic digital skills (compared to an EU average of 85%). Only 31% of Bulgarians have basic software skills, compared to the EU average of 61%. The report states that this indicator is strongly influenced by socio-demographic aspects.

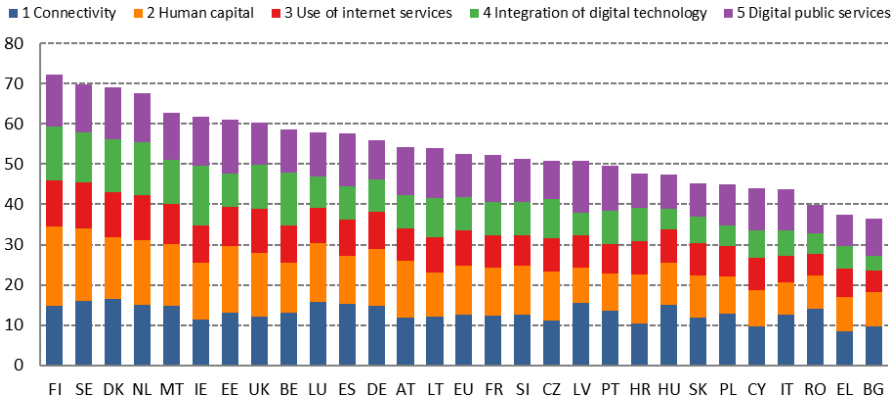

Figure 1. Ranking by the Digital Economy and Society Index (2020)
(Note: Reprinted from DESI 2020, European Commission)

In the current program period, the development of ICT in school education is planned in the Strategy for Effective Application of Information and Communication Technologies in Education and Science of the Republic of Bulgaria (2014-2020). Although the measures are taken and their implementation activities are not fully in sync with the scale of the digital transformation, the emphasis on improving the digital skills of students and pedagogical specialists has been strengthened. From the academic year of 2018-2019, the subject of computer modelling was introduced in the third grade, and upper secondary education, and more hours focused on ICT are planned. According to the national program, "Training for an IT career", extracurricular activities are implemented in secondary schools. In 2019, the National Programme "Digital Bulgaria 2025" was adopted, one of the goals of which is the modernization of the school's ICT education. Main measures related to the provision of adequate infrastructure in the field of ICT in schools assessment of students' digital competencies upon completion of the first high school stage (grade X); modernization of educational content and teaching methods; introduction of the study subject "Computer Modelling" at the initial stage and introduction of training in the "Software and Hardware Sciences" profile; improving the skills of teachers; strengthening cooperation between education, industry and the non-governmental sector; establishing a coordinated approach for effective measures in the field of digital skills and employment.

The continuous and increasing digitization in society, as well as changes in the technology itself, mean that strategies and policies are rapidly becoming obsolete. European countries have to constantly review and develop new strategies, policies, and measures to meet the new demands for high-quality digital education.

Nowadays, every student, as an individual user of Web technologies and a networked citizen of the digital society, must progress from elementary school computer literacy to continuously upgraded high digital literacy, which means knowing the relevant standards, directives, regulations, normative and sub-normative acts and instructions, to comply with requirements, norms, behavior and practical

habits. Areas of conduct that everyone must comply with are also identified, such as etiquette, communication, education, access, commerce, responsibility, rights, safety, and security. In summary, key areas are formed: digital competence, digital ethics, digital sensitivity, and digital participation. Each student as a user has to take care of their own cybersecurity immune system, as one unwise or even inadvertent action can destroy the global immune system of society.

The paper examines educational policy in the IT field and cybersecurity in particular. An analysis has been made of the national training programs in secondary education and the higher education system. The context of the research is based on the main Bulgarian and European political documents, on the basis of which the current educational system in Bulgaria is being developed.

This paper is divided into two main sections. In the first section, a brief literature review is presented to describe the current state and challenges in cybersecurity education. The peculiarities of structuring the educational content in ICT and cybersecurity are considered in the second section as follows: cybersecurity in secondary education in Bulgaria and cybersecurity at the level of higher education in Bulgaria. The conclusion is dedicated to challenging the new reality for education institutions, especially when the needs for digital and also cybersecurity competencies are changing so rapidly.

LITERATURE REVIEW

Since the advent of modern computer systems, information security has been a topic of teaching within various IT disciplines. The recent evolution of cybersecurity shows the need for a conceptual framework of this academic field to provide guidance to higher education when implementing cybersecurity programs. Identifying and describing the competencies, responsibilities, and curriculum content for cybersecurity are among the challenges facing researchers and scientists. The ACM/IEEE (2020) curriculum volumes have generally evolved to incorporate cybersecurity content within each of the existing computing-based degree programs such as Computer Science (CS), Information Systems (IS), Information Technology (IT), Software Engineering (SE) and Computer Engineering (CE). Information Technology (IT2017), which includes a set of core and supplemental information technology domains, also recommends that cybersecurity content occupy approximately 10% of the IT curriculum with most of the material covered throughout the curriculum instead of just in one course (Task Group, 2017). In 2017, a curriculum recommendation and accreditation criteria for a new discipline, "Cybersecurity," in the broader computing space emerged. However, many researchers consider that there is a significant intersection between the evolving discipline of Information Technology and the emerging meta-discipline of Cybersecurity. Ekstrom et al. (2017) argue that Cybersecurity had emerged as the accepted name of what IT2008 called Information Assurance and Security. The terminology and conceptual foundation had evolved significantly. Parrish et al. (2018) examine the global perspective on cybersecurity education for 2030 and cybersecurity as a meta-discipline. The authors have characterized cybersecurity in terms of an abstract set of competencies driven by the need to provide guidance to higher education when implementing cybersecurity programs.

Cybersecurity Skills, Training, and Education Frameworks have been developed by the US National Initiative for Cybersecurity Education (NICE, 2017)., the Institute of Information Security Professionals (2010), etc. Many countries in Europe have defined a national cybersecurity strategy (NCSS), where the European Union Agency for Network and Information Security (ENISA) (2018) provides a good overview. European national strategies often include objectives for building cybersecurity capabilities, enhancing awareness, and providing cybersecurity education. Some initiatives have emerged related to cybersecurity education in general, especially from government organizations aimed at certifying cybersecurity courses and providing guidelines for the subject areas that they expect to be included within the syllabi of cybersecurity modules.

How to provide modern and effective cybersecurity education has been recently discussed by McGettrick (2013), Catota et al. (2019), AlDaajeh et al. (2022), A. J. Blažič (2021) and Ruiz (2019).

Conklin et al. (2014) have identified that the biggest concerns in cybersecurity education are the students' lack of hands-on experience, resulting in a skills mismatch between what the industry would like to see in a candidate for employment, and the skills that the candidates actually possess after graduating. B. J. Blažič (2021) addresses the lack of cybersecurity skills in the European labor force market and the actions taken to improve education in cybersecurity for meeting the identified needs.

Most academic institutions do not include active cybersecurity awareness and training programs in their strategic plans. Slusky and Partow-Navid (2012) briefly analyzed the outcomes of security assessment for a group of students at the College of Business and Economics at California State University, Los Angeles, USA. They observed that the key problem related to cybersecurity awareness is not the absence of required information, as might be expected. Instead, it is the approach used by students while dealing with this information in practical circumstances. The findings were intended to help the college design its syllabus, which included additional information security training.

Al-Janabi and Al-Shourbaji (2016) presented a survey on security awareness in the Middle East, focusing on educational settings and analyzing security awareness among academic staff, researchers, and students. The authors observed that the contributors in the Middle East do not have an essential awareness of the significance of cybersecurity.

Moallem (2019) examined students' attitudes toward cybersecurity in Silicon Valley in California, USA. The author focused on evaluating the cybersecurity level among students in the most advanced technological environment in the world because their behavior is tremendously diverse. College students were not conscious of the safety of their information, even though they were aware that their activities were observed and monitored, and their data were not securely transmitted across the university networks. Therefore, universities should regularly conduct training to change the behavior of students and improve their understanding of the fundamentals of cybersecurity and cyber threats.

In the context of a widespread dependence on increasingly complex digital systems, cyber threats are outpacing societies' ability to effectively prevent and manage them (Terziev & Lyubcheva, 2020). The main reasons for this are related to the development of ICT, the digitization of production processes, and the ubiquitous use of electronic devices and networks to support various business activities. As a result of the electronic interaction at all levels in organizations, the development of electronic commerce and business, of various electronic services, huge amounts of data are accumulated in terms of volume, variety, and rate of growth and change, including sensitive information about employees, customers, products, finances, etc. Quite naturally, the big data collected and used by organizations has become a strategic resource, with a view to extracting useful knowledge from it and improving decision-making and management processes. At the same time, digital assets are subject to deliberate and accidental threats, due to the presence of vulnerabilities in the protection of information systems.

As a result of the above-mentioned factors and their constant development and redefinition, the educational system opens up many new opportunities, but also many new problems and challenges. Today, there is a need for a new vision in teaching and building literacy for working with data, which also includes ensuring information safety when working with modern ICT. Universities are realizing the need for new innovative programs covering information security training even in non-IT specialties (Trifonova, 2018). Integrating cyber security even at an earlier level such as secondary school education will have multiple benefits, as argued by Pencheva et al. (2020). First, it will set young people on the track to pursuing a professional cybersecurity career by equipping them with the right technical and social set of skills. This is important because the shortage of cyber security professionals is likely as we still lack an effective means to bring new people into the workforce. Second, integrating cybersecurity modules into secondary school education could effectively bridge the intergenerational gap between students on the one hand, and their teachers and parents on the other.

Digital competencies are seen as a cross-cutting key competence enabling people to acquire other key competencies such as language, mathematics, study skills, or cultural awareness (Hristova, 2017). An

evolution of digital literacy over the years has been observed in order to adapt to the digital world. That is why it should be a policy priority, especially for educational institutions. Nowadays, developing cybersecurity literacy at an early level including in secondary school and universities in non-IT specialties becomes a compulsory element of the digital literacy of young people.

RESULTS

RESEARCH METHODOLOGY

The paper examines educational policy and practice in the ICT field and cybersecurity in particular in the two major research domains related to the secondary and higher education system in Bulgaria. Document analysis was conducted to establish the policies and teacher practices in secondary schools, and the cybersecurity issues in the curricula have been explored, collected, and analysed in the paper. As far as the next educational level, the research covered 49 universities in the country, whose broad spectrum of study (non-IT) programs and their curricula were investigated and data about the cybersecurity-related subjects studied were collected through the Internet.

The methods of content analysis, comparative analysis, and statistical descriptive analysis were applied based on the data from the examined universities.

CYBERSECURITY IN THE SECONDARY EDUCATION SYSTEM IN BULGARIA

The subject, Information Technologies, was introduced in a Bulgarian school in 1994 in the ninth grade of secondary education. From 1999 to 2000, it was studied as part of the compulsory subjects of the ninth and tenth grades. Subsequently, two levels of preparation (compulsory preparation and profiled preparation) were distinguished for the subject of Information Technologies in the high school stage (9-12 grades). Since 2006, Information Technology has been studied by students as a compulsory subject in junior high school and primary education.

The core set of IT knowledge and skills acquired in secondary education is a foundation of digital competencies on which students improve their future professional skills and increase their confidence and self-esteem. The goal of creative use of the possibilities of modern IT for communication is clearly set in school education in Information Technology. When determining the state educational standard for general education in the ORDER No. 5 of 30.11.2015 (of the Ministry of Education and Science), the expected knowledge, skills, and attitudes in the area of competence in "Electronic Communication" are described in detail. For example, for the junior high school stage of the basic level of education, we read: "Knows the applications of the Internet for communication and information sharing, interacts in a networked environment for data exchange and use of shared resources, collaborate through digital channels, has an idea of the importance of electronic communications for the functioning and development of society in the secondary course."

Communication is one of the five areas included in the European framework for self-assessment of digital competencies (Ghomi & Redecker, 2019) and this includes knowledge and skills in using a wide range of communication tools (mobile devices, SMS, e-mail, chat, video conferencing, blogs, social networks, etc.), create and manage files for collaboration, data exchange, and file and application sharing.

According to the Pre-school and School Education Act (2016), the subject "Information Technologies" is studied as a general educational preparation for 1 hour per week (total 34 hours per year) in junior high school stage of education (grades 5–7), 1 hour each per week (total 36 hours per year) in the first high school stage of education (grades 8–10). "Computer Modelling" is studied for 1 hour per week (a total of 32 hours per year in grade 3 and a total of 34 hours per year in grade 4) in the initial stage of education (grades 1–4).

IT training is aimed at mastering knowledge, skills, and attitudes related to building students' digital literacy. The curricula contain topics that cover all areas included in the European framework for self-assessment of digital competencies (Ghomi & Redecker, 2019): information processing, content creation, communication, cybersecurity, and problem-solving. The more important of them are presented in the subsections below:

Communicate Safety on the Internet

Attention is paid to safe communication on the Internet and the concept of "online bullying" is analysed. The characteristics of online bullying are outlined, and the risks and pitfalls of the Internet are indicated. Forms of cyberbullying (sending/sharing bad, hurtful, or abusive messages on, e.g., social media sites) are discussed.

Attention is paid to technical safety and virus protection, which are important skills in the digital environment.

Basic rules are outlined to help students stay safe online. It is important that students know the ways to seek help outside the school (Bulgarian Centre for Safe Internet, https://www.safenet.bg/bg/).

Protection of Intellectual Property

The protection of intellectual property includes a large number of international agreements prepared with the help of the World Intellectual Property Organisation (WIPO) and the World Trade Organisation (WTO). In addition, the European Union has created additional laws aimed at achieving more effective protection of intellectual property. One part of them regulates the protection of trademarks, patents, and copyrights.

International agreements related to the protection of intellectual property, various license agreements for the use of authors' works, and their designations are briefly discussed in the secondary school curricula. In Table 1 and Table 2, we have summarized the topics related to cybersecurity, distributed by class, and the knowledge that should be acquired at the end of the training course.

Table 1. Cybersecurity knowledge in Bulgarian lower secondary education

GRADE	TOPICS	ACQUIRED KNOWLEDGE
3rd grade	Electronic communication and digital identity	Each student distinguishes between digital and physical identity. Knows the main threats when working in a digital environment and knows where to seek help.
	Safe and responsible online behaviour	Knows the basic rules and threats when working in a digital environment. He knows how to get help. Recognizes false information on the Internet.
4th grade	Information in modern society	Understands that digital resources may not be free to use, copy and distribute. Understands that not all information in the virtual space is reliable.
	Safety conditions in a digital environment	Does not provide personal data in a digital environment. Knows more known threats when working in a digital environment. Knows how to get help when needed. Knows ethical norms when working in an online environment.
5th grade	No topics related to cybersecurity issues	-
6th grade	Real-time communication tools. Rules for children's safety on the Internet	Describes real-time communication software settings for security purposes. Knows the possibilities of real-time communication on the Internet. Knows and follows the rules of safe behaviour on the Internet.
7th grade	Means and methods of information protection	Explains the nature of computer viruses. Explains and applies specific means and methods to protect information.

Table 2 presents the topics related to cybersecurity knowledge in Bulgarian upper secondary education.

Table 2. Cybersecurity knowledge in Bulgarian upper secondary education

GRADE	TOPICS	ACQUIRED KNOWLEDGE
8th grade	No topics related to cybersecurity issues	-
9th grade	Information security in a networked environment	Understands the risks associated with working in a networked environment and implements appropriate protection measures. Knows basic regulatory documents related to personal data protection, copyright (for programs and data), and electronic signature. Knows the principles, main ways, and means of protecting the network from unauthorized access. Sets access rights to resources on a local network. Research major security threats such as viruses, worms, and hacker attacks. Prioritizes threats. It searches the web and selects the best protections for each of the top three priority security threats.
10th grade	Assessing the validity and reliability of information	Understands information dissemination mechanisms and effective ways of searching in an online environment. Evaluates information received electronically for credibility and reliability. Filters e-mail messages to categorize them as spam. Research in which countries spam is declared illegal and punishable and what is the legal framework for it in Bulgaria.
	Technical and organizational security when working in a digital environment	Gives examples of problems that arise when working in a networked digital environment and possible solutions. It indicates ways of reliable digital identification when using public services. Knows the purpose of macros in office applications and knows how to manage their inclusion when using public services. Uses online tools to identify compromised networks. Identifies the presence of a macro in a document. Examines what biometric data is used for identification. Checks if a personal device offers biometric identification. Compares identification methods that can be used to use electronic banking.
11th grade	Security and data protection	Lists security and data protection risks. Describes basic methods and means of data protection. Describes basic data backup methods. Describes components of the main regulatory documents related to the ethical use and guarantee of privacy of personal data.
	Electronic communication and digital identity	Each student distinguishes between digital and physical identity. Knows the main threats when working in a digital environment and knows where to seek help.

Cybersecurity knowledge is the need for broad competence and practical skills of every student in the virtual educational space, even in the computer room, or in the classroom, regardless of the scope of the studied discipline and specialty. It means new in nature scientific qualification and competence, high responsibility, and demandingness.

CYBERSECURITY AT THE LEVEL OF HIGHER EDUCATION IN BULGARIA

The rapidly emerging digitalization and implementation of artificial intelligence combined with the generational characteristics of learners, increased international cooperation, and the desire to ensure equal access to education for all layers of society, have placed qualitatively new requirements on the nature and characteristics of teaching. Part of the answers to these challenges have been given through the opening of academic programs in distance learning, equipping halls, creating the necessary infrastructure, virtual libraries, etc. At the same time, the system proved to be understaffed and unprepared to meet the demands and expectations for innovative methods and forms of teaching. This necessitates the creation of a program for the training of teachers and professors in the field of ICT, who in turn train pupils and students with skills and attitudes for learning in an electronic environment. The lack of sufficiently qualified teachers in higher education institutions who possess digital skills corresponding to modern trends and requirements is the result of several factors. In the last decade, the increased demand for ICT personnel in the labour market has led to a great interest on the part of prospective students in these specialties and, accordingly, to the opening of the corresponding professional directions in many higher schools. At the same time, the system proved to be unprepared in terms of the required number of trained teachers. The likelihood that more graduate students will choose an academic career and become teachers is decreasing due to the high income that comes with working in the specialty in the real sector. Naturally, deficits in the higher education system affect the functioning of the preschool and school education system as well.

The improvement of the quality of higher education with a view to digital transformation is in accordance with the Law on Higher Education, the Strategy for the Development of Higher Education in the Republic of Bulgaria for the period 2021-2030, the policies for the development of state higher education institutions, the Conclusions of the Council of the EU on digital education in the European knowledge societies and the Rome Communiqué of the Ministers of the Member States of the Bologna Process.

Based on the conducted research, 67 key professions/positions were identified, as well as the basic and specific digital skills required for each one of them. They are divided into five categories, according to the European Digital Competence Framework DigComp 2.2: "Information and data literacy," "Digital communication and collaboration," "Digital content creation," "Safety," and "Problem-solving." In addition, we can say that training is increasingly closely related to digital skills. Retraining and acquiring new competencies is also unthinkable without digital knowledge and skills.

The system of higher education in Bulgaria includes 49 higher education institutions, 36 of which are public and 13 are private. Higher education institutions in Bulgaria are of three main types: universities, specialized higher education institutions, and independent colleges. They train students, doctoral students, and specialists. The higher education in Bulgaria is compatible with the European one and includes the following degrees:

- **Professional Bachelor in** ... – with the acquisition of no less than 180 credits and a minimum period of preparation of 3 years according to the curriculum;
- **Bachelor's** Degree – with the acquisition of no less than 240 credits and a minimum period of preparation of 4 years according to the curriculum;
- **Master's** Degree – with the acquisition of no less than 300 credits and with a study period of 5 years according to the curriculum or no less than one year after a "bachelor's" degree (60 credits), respectively, no less than two years after "Professional Bachelor of ..." (120 credits);
- **Doctor** – educational and scientific degree after the master's degree.

Training in each of the degrees is conducted in accordance with the Classifier of Higher Education Areas and Professional Fields. There are 9 areas of higher education divided into 52 professional

fields. Within the framework of academic autonomy, each higher education institution independently determines the professional areas and specialties in which it conducts training. The forms of education are regular, part-time, and distance learning.

The bachelor's degree is the main stage of higher education while master's programs offer an in-depth focus on a specific area. For this reason, the study is focused on undergraduate (Bachelor) studies.

The curricula in higher education institutions are built on the understanding that ICT skills are sufficiently formed in secondary school and can be the basis for the successful upgrading of specific skills. The observations show that the entry level of ICT with which first-year students enter is satisfactory and cannot be a good basis for a successful upgrade. The secondary school curricula are focused mainly on theoretical knowledge in the field, and practical performance tasks remain isolated from real-world situations. As a result, after exiting the specific learning content, ICT tasks cannot be recognized. In this situation, students choose to find and take a ready-made solution to the problem, which they present as their own because they do not have the necessary competence to perform the task and the requirements set for it. In this way, they do not actively participate in the individual stages of the process of building the information product and do not independently walk the path to the final decision. Their training remains at the level of an ordinary computer-literate user of information resources who uses technology at a superficial level.

The digital training of future specialists is an actual task for all levels of educational structures. It is a guarantor of adequate interaction between specialists and society. In order to form the components of digital competence – interactive use of technologies and didactic interpretation of the possibilities of ICT – higher education institutions should direct the training to a concrete deepening of the available knowledge and skills. For this purpose, it is necessary to diagnose the level of ICT knowledge and skills possessed by first-year students, to find out where the gaps are and the most frequently occurring errors. This diagnosis will guide the way in which ICT training should be conducted for first-year students. Realizing the potential of ICT requires students to have a basic level of preparation to recognize the basic activities they can perform with the computer. The students must be able to solve basic tasks that involve specific sequences of activities. They need to be able to name and explain the activities performed. This is a prerequisite for the manifestation of reflexive processes that have developing potential for learners.

We have found a wide variety of IT subjects studied in non-technical university specialties that cover fundamental aspects of ICT and build applied knowledge and skills related to information processing, communication, and some cybersecurity issues. Most of them are basic courses studied in the first or second year such as Information Technology, Information Systems, Informatics, Digital Technologies, Information Systems and Technologies, Information and Communication Technologies, etc. In some cases, the courses aim at both the formation of basic information and digital skills and competencies, as well as their orientation in a specific field, for example, the course "Information and Communication Technologies in Education and Work in a Digital Environment" in the major "Primary School Pedagogy," or "Digital Technologies in Agriculture" in the major "Agricultural Engineering," etc.

In Figure 2 and Figure 3, we have summarized the collected data from universities' websites related to the number of majors and the number of non-IT majors distributed by universities. We have focused our research on developing cybersecurity literacy in non-IT universities' specialties which becomes a compulsory element of the digital literacy of young people.

In Figure 2, a comparison of universities by number of bachelor programs studied in them is shown.

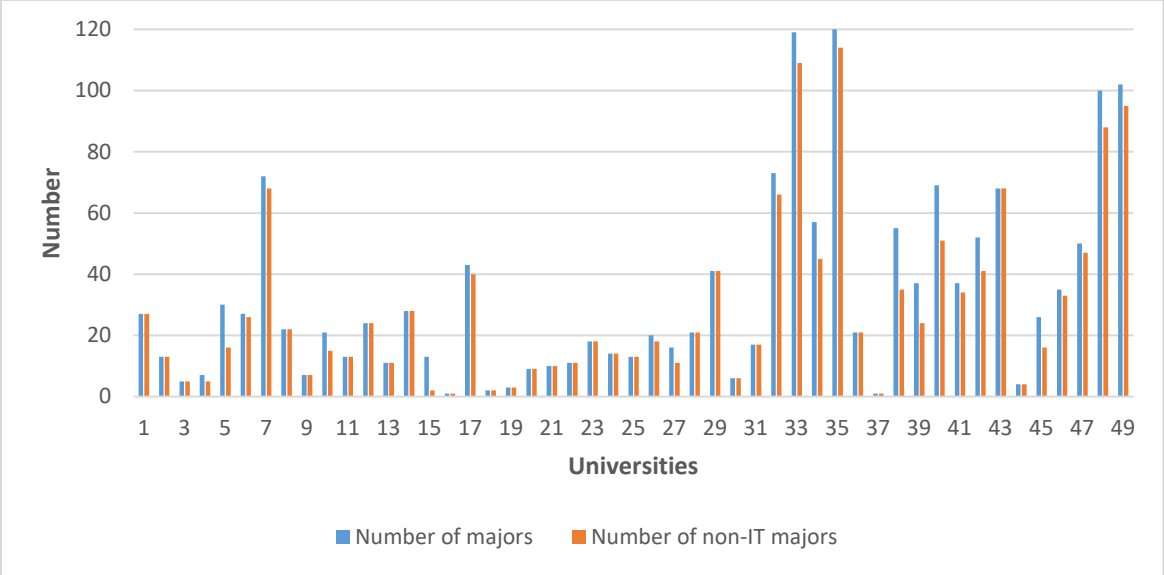

Figure 2. Comparison by number of majors and number of non-IT majors

Figure 3 presents a comparison of studying IT in non-IT specialties in 49 universities.

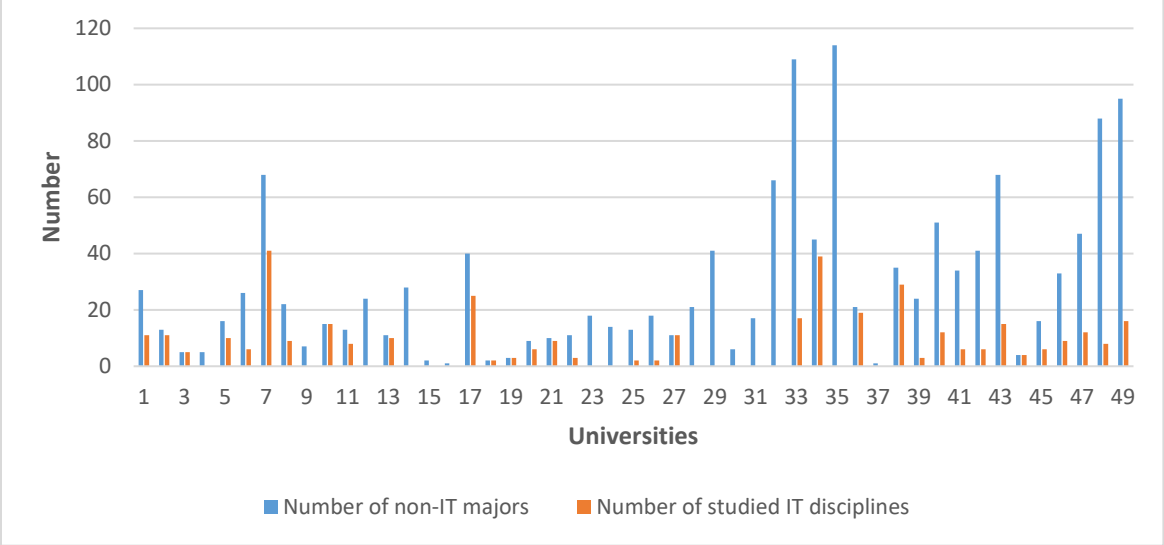

Figure 3. A comparison of studying IT in non-IT specialties

In the non-IT specialties of the different universities, IT is taught in the interval from 0 to 41 of the cases (grouped into 19 variants depending on the repetitions) in some universities.

Figure 4 shows a graph of the distribution of studied IT courses in non-IT specialties.

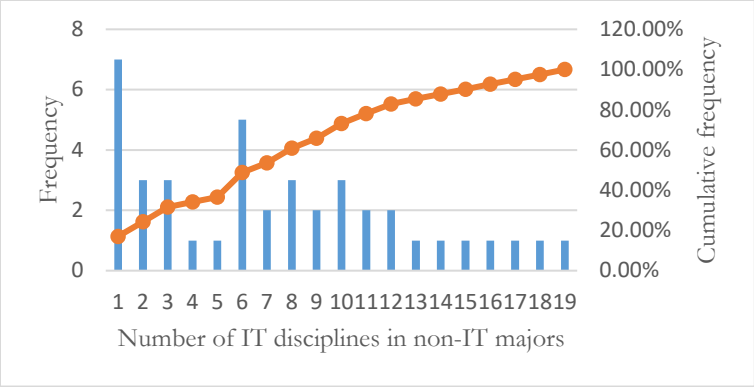

Figure 4. Combined distribution chart

The study covered 49 universities whose curricula were examined. At some of the universities, the curricula were not available, so the number of universities considered is 41. On average, 9.51 of the non-IT majors in these universities teach IT courses (mean = 9.51, standard error = 1.52, median = 8, mode = 0). In 7 universities, IT courses are not taught in non-IT majors (minimum = 0), and in one of the universities in 41 non-IT majors, IT courses are taught. On average, 9 courses are studied in non-IT majors at universities in Bulgaria related to the field of IT. One of the limitations of this study is that it is not possible to account for specific topics studied in IT subjects as in secondary school. These IT courses cover all areas of digital and cybersecurity literacy at different levels. More detailed research would require the examination not only of the specialty curricula but also of the content of studied courses.

CONCLUSION

The adaptation of students to the challenges of the digital society and new learning practices requires determining more effective ways to attract, encourage and motivate them in the direction of acquiring quality theoretical and practical-applied knowledge and skills for working with ICT. Access to computers and the Internet, and the ability to work with some basic software applications and tools do not always lead to the acquisition of digital competence by students; many of the young people who come to university do not have the necessary skills to use digital technologies, due to the fragmented and superficial use of information.

In this regard, the efforts of university teachers should be directed to support various appropriate ways of using ICT and interactive communication in the learning process, which can improve students' abilities for critical thinking, effective communication, and collaborative scientific problem-solving. An important place in this direction is the inclusion of students in various courses to increase their digital competence. The compulsory (not only optional) study courses represented in the curricula of various specialties are particularly suitable, which would provide the necessary knowledge and skills for using digital technologies.

The competencies related to data security and ensuring proper access to data are other components of data literacy. This raises a number of issues and challenges related to data ownership, privacy, and other sensitive areas of data access and transfer. Apparently, in the curricula of non-IT majors, information security does not occupy its important place, which is assigned to it by the current reality of an ever-increasing threat of cyber-attacks.

Attracting the students to additional short-term or long-term study courses (a paid form of study) can also contribute to the acquisition of important knowledge and skills that are not given enough space in the curricula. The holding of scientific seminars, the possibility of access to online lessons, e-textbooks, and other forms of increasing the digital competence of students, through which one can expect to develop a wide range of skills for searching, identification, critical evaluation, should

not be underestimated and use of information for a more independent and creative behavior in a digital environment.

In order to master these skills, solid basic training in ICT and cybersecurity is needed, which guarantees the permanent preservation of what has been learned and its transfer to different situations. The sequential passage through the stages of formation of digital competence and the activities involved in them, ensures the transformation of general concepts in the understanding of ICT in the educational process into concrete implementations of individual ideas, reflecting the place and role of ICT in the educational process. With a successful transition from basic ICT skills to digital and cybersecurity skills, the cognitive outlook of the students also changes.

This paper contributes to the body of knowledge by providing evidence that in the curricula of non-IT majors, information security does not occupy the important place that is assigned to it by the current reality of an ever-increasing threat of cyber-attacks.

ACKNOWLEDGMENT

This work has been supported by the project "Cybersecurity in practice for non-IT oriented HE courses" - Erasmus+ KA2 - KA220-HED - Cooperation partnerships in higher education 2021-1-TR01-KA220-HED-000031993.

REFERENCES

ACM/IEEE. (2020). *Computing curricula 2020: Paradigms for global computing education*. https://www.acm.org/binaries/content/assets/education/curricula-recommendations/cc2020.pdf

AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Choo, K-K. R. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. *Computers & Security*, *119*, 102754. https://doi.org/10.1016/j.cose.2022.102754

Al-Janabi, S., & Al-Shourbaji, I. (2016). A study of cyber security awareness in educational environment in the Middle East. *Journal of Information & Knowledge Management*, *15*(1), 1650007. https://doi.org/10.1142/S0219649216500076

Blažič, A. J. (2021). New approach in cybersecurity education – Introducing new practices and innovations. *Proceedings of the 13th International Conference on Education and New Learning Technologies*, 6619-6626. https://doi.org/10.21125/edulearn.2021.1340

Blažič, B. J. (2021). The cybersecurity labour shortage in Europe: Moving to a new concept for education and training. *Technology in Society*, *67*. https://doi.org/10.1016/j.techsoc.2021.101769

Catota, M., Morgan, M. G., & Sicker, D. C. (2019). Cybersecurity education in a developing nation: The Ecuadorian environment. *Journal of Cybersecurity*, *5*(1), 1-19. https://doi.org/10.1093/cybsec/tyz001

Conklin, W. A., Cline, R. E., & Roosa, T. (2014, January). Re-engineering cybersecurity education in the US: An analysis of the critical factors. *Proceedings of the 47th Hawaii International Conference on System Sciences*, *Waikoloa, HI, USA*, 2006-2014. https://doi.org/10.1109/HICSS.2014.254

Ekstrom, J., Lunt, B., Parrish, A., Raj, R., & Sobiesk, E. (2017). Information technology as a cyber science. *Proceedings of the 18th Annual Conference on Information Technology Education* (pp. 33–37). Association for Computing Machinery. https://doi.org/10.1145/3125659.3125697

European Commission. (2020a). *Europe 2020: A strategy for smart, sustainable and inclusive growth*. Publications Office of the European Union. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:2020:FIN:EN:PDF

European Commission. (2020b). *Digital Agenda for Europe 2020*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010DC0245R(01)&from=DA

European Commission. (2020c). *Digital Economy and Society Index (DESI) 2020*. https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2020

European Commission. (2020d). *Digital Education Action Plan (2021-2027).* https://bit.ly/3DlhVKc

European Commission. (2020e). *A Digital Single Market Strategy for Europe.* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015SC0100

European Commission. (2020f). *Strategic framework.* https://education.ec.europa.eu/about-eea/strategic-framework

European Union Agency for Cybersecurity (ENISA). (2018). *National cybersecurity strategies.* https://www.enisa.europa.eu/topics/national-cyber-security-strategies/

Eurydice (2001). *Information and communication technology in European Education Systems.* http://www.sel-gipes.com/uploads/1/2/3/3/12332890/2001_eurydice_-_icteurope.edu.pdf

Ferrari, A. (2014). *DIGCOMP: A framework for developing and understanding digital competence in Europe.* http://www.openeducationeuropa.eu/nl/elearning_papers

Hristova, T. (2017). Always connected: Digital skills among the students. *Postmodernism Problems*, *7*(3), 297-332.

Ghomi, M., & Redecker, C. (2019, May). Digital competence of educators (DigCompEdu): Development and evaluation of a self-assessment instrument for teachers' digital competence. In *CSEDU (1)* (pp. 541-548).

Kampylis, P., Punie, Y., & Devine, J. (2015). Promoting effective digital-age learning: A European framework for digitally-competent educational organisations. *EUR 27599 EN*, Publications Office of the European Union, Luxembourg.

McGettrick, A. (2013). Towards effective cybersecurity education. *IEEE Security and Privacy, 11*(6), 66-68. https://doi.org/10.1109/MSP.2013.155

Moallem, A. (2019). Cyber security awareness among college students. In T. Ahram, & D. Nicholson (Eds.), *Advances in human factors in cybersecurity* (pp. 79-87). Springer. https://doi.org/10.1007/978-3-319-94782-2_8

National Programme Digital Bulgaria. (2019). https://www.mtc.government.bg/sites/default/files/uploads/it/09-12-2019_programa_-cifrova_bulgariya_2025.pdf

NISE (2017). National Initiative for Cybersecurity Education, National Cybersecurity Workforce Framework. https://www.nist.gov/file/359261

Parrish, A., Impagliazzo, J., Raj, R., Santos, H., Asghar M., Josang A., Pereira, T., & Stavrou, E. (2018). Global perspectives on cybersecurity education for 2030: A case for a meta-discipline. *ITiCSE 2018 Companion: Proceedings Companion of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education* (pp. 36–54). Association for Computing Machinery. https://doi.org/10.1145/3293881.3295778

Pencheva, D., Hallett, J., & Rashid, A. (2020). Bringing cyber to school: Integrating cybersecurity into secondary school education. *IEEE Security & Privacy*, *18*(2), 68-74. https://doi.org/10.1109/MSEC.2020.2969409

Pre-School and School Education Act. (2016). https://lll.mon.bg/uploaded_files/ZAKON_za_preducilisnoto_i_ucilisnoto_obrazovanie_EN.pdf

Redecker, C. (2017). *European framework for the digital competence of educators: DigCompEdu*. Publications Office of the European Union, Luxembourg. https://doi.org/10.2760/159770

Ruiz, R. (2019, January). A study of the UK undergraduate computer science curriculum: A vision of cybersecurity. *Proceedings of the IEEE 12th International Conference on Global Security, Safety and Sustainability, London*, UK, 1-8. https://doi.org/10.1109/ICGS3.2019.8688137

Slusky, L., & Partow-Navid, P. (2012). Students information security practices and awareness. *Journal of Information Privacy and Security*, *8*(4), 3-26. https://doi.org/10.1080/15536548.2012.10845664

Socrates Programme. (2000-2006). MINERVA sectoral programme. https://eur-lex.europa.eu/EN/legal-content/summary/socrates-phase-ii.html

Strategy for Effective Application of Information and Communication Technologies in Education and Science of the Republic of Bulgaria. (2014-2020). https://www.stragetybg.

Task Group on Information Technology Curricula. (2017). *Information technology curricula 2017: Curriculum guidelines for baccalaureate degree programs in information technology*. Association for Computing Machinery. https://doi.org/10.1145/3173161

Terziev, V., & Lyubcheva, M. (2020). Internal and external challenges in front of the higher education. *Business Management*. https://dlib.uni-svishtov.bg/bitstream/handle/10610/4400/8b5ed1997a218758d3a5ffa13e3f0c3e.pdf?sequence=1

The Institute of Information Security Professionals. (2010). *IISP Skills Framework*. https://apmg-international.com/sites/default/files/documents/products/iisp_skills_framework_v1_0.pdf

Trifonova, M. (2018). Digital-pedagogical competencies (strategy - from a consumer to a creative-proactive user). *Education*, *VIII*(8), 10-17.

Vuorikari, R., Kluzer, S., & Punie, Y. (2022). *DigComp 2.2, the Digital Competence Framework for Citizens - With new examples of knowledge, skills and attitudes*. Publications Office of the European Union. https://doi.org/10.2760/490274

AUTHORS

Svetlana Syarova is a Chief Assistant Professor in the Computer Science Department at the University of Library Studies and Information Technologies. In 2022, she obtained her PhD degree from ULSIT in Automated Systems for Information Processing and Management. Her publications and main research interests are in the field of Cybersecurity, Informing Science, and Data Science.

Stefka Toleva-Stoimenova is an Associate Professor in the Computer Science Department at the University of Library Studies and Information Technologies. She obtained her MSc degree in Industrial Automation from the Faculty of Automation and System Design, Technical University – Sofia. In 2011, she obtained her PhD degree from ULSIT in Automated Systems for Information Processing and Management. Her publications and main research interests are in the field of Informatics, Informing Science, and Data Science.