Development of Virtual Laboratories and Innovative Cybersecurity Courses for Distance Learning

Oleksandr Lemeshko[1], Oleksandra Yeremenko[1], Maryna Yevdokymenko[1], Ievgeniia Kuzminykh[1], and Amal Mersni[1]

[1] *Kharkiv National University of Radio Electronics, Nauky Ave. 14, Kharkiv, 61166, Ukraine*

Abstract

The article is devoted to developing virtual laboratories and innovative cybersecurity courses for distance learning due to the urgent need for effective education in the current conditions that should include and supplement the modern theoretical content of the relevant courses with the necessary practical skills. Currently, the problem of the organization of practical and laboratory works acquires special importance when the demanded level of knowledge requires training laboratories to be equipped with the necessary modern equipment and corresponding network technologies. Recently, the trend of virtualization of both networks and computers has become popular and intensive, which allows the development and implementation of more flexible types of virtualized laboratory solutions for distance learning. Moreover, virtualization tools are extremely useful in teaching and learning in the field of cybersecurity, as they are effectively applied in simulating various types of attacks, without harming the physical equipment or the entire user network. In turn, the basis for preparing innovative courses for the next generation of cybersecurity experts is the availability of specific servers for the rapid deployment of the proposed Cybersecurity Virtual Laboratory (CVLab) and its direct implementation in the educational process of the university. Introducing the CVLab will have a significant impact on improving the quality of education in higher education institutions, as well as promote research and teaching experience for researchers and scholars.

Keywords

Cybersecurity, Virtual laboratory, Education, Distance Learning, Innovative Courses, Cyber Resilience, IoT Security

1. Introduction

Currently, in conditions of distance learning of students, the problem of the organization of practical and laboratory works acquires special importance [1–5]. This mainly applies to technical universities, where training in normal conditions is carried out on real equipment and using specialized software. As a result, there is an urgent need to create virtual labs as an effective platform for distance learning for students, particularly in the field of cybersecurity. In this case, one of the effective solutions is to create and deploy a Cybersecurity Virtual Laboratory (CVLab) for distance learning, which will help ensure continuous quality training of future professionals. Besides, distance learning must not be for informational purposes only. Therefore, the formation of practical skills of students requires rapid development and implementation of effective means of distance learning. The technologies of virtualization of networks and computers allow the development and introduction of flexible virtualized laboratories.

The education of future cybersecurity professionals should include and supplement the modern theoretical content of the relevant courses with the necessary practical skills [6–11] (Fig. 1). In the field of cybersecurity education, it is assumed that teachers and practical/laboratory work under their

CPITS-II-2021: Cybersecurity Providing in Information and Telecommunication Systems, October 26, 2021, Kyiv, Ukraine
EMAIL: oleksandr.lemeshko.ua@ieee.org (O. Lemeshko); oleksandra.yeremenko.ua@ieee.org (O. Yeremenko); maryna.yevdokymenko@ieee.org (M. Yevdokymenko); yevheniia.kuzminykh@nure.ua (I. Kuzminykh); amal.mersni@nure.ua (A. Mersni)
ORCID: 0000-0002-0609-6520 (O. Lemeshko); 0000-0003-3721-8188 (O. Yeremenko); 0000-0002-7391-3068 (M. Yevdokymenko); 0000-0001-6917-4234 (I. Kuzminykh); 0000-0001-8718-5471 (A. Mersni)

guidance should motivate students to perform and solve practical and problem-oriented tasks on real equipment. At the same time, students under the guidance of a teacher can perform such tasks individually or in groups with a limited number of participants in the learning process, thus acquiring soft skills of communication and cooperation [6]. This model is effective and provides the acquisition of the required practical skills. In addition, the quality of education and the accumulation of the demanded level of knowledge require that training laboratories be equipped with the necessary modern equipment, network technologies, as only such conditions and work with real technologies and cybersecurity will allow students to confirm theoretical knowledge in practice.

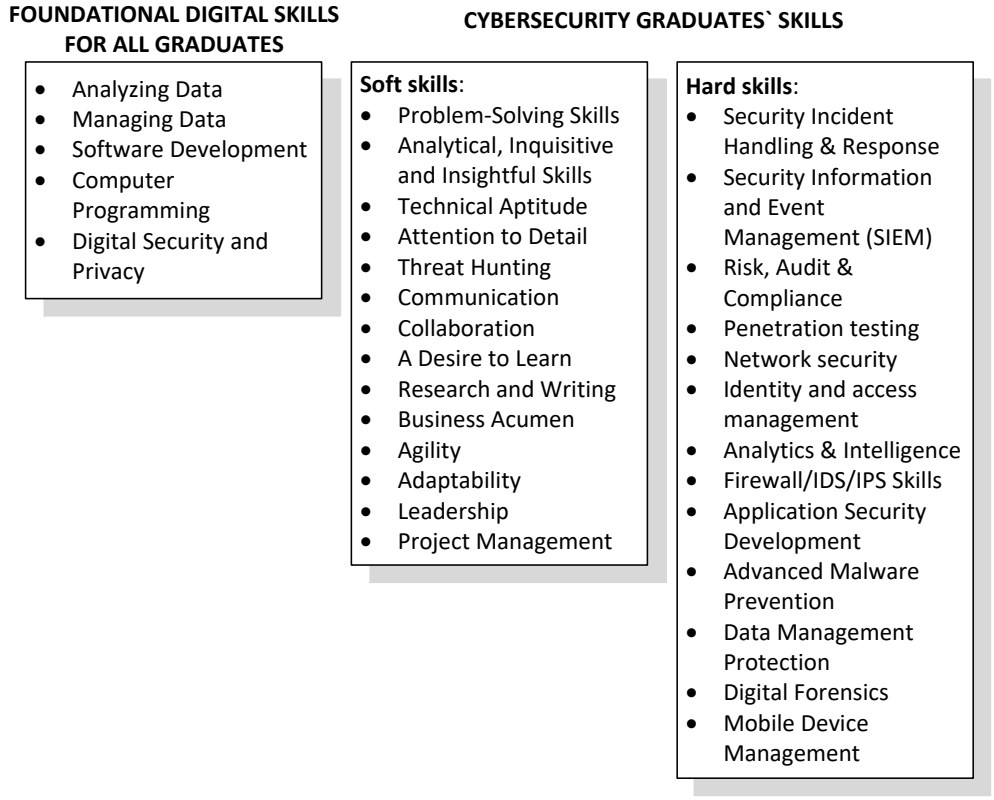

Figure 1: Cybersecurity graduates' skills

2. Specifics of Creating the Cybersecurity Virtual Laboratory for Distance Learning

In recent years, the trend of virtualization of both networks and computers has become popular and intensive, which allows us to develop and implement more flexible types of virtualized laboratory solutions, including for distance learning [6, 9, 10, 12-22]. Moreover, virtualization functionality is widely supported by almost all service and network providers. The number of virtualization tools is increasing, as well as the latest network equipment created to work in a virtual environment [6, 12, 15, 16, 19-21]. Thus, virtualization allows us to overcome the limitations of traditional networks and hardware network laboratories, given their high cost, power consumption, stability, and the limited number of devices, remote access, etc. All this indicates the significant potential of virtualized remote access laboratories.

In general, a Cybersecurity Virtual Laboratory will use appropriate computer equipment (powerful servers or cluster servers) for distance learning. Thus, such laboratories allow you to run the required number of devices per student and even simulate complex networking scenarios needed to perform practical and laboratory work on cybersecurity (network security, penetration testing, digital forensics, etc.). Therefore, virtualization technologies are currently seen as the only way to deploy future cybersecurity laboratories for distance learning and their long-term resilience in quarantine and isolation.

Virtualization allows you to create and use virtual environments for a physical machine (computer), network, or operating system. In addition, virtual environments allow you to use different operating systems or even networks on a single physical machine (Fig. 2) [12]. Virtualization tools are also particularly useful in teaching and learning in the field of cybersecurity, as they are effectively used to simulate various types of attacks, without harming the physical machine (equipment) or the entire user network [11]. It should be noted that even well-known and widespread attacks require multiple hosts and resources for their modeling and investigation.

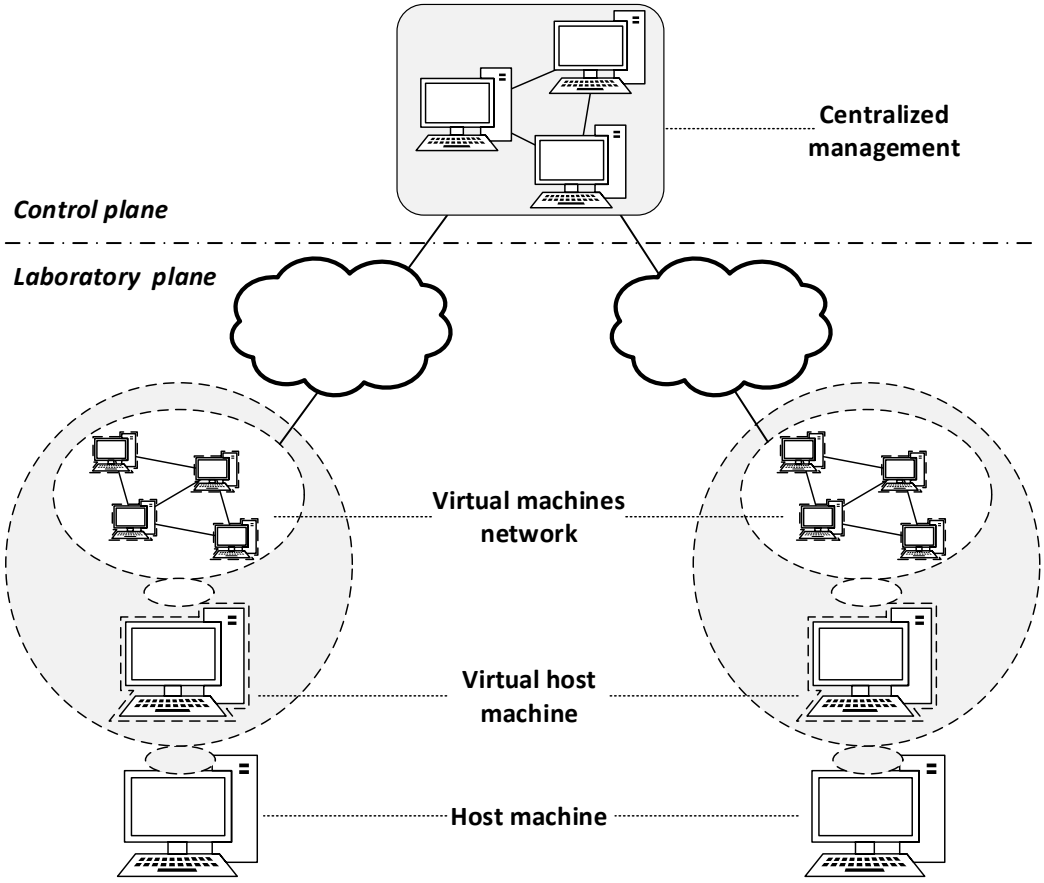

Figure 2: The preliminary architecture of the CVLab [12]

Characteristics of some existing virtual cybersecurity laboratories are presented in Table 1 [9, 10, 12-19].

Therefore, virtualization can be configured on both the desktop and the cloud infrastructure. The virtual desktop environment allows you to use virtual machines with different operating systems that share the resources of the host computer [6, 17]. This allows students to run programs that require different platforms. The main problem with virtualization on a desktop computer is the large size of the virtual machine. In addition, students must have high-performance computers to run multiple virtual machines. It should also be noted that virtual machines might require special configuration, such as installing and configuring specialized cybersecurity software and libraries, which requires additional skills from students who need to perform the configuration themselves. In this case, an alternative solution may be establishing a cloud environment for virtualization, which students can also access remotely outside the university.

The basis for preparing courses for the next generation of cybersecurity experts is the availability of specific servers for the rapid deployment of a Cybersecurity Virtual Laboratory and its direct implementation in the educational process of the university.

Table 1
Existing virtual cybersecurity laboratories

Laboratory	Description
ReSeLa [9, 10]	A virtual platform based on multiple virtual machines, designed to provide students with remote access to experiment with malware and ethical hacking in a secure environment.
DVCL [12]	A distributed virtual computer lab for cybersecurity and network technology training. The laboratory was implemented for use both in distance learning and on campus. This has been made possible by the extension of the basic Virtual Security Lab (VCL) through distribution, central management, assisted learning, and security.
CLaaS (Cybersecurity Lab as a Service) [13]	CLaaS uses cloud computing and virtualization technologies to conduct virtual cybersecurity experiments and gain practical experience on the vulnerabilities used to launch cyber-attacks, how to fix them, and how to strengthen the protection of cyber resources and services.
SEED Labs [14]	SEED Labs provide a built-in virtual machine image that is pre-configured for 30 cybersecurity labs that cover a wide range of computer and information security topics, including software security, network security, web security, operating system security, and mobile application security.
VCCLL (Virtual Cybersecurity Collaborative Learning Laboratory) [15]	An inter-institutional laboratory that offers innovative, practical, collaborative learning experiences aimed at preventing and reducing real-time cyberattacks. Using a well-established and relatively common malicious code (exploits) in a virtual laboratory, students will experience multidimensional simultaneous attacks and learn to solve, correct, and resist such actions in a special shared environment.
VLabNet [16]	An integrated learning environment for both information security and computer science using open-source Xen virtualization technology.
Tele-Lab IT-Security [17, 18]	Cloud platform for practical cybersecurity education.
Distributed laboratory architecture for game-based learning in cybersecurity and critical infrastructures [19]	Distributed remote laboratory for cybersecurity training and infrastructure protection systems using virtualization technologies, cloud computing, and Game-Based Learning (GBL).

According to the main goal of CVLab, namely the organization of an effective distance learning process, it is necessary to implement a number of activities, namely:

1. Organizing the purchase of server equipment according to the technical recommendations and computing resources demands.
2. Deploying and launching CVLab for distance learning.
3. Testing CVLab by performing practical and laboratory work to verify its proper operation, as well as eliminating possible errors.

4. Providing open access CVLab for all target groups in Ukraine, namely students and teachers.
5. Organizing online webinars on the possibilities of using CVLab for students and teachers.
6. Dissemination of information about CVLab and its capabilities through social networks and internet resources in order to interest students at various universities in Ukraine, where they are trained in cybersecurity.
7. Effective quality control (internal quality control, monitoring, and evaluation).

Moreover, the rapid provision of a virtual distance learning CVLab platform will help to ensure the full-fledged learning of students during the quarantine. Such a virtual platform will contain all the necessary tools, software, as well as recommendations for laboratory and practical work of basic training courses, such as Network & Cloud Security, Secure Software Development, Malware Analysis, Web Security, Penetration Testing, and Ethical Hacking, Digital Forensic, etc.

3. Impact of Implementing the Cybersecurity Virtual Laboratory

Introducing the CVLab and developing the innovative courses on cybersecurity, as well as integrating into the educational process of Ukrainian higher education institutions (HEIs) has a significant impact in the following:

- raising awareness about cybersecurity policies and facilitating future cooperation between companies and security regulatory bodies;
- fostering of understanding the cybersecurity policies through a series of training courses;
- improving the quality of education in the HEIs.

In addition, the introduction of CVLab will promote research and the first teaching experience for young researchers and scholars. The CVLab development team members are young scientists and teachers with broad experience in teaching specialized disciplines in the field of cybersecurity. The involvement of young researchers will entail successful implementation of the CVLab objectives, which will be achieved both through self-training and independent research in the field of cybersecurity, and jointly as a team, by attracting external experts in this field, internships in industry, and exchanging experience on the international conferences.

Extremely important that CVLab deployment will foster the publication and dissemination of the results of academic research. Nowadays, cybersecurity research and development are important all over the world. Cyber-attacks are on the increase and a connected economy and society that is more vulnerable to cyber threats and attacks requires stronger defenses. The main goal and principles of Cybersecurity Strategy are to foster a reliable, safe, and open cyber ecosystem that should remain valid. However, the continuously evolving and deepening threat landscape demand more action to withstand and deter attacks in the future.

In accordance with the Cyber Security Strategy of Ukraine, the main objective is also to create conditions for the safe functioning of cyberspace, application of cyberspace to benefit individuals, society, and the State. However, the research of Ukrainian scientists focused on specific threats and attacks in narrow areas, and the research itself is technical in nature. Nevertheless, cybersecurity is not limited to network, information security, and technical protection. Therefore, the urgent task of conducting comprehensive research in Ukraine arises, aimed at developing and implementing the most effective regulatory protection mechanisms.

Therefore, carrying out research on cybersecurity topics will allow to deepen knowledge, broaden the outlook, and highlight the best practices for their further dissemination at the territory of Ukraine. Publication of articles in scientific and technical journals as well as in local and regional press and participation in international conferences will disseminate the knowledge and experience and exchanging cybersecurity information.

The development of new and modernization of existing courses will be based on analyzing challenges in the cybersecurity area in Ukraine and worldwide with getting feedback from industry, public, and government stakeholders on skills and knowledge demands in Ukraine. To ensure the sustainability of the CVLab results, all the courses will be implemented in the educational curriculum at Ukrainian universities, and delivered material, including publications could be accessed free on the website of the project.

According to the key objectives for cybersecurity and information and communications technology, cybersecurity certification the network and information systems, as well as electronic communication networks and services play a vital role in society and have become the backbone of economic growth.

Information and communications technology (ICT), IoT, and Smart Infrastructures underpin the complex systems which support everyday social activities, connect people and devices, keep our economies running in key sectors such as health, energy, finance, transport, and, in particular, support the functioning of the internal market. In this context, the security and certification of the products, services, and processes become significant relevant areas both in Ukraine and all over the world.

To make the Ukrainian market more familiar with the current standards and policies in cybersecurity, the CVLab team will modernize existing courses expanding the content with cybersecurity policies and best practices in the specific areas as IoT, namely cyber resilience and ICT services that are relevant for graduates in their professional life. These courses will enhance students` professional skills and their competitiveness in the labor market.

4. Innovative Courses Example and Description

As part of the implementation of CVLab, it is planned to develop the following innovative specialized courses, which are relevant today and include the scientific results of young scientists involved in the deployment of the laboratory [23-31].

Among them, the course titled "Best practices in the cyber resilience strategy" can be distinguished, the brief description of which is presented below.

The purpose of the course is to provide knowledge in current frameworks, modern methods of protecting networks and cloud systems. The students will obtain knowledge about cyber resilience means, practical skills in deep packet inspection systems, secure routing, fault-tolerant network and systems, firewalls, access control methods of protection, software-defined networks, and cloud security principles.

Course syllabus:

1. Towards a Global Cyber Resilience Framework

Goal: to study the current understanding of cyber resilience based on getting an overview of what sort of resilience measures are currently in place, as well as highlight any glaring gaps in efforts.

2. The cyber resilience strategy

Goal: to study best practices aimed at providing three core pillars of the Eurosystem's cyber resilience strategy.

3. Analysis of Cyber Defense Policy Framework

Goal: to study about Cyber Defense Policy Framework for the consistent implementation promotion of the relevant framework, which is essential to increasing cyber resilience.

4. The main concepts of secure routing in reliable networks.

Goal: to know characteristics of existing network security methods in infocommunications; analysis of secure routing methods in the communication networks; improving secure routing methods.

5. Network security metrics evaluation.

Goal: to know the probability of compromising the network elements (links, nodes, routes, network segments); existing and novel methods of evaluating the probability of compromise.

6. Fault-tolerant routing as the approach for ensuring cyber resilience in the modern network architectures and clouds.

Goal: to know default gateway protection within fault-tolerant routing; inter-area fast rerouting in the case of hierarchical routing; fast rerouting with load balancing in software-defined networks; fault-tolerant cloud infrastructures.

The course teaches strategic documentation and cybersecurity approaches of the EU frameworks for ensuring the cyber resilience of ICT. The course also combines EU frameworks and technical knowledge about the fundamentals of SDN, cloud, virtualization technologies, IPS/IDS, advanced VPN protection, secure routing, design a fault-tolerant network to protect network elements.

Also, currently considerable interest in a course called "Best practices for IoT and Smart Infrastructures", which description is as follows.

The purpose of the course is to define security measures for IoT in the entailed complexity that is brought by the diversity of application areas for IoT. This course helps to understand what needs to be secured and what security measures to implement in order to protect the Internet of Things from cyber threats. During the course, the differences in apportioning risk to distinct environments in each IoT domain will be considered as well as threats and risks related to the IoT devices.

Course syllabus:

1. IoT Security Standards Gap Analysis

Goal: to study and analyze the gaps in IoT security and provide guidelines for the development or repositioning of standards.

2. Baseline Security Recommendations for IoT

Goal: to study best practices to help secure IoT products and systems including physical security, device secure boot, secure operating system, application security, encryption, network connection, and so on (IoT Security Foundation).

3. Security and Resilience of Smart Home Environments

Goal: to study securing Smart Home Environments from cyber threats by highlighting good practices that apply to every step of a product lifecycle: its development, its integration in Smart Home Environments, and its usage and maintenance until end-of-life. The study also highlights the applicability of security measures to different types of devices. The good practices apply to manufacturers, vendors, solution providers for hardware and software, and developers.

4. Good Practices for Security of Internet of Things in the context of Smart Manufacturing

Goal: to study and analyze the security and privacy challenges related to the evolution of industrial systems and services precipitated by the introduction of IoT innovations. Introduce the good practices to ensure the security of IoT in the context of Industry 4.0/Smart Manufacturing, while mapping the relevant security and privacy challenges, threats, risks, and attack scenarios.

5. Security of IoT cloud services

Goal: to provide a high-level overview on the security issues to IoT developers and IoT integrators that make use of IoT Cloud Computing and Cloud Service Providers (CSPs) of IoT Cloud offerings.

6. Cybersecurity Challenges and Recommendations for industrial IoT

Goal: to study the main challenges to the adoption of the security measures and security of Industry 4.0 and Industrial IoT. To get acquired with recommendations to different stakeholder groups in order to promote Industry 4.0 cybersecurity and facilitate wider take-up of relevant innovations in a secure manner.

7. Vulnerability Disclosure in the Internet of Things Product (IoT security foundation)

Goal: study how to report newly discovered security vulnerabilities to the product or service-providing organization and make the public announcement of security vulnerabilities by that organization.

8. IoT Security Compliance Framework (IoT security foundation)

Goal: to study how Framework sets out a comprehensive set of security requirements for aspects of the organization and product. To learn how to do a risk assessment of the IoT products, how to create a Compliance Checklist, understand how to provide a list of countermeasures to reduce any security risk.

The course will increase the awareness of participants about what measures according to EU cybersecurity policies should be implemented to protect IoT and Smart Infrastructure from cyber threats. Given the pervasiveness and massive deployment of the IoT concept, cyber threats against it have real consequences on the safety of citizens and industrial objects.

5. Conclusion

It should be mentioned that the introduction of a cybersecurity virtual laboratory (CVLab) aimed at improving the effectiveness of distance education meets the objectives of the Cyber Security Strategy of Ukraine, as well as priorities and areas of its provision, ranging from general digital literacy to training of security sector actors [32]. At the same time, among the advantages of CVLab implementation are the following.

Ease of use and implementation in the educational process. After installing CVLab, students can perform practical and laboratory works both on the server and on their personal device, after

downloading the image of the virtual laboratory at a convenient time. Teachers can create instructions and guides for laboratory work, whereas students can access and create feedback.

Versatility and efficiency. Due to the fact that CVLab will include training courses that are part of the basic curriculum in the field of cybersecurity, this virtual platform will be able to cover most universities in which students study in this specialty.

Availability. CVLab courses will be publicly available. Students and teachers can use this virtual laboratory for distance learning in the field of cybersecurity.

Sustainability. Using CVLab is an effective tool for distance learning not only during the global pandemic, but will be useful in the educational process during any period of student learning.

Technical support. Periodic updating of the platform and support as needed are provided.

6. References

[1] K.E. Ehimwenma, P. Crowther, M. Beer, Formalizing Logic Based Rules for Skills Classification and Recommendation of Learning Materials, International Journal of Information Technology and Computer Science (IJITCS) 10(9) (2018) 1-12. doi: https://doi.org/10.5815/ijitcs.2018.09.01.

[2] S.E. Adekunle, O.S. Adewale, O.K. Boyinbode, Appraisal on Perceived Multimedia Technologies as Modern Pedagogical Tools for Strategic Improvement on Teaching and Learning, International Journal of Modern Education and Computer Science (IJMECS) 11(8) (2019) 15-26. doi: https://doi.org/10.5815/ijmecs.2019.08.02.

[3] S. Azouzi, J.E. Hajlaoui, Z. Brahmi, S. Ayachi Ghannouchi, Collaborative E-Learning Process Discovery in Multi-tenant Cloud, International Journal of Intelligent Systems and Applications (IJISA) 13(2) (2021) 21-37. doi: https://doi.org/10.5815/ijisa.2021.02.02.

[4] M.A. Al-Hagery, M.A. Alzaid, T.S. Alharbi, M.A. Alhanaya, Data Mining Methods for Detecting the Most Significant Factors Affecting Students' Performance, International Journal of Information Technology and Computer Science (IJITCS) 12(5) (2020) 1-13. doi: https://doi.org/10.5815/ijitcs.2020.05.01.

[5] O.W. Adejo, I. Ewuzie, A. Usoro, T. Connolly, E-Learning to m-Learning: Framework for Data Protection and Security in Cloud Infrastructure, International Journal of Information Technology and Computer Science (IJITCS) 10(4) (2018) 1-9. doi: https://doi.org/10.5815/ijitcs.2018.04.01.

[6] P. Segeč, M. Moravčík, M. Kontšek, J. Papán, J. Uramová, O. Yeremenko, Network virtualization tools – analysis and application in higher education, in: Proceedings of the 2019 17th International Conference on Emerging eLearning Technologies and Applications (ICETA), IEEE, 2019, pp. 699-708. doi: https://doi.org/10.1109/ICETA48886.2019.9040148.

[7] V. Buriachok, V. Sokolov, Implementation of Active Learning in the Master's Program on Cybersecurity, in: Hu Z., Petoukhov S., Dychka I., He M. (eds) Advances in Computer Science for Engineering and Education II. ICCSEEA 2019, volume 938 of Advances in Intelligent Systems and Computing, Springer, Cham, 2020, pp. 610-624. doi: https://doi.org/10.1007/978-3-030-16621-2_57

[8] Z. B. Hu, V. Buriachok, V. Sokolov, Implementation of Social Engineering Attack at Institution of Higher Education, in: Proceedings of the 1th International Workshop on Cyber Hygiene & Conflict Management in Global Information Networks (CybHyg), Oct., 2019, vol. 2654, pp. 155-164.

[9] A. Carlsson, I. Kuzminykh, R. Gustavsson, Virtual Security Labs Supporting Distance Education in ReSeLa Framework, in: Auer M., Tsiatsos T. (eds) The Challenges of the Digital Transformation in Education. ICL 2018, volume 917 of Advances in Intelligent Systems and Computing, Springer, Cham, 2019, pp. 577-587. doi: https://doi.org/10.1007/978-3-030-11935-5_55.

[10] A. Carlsson, R. Gustavsson, L. Truksans, M. Balodis, Remote Security Labs in the Cloud ReSeLa, in: Proceedings of the 2015 IEEE Global Engineering Education Conference (EDUCON), IEEE, 2015, pp. 199-206. doi: https://doi.org/10.1109/EDUCON.2015.7095971.

[11] D. Mouheb, S. Abbas, M. Merabti, Cybersecurity Curriculum Design: A Survey, in: Pan Z., Cheok A., Müller W., Zhang M., El Rhalibi A., Kifayat K. (eds) Transactions on Edutainment XV, volume 11345 of Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 2019, pp. 93-107. doi: https://doi.org/10.1007/978-3-662-59351-6_9.

[12] J. Haag, H. Vranken, M. van Eekelen, A Virtual Classroom for Cybersecurity Education, in: Pan Z., Cheok A., Müller W., Zhang M., El Rhalibi A., Kifayat K. (eds) Transactions on Edutainment XV, vol 11345 of Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 2019, pp. 173-208. https://doi.org/10.1007/978-3-662-59351-6_13.
[13] C. Tunc, S. Hariri, F. De La Peña Montero, F. Fargo, P. Satam, Y. Al-Nashif, Teaching and Training Cybersecurity as a Cloud Service, in: Proceedings of the 2015 International Conference on Cloud and Autonomic Computing, IEEE, 2015, pp. 302-308. doi: https://doi.org/ 10.1109/ICCAC.2015.47.
[14] SEED Labs, 2002. https://seedsecuritylabs.org/
[15] J. Murphy, E. Sihler, M. Ebben, L. Lovewell, G. Wilson, Building a Virtual Cybersecurity Collaborative Learning Laboratory (VCCLL), in: Proceedings of the International Conference on Security and Management (SAM) (p. 1). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), 2014, pp. 1-5.
[16] V.J. Powell, C.T. Davis, R.S. Johnson, P.Y. Wu, J.C. Turchek, I.W. Parker, VLabNet: the integrated design of hands-on learning in information security and networking, in: Proceedings of the 4th annual conference on Information security curriculum development, 2007, pp. 1-7.
[17] C. Willems, C. Meinel, Tele-lab IT-security: An architecture for an online virtual IT security lab, International Journal of Online and Biomedical Engineering (iJOE) 4(2) (2008) 31-37.
[18] C. Willems, T. Klingbeil, L. Radvilavicius, A. Cenys, C. Meinel, A distributed virtual laboratory architecture for cybersecurity training, in: Proceedings of the 2011 International Conference for Internet Technology and Secured Transactions, IEEE, 2011, pp. 408-415.
[19] J. Cano, R. Hernández, S. Ros, L. Tobarra, A distributed laboratory architecture for game based learning in cybersecurity and critical infrastructures, in: Proceedings of the 2016 13th International Conference on Remote Engineering and Virtual Instrumentation (REV), IEEE, 2016, pp. 183-185. doi: https://doi.org/10.1109/REV.2016.7444461.
[20] K. Nance, B. Hay, R. Dodge, A. Seazzu, S. Burd, Virtual laboratory environments: Methodologies for educating cybersecurity researchers, Methodological Innovations Online 4(3) (2009) 3-14.
[21] D. Moritz, C. Willems, M. Goderbauer, P. Moeller, C. Meinel, Enhancing a virtual security lab with a private cloud framework, in: Proceedings of the 2013 IEEE International Conference on Teaching, Assessment and Learning for Engineering (TALE), IEEE, 2013, pp. 314-320. doi: https://doi.org/10.1109/TALE.2013.6654452.
[22] K. Salah, M. Hammoud, S. Zeadally, Teaching cybersecurity using the cloud, IEEE Transactions on Learning Technologies 8(4) (2015) 383-392. doi: https://doi.org/10.1109/TLT.2015.2424692.
[23] O. Lemeshko, O. Yeremenko, A. Shapovalova, A. M. Hailan, M. Yevdokymenko, M. Persikov, Design and Research of the Model for Secure Traffic Engineering Fast ReRoute under Traffic Policing Approach, in: Proceedings of the 2021 IEEE 16th International Conference on the Experience of Designing and Application of CAD Systems (CADSM), IEEE, 2021, pp. 23-26. doi: https://doi.org/10.1109/CADSM52681.2021.9385253.
[24] O. Lemeshko, O. Yeremenko, M. Yevdokymenko, A. Shapovalova, T. Radivilova, D. Ageyev, Secure Based Traffic Engineering Model in Softwarized Networks, in: Proceedings of the IEEE International Conference on Advanced Trends in Information Theory ATIT, IEEE, 2020, pp. 1- 4. doi: https://doi.org/10.1109/ATIT50783.2020.9349301.
[25] O. Lemeshko, O. Yeremenko, M. Yevdokymenko, A. Shapovalova, A.M. Hailan, A. Mersni, Cyber Resilience Approach Based on Traffic Engineering Fast ReRoute with Policing, in: Proceedings of the 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IEEE, 2019, pp. 117-122. doi: https://doi.org/10.1109/IDAACS.2019.8924294.
[26] O. Lemeshko, O. Yeremenko, A. Shapovalova, M. Yevdokymenko, A. Akulynichev, V. Porokhniak, Research of Secure Routing with Load Balancing and Compromise Probability Behavior Account, in: Proceedings of the IEEE EUROCON 2021 - 19th International Conference on Smart Technologies, IEEE, 2021, pp. 296-299. doi: https://doi.org/10.1109/ EUROCON52738.2021.9535642.
[27] O. Lemeshko, O. Yeremenko, M. Yevdokymenko, B. Sleiman, System of Solutions the Maximum Number of Disjoint Paths Computation Under Quality of Service and Security Parameters, in: M. Ilchenko, L. Uryvsky, L. Globa (Eds.), Advances in Information and Communication Technology

and Systems. MCT 2019, volume 152of Lecture Notes in Networks and Systems, Springer, Cham, 2021, pp. 191-205. doi: https://doi.org/10.1007/978-3-030-58359-0_10.
[28] O. Lemeshko, M. Yevdokymenko, M. Yeremenko, I. Kuzminykh, Cyber Resilience and Fault Tolerance of Artificial Intelligence Systems: EU Standards, Guidelines, and Reports, in: Proceedings of the Selected Papers on Cybersecurity Providing in Information and Telecommunication Systems (CPITS 2020), CEUR, 2020, pp. 99-108. http://ceur-ws.org/Vol-2746/paper9.pdf.
[29] I. Kuzminykh, A. Carlsson, Analysis of Assets for Threat Risk Model in Avatar-Oriented IoT Architecture. In: Galinina O., Andreev S., Balandin S., Koucheryavy Y. (eds) Internet of Things, Smart Spaces, and Next Generation Networks and Systems. NEW2AN 2018, ruSMART 2018, volume 11118 of Lecture Notes in Computer Science, Springer, Cham, 2018, pp. 52-63. doi: https://doi.org/10.1007/978-3-030-01168-0_6.
[30] M. TajDini, V. Sokolov, I. Kuzminykh, S. Shiaeles, B. Ghita, Wireless Sensors for Brain Activity—A Survey, Electronics 9 (2020) 2092. https://doi.org/10.3390/electronics9122092.
[31] I. Kuzminvkh, Development of traffic light control algorithm in smart municipal network, in: Proceedings of the 2016 13th International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET), IEEE, 2016, pp. 896-898. doi: https://doi.org/10.1109/TCSET.2016.7452218.
[32] Cybersecurity Strategy of Ukraine, Decree of the President of Ukraine from 15.03.2016. 96/2016. https://zakon.rada.gov.ua/laws/show/96/2016#n11.