I.J. Modern Education and Computer Science, **2021, 6, 60-68**
Published Online December 2021 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijmecs.2021.06.06

Increasing Teacher Competence in Cybersecurity Using the EU Security Frameworks

Ievgeniia Kuzminykh
Department of Informatics, King's College London, London, WC2B 4BG, UK
Department of Infocommunication Engineering, Kharkiv National University of Radio Electronics, Kharkiv, Ukraine
E-mail: ievgeniia.kuzminykh@kcl.ac.uk

Maryna Yevdokymenko, Oleksandra Yeremenko and Oleksandr Lemeshko
Department of Infocommunication Engineering, Kharkiv National University of Radio Electronics, Kharkiv, 6100, Ukraine
E-mail: {marina.ievdokymenko, oleksandra.yeremenko}@nure.ua

Received: 10 April 2021; Revised: 29 June 2021; Accepted: 15 September 2021; Published: 08 December 2021

Abstract: A study was undertaken to identify the missing skill and expertise of teachers and other stakeholders in the field of EU cyber security regulatory documents and frameworks. In order to increase the knowledge in this area and promote the EU security frameworks the model for the continuous building of teacher competence has been proposed and planned to be implemented in Ukraine. The proposed model will contribute towards improving the excellence of educators and academics, as well as increase competitiveness of educational programmes on cybersecurity among similar institutions in the EU countries. Various studies focused on the development of competence of the students to prepare them for the job market and build a comprehensive portfolio, education-business partnerships and collaboration. However, the issue of developing teacher expertise to achieve high quality of education remains open. We highlighted the importance of creating a cybersecurity ecosystem through the cooperation with different stakeholders and by implementing the model for continuous development of teacher competence.

Before building the model the overview and analysis of different teacher professional development approaches were conducted. Analysis showed that for our goal the best suitable approach is a model that consists of two stages based on self-education and group education approaches with 7 processes inside. The study revealed that competence may be achieved through a number of activities which may be grouped under four generic categories: student and staff training, academic and business seminars, business-oriented roundtable debates, and research. The model uses as main methods of achieving a better quality of education in cybersecurity the development of new training courses and modernization of educational programs, and for raising awareness among businesses and regulatory bodies - the workshops and roundtables.

Index Terms: Teacher competence, Professional development, Cybersecurity framework, Group training, Self-education.

1. Introduction

Recent years witnessed an increasing number of high-level cyberattacks targeting Ukrainian state agencies, critical infrastructure and the private sector as stated in the conflict report of the Center for Security Studies [1]. One of the most publicized incidents took place in 2015, when a cyberattack deactivated a power grid providing electricity for 225,000 people in western Ukraine; as part of the attack, hackers also sabotaged the power distribution equipment through a DDoS attack on a call centre, which further delayed the restoration of power supply. Further, in 2017, the attack of the NotPetya malware affected not just Ukraine, its intended victim, but went out to numerous machines around the world, from hospitals in Pennsylvania to a chocolate factory in Tasmania. After political and territorial changes in 2014, the problem of the information security in Ukraine sharply increased, as Ukraine became a platform for a Cyber and Information warfare that had the society-wide effects on the Ukrainian society, politics, economy, technology, and international relations [2]. Cyber espionage, targeted attacks on grid systems, ransomware that covered the attack of collecting personal data, and weak security of web sites caused the leakage of information and defacement. According to a report by the Centre for Security Studies [1], the average economic damage is estimated to be US$22,000 per minute of website unavailability and the average estimated duration of these attacks was 54 minutes.

All that cyberattacks highlighted weakness of the Ukrainian cyberspace and lack of cyber security experts. The need for strong international cooperation and capacity building to address cybersecurity needs, strengthening of the legal framework for cybersecurity is now a top priority for Ukraine [3]. These needs were highlighted in the set of legal documents of Ukraine [4] related to security provision: National Security Strategy; Cybersecurity Strategy of Ukraine; Law of Ukraine "On the Basic Principles of Ensuring the Cyber Security of Ukraine".

The experience of EU in the legalisation of cybersecurity standards and best practices as highlighted in the report of European Court of Auditors [5] could help Ukraine to achieve a higher cybersecurity safety level and be able to withstand the constant attacks against its cyberspace that further affect countries all over the world, as it was the case with the NotPetya ransomware that affected multinational companies such as the as Danish shipping operator Maersk, the US pharmaceutical producer Merck, the European branch of TNT Express, the French construction company Saint-Gobain, the food producer Mondelēz, and the Reckitt Benckiser manufacturing company. In line with these efforts, the EU is developing a suite of European cybersecurity standards that aim to deter and respond to cyber-attacks which constitute an external threat to the EU and its partner states by producing practices and guidelines on how to implement and enhance security, how to prevent cybersecurity attacks, and provide cybersecurity hygiene. The European Cyber Security Organisation (ECSO), the European Union Agency for Cybersecurity (ENISA), the IoT Security Foundation, and the Council of the EU are the leading organisations for providing businesses, companies, and individuals with best practices in area of the security. Collectively, such organizations provide frameworks for exchanging cybersecurity information between stakeholders as well as establish regulatory documents such as the EU Cybersecurity plan to protect open Internet and online freedom and opportunity [6], NIS (National Information Security) directives, Principles for Internet of Things Security [7], Standards in support of the Cybersecurity Certification, and many others.

While they represent the emerging common practice, there is an issue with their promotion and dissemination in Ukraine. Such frameworks and regulatory documents are relatively new for the Ukrainian businesses and individuals, and learning of this topic is not included in the Ukrainian HEI educational cybersecurity programmes. There were number of attempts and initiatives aimed to help the Ukrainian universities in implementing the lifelong learning [8-10] and developing a training environment [11-13] similar to the EU principles through a series of international projects, but they were typically limited to technical subjects linked to the area of cybersecurity. The research of Ukrainian scientists mostly focused on specific threats and attacks in narrow areas as malware [14] and Internet of things [15,16], and the researches itself is technical in nature [17,18]. However, from a wider perspective, cybersecurity is not limited to network, information security, and technical protection, but also encompasses the need to educate the young generation of experts in cyber security. From an implementation perspective, this requires improving the quality of higher education through the EU internationalization agenda [19], to provide training assisted by the business sector, to apply and be aware of new protection and prediction methods against cyberattacks by developing new and innovative education programmes.

In our work we propose a model of continuous integration of the EU cybersecurity frameworks into the education process of Ukraine. The purpose of the model is to build the necessary competence in cybersecurity by promoting and disseminating the European expertise and good practice in cybersecurity to the business sector, legal regulatory bodies, and government institutions of Ukraine, as well as to the scientific and educational institutions. The implementation of such European practices will allow to:

- Improve the content of the education, quality and efficiency of expert's trainings.
- Develop and implement the educational programs compatible with EU universities.
- Develop the university-enterprise cooperation.
- Provide the measures for the improvement of staff qualifications.
- Establish a consortium for integration of the university-led research into the European and world research space through joint scientific programs.

Moreover, this model can be adopted by other countries and institutes that suffer from the lack of cybersecurity expertise.

The remainder of the paper is structured as follows: first we discuss related works and existing approaches in building teacher competence, then we propose the model of increasing teacher competence for strengthen the cybersecurity expertise and discuss the benefits of the proposed model.

2. Problem Statement and Related Works

There are several approaches of building the competence of teachers and, accordingly, their quality of teaching. The level of expertise and professionalism of the teacher plays a decisive role in determining the quality of the education system since it supports and guides teachers' continuous professional development and affects the level of achievement and academic performance of students, as reported in [20, 21]. A wide range of teacher professional development approaches are reported on in the literature [22] and several studies have provided various classification systems [23, 24]. In general, three approaches can be used for formation of professional competence:

(1) Training in groups.
(2) Individual training.
(3) Self-education.

Before we consider each of the approaches of building competence, it should be noted that, in addition to professional competence, the process requires the establishment of teacher pedagogical competence. Both factors affect the quality of and effectiveness of teaching and the level of the education system, as showed by [21, 25] but require different process to achieve satisfactory expertise. Professional competence refers to the content of information presented by the teacher while pedagogical competence refers to the way in which the teacher delivers this information, through a lesson study [26, 27], didactics [28], video clips [29], simulation [30], experimental study [31], or other activities. In our work, we will focus on strengthening the professional competence through the replenishment of knowledge and its subsequent dissemination.

The training in groups approach focuses on delivering a face-to-face training program to university teachers. It is the most widespread approach and popular among different professional developing programs. A significant proportion of the international programmes fostering exchange of the experience and capacity building in higher education relies on this approach by providing training of secondary and higher education instructors. The results of the projects under such programmes are later reflected in the publications showing success of group teacher training. The project described by [32] included a training program for teachers divided in two stages: an online training package associated with a number of general points (in the case focusing on the Global Teacher Key Competency Framework) and face-to-face training that each participant should attend after completing first stage. The authors within the other studies [33-35] highlighted the importance of continuous feedback with trainees on the content and their experience to facilitate participant learning, also reenforced by results of Teaching and Learning International Survey [36,37]. The approach undertaken by the participants of the project [38] for raising teacher competence in cybersecurity was to provide a series of training sessions, workshops, summer schools, coupled with the deployment of a virtual environment for teaching and learning tasks.

Individual training improves teacher expertise in one particular area [39] and is more inherent to the teacher internship programs at the enterprise, requires mentoring from the trainer side and individual support. This approach can be used to align the teacher competence frameworks to 21st century challenges related to digital transformation [40]. The authors in [41] tackling the digital revolution challenge in education system and highlight the need to rely on stakeholders' agreement on what shapes quality teachers (policymakers, technology businesses). The training from stakeholders might be conducted for establishing and strengthening the understanding of a specific application, tool, environment, or case study. Individual training could be carried out through the assistance of more mature teacher to gain expertise, so called teaching assistant model analysed in [42]. This study showed that regardless the easiness of implementation of teaching assistant model and good way for professional growth, it has series of shortcomings as a limited communication with mentor (only during in class activity), lack of feedback, not effective workload separation. Brevik et al. in [43] showed how a small private online course integrates professional competence and responds to challenges by transforming teachers into opportunities for their professional development. Carlsson et al. in [11] delivered an individual training programme on how to install and run a virtual laboratory for cybersecurity and, in parallel, they supported the attending teachers with the deployment of their own laboratory exercises.

Self-education is an important factor of teaching expertise growth. According to the EU initiative [44] on increasing the quality of teaching and learning and improvement the support for the profession, the process of developing teacher competence can stimulate engagement in their professional development. Several reports [36,37] highlighted that many teachers do not find suitable professional development and feel that they require more than they currently receive. Therefore, it is necessary to establish a framework of systematic programmes to assess the learning needs of teachers, which can take various forms of feedback, surveys, followed by provisioning of relevant individualised training. A considerable proportion of teachers stated that they cannot attend professional development due to conflicting work schedules; for such a category the most suitable approach for building a competence would be self-education.

Given the fact that acquired knowledge is indelible, teachers can enhance their proficiency through reading, watching, or listening materials relevant to their subject of interest. Self-education is part of the teaching and learning scholarship that stands to grounding teacher in discipline-specific and pedagogic knowledge and research, through engagement with the literature, analysing teaching through critical reflection on learning of students and, as a result, further develop teaching material and scholarship of teaching and learning (SoTL) [45-47].

Since many studies focused on the development of competence of the students to prepare them for the job market [48-50] and build a comprehensive portfolio [51], the issue of developing teacher expertise remains open. The authors [50,52-54] highlighted the importance of creating a cybersecurity ecosystem through the cooperation with local businesses, industries, and educational institutions to successfully achieve the competency-based education in computer science. Fig. 1 shows the cybersecurity ecosystem that consists of multiple players, all of whom either participate in or influence the way the field develops and/or operates [53]. As natural ecosystems, the cybersecurity ecosystem consists of a variety of diverse participants that located on macro- and micro-levels that interact for multiple purposes. Key

macro stakeholders include governments, regulators, policy makers, and standards-setting organizations and bodies (such as the International Organization for Standardization, the Internet Engineering Group, and the National Institute of Standards and Technology). Key micro stakeholders include end users, consumers, governments, private companies, corporations, SMEs, financial institutions and security consultants who micro-connect other players. All for those players collaborates and work together to enhance the security posture of the state, nations and the globe.

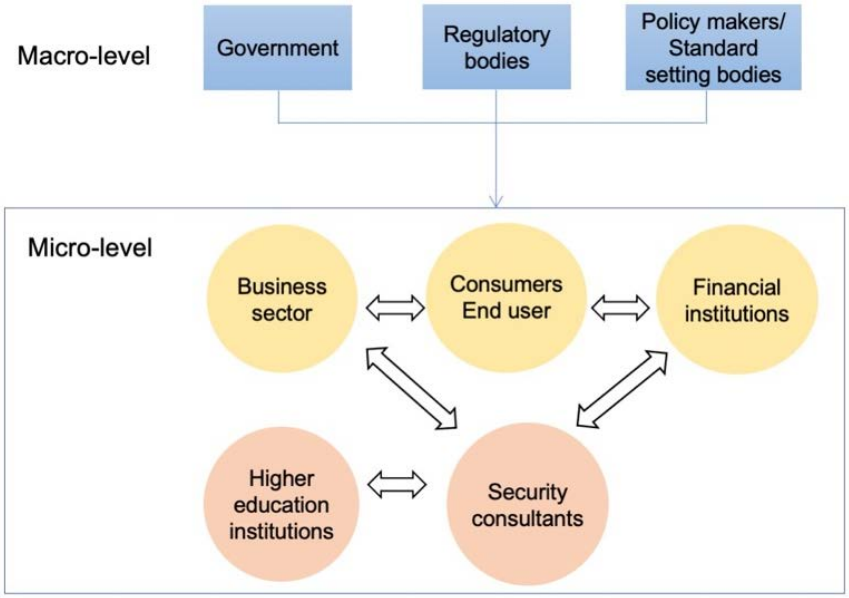

Fig.1. Cybersecurity ecosystem.

In our paper we propose to engender the teacher professional competence through a series of complex methods, including self-education, group training, and involving businesses for testing the replication of EU standards in the Ukrainian environment.

3. Methods of Formation the Cybersecurity Competence

Given the purpose of the study and the requirements for model implementation stated at the end of introduction section, we propose next two approaches to strengthen the cybersecurity expertise through the promotion and dissemination of the EU security frameworks:

(1) develop an in-depth understanding of the EU cybersecurity context;
(2) deliver a series of cybersecurity training courses.

The first option involves studying the strategic documentation and cybersecurity approaches of the EU Frameworks for Exchanging Cybersecurity Information (FESI) and actively encourage the academic staff and students to participate in the study with the aim of promoting the European values and popularization of such frameworks in Ukraine. The second alternative aims to develop and deliver a new training course on the EU frameworks for exchanging cybersecurity information and/or modernize existing courses expanding the content with EU cybersecurity policies and best practices. The combination of the two methods leads to a continuous cybersecurity competence formation model and is presented on Fig. 2.

The process starts with understanding the context of cybersecurity information exchange in Europe and the self-education of the trainers who subsequently share and impart the knowledge with target groups, including higher education institutions, business sector and government regulatory bodies. Self-education is one of the forms of achieving professional competence according to a report from European Commission [44] which highlights that, in the absence of mentors, there are no opportunities for achieving competence through other forms as group or individual training. The next stage includes the design of education material that could be delivered to target groups. The sharing of knowledge will be achieved through the training stage, which is the core, defining stage of the model. The test stage includes the evaluation of the delivered material through feedback from the trainees as well as from business sector following dissemination or sharing events, including seminars, workshops and roundtables. Analysis of the obtained feedback will foster the improvement of the content of the courses for the next delivery cycle in this continuous model, aiding the process of cybersecurity competence building and improving the perception and understanding of the business sector, as well as initiating discussions about the challenges and ways of implementing the EU standards in

Ukraine. By implementing the EU cybersecurity policies in the Duplicate stage, the companies enhance the quality of IoT and ICT products and services and, in future, foster the standardization process in line with the EU standards.

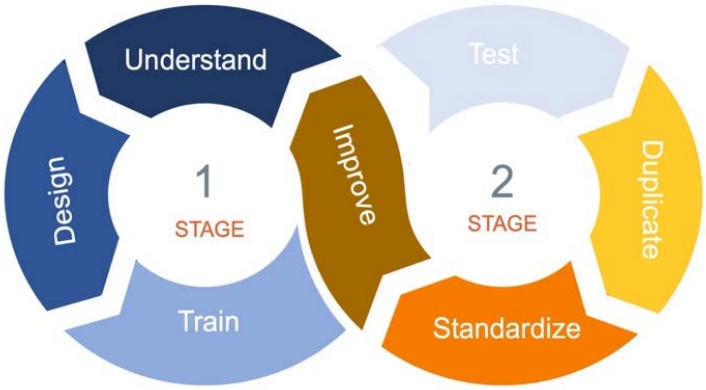

Fig.2. Framework for cybersecurity competence formation.

The model of continuous integration of EU cybersecurity practices during each of the stages includes the activities presented in Fig. 3.

Competence formation may be achieved through a number of activities, which may be grouped under four generic categories: HEI student and staff cybersecurity training, academic and business staff cybersecurity seminars, business-oriented roundtable debates, and research on the current state of awareness of the target groups (teachers, students and companies) about EU frameworks for the information exchange in cybersecurity and EU cybersecurity policies. Each of the four categories focuses on a different type of information dissemination/sharing. The training aims to prime the process in order to ensure the next generation is sufficiently prepared. The seminars provide an opportunity for dissemination directed at the commercial sector, in parallel with roundtables to ensure that the views of businesses are taken into account. Finally, the research continuously evaluates and improves the process to ensure an optimal process.

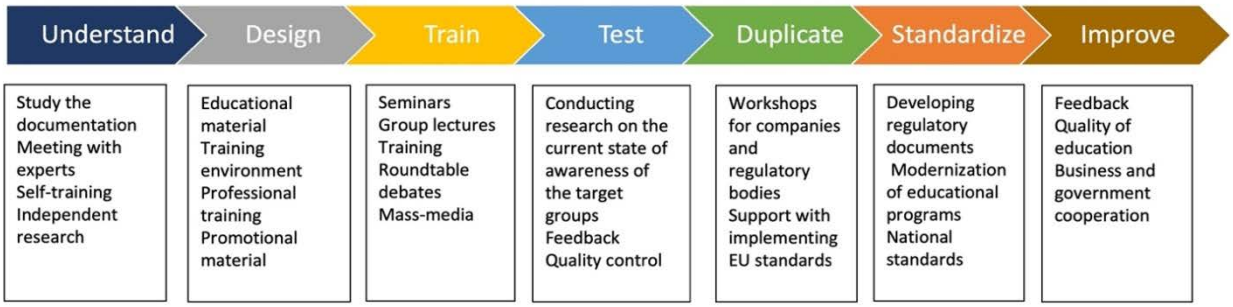

Fig.3. Activities under each stage of the model.

Beyond the technical requirements, in order to successfully enhance cybersecurity competence, the society needs to strengthen the informative and methodological basis about EU cybersecurity frameworks in Ukraine, identify enforcing organisations within the EU regulatory framework, design a methodology for replicating the principles, organisational structures, and best practices of FESI into the business sector, regulatory, and government bodies of Ukraine, as well as develop courses about EU practices in cybersecurity and integrating into the educational process of the universities of Ukraine.

4. Discussion: Benefits of Proposed Model for Formation of Competence

The continuous model of cybersecurity competence formation across all sectors and levels of society is essential, given the growing global cybersecurity skills shortfall. The main benefit of implementing this model will be awareness raising of the EU best practices and foster future involvement and dialogue between beneficiaries in Ukraine. As stated in [44], [3] there is an increasing need for developing and delivering new training courses about EU frameworks for exchanging cybersecurity information for students, teachers and representatives of civil society actors, politicians, civil servants, education and media representatives at various levels.

In this context, development of new curriculum and modernization of existing courses should be based on analysing challenges in cybersecurity area in countries of European Union and Ukraine and getting feedback from industry, public and government stakeholders on skills and knowledge demand on integration EU cybersecurity frameworks in Ukraine.

The involvement of young researchers entails the effective and sustainable dissemination of European cybersecurity practices. The implementation of the above-mentioned self-training and independent research in the field of European FESI can be strengthened by attracting external experts in this field that will foster internships with European universities and exchanging experience on the international conferences.

Awareness raising and implementing the framework for the cybersecurity competence formation in Ukraine according to the EU standard has three direct beneficiaries: HEIs, teachers and students, and the wider business sector. The developed and modernized courses implemented within the HEI curricula will increase quality of education and internationalization of the educational program in cybersecurity by introducing new courses that align the university context to the European values and allow building awareness of EU cybersecurity framework and best practices in Ukraine. The students attending the training courses on EU frameworks for exchanging cybersecurity information and cybersecurity policies will significantly improve their prospects for education, internships or employment, both in Ukraine and abroad. The completion of such courses will allow the students to acquire competence in the field of European integration, standardization and following cybersecurity good practice, which can subsequently be used to support their future careers.

The academic staff will strengthen their skills through self-education, exchange of expertise and ideas during conferences, seminars, debates, and meetings with the companies and the cybersecurity regulatory bodies. It will contribute to their continuous professional development and will give the young researchers the opportunity to understand the European direction, values and studies that will lead to more active citizenship.

For the business sector, raising awareness about the EU cybersecurity policies will facilitate future cooperation between companies and security regulatory bodies in Ukraine, as well as enhance the quality of their products and services through the implementation of EU cybersecurity policy. Following consensus from the participating companies, the process will also lead to future standardization of IoT and ICT products and services according to EU standards. For businesses, the security and certification of the products, services and processes become the significant important areas both in European countries and all over the world.

5. Conclusions

Technologies are opening up a whole new world of opportunities, with new products and services becoming integral parts of our daily lives. Beyond their benefits, the ubiquity and pervasiveness of IT systems information exchange also increase the risk of cyberattack, the societal and economic impact of which continues to mount. To counteract this expanding threat, the EU countries accelerate efforts to strengthen cybersecurity by developing cybersecurity framework including policies and regulatory documents. While in EU they are embedded in the overall evolution of the educational and regulatory framework, such policies are relatively new for the Ukrainian businesses and individuals, and their promotion is not included in the Ukrainian HEI's programmes. policy makers, educators and academics

The proposed model for cybersecurity competence formation will contribute towards improving the excellence of educators and academics in the Ukrainian HEIs and increase competitiveness of educational programmes on cybersecurity and ICT among similar HEIs in the EU countries by introducing new courses that align the university context to the European values.

The dissemination of knowledge on the first stage of the model will build the necessary critical mass for future development and ensure the Europeanization of studies in higher education, as well as provide the necessary knowledge and experience for consulting companies, policy makers and government agencies for effective integration at the regional and national levels.

The companies will be able to raise awareness about the EU cybersecurity policies through the series of open lectures and roundtables, which, in turn, will be facilitating future cooperation between the businesses and the security regulatory bodies in Ukraine, will enhance the quality of IoT and ICT products and services, and, in future, foster the standardization process in line with the EU standards.

Acknowledgment

This work was supported by the Erasmus + under Jean Monnet Grant for project "Integrating the EU cybersecurity framework and policies in Ukraine", No.621250-EPP-1-2020-1-UA–EPPJMO–MODULE.

References

[1] M. Baezner, "Cyber and Information warfare in the Ukrainian conflict", report, Center for Security Studies (CSS), ETH Zürich, 2018.

[2] A. Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hacker*, Doubleday, 2019.

[3] L. Streltsov, "The System of Cybersecurity in Ukraine: Principles, Actors, Challenges, Accomplishments", *Eur. J. Sec. Research*, Vol.2, pp. 147–184, 2017, https://doi.org/10.1007/s41125-017-0020-x.

[4] V. Roller, S. Gogonyants, I. Koropatnik, "Legal background of cyber defence in Ukraine", *J. Scie. Papers Social Dev.and Sec.*, Vol. 9, No.4, p. 74, 2019. https://doi.org/10.33445/sds.2019.9.4.5.

[5] European Court of Auditors**,** "Challenges to effective EU cybersecurity policy", briefing paper, 2019, https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf.

[6] European Commission, "EU Cybersecurity plan to protect open internet and online freedom and opportunity", press release, 2013, https://ec.europa.eu/commission/presscorner/detail/en/IP_13_94.

[7] IoT security foundation (IoTSF), "Establishing principles for internet of things security", brochure, 2015, https://www.iotsecurityfoundation.org/wp-content/uploads/2015/09/IoTSF-Establishing-Principles-for-IoT-Security-Download.pdf

[8] T. Strelkova, O. Lemeshko, M. Yevdokymenko, O. Yeremenko, I. Kuzminykh, "Experience of adaptation and organization of Distance Learning in Ukrainian Universities", in *Handbook of Research on Inequities in Online Education During Global Crises*, L. Kyei-Blankson, J. Blankson, E. Ntuli, Eds. IGI Global, 2021, unpublished.

[9] O. Sukhodolia, "Implementation of the Concept of Critical Infrastructure Protection in Ukraine: Achievements and Challenges", *Inf. & Sec.: Int.J.*, Vol.40, No.2, pp. 107-119, 2018, https://doi.org/10.11610/isij.4008.

[10] D. G. Bobro, S.P. Ivanyuta, S.I. Kondratov, O.M. Sukhodolya, *Organizational and Legal Aspects of Security and Resilience of Critical Infrastructure of Ukraine*. Kyiv: NISS, 2019.

[11] A. Carlsson, I. Kuzminykh, R. Gustavsson, "Virtual Security Labs Supporting Distance Education in ReSeLa Framework", in *The Challenges of the Digital Transformation in Education*, M. Auer, T. Tsiatsos, Eds. Springer: Cham, 2019, pp. 577-587.

[12] O. Lemeshko, O. Yeremenko, M. Yevdokymenko, I. Kuzminykh, "Features of designing the virtual laboratory in cybersecurity for distance learning", *New Collegium*, Vol.3, pp.41-45, 2020.

[13] O. Yeremenko, M. Yevdokymenko, I. Kuzminykh, A. Kruhlova, "Cybersecurity Virtual Laboratory for distance learning", poster in 7th ACM Celebration of Women in Computing: womENcourage, 24-27 September, 2020, Baku, Azerbaijan.

[14] A. Adamov, A. Carlsson, & T. Surmacz, "An Analysis of LockerGoga Ransomware", in *2019 IEEE East-West Design & Test Symposium (EWDTS)*, Batumi, Georgia, 2019, https://doi.org/10.1109/EWDTS.2019.8884472.

[15] I. Kuzminykh, A. Carlsson, "Analysis of Assets for Threat Risk Model in Avatar-Oriented IoT Architecture", in *Internet of Things, Smart Spaces, and Next Generation Networks and Systems*, O. Galinina, S. Andreev, S. Balandin, Y. Koucheryavy, Eds. Springer: Cham, 2018, pp. 52-63, https://doi:10.1007/978-3-030-01168-0_6.

[16] I. Kuzminykh, B. Ghita, J.M. Such, "The Challenges with Internet of Things for Business", arXiv:2012.03589 [cs.CR], 2020, unpublished.

[17] Y. Kuzminykh, M. Fliustikova, "Mechanisms of ensuring security in Keystone service", *Problemi telekomunìkacìj*, Vol.2 No.25, pp.78-96, 2019, https://doi.org/10.30837/pt.2019.2.06.

[18] M. TajDini, V. Sokolov, I. Kuzminykh, S. Shiaeles, & B. Ghita, "Wireless Sensors for Brain Activity – A Survey", *Electronics*, Vol.9 No.12, 2092, 2020, https://doi.org/10.3390/electronics9122092.

[19] M. Yemini, J. Hermoni, V. Holzmann, L. Shokty, W. Jayusi, N. Natur, "The implementation of internationalisation in Israeli teacher training colleges", *Eur J Educ.*, Vol.2017, No. 52, pp. 546–557, 2017, https://doi.org/10.1111/ejed.12239.

[20] V. Kumar, "The Influence of Teacher's Professional Competence on Students' Achievement", *IOSR Journal of Engineering*, Vol. 3, No.11, pp. 12-18, 2013.

[21] Liakopoulou, M. "The Professional Competence of Teachers: Which qualities, attitudes, skills and knowledge contribute to a teacher's effectiveness?", *Int. J. Human and Soc Scie*, Vol.1, No.21, pp.67-78, 2011.

[22] R. R. Bodine, P. L. Slot, P. P.M. Leseman, "Increasing teachers' intercultural competences in teacher preparation programs and through professional development: A review", *Teaching and Teacher Edu*, Vol. 98, 103236, 2021.

[23] H. Parkhouse, C.Y. Lu, V.R. Massaro, "Multicultural education professional development: A review of the literature", *Review of Edu. Research*, Vol. 89, pp.416-458, 2019, https://doi.org/10.3102/0034654319840359.

[24] S. Civitillo, L.P. Juang, M.K. Schachner, "Challenging beliefs about cultural diversity in education: A synthesis and critical review of trainings with pre-service teachers", *Edu. Research Rev*, Vol. 24, pp. 67-83, 2018.

[25] L. Moghtadaie, & M. Taji, "Explaining the requirements for teacher's development based on professional competencies approach", *Edu. Research and Reviews*, Vol.13 No.14, pp. 564-569, 2018, https://doi.org/10.5897/ERR2018.3583.

[26] S. Aimah, S. Ifadah, M. D. A. Bharati, "Building Teacher's Pedagogical Competence and Teaching Improvement through Lesson Study", *Arab World English J.*, Vol.8, No.1, pp. 66-78, 2017, https://doi.org/10.24093/awej/vol8no1.6.

[27] G. Næsheim-Bjørkvik, N. Helgevold, S. Østrem, "Lesson Study as a professional tool to strengthen collaborative enquiry in mentoring sessions in Initial Teacher Education", *Eur. J. Teacher Edu*, Vol.42, No.5, pp. 557-573, 2019.

[28] L. Mata, "Experimental research regarding the development of methodological competences in beginning teachers", *Procedia - Social and Behavioral Sciences*, Vol.29, pp.1895 – 1904, 2011.

[29] P. T. Thu Khine, H. P. P. Win, T. M. Naing, "Towards Implementation of Blended Teaching Approaches for Higher Education in Myanmar", *Int. J. Edu and Management Eng*, Vol.11, No.1, pp. 19-27, 2021.

[30] M. Osaci, " Numerical Simulation Methods of Electromagnetic Field in Higher Education: Didactic Application with Graphical Interface for FDTD Method ", *Int. J Modern Edu and Comp Sci*, Vol.10, No.8, pp. 1-10, 2018.

[31] S. Taber Keith, "Experimental research into teaching innovations: responding to methodological and ethical challenges", *Studies in Scie. Edu*, Vol.55 No. 1, pp. 69-119, 2019, https://doi.org/10.1080/03057267.2019.1658058.
[32] L. R. Betts, B. Huntington, L. ‐ S. Iao, G. V. Dillon, T. Baguley, P. Banyard, "Developing a competency ‐ based education training programme for university tutors", *J Competency-based Edu*, Vol.4, No.4, e01200, 2019.
[33] C. Sturgis, "Reaching the tipping point: Insights on advancing competency education in New England", Competency Work report, 2016, https://files.eric.ed.gov/fulltext/ED590523.pdf.
[34] S. Tharayil, M. Borrego, M. Prince, K. A. Nguyen, P. Shekhar, C. J. Finelli, & C. Waters, "Strategies to mitigate student resistance to active learning", *Int. J. STEM Edu*, Vol.5 No.7. 2018, https://doi.org/10.1186/s40594-018-0102-y.
[35] V. Symeonidis, "Teacher competence frameworks in Hungary: A case study on the continuum of teacher learning", *Eur.J. Edu.*, Vol.54, No.4, pp. 400–412, 2019, https://doi.org/10.1111/ejed.12347.
[36] TALIS 2018 Results, "Teachers and School Leaders as Lifelong Learners", The OECD Teaching and Learning International Survey, Vol.1, 2019, https://www.oecd-ilibrary.org/education/talis-2018-results-volume-i_1d0bc92a-en.
[37] TALIS 2018 Results, "Teachers and School Leaders as Valued Professionals", The OECD Teaching and Learning International Survey, Vol. 2, 2020, http://www.oecd.org/education/talis-2018-results-volume-ii-19cf08df-en.htm.
[38] Educating the Next generation experts in Cyber Security (ENGENSEC): the new EU-recognized Master's program, project, (2017), http://engensec.eu/about-the-project/.
[39] E. Villegas-Reimers, "Factors to consider when planning, implementing and assessing the professional development of teachers", Chapter V in *Teacher professional development: an international review of the literature*, UNESCO: International Institute for Educational Planning, 2003.
[40] M. Binkley, O. Erstad, J. Hermna, S. Raizen, M. Ripley, M. Miller ‐ Ricci, M. Rumble, "Defining twenty ‐ first century skills", in *Assessment and teaching of 21st century skills*, P. Griffin, E. Care, B. McGaw, Eds. Dordrecht, The Netherlands: Springer, 2012.
[41] F. Caena, C. Redecker, "Aligning teacher competence frameworks to 21st century challenges: The case for the European Digital Competence Framework for Educators (DigcompeDu)", *Eur. J. Edu.*, Vol. 54, pp.356–369, 2019.
[42] M. Baeten, M. Simons, W. Schelfhout, R. Pinxten, "Team teaching during field experiences in teacher education: Exploring the assistant teaching model", *Eur. J. Teacher Edu.*, Vol.41, No.3, pp.377-397, 2018.
[43] L.M. Brevik, G. B. Gudmundsdottir, A. Lund, T. Aanesland Strømme, "Transformative agency in teacher education: Fostering professional digital competence", *Teaching and Teacher Edu.*, Vol. 86, 102875, 2019, https://doi.org/10.1016/j.tate.2019.07.005.
[44] European Commission, "Supporting teacher competence development for better learning outcomes", report, 2013, https://ec.europa.eu/assets/eac/education/policy/school/doc/teachercomp_en.pdf.
[45] E. Boyer, *Scholarship reconsidered: Priorities of the professoriate*, San Francisco, CA: Jossey-Bass, 1990.
[46] J. Fanghanel, J. Pritchard, J. Potter, & G. Wisker, "Defining and supporting the scholarship of teaching and learning (SoTL): A sector-wide study", advanceHE project report, York: HE Academy, (2016), https://www.advance-he.ac.uk/knowledge-hub/defining-and-supporting-scholarship-teaching-and-learning-sotl-sector-wide-study.
[47] J. Glaesser, "Competence in educational theory and practice: a critical discussion", *Oxford Review of Education*, Vol.45, No.1, pp. 70-85, 2019. https://doi.org/10.1080/03054985.2018.1493987.
[48] A. Baumgartner, C. Müller, R. Fengler, F. Javet, "Development of application ‐ oriented competency frameworks: Empirical findings from the validation of such a framework by means of an employer survey", *J. Competency-based Edu.*, Vol. 3 No.4, e01177, 2018, https ://doi.org/10.1002/cbe2.1177.
[49] O. Zlatkin-Troitschanskaia, H.A. Pant, C. Lautenbach, D. Molerov, M. Toepper, S. Brückner, *Modeling and Measuring Competencies in Higher Education: Approaches to Challenges in Higher Education Policy and Practice*, Springer VS: Wiesbaden, 2017, https://doi.org/10.1007/978-3-658-15486-8.
[50] M. Hagan ‐ Short, P. Addison, "Competency ‐ based education: Multiple approaches ‐ a single institution", *J. Competency-based Edu.*, Vol.4, No. 3, e01194, 2019, https://doi.org/10.1002/cbe2.1194.
[51] E. G. Gutsu, E. V. Kochetova, & I. V. Ivanova, "Modern methods of implementation of competent approach in the system of professional training of university teachers", *Vestnik Mininskogo universiteta*, Vol.4, No.8, p.27, 2014.
[52] O. Lemeshko, M. Yevdokymenko, O. Yeremenko, I. Kuzminykh, "Cyber Resilience and Fault Tolerance of Artificial Intelligence Systems: EU Standards, Guidelines, and Reports", in *CEUR Workshop Proceedings* (CPITS'20), Vol. 2746, pp.99-108, 2020.
[53] R. Arun, "The Cyber Security Ecosystem: Collaborate or Collaborate: It's Your Choice", 2015 [Online]: http://www.circleid.com/posts/20151013_cyber_security_ecosystem_collaborate_or_collaborate_your_choice/.
[54] S. Riley, "Cyber Hygiene & Attack Analysis Methodology", CISO Central, 2020 [Online]: https://www.ciso-central.org/organisation/cyber-hygiene-attack-analysis.

Authors' Profiles

Ievgeniia Kuzminykh received her PhD in telecommunications in 2013 from Kharkiv National University of Radio Electronics, Ukraine where she is currently a Visiting Associate Professor. From 2017 to 2020, she was a Senior Lecturer with the computer science department in Blekinge Institute of Technology, Sweden. From August 2020 she is Lecturer in Cybersecurity with King's College London. She has coauthored over 40 publications. Her research interests include cybersecurity, IoT, security aspects of cloud and networks.

Maryna Yevdokymenko received her PhD in telecommunications in 2010 from Kharkiv National University of Radio Electronics, Ukraine where she is currently an Associate Professor. From 2016 to 2019, she was a visiting Lecturer with the computer science department in Blekinge Institute of Technology, Sweden. She has coauthored over 100 publications. Her research interests include Cybersecurity, Network Security, Network Resilience, Fault-Tolerant Routing, Quality of Service, Quality of Experience, IoT, and Cloud Computing.

Oleksandra Yeremenko received her PhD in telecommunications in 2008, and DrSc in telecommunications in 2018 from Kharkiv National University of Radio Electronics, Ukraine where she is currently a Professor. She has coauthored over 180 publications. Her research interests include Future Networks, Future Internet, Quality of Service, Network Resilience, Flow-based Networking, Fault-Tolerant Routing, Network Security, Software-Defined Networking, and Cloud Computing.

Oleksandr Lemeshko received his PhD in arms and military equipment in 1999 from Kharkiv Institute of the Air Force, and DrSc in telecommunications in 2005 from Kharkiv National University of Radio Electronics. He is currently a Head of the V.V. Popovskyy Department of Infocommunication Engineering at the Kharkiv National University of Radio Electronics. He has coauthored over 340 publications. His research interests include Traffic Management, Optimization in Telecommunications, Wireless Networks, Routing, Traffic Engineering, Quality of Service, Quality of Experience, Hierarchical Routing, Network Security, Network Resilience, and Fault-Tolerant Routing.

How to cite this paper: Ievgeniia Kuzminykh, Maryna Yevdokymenko, Oleksandra Yeremenko, Oleksandr Lemeshko, " Increasing Teacher Competence in Cybersecurity Using the EU Security Frameworks", International Journal of Modern Education and Computer Science(IJMECS), Vol.13, No.6, pp. 60-68, 2021.DOI: 10.5815/ijmecs.2021.06.06