The Introduction of Ethics into Cybersecurity Curricula

Lyudmyla Adaryukova[1][0000-0002-0159-976X], Oleksii Bychkov[2][0000-0002-9378-9535], Kateryna Merkulova[2][0000-0001-6347-519], Alla Skyrda[1][0000-0001-8254-7592]

[1] Donetsk national technical university, 85300 Donetsk region, Pokrovsk, Ukraine
[2] Taras Shevchenko national university of Kyiv, 02000 Kyiv, Ukraine
l.b.adaryukova@gmail.com, bos.knu@gmail.com,
kate.don11@gmail.com, alla.skyrda@ukr.net

Abstract. The article is devoted to the analysis of the problem of teaching professional ethics to future cybersecurity specialists. It is stated that professional tasks of cybersecurity specialists nowadays cannot always be solved using the identified procedures and guidelines. The dilemmas that arise are not always supported by the corresponding laws, rules or codified standards due to the much faster development of the technological basis compared to the legislative support of the professional activity. Thus, the cybersecurity specialists can face unpredictable problems that can require ethical awareness. The article analyses three international educational efforts in creating educational standards for the cybersecurity course: the National Initiative for Cybersecurity Education (NICE), the Cyber Education Project (CEP), Cybersecurity Curricula 2017 and the role of ethics in each. As well as that, the article looks at the national educational standard for this course and the international experience of embedding ethics into cybersecurity curricula, suggesting that the introduction of the ethical component into the national educational programmes would benefit the educational process.

Keywords: Cybersecurity Curricula, Cybersecurity Ethics, Ethical Awareness.

1 Introduction

1.1 Problem Statement

It is estimated that the population of the Internet doubles every 100 days, a bigger part of our lives being transferred into the cyberspace. All spheres of our everyday and professional lifestyles depend on the security of the private information in the cyberspace. Nowadays people have started talking not only about the IT revolution, but about a more important question - according to some researchers – how to survive this IT revolution [1]. Information technology has broken some records in the speed of its development, while other systems that are closely connected with this layer of the human activity – e.g. education, law – struggle to keep up with the speed of its change and development. That is why there is an ever-growing gap between the demand and supply in cybersecurity: demand in highly qualified professionals (it is estimated that the shortage in skilled workers is about 1.5 million in 2019 [2]) and the possibilities of educational institutions to ‘produce’ them; demand in strict legislative framework (like in the medical sphere) and the currently available legal support and protection, which is far from being sufficient.

The security of information in the cyberspace nowadays is not only about solving technical and technological problems, as all the solutions in the sphere of cybersecurity depend on people. That is why it is urgent to talk about the role and importance of a human factor in protecting this asset, especially when there are no regulations according to which it is easy to act. In this context we believe that it is necessary for educational establishments to develop ethical awareness in students future cybersecurity specialists, as ethics can help them make urgent decisions in unprepared and unpredictable situations, not described in the textbooks or standardized codes of conduct.

Ukrainian higher educational establishments have introduced cybersecurity educational courses only recently. To meet the international standards of these educational programs and the demands of the industry it is essential to examine the theoretical grounds of cybersecurity specialists’ professional education as well as the experience of foreign higher educational establishments in introducing all vital aspects, professional ethics in particular, into the curriculum. The analysis and further adaptation of their experience to the national context will result in the increase of the efficiency of the national cybersecurity academic programmes and higher levels of professional awareness of cybersecurity graduates.

1.2 Related Work

The research into the adequacy of the cybersecurity needs and the ability of educational systems to meet them has been conducted internationally for rather a long period of time. One of such efforts to examine various formal and informal cybersecurity educational attempts was carried out in 2013 and resulted in a substantial ‘Report on EU practice for cyber security education’ [3]. By comparing some cybersecurity programmes in the USA, the UK, China, Brazil, India, Canada, Australia, Russia and other countries the authors make conclusions on different levels of cybersecurity education development and readiness of educational establishments to meet the needs of the industry in these countries. It is noted that in some countries, like the USA, there is a strong link between the cybersecurity education and military and security institutions, which enhances this professional training efficiency. Whereas in some countries (as of 2013, in India, for example) there is no formal study programme on cybersecurity. The report suggests key initiatives to help develop educational programmes that should be considered with a view to making the professional training more effective and addressing current and future issues.

To assess the state of Ukrainian higher cybersecurity education it is necessary to examine the experience of educationalists in other countries. A number of efforts have been made in order to evaluate the state of cybersecurity education in different countries on their national levels. Lehto [4] devoted the research to the assessment of the state of cybersecurity educational and research systems at various educational establishment of Finland. The conclusion he has made is that, although the national and international requirements are being met at Finnish universities, there is still the lack of clear vision of the skills and competencies involved. Catota et al. [5] look into the problems of cybersecurity education in Ecuador and state the presence of few attempts to introduce cybersecurity at universities, which are limited by poor technical resources, absence of coordination between education and business. The research suggests a range of options to be taken to improve this situation. These works show that the situation in cybersecurity education of Ukraine is not unique regarding the existing challenges, presenting at the same time some valuable information on educationalists' attempts to overcome those obstacles.

Another aspect of importance for the present research is the attempts to develop cybersecurity curricula. These issues are discussed by Santos et al. [6], the gravest being the absence of unanimity concerning the notions, standards and methods associated with cybersecurity. The authors identify the proposals for institutions that can assist with the development of the cybersecurity programmes. A substantial research has been done by Mouheb et al. [7] into the efforts of advanced countries to frame cybersecurity curricula at the levels of the government and organizations. Those curriculum designs are divided into three categories: education, industry, government/defense. The researchers determine their strong points alongside with their own suggestions in order to help educationalists develop more efficient cybersecurity curricula.

Cybersecurity education in Ukraine has been the object of research from different points of view. Thus, Danyk Yu. and Zinchenko A. [8] devote their efforts to the analysis of cybersecurity education peculiarities. They suggest introducing cybersecurity education at all stages of the national educational system, beginning with preschool, identifying the need of our country to raise the general level of cybersecurity awareness in the society. Diorditsa I. [9] looks into the issues of higher cybersecurity education from the point of view of administrative and legal regulation. The author identifies the problems of educational standards determination, low level of readiness of educational establishments to train cybersecurity professionals. So, researchers examine many aspects that must be taken into account while developing cybersecurity curricula. However, the importance of teaching ethics to cybersecurity students and its incorporation into the curriculum has not been in the focus of educationalists' attention.

Thus, **the aim of this article** is to ground the role of ethics in the formation of a cybersecurity professional, review national and international attempts of creating cybersecurity curricula and introducing ethics into them, as well as analyse the international experience of teaching ethics to cybersecurity students in order to meet the national needs of their professional education.

2 The Importance of Ethics in Cybersecurity Education to Face the Challenges of Future Professional Activities

2.1 The Notions of Law and Ethics in Cybersecurity

In the context of ever-growing threats despite ever-growing cyber protection funding it is of great importance to deal with the phenomena of Cyber Law and Cyber Ethics. First of all, to gain a deeper understanding of the issue, we should identify the difference between the notions of Law and Ethics. According to Merriam-Webster dictionary, a law is ‘a binding custom or practice of a community : a rule of conduct or action prescribed ... or formally recognized as binding or enforced by a controlling authority’ [10]; while ethics is ‘a set of moral principles; a theory or system of moral values’ [11].

Thus, with laws we must have an authority (external control) controlling how people obey them, whereas with ethics the control has the internal character. Another extremely important difference is the legally determined punishment that is always present in case of the failure to abide by the law and which is not present in case of the failure to ‘behave ethically’.

Another important aspect when talking about Law and Ethics in cybersecurity is the fact that they are definitely interconnected: ethics makes the basis for laws. And, although the ethics is a ‘vague’ phenomenon compared to the legislation of a particular sphere, it is sometimes the only tool that the professionals have in order to solve the problems where laws cannot be applied [1]. Many researchers attempting to analyse the state of legal protection of cyber space mention the inadequate level of legislative support of cyberspace activities on the national and international levels. The cases where there are no laws are quite common. Moreover, many researchers notice that even if there are corresponding laws and criminal responsibility for breaking these laws, still the cases of prosecution are rare, which results in no deterrent value of such laws. ‘In comparison to other federal crimes, CFAA (Computer fraud and abuse act) offenses are not charged frequently and prosecuting someone engaged [in] computer security research is extremely rare’ [12].

2.2 The Legislative Support of the National Cybersecurity Activities

The situation in Ukraine is even more confusing. The draft of the bill of Ukraine ‘On the basics of providing the cybersecurity of Ukraine’ was proposed in 2015. It took Verkhovna Rada 2 years to pass this law and it became law only on May, 9, 2018. Researchers [13] argue that it could have taken even longer but for virus Petya in summer 2017, which was the first in the history of Ukraine massive cyber attack to affect the whole country. The problem with this law on cybersecurity is, apart from the inadequacy of the content made up in 2015 and the current situation, the declarative character of the law [13]. It gives the definitions of the basic terms and phenomena in the sphere of cybersecurity, which are at the same time new to the legislation of Ukraine. It also states that the violation of laws in the sphere of cybersecurity presupposes civil, administrative and criminal responsibility. However, none of these codes mentions ‘cyberspace’ in any form or context. For example, the criminal code of Ukraine presupposes responsibility for the crimes connected with the use of electronic computing machines (computers), systems and computer networks and electrical communication networks. But there is no mentioning of a ‘cyberspace’ or the responsibility for a ‘cyber crime’. This definitely complicates the situation with prosecuting cases identified as cyberattacks. In addition, the law does not presuppose any responsibility at all for posts or other kinds of activity in social networks, blogs, etc.

In this context the cybersecurity professionals often appear in unpredictable situations with the necessity ‘to make crucial decisions in the midst of professional practice, often with little guidance’ [14]. The researchers also emphasize that there is no codified framework of ethics in the realm of cybersecurity, unlike in other spheres. There is no agreement on common ethical principles. To top it all – many educationalists still think that it is impossible to provide a universal ethical framework [15]. The researchers believe that ‘it is imperative that cybersecurity professionals are educated in a way that cultivates and develops wide-ranging capacities, skills, and dispositions that will prepare them to recognize and cope with the ethical and technological conundrums before them’ [14].

We agree with the authors that with such indefinite situation with legal support and general vagueness of understanding what is ethical and what is not, the educational establishments have to teach the students future cybersecurity specialists the basics of ethics, develop ethical awareness and skills to apply ethical principles in their future professional practices. However, we strongly believe that these efforts must be guided by the standardized guidelines.

2.3 The International Educational Efforts on Creating Cybersecurity Standards

General Overview of International Cybersecurity Curriculum Attempts. We believe it will be useful to give a short overview of the latest attempts to define the academic parameters of cybersecurity.

The National Centers of Academic Excellence (CAE) with the initiative of National Security Agency created and introduced the first programme in the USA in 1998. On its basis the content of academic programmes of a cybersecurity discipline was identified. On the other hand, the research was being done from the point of view of the workforce demands. The National Institute for Standards and Technology initiated the workforce-based effort called the National Initiative for Cybersecurity Education (NICE). This led to the formation of the workforce-based framework of 7 job categories, 33 speciality areas and 52 work roles. Next, in 2013 the Cyber Education Project (CEP) was formed, which resulted in the formation of the joint task force of the Association for Computing Machinery, IEEE Computer Society, International Federation for Information Processing, and Association for Information Systems to do further research into the curricular needs of the cybersecurity. The result of the joint task force was Cybersecurity Curricula 2017, which presents the curriculum guidelines for post-secondary degree programmes in cybersecurity. According to Sobel Ann et al.

[16] it ‘builds on the content defined by the CAE program but offers a broader, more flexible view, with many different selections and arrangements of topics to reflect different emphases consistent with different types of jobs and career paths’. We agree that in order to make the educational process most efficient, it is necessary to have standards, which will make the basis for learning outcomes and contents of different programmes in cybersecurity.

The Presence of Ethics in the International Cybersecurity Curriculum Attempts. It is important for our research to identify how ethical questions in training cybersecurity specialists are addressed in all these efforts.

According to NICE Cybersecurity Workforce Framework, the professional ethics is included in the knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy; and in the knowledge of ethical hacking principles and techniques. We agree with Blanken-Webb et al. [14] that, although knowledge of laws is extremely important for the professional activities of cybersecurity specialists, it should be only one element of teaching ethics to students. It is vital to train the skills of analyzing the situation based on this knowledge. As the authors put it: ‘memorizing relevant laws and codes of ethics is not ethics education. Or, at the very least, it is not the kind of ethics education that will prepare the urgently needed decision makers of tomorrow in the realm of cybersecurity’ [14]. We agree that although it is definite that the knowledge of basic rules and national and international laws is important, the innovative character of the professional activity of future cybersecurity specialists calls for the innovative approach in teaching ethics. Some rules and guidelines can be applicable to some situations, as we understand that the general ethical practices have been more or less the same for centuries. However, the context created by cybertechnologies is unique, meaning that decisions made by the professionals in this sphere are also unique and impossible to have been predicted. ‘These are precisely the kinds of ethical questions that cannot be decided by social convention because there are no absolute rules and practices that precisely apply’ [17].

Among the knowledge units of CAE, one of the non-technical core units is Policy, Legal, Ethics and Compliance (PLE) and one of the optional knowledge units is Cybersecurity Ethics (CSE). The intent of the Policy, Legal, Ethics, and Compliance Knowledge Unit is ‘to provide students with and understanding of information assurance in context and the rules and guidelines that control them’ [18]. The outcomes should be the knowledge of the applicable laws and policies related to cyber defence and the ability to describe the major components of each pertaining to the storage and transmission of data; the knowledge of the responsibilities related to the handling of data as it pertains to legal, ethical and/or agency auditing issues; the knowledge of the interconnection between the type of legal dispute (civil, criminal, private) and the evidence used to resolve it [18]. However, as mentioned above, we believe that it is not enough for teaching ethics in cybersecurity because, on the one hand, it is really hard to talk about laws and rules with the constantly changing technical platform of cybersecurity, and, on the other hand, teaching ethics is not only about learning laws, rules and knowing your responsibilities; it is more about bringing up some deeper understanding and confidence in the moral dilemmas. Closer to solving these problems, the way we see it, is an optional knowledge unit Cybersecurity Ethics, which intends to provide the students with an understanding of ethics in a cyber context, to examine typical situations where ethical dilemmas arise and to provide the students with tools for ethical decision making. The examination of diverse ethical dilemmas, the analysis of practices that can cause ethical conflicts, the understanding of the role of cybersecurity in supporting and encouraging ethics can provide the students with ethic-based decision tools. So, we consider this knowledge unit an important element of any cybersecurity programme.

Finally, the result of the joint task force presents the curriculum guidance in cybersecurity education Cybersecurity Curricula 2017 [19]. The authors pay more attention to the ethical issues in the education of future cybersecurity specialists, including the ethics in the definition of the cybersecurity discipline: ‘A computing-based discipline involving technology, people, information, and processes to enable assured operations in the context of adversaries. It involves the creation, operation, analysis, and testing of secure computer systems. It is an interdisciplinary course of study, including aspects of law, policy, human factors, ethics, and risk management’ [19]. The authors explain that academic programmes are ‘informed by the interdisciplinary content’, which involves ethics among other mentioned aspects, and ‘driven by the needs and perspectives of the computing discipline that forms the programmatic foundation’ [19]. From the very definition we see that ethics in this case is not only about knowing and following laws and rules. The authors underline that each cybersecurity curriculum must have a ‘strong emphasis on ethical conduct … associated with the field’ [19]. So, the issues of ethics are incorporated in most knowledge areas. The curricular content for each knowledge area includes the essentials, knowledge units and the topics. The essentials, according to the authors, ‘across the knowledge areas capture the cybersecurity proficiency that every student needs to achieve regardless of program focus’ [19]. Cyber ethics is one of the essentials (societal essentials) and also one of the knowledge units within the knowledge area ‘Societal security’, which aims ‘to give students a foundation for both understanding and applying moral reasoning models to addressing current and emerging ethical dilemmas on an individual and group (professional) level’ [19]. It also opens the discussion about the unique or general character of ethics in computing, as well as the connection of the national culture and ethical practices. Talking about law and ethics, the authors point out the constant character of ethical values and evolving character of laws. Thus, we can see that cybersecurity ethics is incorporated in all knowledge areas to a greater or a lesser extent. The authors make a lot of effort to emphasize the axiological character of this aspect of the students’ future professional activity. They claim that teaching ethics is not only about learning rules and codes, it is more about responsibility, values, culture, which should be represented in any cybersecurity programme. We agree with the authors and believe that these curriculum guidelines should be the basis for Ukrainian educationalists while developing national cybersecurity educational programmes.

2.4 The National Educational Effort on Creating the Cybersecurity Standard

We believe that the analysis and research of the currently working curriculum guidelines can give useful experience of writing educational programmes for the national higher education. Unfortunately, we must admit that in our country the formal basis is quite often behind the needs of the educational process. Thus, the speciality 'Cybersecurity' appeared according to the resolution of the Cabinet of Ministers of April, 29, 2015 N266 'On the approval of the list of knowledge areas and specialities of higher education' [20]. And only 3 years later, the Decree of the Ministry of Education and Science of Ukraine of October, 4, 2018 approved the standard of higher education on speciality 125 'Cybersecurity' (bachelor degree) [21]. Before the approval of the standard there was a situation when different higher educational establishments understood the aims of this course differently, sometimes even not differentiating a cybersecurity specialist training from the training of many other IT specialists.

Having looked at the national educational standard of this speciality, we can state that there is no mentioning of the notion of the current research – professional cybersecurity ethics or other ethical issues. The closest in the understanding of professional ethical behaviour, in our opinion, are the following competences:

General competence N6: The ability to realize the rights and duties of a member of the society, be aware of the values of the civil (free democratic) society and the necessity of its sustainable development, the rule of law, rights and freedoms of a person and citizen of Ukraine. The corresponding learning outcome is to understand the values of the civil (free democratic) society and the necessity of its sustainable development, the rule of law, rights and freedoms of a person and citizen of Ukraine. We believe that professional ethics is one of the values of the civil society. However, the clarification would be much appreciated.

Professional competence N1: The ability to use the legislative and normative legal basis, as well as the national and international requirements, practices and standards with the aim of performing professional activity in the sphere of information and/or cybersecurity. The corresponding learning outcome is to act according to the legislative and normative legal basis of Ukraine, as well as the requirements of the corresponding standards, including international ones, in the sphere of information and/or cybersecurity. However, as we have mentioned above, we believe that the professional activity based on the knowledge of and the ability to use the corresponding laws, requirements, standards and procedures is not always possible due to the insufficient character of the legislative basis.

2.5 The International Experience of Introducing Emphasis on Ethics into Cybersecurity Curricula

In our opinion, to improve the national educational practices in the most efficient way it is necessary to examine the international experience of introducing ethics education into cybersecurity programmes. We have analysed several examples of such practices [14, 22] and noticed that first and foremost in these attempts, according to the authors, is the necessity to familiarise students with basic ethical theories that can help to develop their ethical awareness by viewing the dilemma from different perspectives.

The authors [22] argue that this will provide deeper understanding of the ethical principles students base their judgements on, as quite often they have only intuitive understanding of what is right and what is wrong. Moreover, these theories should help them understand that although the Internet might have started as a ‘lawless jungle’ [23] and the underlying technology is constantly changing, it still has some principles that have always been guiding the development of the humankind. The educationalists suggest that it is possible to present three basic ethical frameworks close to the Western philosophical tradition: deontological ethics, utilitarianism and virtue ethics. The knowledge about these theories should definitely help students to understand the notion of ethical value.

We believe it will be beneficial to present here a short description of these ethical theories (Fig. 1).

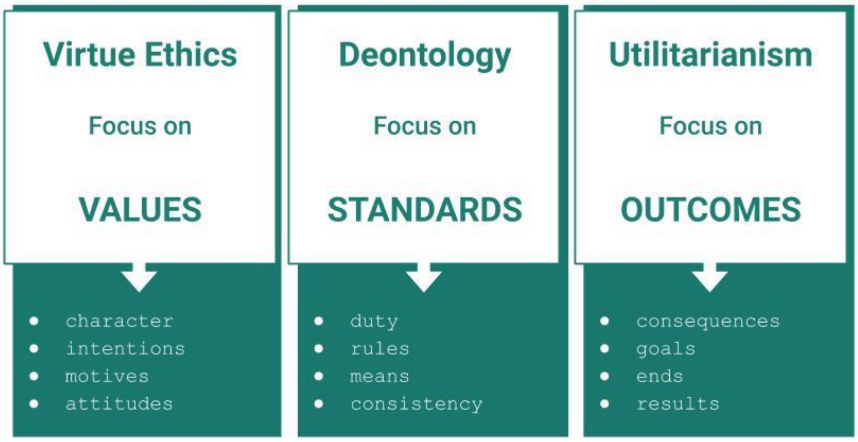

Fig. 1. Comparison of ethical traditions.

The focus of deontological ethics is the motives of a person, the choice of actions based on what a person ought to do, on their duty or obligation. To understand what is your duty you need to, according to Kant, be guided by the Categorical Imperative, to treat others as you would like them to treat you [22]. So, with this approach the moral value of events and actions are more important than the consequences. In contrast, utilitarianism centres on consequences, results and outcomes. The action is assessed on how good its result is regardless the motives, thus viewing the actions that result in good outcomes as having moral value. And good in this ethical framework is identified as what brings about happiness to as many people as possible. The researchers [23] illustrate the difference of these ethical approaches in solving the following ethical problems: when the outcome of the case is the creation of the efficient autonomous transportation system, the collection of data and experimenting with the help of artificial intelligence applications may be sufficiently justified. However, in medicine the trials and experimentation are impossible to justify by the consequences and outcomes they will have for the humanity. The end does not justify the means.

Virtue ethics looks at the person as an agent, at their character, meaning that ‘if a person is virtuous, then his or her actions are thought to be ethical’ [22]. As for the ‘list’ of virtues that a person or a cybersecurity professional must have, there is, of course, no ultimate variant. However, the researchers [23] emphasize the danger of treating cybersecurity situations as belonging to a different world, thus trapping into a dualistic world view that can easily ‘open the door for double morality’ [23]. They illustrate their viewpoint by saying that it would be strange to behave morally acceptably at home but to steal or break the law in any other way in the cyberspace using another identity. Among the universal virtues the authors mention integrity, compassion, care, reliability, respect, generosity, etc.

Of course, the students are familiar with these ethical theories: they have definitely heard the ‘Golden rule’ of ethics, they understand that they must try to predict the consequences of their actions, they know that they must perform their duty and that the happiness of other people should be the logical outcome of their (professional) activity, as well as everybody will say that it is good to be reliable and generous but bad to be disrespectful or careless. However, the researchers believe that it still is necessary to introduce these or some other ethical theories to understand how students perceive them, how they incorporate these ethical codes into their belief systems. Moreover, this theoretical knowledge helps to ‘separate technological features from their ethical implications, thereby preparing students to examine security issues’ [22].

Another important feature of introducing the theoretical ethical dimension into the educational process of future cybersecurity specialists is the fact that it is impossible simply to justify what is right and what is wrong and not mention the development of an agent of this or that action. So, formation of skill and knowledge of ethical reasoning is the first step of a cybersecurity educational programme, the second step being the cultivation of ‘dispositions to utilize these skills well’ [14]. The development of the culture of dialogue and cooperation, understanding your own and other people’s accountability for the outcomes of any actions and learning from the previous ethical cases will result in the growing of the community, which some researchers [14] consider the aim of the embedding ethics into cybersecurity curriculum. We agree with these authors that the development of a specialist’s personality in the result of exposure to theoretical and practical ethical issues should be the most important outcome of any cybersecurity curriculum.

3 Conclusion

To sum up, it is stated that more attention to the ethical issues while developing theoretical and practical support of educational curricula (at the national and international levels) of future cybersecurity specialists would be beneficial for all participants: for educators in terms of developing more precise educational tasks, for students in terms of developing confidence in many unpredictable situations of their professional future, for employers in terms of finding more highly-qualified workforce, and for the states in terms of securing better protection against the threats of the cyber world.

Further research should be made into the factual content of the current cybersecurity ethics programmes of foreign educational establishments in order to introduce this aspect into the national cybersecurity curriculum as a separate course or as a part of some other courses.

References

1. Aşuroğlu, T., Gemci, C.: Role of ethics in information security. In: International conference of advanced technology & sciences, pp. 141-144. Selcuk University, Konya, Turkey (2016), https://www.researchgate.net/publication/307863852_Role_of_Ethics_in_Information_Security, last accessed 2020/01/25.
2. Furnell, S., Fischer, P., Finch, A.: Can't get the staff? The growing need for cyber-security skills. Computer Fraud & Security 2, 5-10 (2017).
3. European Commission Tempus Project. Report on EU Practice for Cyber Security Education, TEMPUS (Trans-European Mobility Programme for University Studies) program, European Union, 2013.
4. Lehto M.: Cyber Security Competencies: Cyber Security Education and Research in Finnish Universities. In: ECCWS2015-Proceedings of the 14th European Conference on Cyber Warfare & Security: ECCWS 2015, pp. 179–88. Hatfield, UK: University of Hertfordshire, Academic Conferences and Publishing International Limited (2015).
5. Catota, F., Granger Morgan, M., Sicker, D.: Cybersecurity education in a developing nation: the Ecuadorian environment. In: Journal of Cybersecurity, vol. 5, Issue 1, pp (2019).
6. Santos, H., Pereira, T., Mendes, I.: Challenges and reflections in designing Cyber security curriculum. In: 2017 IEEE World Engineering Education Conference (EDUNINE), pp 47-51 (2017).
7. Mouheb, D., Abbas, S., Merabti, M. Cybersecurity Curriculum Design: A Survey. In: Pan Z., Cheok A., Müller W., Zhang M., El Rhalibi A., Kifayat K. (eds) Transactions on Edutainment XV. Lecture Notes in Computer Science, vol 11345, pp. 93-107. Springer, Berlin, Heidelberg (2019).
8. Danyk, Yu., Zinchenko, A. Cyber education and its peculiarities. In: Military education, 2, pp. 67-84 (2018). (In Ukrainian)
9. Diorditsa, I. Educational standards of training cybersecurity specialists. In: Jurnalul juridic national: teorie şi practică. 1 (23), pp. 46-49 (2017). (In Ukrainian)
10. Law, Merriam-Webster.com Homepage, https://www.merriam-webster.com/dictionary/law, last accessed 2019/12/18.
11. Ethic, Merriam-Webster.com Homepage, https://www.merriam-webster.com/dictionary/ethic, last accessed 2019/12/18.
12. Bailey, M., Dittrich, D., Kenneally, E., Maughan, D.: The menlo report. In: IEEE Security and Privacy, vol. 10 (2), pp. 71-75 (2012).
13. Lytvyn, A.: What will the new law on cybersecurity give to Ukraine. https://biz.censor.net.ua/columns/3069149/scho_dast_ukran_noviyi_zakon_pro_kberbezpeku, last accessed 2019/12/23.
14. Blanken-Webb, J., Palmer, I., Deshaies, S-E., Burbules, N.C., Campbell, R.H., and Bashir, M.: A Case Study-based Cybersecurity Ethics Curriculum. In: (USENIX) Workshop on Advances in Security Education (ASE 18), (USENIX) Association, Baltimore, MD (2018).

15. Kenneally, E., Bailey, M.: Cyber-security Research Ethics Dialogue & Strategy Workshop. ACM SIGCOMM Computer Communication Review (CCR) 4 (2), 76-79 (2014). http://mdbailey.ece.illinois.edu/publications/ccr-2014.pdf, last accessed 2019/12/23.
16. Sobel, A., Parrish, A., Raj, R.K.: Curricular Foundations for Cybersecurity. IEEE Computer 52 (3), 14-17 (2019), https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8677331, last accessed 2019/12/23.
17. Johnson, D.G., Miller, K.W.: Computer Ethics: Analyzing Information Technology, 4th edn. Pearson, (2009).
18. CAE-CD Knowledge Units, https://www.iad.gov/NIETP/documents/Requirements/CAE-CD_2019_Knowledge_Units.pdf?trackDocs=CAE-CD_2019_Knowledge_Units.pdf, last accessed 2019/12/25.
19. Burley, D., Bishop, M., Buck, S., Ekstrom, J., Futcher, L., Gibson, D., Hawthorne, E., Kaza, S., Levy, Y., Mattord, H., et al.: Cybersecurity curricula 2017. Version 0.75 Report 12 (2017). https://europe.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf, last accessed 2019/12/26.
20. Cabinet of Ministers of Ukraine Homepage, https://www.kmu.gov.ua/npas/248149695, last accessed 2019/12/27.
21. Ministry of Education and Science of Ukraine Homepage, https://mon.gov.ua/ua/osvita/visha-osvita/naukovo-metodichna-rada-ministerstva-osviti-i-nauki-ukrayini/zatverdzheni-standarti-vishoyi-osviti, last accessed 2019/12/27.
22. Dark, M., Epstein, R., Morales, L., Countermine, T., Yuan, Q., Ali, M., Rose, M., Harter, N.: A framework for information security ethics education. In: Proceedings of the 10th Colloquium for Information Systems Security Education, pp. 109-115. University of Maryland, Adelphi, MD (2007). https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2007-87.pdf, last accessed 2019/12/24.
23. Stückelberger, Ch., Duggal, P. (Eds.): Cyber Ethics 4.0: Serving Humanity with Values (2018), https://www.globethics.net/documents/4289936/13403236/Ge_Global_17_web_isbn9782889312641.pdf/, last accessed: 2019/12/24.