

Model of Integration of Cyber Defense Exercises (CDX) in the Process of Training an Information Security Specialist in University

Zinaida V. Semenova¹^a, Natalya A. Moiseeva²^b and Elena V. Tolkacheva¹^c

¹The Siberian State Automobile and Highway University, St. P. Nekrasov 10, Omsk, Russia

²Omsk State Technical University, Mira ave. 11, Omsk, Russia


Keywords: Information Security, Cybersecurity Education, Cyberattack, Cyber Defense Exercises (CDX), Socio-Technical Testing, Training an Information Security Specialist, Model of Integration of CDX.


Abstract: Against the background of improving the skill of cybercriminals, there is a crisis of expert knowledge of the majority of information security specialists and, as a result, a lack of a sufficient number of highly qualified security personnel. Many experts note the importance of cyber defense exercises as a significant tool for the continuous development of information security competencies. It is revealed that actually there is no system approach to the use of cyber defense exercises in the educational process of universities. In this regard, the purpose of this article is to solve the problem of system integration of cyber defense exercises in the process of training a future information security specialist. This research paper uses the general scientific dialectical method, theoretical and methodological analysis and generalization of technical, scientific and educational-methodical literature, scientific works of domestic and foreign scientists in the field of cybersecurity and cyber defense exercises. It allows to develop a model for integrating cyber defense exercises into the process of training an information security specialist, which reflects how various forms of cyber defense exercises are used at different stages of training (sociotechnical testing, red-teaming, etc.). It is described the mechanism of integration at the level of individual disciplines, a set of disciplines, within the framework of industrial practices and within the framework of the final state certification. In addition, the participation of students in the corresponding scenarios of cyber defense exercises is considered. Integration of the developed model makes possible to improve the quality of training of students, to develop competencies required by a highly qualified information security specialist.


1 INTRODUCTION

For several decades, the modern world has been in constant technological revolution and digital transformation of absolutely all spheres of the information society. In response to the dynamically changing digital reality, cyberattacks by cybercriminals are increasing worldwide, threatening the existence of an innovative digital world of Industry 4.0. It should be noted that cyberattacks are among the five global threats on a par with the social consequences of pandemics and climate change. The World Economic Forum estimates that global economic losses from cyberattacks could reach \$8 trillion by 2022 (Fokin, 2020).

Simultaneously, there is an acute shortage of highly skilled information security (IS) professionals capable of withstanding modern cyber threats in the global Industry 4.0 labor market. Symantec CEO Michael Brown notes that the number of job openings for cybersecurity professionals is steadily increasing, with about a quarter of those positions going unfilled. Furthermore, experienced IS professionals are not always prepared to respond adequately to modern malicious cyberattacks (Hautamäki et al., 2019; Knüpfer et al., 2020; Malatji et al., 2019; Østby et al., 2019), indicating a lack of trained personnel. It should be noted that this problem is not new. For example, Cisco Cyber Security's 2018 annual report highlights that the percentage of employees whose competence

^a <https://orcid.org/0000-0003-4513-6019>

^b <https://orcid.org/0000-0002-9502-3891>

^c <https://orcid.org/0000-0003-2685-7574>

level is not sufficient to repel serious cyberattacks is not decreasing year after year. Moreover, judging by this analytical report, from 2015 to 2017, there was even a trend of a slight increase in this indicator (Fig. 1).

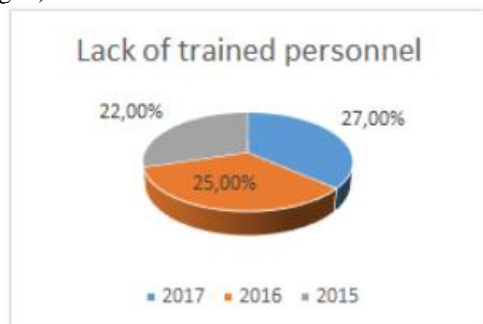


Figure 1: Statistics of low employee training (Based on Cisco's 2018 research report).

As the chart shows, a quarter of employees are not capable of preventing and investigating cybercrime due to low cybersecurity awareness.

Even though many universities around the world place significant emphasis on training IS professionals (Granasen et al., 2016; Hatzivasilis et al., 2020; Ošlejšek et al., 2018; Petullo et al., 2016; Wang et al., 2018), the gap between the demand for qualified IS personnel, and the corresponding supply continues to grow, as many experts point out (Hatzivasilis et al., 2020; Hautamäki et al., 2019; Østby et al., 2019). In fact, university graduates join the ranks of IS specialists with a low level of training.

To effectively deal with cyber threats, the level of competence of both the novice and the experienced security professional must constantly improve. Cybersecurity experts agree that cyber training conducted regularly makes a significant contribution. We fully share the authors' view that one of the main professional development tools used in cybersecurity is cybersecurity exercises (Dewar, 2018; Lukatsky, 2018, 2020; Petrenko, 2015; Seker, 2018; Yamin et al., 2018, 2019). This has been confirmed in research studies and reports from companies implementing the service of preparing and delivering such training (Moore et al., 2017).

While the theory and practice of cyber training for current IS officers, organizational leaders, and rank-and-file personnel has been around for decades, the integration of cyber training into future cybersecurity specialists' training has not yet been fully resolved. To date, there is a lack of a systematic approach and perspective on the application of cyber studies in the training of students - future IS specialists.

Next, in this article, we will present an analysis of publications that address various aspects of cyberlearning and highlight cyberlearning for students. We also describe our developed model for integrating cyber studies into the IS specialist training process and recommendations for its implementation in the university's educational process.

2 STUDY METHODOLOGY

The theoretical conclusions obtained in this study are based on the study and analysis of technical, scientific, and educational literature, scientific works of domestic and foreign scientists in the field of cybersecurity (Dewar, 2018; Lukatsky, 2018, 2020; Petrenko, 2015; Seker, 2018; Yamin et al., 2018, 2019) and cyber studies (Vykopal, J., O. D. Arkhangelsky, A. B. Lukatsky, A. A. Petrenko et al.). When developing the model of integration of cyberlearning, we relied on the general systems theory provisions (V. G. Afanasiev, L. von Bertalanffy, I. B. Blauberg, V. H. Sadovsky et al.), including the theory of modeling as one of the dialectical methods of studying and transforming systems (A. H. Dakhin, L. I. Novikova, V. A. Stoff et al.).

3 STUDY RESULTS

As the analysis of works (Granasen et al., 2016; Hatzivasilis et al., 2020; Ošlejšek et al., 2018; 2016; Wang et al., 2018, etc.) shows, there is a problem in the global practice of training future IS professionals since a university graduate usually does not possess the necessary level of competencies that allow them to effectively perform the job duties concerning the prediction, prevention, and mitigation of cyberattacks. Given the significant number of unfilled positions, many organizations prefer to hire cybersecurity professionals with specific expertise for specific tasks and are unwilling to invest in entry-level positions. Besides, the situation is not always good with internal training.

Moreover, according to an American analyst, cybersecurity instructor, and author of books on computer network security (Sanders, 2017, 2020) the field of information security is in a state of growing cognitive crisis. With the increasing amount of freely available information and the availability of modern technology, the university education system poorly copes with developing the skills necessary for

students to be competent practitioners. Most young professionals, recent students, are forced to build their careers relying on more mature colleagues' self-education and experience. At the same time, universities, in general, cannot produce job-ready graduates.

According to IS professionals, a cognitive revolution is needed to overcome the cognitive crisis, and three things need to happen:

1. Everyone should thoroughly understand the essence and peculiarities of the processes based on the study's study.

2. Experts need to develop replicable learning methods and techniques.

3. Educators should promote and develop students' practical thinking.

As noted above, cyber education has great potential to shape the practical experience for future IS specialists. Today, there is some international experience in integrating cybersecurity exercises into the educational process.

For example, presenting 20 years of experience in integrating large-scale cyber defense exercises into the computer science and information technology curriculum at the United States Military Academy, the authors (Petullo et al., 2016) emphasize that such integration is based on The Cyber-Defense Exercise (CDX), which takes place once a year and lasts for four days (13 hours each day). Students are excused from other classes during this period. Students' main challenge in CDX is to design, build, and protect an objectively complex network that students themselves have not yet encountered during their time at the academy.

The authors agree with a number of criticisms of CDX. Still, they are convinced that, with the right use of resources, events such as CDX provide a useful educational experience with a well-designed strategy.

It should be noted that CDX is an optional educational activity involving only a select group of students, predominantly computer science and information technology majors. In addition - these are students, usually in their final year of study. Another special feature is that the CDF requires interdisciplinary knowledge and takes place under a systems engineering course umbrella.

The United States Military Academy also has a long history of students participating in Capture The Flag (CTF) competitions. Unlike CDX, where the training is aimed solely at defense, CTF competitions, as a rule, may emphasize defense, or - on the attack, or both of the attack and defense.

It should be noted that the CTF format is the most widely integrated cyberlearning into the learning

process. The authors of many publications argue that cybersecurity skills should be developed not only through conventional methods and forms, such as lectures, seminars, and labs, but also through more active methods with a practical orientation (Mansurov, 2016; Minzov et al., 2019; Vykopal et al., 2017).

Simultaneously, teachers see some limitations for implementing CTF cyberlearning into the educational process, considering only such opportunities as the organization of masterclasses, specialized lecture classes on the most complex topics to prepare students for competitions (Mansurov from his article can be added). According to the author, these limitations are due to the rigid structure of the curriculum and insufficient hours devoted to mastering the most significant (from a cybersecurity point of view) disciplines. Here again, we can state that higher-level cybersecurity competency building is optional and does not focus on each student.

Highlighting the experience accumulated at the Faculty of Physics and Engineering of Altai State University, A.V. Mansurov emphasizes that elective classes deal with a dissected problem into its components, and, at the first stage, for each selected component, the knowledge and skills needed to understand the essence and peculiarities of the processes stated within the problem are identified. The author considers it especially important to develop reflection so that the learner can be fully aware of what he already knows and what additional knowledge he needs.

Some authors emphasize that the implementation of gaming technologies in cybersecurity is hindered by the fear of educational institutions' administration to obtain through such training an unethical hacker who can cause certain problems (Minzov et al., 2019).

Obviously, in this case, according to the authors, the emphasis should be placed on mastering technologies and methods of creating secure, fault-tolerant IS, forming professional ethics. At the same time, among the educational technologies, the combination of such didactic technologies as a game, role-playing, and problem-based is proved to be effective. This is exactly the combination that characterizes CTF format competitions.

At the same time, it is proposed to use the time of independent training (following the FSES - 50% of the total curriculum), summer schools, and other forms of extracurricular activities to prepare and conduct competitions. Once again, it is about the lack of systematic and optional integration of cyber studies into the training of cybersecurity specialists.

As noted by educators from Finland in their review (Hautamäki et al., 2019), there are few articles highlighting experiences of integrating CDX into the educational process, and there is also almost no research on cybersecurity pedagogical practices, so further research is needed towards developing pedagogical principles of CDX for information security learners.

4 DISCUSSION OF RESULTS

An analysis of the sources showed that integrating cyber studies into the educational process to train a future cybersecurity professional is welcomed in both the pedagogical and professional communities. That said, some experience has already been accumulated.

Some important features characterize our concept of integration. First, we believe that cybersecurity exercises should go from optional to mandatory. This means that each student has to go through a whole series of cyberlearning. Secondly, within each of the 11 semesters (which is how long information security specialist training in Russian universities takes), a student must be involved in cyber studies. Thirdly, the student must gain experience in various types of cybersecurity exercises over the course of the studies. Fourth, by participating in the same type of cyberlearning repeatedly, the student must go through different roles.

We are convinced that the first exercises should take place already in the first semester, and by type, it should be socio-technical testing.

And here, we focus on the term "socio-technical teachings" because of its ambiguity.

To test and determine the level of employee awareness and minimize the risks associated with human factors, it is advisable and essential to conduct penetration tests using technical methods. Still, non-technical methods such as social engineering can also be applied. In IS, social engineering refers to the psychological manipulation of people to commit certain acts or disclose confidential information.

In Russian cybersecurity realities, IS specialists have defined and use the concept of "sociotechnical testing".

Positive Technologies, an international company, specializing in IS software development, proposes that sociotechnical testing should be understood as a penetration test conducted using social engineering methods to determine employees' level of IS awareness. The testing process determines the response of IS personnel to organizational intrusion techniques used by attackers. It should be noted that

organizational aspects of IS are the most important component of the information protection system.

Outside Russia, the term "social engineering penetration testing" is used. The authors (Watson et al., 2014) write that the purpose of social engineering penetration testing is to verify employee compliance with IS policies and practices defined by management. The result of such testing should provide the company with information about how easily an intruder could persuade employees to violate security rules; disclose or give access to confidential information. In doing so, the company will have a better understanding of how successful their safety training is.

As we can see, in essence these terms ("sociotechnical testing" and "social engineering penetration testing" coincide completely. In what follows, we will use the term "sociotechnical testing".

During the first semester of study, it is advisable to conduct socio-technical testing exercises for first-year students. To organize student participation in the first few weeks of the semester, students need to be engaged in the learning corporate information environment. Such an environment could be, for example, a simplified model of an enterprise information system that includes an enterprise mail server and a simplified electronic document management system. Through corporate mail, students can get logins and passwords to enter various information systems of the university. In the electronic document management system, they can access the department's internal documents concerning the organization of the educational process. Sociotechnical exercises may include sending phishing emails to corporate email accounts. If a student clicks on phishing links, access to the electronic document management system and corporate email access may be blocked. The incidents would then need to be investigated jointly. It is advisable to develop several scenarios (several legends) so that each of them considers the psychological characteristics of the student to the greatest extent.

The scope of this publication does not allow us to characterize in detail the cyberlearning of each semester. However, in general terms, the types of cyberlearning for each semester are presented in Table 1.

Table 1: Step-by-step model of cyberlearning integration in the university educational process.

Se me ste r nu m be r	Type of cyber training	Disciplines	Note
1	Sociotechni cal testing	"Introduction to Specialty"/ "Computer Science."	During the first semester, conditions are created to form the sustainable need for students to use corporate e-mail and electronic resources of the department.
2	CTF- Task- based	"IS Fundamentals/P rogramming Languages	Players (students) are given a set of tasks (tokens) to which they have to find the answer. The subject matter of the assignments is based on the content of the disciplines of the respective semester
3	CTF- Task- based	"Programming languages"/ "Mathematical logic and algorithm theory"/ "Data processing structures and algorithms"/ "Database management systems"	
4	CTF- Attack- Defense (Blue team)	"Operating Systems"/ "Organization of computers and computer systems"/ "Technology and programming techniques"	Team Play Organization. The subject matter of the assignments is based on the content of the disciplines of the respective semester
5	CTF- Attack- Defense (Blueteam)/ Sociotechni cal Exercise	"Methods and Means of Cryptographic Protection of Information"/"In formation Transmission Networks and Systems	Prepare socio- technical exercises for first-year students

6	Blue team\ Red team	"Database systems security"/ "Integrated Data Analysis Methods and Tools"/ "Operating Systems Security"/ "Introduction to Switching, Routing and Wireless Networks"	Team interaction when performing penetration tests.
7	Blue team\ Red team\ White team	"World Information Resources and Networks/Infor mation Protection Software and Hardware	Some students participate in the preparation of cyberstudies
8	Blue team\ Red team\ White team\ Green team	"Computer network security"/"Softw are-hardware protection of information"	All students participate in the development and production of assignments, and in accordance with the topics of all their coursework during the period of study
9	Blue team\ Red team\ White team\ Green team\ Yellow team	"Information security in distributed information systems and data centres"	Yellow Team consists of students with pronounced research skills.
10	Blue team\ Red team\ White team\ Green team\ Yellow team	"Information security management"/ "Methods of detecting violations of information security of information- management, information- logistic and automated systems, their certification"	All students are involved in developing and setting assignments, and in accordance with the topic of their internship
11	Blue team\ Red team\ White team\ Green team\ Yellow team	Final Exam	All students participate in the development and setting of assignments, and in accordance with the topics of their thesis

As shown in the table, the model we developed represents a continuous process of developing cybersecurity competencies in integrating cyber education into IS specialist training.

As a prospect of further research into integrating cyberlearning into the educational process of IS specialists' training, we see the development of cyberlearning methodology and assessment of its performance at the appropriate stage of the integration model we presented (see Table 1).

5 CONCLUSIONS

The following conclusions were drawn as a result of the study.

1. The role and significance of cyber-teaching in training future IS specialists and in the formation of students' ideas about their role in solving the problems of neutralizing cyber-attacks in future professional activity is shown.

2. It is proved that the basis of experts' preparation on IS should be the system approach promoting step-by-step mastering of methods and technologies of repulsion of cyberattacks. The model of cyberlearning integration that we have developed serves to implement a systematic approach to student learning.

3. The eleven stages of cyberlearning integration are identified, according to which the types of cyberlearning and the disciplines studied are presented, the content of which can form the basis of cybersecurity exercises.

ACKNOWLEDGEMENTS

The team of authors would like to thank other authors of scientific works on the topic of this study, who inspired us to continue studying at the world level the problem of integration of cyber studies in the process of training future IS specialists; students who actively participate in the practical implementation of our scientific developments, as well as each other for coordinated work in the preparation of this article.

REFERENCES

Dewar, Robert S. (2018). Cybersecurity and Cyberdefense Exercise. CSS CYBER DEFENSE REPORT *Center for Security Studies (CSS), ETH Zürich*. URL: [https://css.ethz.ch/content/dam/ethz/special-](https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2018-10-Cyber_Exercises.pdf)

[interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2018-10-Cyber_Exercises.pdf](https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2018-10-Cyber_Exercises.pdf)

Fokin N. (2020). Cybercrime has escalated into a pandemic. URL:

https://www.vedomosti.ru/forum/technologii_novoj_realnosti/columns/2020/12/02/849244-kiberprestupnost

Granasen, M. and Granåsen, D. (2016). Measuring team effectiveness in cyber-defense exercises: a cross-disciplinary case study. *Cognition, Technology & Work*, 18: 121-143. DOI: 10.1007/s10111-015-0350-2.

Hatzivasilis, G., Ioannidis, S., Smyrlis, M., Spanoudakis, G., Frati, F., Goeke, L., Hildebrandt, T., Tsakirakis, G., Oikonomou, F., Leftheriotis, G. and Koshutanski, H. (2020). Modern Aspects of Cyber-Security Training and Continuous Adaptation of Programmes to Trainees. *Applied Sciences*. 10. 5702. DOI: 10.3390/app10165702

Hautamäki, J., Karjalainen, M., Hämäläinen, T. and Häkkinen, P. (2019) Cyber security exercise: literature review to pedagogical methodology. 13th annual International Technology. In *Proceedings of the Education and Development Conference*, pages 3893–3898. DOI: 10.21125/inted.2019.0985

Knüpfer M. et al. (2020) Cyber Taxi: A Taxonomy of Interactive Cyber Training and Education Systems. In: Hatzivasilis G., Ioannidis S. (eds) *Model-driven Simulation and Training Environments for Cybersecurity. MSTEC 2020. Lecture Notes in Computer Science*, volume 12512. Springer, Cham. https://doi.org/10.1007/978-3-030-62433-0_1

Lukatsky A.V. (2018) Cyber defense exercises for company management. *IT-Manager*. 5. URL: <https://www.it-world.ru/cionews/security/139202.html>

Lukatsky A.V. (2020) Cyber defense exercises are the lot for very mature customers. URL: <https://www.anti-malware.ru/interviews/2020-03-23/32270>

Malatji, M. & Solms, Sune & Marnewick, Annlizé. (2019). Socio-technical systems cybersecurity framework. *Information and Computer Security*. 27. DOI: 10.1108/ICS-03-2018-0031.

Mansurov, A.V. (2016). CTF-Oriented Paradigm for Studying Practical Information Security Issues. *International scientific journal "Symbol of Science"*. 8. pages 69-73.

Minzov, A.S., Nevsky, A.Yu., Baronov, O.R. (2019). Application of game methods in the training of specialists in the sphere of computer security. *Innovative, information and communication technologies*, 1. pages 26-29

Moore, E., Fulton, S. and Likarish, D. (2017). Evaluating a multi agency cyber security training program using pre-post event assessment and longitudinal analysis. In *IFIP World Conference on Information Security Education*, pages 147–156. Springer

Ošlejšek, R., Vykopal, J., Burská, K. and Rusňák, V. (2018). Evaluation of Cyber Defense Exercises Using Visual Analytics. *Process 2018 IEEE Frontiers in Education Conference (FIE), San Jose, CA, USA*, pages 1-9. DOI: 10.1109/FIE.2018.8659299

- Østby, G., Berg, L., Kianpour, M., Katt, B. and Kowalski, S. (2019). A Socio-Technical Framework to Improve cyber security training: A Work in Progress *Proceedings of STPIS'19*, pages 81-96.
- Petrenko, A.A., Petrenko, S.A. (2015). Cyber training: ENISA guidelines. *Cyber security issues*, 3 (11): 2-14.
- Petullo, W.M., Moses, K., Klimkowski B., Hand R., and Olson K. (2016). The Use of Cyber-Defense Exercises in Undergraduate Computing Education In *Proceedings of the 2016 USENIX Workshop on Advances in Security Education, ASE '16*, Washington, DC, USA., USENIX Association. <https://www.flyn.org/publications/2016-CDX.pdf>
- Sanders, C. (2017). *Practical Packet Analysis*, 3rd edition. William Pollock. <https://malwareanalysis.co/wp-content/uploads/2019/10/Practical-Packet-Analysis-Using-Wireshark-to-Solve-Real-World-Problems.pdf>
- Sanders, C. (2020). *Intrusion Detection Honeypots: Detection through Deception* Paperback. Applied Network Defense.
- Seker, E. and Ozbenli, H. (2018). The Concept of Cyber Defence Exercises (CDX): Planning, Execution, Evaluation. pages 1-9. DOI: 10.1109/CyberSecPODS.2018.8560673.
- Vykopal, J.; Vizváry, M.; Oslejsek, R.; Celeda, P.; and Tovarnak, D. (2017). Lessons learned from complex hands-on defence exercises in a cyber range. In *Frontiers in Education Conference (FIE)*, pages 1–8. IEEE.
- Wang, P., Dawson, M. and Williams, K. (2018). Improving Cyber Defense Education through National Standard Alignment: Case Studies. *International Journal of Hyperconnectivity and the Internet of Things*. 2, pages. 12-28. DOI: 10.4018/IJHIoT.2018010102.
- Watson, G., Mason, A. and Ackroyd, R. (2014). *Social Engineering Penetration Testing*. Syngress. 1st edition. DOI: 10.1016/C2013-0-12926-1
- Yamin, Muhammad M., Katt, B. (2018). Inefficiencies in Cyber-Security Exercises Life-Cycle: A Position Paper. In *Proceedings of the AAAI Symposium on Adversary-Aware Learning Techniques and Trends in Cybersecurity (ALEC 2018)*. http://ceur-ws.org/Vol-2269/FSS-18_paper_3.pdf
- Yamin, Muhammad M. and Katt, B. (2019). Cyber Security Skill Set Analysis for Common Curricula Development. DOI: 10.1145/3339252.3340527