

Aliya Abdiraman^{1*}, Laura Aldasheva¹, Bekzhan Darmenov¹,
Taalaibek Omurzakov¹, Alma Zakirova¹

¹Astana IT University, Astana, Kazakhstan
E-mail: aliya.abdiraman@astanait.edu.kz

Comparative analysis of application platform for learning cybersecurity through the Capturing the Flag Competitions

Abstract. *Cyberpolygon is a platform designed to train students in the field of cybersecurity in order to obtain professional skills. In this regard, Astana IT University created a project aiming at the development of a cyberpolygon with various vectors for the exploitation of cyberattacks. This project allows more than ten students to work on the platform at the same time and gain Red/Blue teaming skills. This article provides a methodology for the development of the Cyberpolygon platform. Further, through the Cyberpolygon, experimental training was conducted among the students of the second year of study at Astana IT University, which allows for solving real problems through the cyberpolygon. The performance testing and study of the platform were carried out by the methods of comparative analysis.*

Keywords: *cyberpolygon, vulnerabilities, red teaming, blue teaming, educational platform, cyber-attacks, cybersecurity training, practical skills.*

DOI: doi.org/10.32523/2616-7263-2023-145-4-49-57

1. Introduction

Today, ensuring the information security of the enterprise infrastructure is the main task of a specialist in the field of information security (IS). Indeed, in order to ensure and maintain the cybersecurity of an enterprise at a high level, it shows the level of awareness of information security employees. In this regard, students need not only theoretical skills but also practical skills in detecting new information security threats. Therefore, the main goal of the development of such platforms is to bring the level of education of students in the field of information security from lectures and laboratory work to competitions between the “red” and “blue” teams. One of the novel methods in training students within the educational program “Cybersecurity” is the use of specialized cyber training platforms, where students can not only analyze security measures by scanning IT assets for possible vulnerabilities but also bring the attack to its logical conclusion according to a pre-compiled scenario written by teachers.

The significance of this research lies in the increasing significance of cybersecurity in today’s digital world. With the ongoing adoption of digital technologies, the complexity of cyber threats and attacks has risen, creating substantial risks for governments, organizations, and individuals. As a result, there is an urgent requirement to cultivate proficient cybersecurity experts who can comprehend, prevent, and minimize these threats.

It is important to note that the number of cybercrimes is increasing every year. For example, according to analysts at Webtotem, by 2025, the cost of covering cyberattacks will reach about \$10.3 trillion. Today, small and medium-sized businesses are most susceptible to cyberattacks due to the lack of specialists in the field of information security [1]. Figure 1 clearly shows the statistics of the Computer Incident Response Service of JSC “Public Service” in the period from July to September of the current year [2]. According to statistics [2] as shown in the figure 1,

the largest number of cybersecurity threats in Kazakhstan falls on botnets, lack of access to IR, malware, denial of service, unauthorized access and phishing.

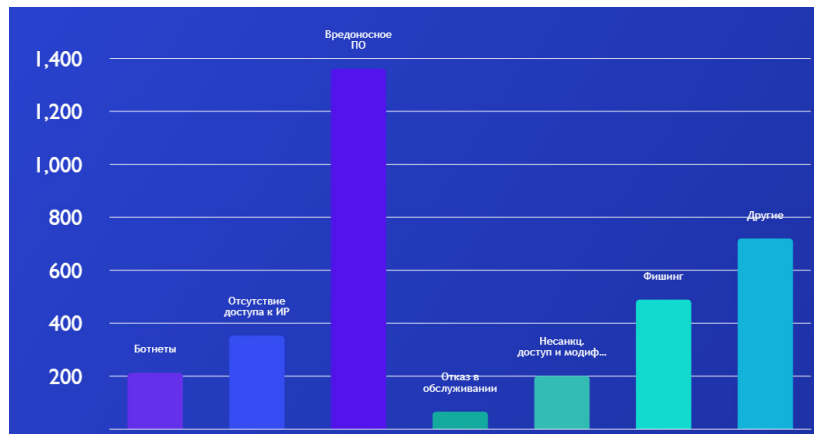


Figure 1. Statistics of incidents in the Republic of Kazakhstan in the period from July to September 2022

The above cyber-attacks most often occur in connection with the transition of many business processes to IoT technologies, therefore, attackers are trying to disable the infrastructure of private and public sector enterprises. Therefore, the best solution to prevent IS threats is to use Cyberpolygons in preparing future information security specialists.

A detailed technical description of the cyberpolygon, a comparative analysis among existing learning platforms, a review of domestic and foreign cyberpolygons, the results of an experimental study evaluating the effectiveness of the developed platform, and a detailed description of the proposed teaching method are presented in the Results and Discussion section.

2. Results and Discussion

During the study, a review of existing cyberpolygons in the country and abroad was carried out. Table 1 presents the existing cyberpolygons.

Table 1. Review of existing cyberpolygons in the country and abroad [3-7]

Name	Provider	Short description of the platform
Ampire	Perspective Monitoring	Ampire cyberpolygon emulates a typical organization, including banks, industrial enterprises, and offices, and the various attack routes that can be taken. The facility comes with a range of network templates, with the option of creating new ones to suit client preferences. The attack scenarios are continually updated based on real-life customer security analysis by Perspective Monitoring. In addition, the SOC model on the platform is based on the company's years-long work with clients.
BI.ZONE Cyber Polygon	BI.ZONE	Sber and BI.ZONE, a member of the Sber ecosystem, organize Cyber Polygon annually with the backing of Interpol and the Cybersecurity Center of the World Economic Forum. The conference offers a blend of virtual sessions, cyber security training for business teams, and informative presentations by industry specialists. High-ranking personnel from global organizations also attend [4].

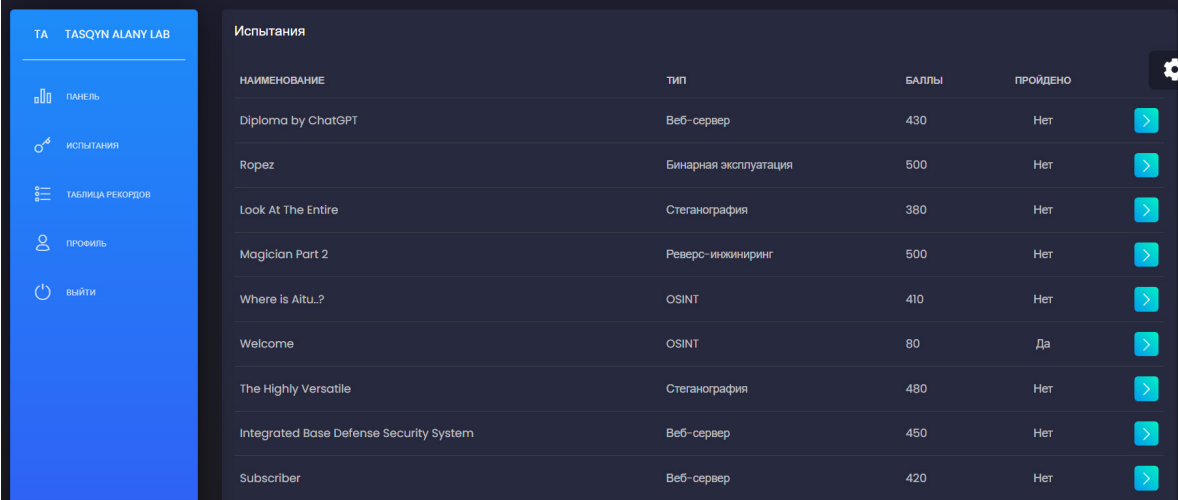
Jet CyberCamp	Jet InfoSystems	The Jet CyberCamp was introduced to the market in September 2021 as an internal development program initially designed for training company employees in areas such as conducting pentests and working in the 1st and 2nd lines of the Jet CSIRT cybersecurity center. The cyberpolygon course encompasses theoretical and practical classes that emphasize the application of acquired skills. The training begins with the sharing of expertise and problem-solving techniques by Jet Infosystems professionals, ranging from pentesting to incident investigations. Cyber students are then exposed to all aspects of cyber threats, including attack preparation by hackers and blocking such attacks. The scenarios used as cyber exercises may involve investigating past attacks or preventing future ones.
The Standoff	Positive Technologies	The initial cyber competition known as the oldest cyberpolygon of Russia began in 2011 as a CTF event held during the Positive Hack Days forum. As the format evolved to address genuine business problems, it transformed into comprehensive cyber studies where the targeted infrastructure was relocated to a simulation space for onlookers and participants to witness the consequences of cyber-attacks, such as causing a train to derail by penetrating the railway control system. In 2016, the first cyber conflict between attackers and defenders took place in a training terrain that replicated essential elements of an entire city's information infrastructure. Over time, the city became a virtual nation that encompassed whole industries instead of just individual firms.
Check Point Cyber Range	CheckPoint	The Cyberpolygon created by Check Point utilizes gamification as a principle to increase the engagement of participants in the learning process. It caters to both the attackers and defenders involved in the confrontation. The training program focuses on identifying and addressing vulnerabilities in various areas such as operating systems, applications, and web applications. Additionally, it includes education on utilizing Check Point solutions to safeguard corporate networks against cyberattacks.

The analysis revealed that there are no cyberpolygons within the educational institution of Kazakhstan. However, in Kazakhstan there is a TSARKA cyberpolygon [8], which is a paid platform for training information security specialists. Likewise, Astana IT University has developed a cyber training ground for training students in practical skills in the field of information security. This platform allows more than 10 students to work on the system simultaneously. The training ground was developed as a web application based on the classic game "capture-the-flag" via bubble.io. In turn, bubble.io is a tool for creating multi-user web applications without code.

In parallel with the technical and software implementation of the test site, a script for demonstrating the assignment for students was also worked out. In order to increase students' enthusiasm, the user interface of the cyberpolygon was developed on the basis of the famous game "Stalker", where the player, completing tasks along the way, will meet hints for finding "flags". The AITU Cyberpolygon interface consists of interconnected components such as challenges, story mode, courses. That is, in the courses part, materials for self-study are provided, in the challenges part, tasks of the easy, middle, hard, insane levels are prepared. Each task, depending on the level of complexity, is evaluated by points. It is worth noting that a student can go to the story mode part after completing the tasks in the challenges part and getting 300 points. In order

to motivate students, an updated leaderboard has been developed, in which students can see their names and the number of points they have scored relative to other participants. Figure 2 shows the user interface of the cyberpolygon «Taskyn alany lab».

The cybertraining platform is a comprehensive, interactive, and engaging learning environment designed specifically for students of Astana IT University and the military department to develop practical cybersecurity skills and foster collaboration among participants. The platform features a range of hands on learning materials, a user-friendly interface, and a modular and scalable architecture, making it a valuable resource for cybersecurity education.



The screenshot shows the user interface of the 'Taskyn alany lab' cybertraining platform. On the left is a blue sidebar with navigation options: 'ТА TASQYN ALANY LAB', 'ПАНЕЛЬ', 'ИСПЫТАНИЯ', 'ТАБЛИЦА РЕКОРДОВ', 'ПРОФИЛЬ', and 'ВЫЙТИ'. The main area is titled 'Испытания' and displays a table of tasks. The table has columns for 'НАИМЕНОВАНИЕ', 'ТИП', 'БАЛЛЫ', 'ПРОЙДЕНО', and a settings icon. The tasks listed are: Diploma by ChatGPT (Веб-сервер, 430, Нет), Ropez (Бинарная эксплуатация, 500, Нет), Look At The Entire (Стеганография, 380, Нет), Magician Part 2 (Реверс-инжиниринг, 500, Нет), Where is Aituu? (OSINT, 410, Нет), Welcome (OSINT, 80, Да), The Highly Versatile (Стеганография, 480, Нет), Integrated Base Defense Security System (Веб-сервер, 450, Нет), and Subscriber (Веб-сервер, 420, Нет). Each row has a blue arrow icon on the right.

НАИМЕНОВАНИЕ	ТИП	БАЛЛЫ	ПРОЙДЕНО
Diploma by ChatGPT	Веб-сервер	430	Нет
Ropez	Бинарная эксплуатация	500	Нет
Look At The Entire	Стеганография	380	Нет
Magician Part 2	Реверс-инжиниринг	500	Нет
Where is Aituu.?	OSINT	410	Нет
Welcome	OSINT	80	Да
The Highly Versatile	Стеганография	480	Нет
Integrated Base Defense Security System	Веб-сервер	450	Нет
Subscriber	Веб-сервер	420	Нет

Figure 2. Cyberpolygon user interface «Taskyn alany lab»

Key components of the cybertraining platform include:

1. Hands-on Learning Materials: The platform offers a diverse collection of Capture the Flag (CTF) tasks, labs, and simulated attack scenarios, covering various aspects of cybersecurity, such as vulnerability assessment, penetration testing, network security, cryptography, and incident response. These materials cater to different skill levels and learning objectives, providing students with the opportunity to apply theoretical knowledge in practical settings.

2. User-friendly Interface: The platform's interface is designed to be intuitive, interactive, and visually appealing, ensuring a smooth and engaging user experience. Navigation and access to learning materials are streamlined, allowing students to quickly find and participate in tasks and simulations that match their interests and skill levels.

3. Collaboration and Knowledge Sharing: The platform fosters a sense of community among students by encouraging interaction, collaboration, and knowledge sharing. It includes features such as chatrooms, forums, and leaderboards that allow students to communicate, discuss problems, and learn from one another, enhancing their learning experience and preparing them for teamwork in their future careers.

4. Integration with Existing Curriculum: The cybertraining platform is designed to complement and enhance the traditional classroom-based cybersecurity education at Astana IT University and the military department. By integrating the platform with the existing curriculum, students can reinforce their theoretical understanding through hands-on practice, leading to a more comprehensive grasp of cybersecurity concepts and techniques.

5. Scalable and Modular Architecture: The platform's architecture is designed to be scalable and modular, allowing for future expansion and customization as the cybersecurity landscape evolves. New techniques, technologies, and threats can be easily incorporated into the platform, ensuring that it remains relevant and effective in preparing students for real-world cybersecurity challenges.

6. Assessment and Evaluation: The cybertraining platform includes mechanisms for tracking students' progress and performance, enabling educators to assess the effectiveness of the training and identify areas for improvement. Students can also receive feedback and recommendations to help them refine their skills and address any weaknesses. According to Miller and Smith in their article "Cyber Polygons: A New Paradigm for Cyber Security Training and Exercise" published in the Journal of Cybersecurity, they introduce the concept of 'cyber polygons' as a new approach to cybersecurity training. This paradigm emphasizes the importance of practical, scenario-based training exercises that mimic real-world cyber threats, thereby providing learners with a more realistic and engaging training experience.

Depending on the tasks and specifics, the cyberpolygon infrastructure usually includes some application software / services that provide the main business processes. It can also be not only software, but also specialized hardware solutions. The maximum proximity to the real infrastructure ensures the quality of the cyberpolygon, but increases its cost. Companies must maintain a balance in this matter.

As for the evaluation of the effectiveness and performance of the use of the cyberpolygon in the process of teaching students, a study was conducted. This study involved 66 students who were divided into two groups. The first group consisted of 29 students who completed the tasks of the cyberpolygon with materials in the courses tab. In turn, the second group consisted of 37 students who completed tasks with the help of books [9-11]. To conduct an experimental study, the tasks presented in Table 2 were selected.

Table 2. List of tasks

Task	Level of difficulty	Description of the task
Stalin For Time	Hard	This quest is about winning World War II and one small event during that. This is called OSINT, and in the course of the decision, we must come to the conclusion that Eugene Holdey stole the watch as a trophy
Cable Castaways	hard	This task was focused more on programming. It was necessary to write a script that would help untangle the wires and after that they should have received a picture with a flag
Long story	middle	This is another OSINT task with elements of forensics. The participant needed to solve various riddles and solve ciphers in one stage in order to get a flag at the end
Stalker	Easy	This task is related to the game Stalker, which is due out this year. And the participants had to learn and write down
Awesome music	Easy	Participants are given regular music and with the help of steganography, they had to find a flag that was hidden in the music itself

According to Table 2, tasks of the hard level were estimated at 300 points, middle - 150 points, easy - 100 points. The study revealed that the students of the first group perform tasks faster than the second group. Here, Table 3 shows the login and points earned in the student platform. It is worth noting that students used different logins to register in the system..

Table 3. Student results

Number of students	Points scored
1	900
1	800
3	750
2	350

3	300
12	250
7	150
8	100
30	0

As can be seen from the table of towers, 29 students who used the cyberpolygon materials completed the tasks with a minimum score of 250. Students who completed the tasks with the help of books [9-11] scored a maximum score of 150 of the easy level. In turn, the students who used the materials of the cyberpolygon coped with the tasks of all levels. The histogram shown in Figure 3 clearly shows the results of an experimental study.

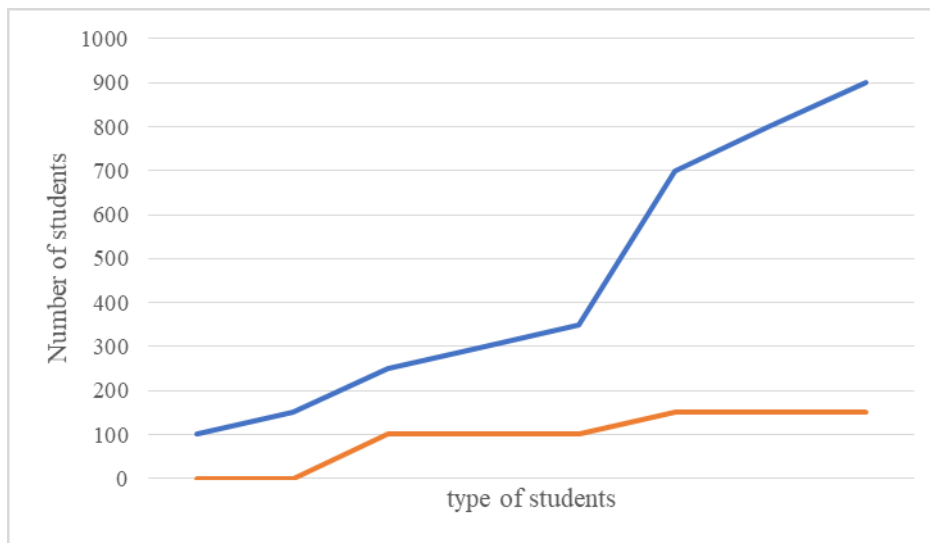


Figure 3. Ranking the results by points and materials used

It is worth noting that the term “cyberpolygon” is gaining more and more popularity as a platform for conducting exercises for information security specialists. The main principle of working on such platforms is built on the competitive effect between teams. The cyberpolygon of Astana IT University is built based on the Stalker game of the same name.

3. Conclusion

The purpose of this article is to study and create a full-featured web application using JavaScript capabilities in PERN stack with Bubble.io and the development of a prototype based on it. The project consists of 3 huge parts, each technology required a significant amount of time for detailed study and implementation of the idea. The basic concepts and main advantages of using the stack are discussed in detail, followed by a detailed explanation of the implementation process. The prototype created was an application for teaching students on the way to becoming real hackers. The assigned tasks were strictly fulfilled. On the way to the release of this web platform, a lot of new material was studied, and various programming languages were used, such as JS, C++, Python, Java, PHP etc. It may seem that this is bad when a project has so much diverse content, but there is an easy explanation behind it. The fact is that the web application is fully written in JS (ReactJS+NodeJS), as well as on bubble.io, the rest of the programming languages were used on virtual machines or on a docker configured in our physical server on the Windows operating system.

References

- 1) Johnatan B. Analysis cyberpolygon. [Electronic resource]. Available at: <https://cybersec.kz/solutions/polygon> (Accessed: 15.01.2023).
- 2) State technical service annual report. [Electronic resource]. Available at: <https://sts.kz/achievements-srki/> (Accessed: 15.03.2023).
- 3) Cyberpolygon Ampire. [Electronic resource]. Available at: <https://www.amonitoring.ru/product/ampire/> (Accessed: 15.03.2023).
- 4) BI.ZONE. (n.d.). Cyber Polygon. Cyber polygon. [Electronic resource]. Available at: <https://cyberpolygon.com/ru/> (Accessed: 15.08.2023).
- 5) Jet CyberCamp 2022. (n.d.). CyberCamp. [Electronic resource]. Available at: <https://cybercamp.su/> (Accessed: 15.08.2023).
- 6) Positive Technologies. (n.d.). The Standoff recap. [Electronic resource]. Available at: <https://www.ptsecurity.com/ww-en/about/events> (Accessed: 15.08.2023).
- 7) CheckPoint. (n.d.). Cyber Range. [Electronic resource]. Available at: <https://training-certifications.checkpoint.com/#/courses/Cyber%20Range%20Cloud-%20BLUE> (Accessed: 15.08.2023).
- 8) The results of the second-level web resources of the Republic of Kazakhstan for analyzing the security of banks. [Electronic resource]. Available at: <https://cert.kz/files/reports/kz-banks-security-report-webtotem-2021.pdf> (Accessed: 15.08.2023).
- 9) Scott N. Schober, Craig W. Schober Senior Cyber: Best Security Practices for Your Golden Years, ScottSchober.com Publishing - 2021. 234 p.
- 10) Nitul Dutta, Nilesh Jadav, Sudeep Tanwar, Hiren Kumar Deva Sarma, Emil Pricop Cyber Security: Issues and Current Trends (Studies in Computational Intelligence, 995) 1st ed. 2022.
- 11) Jeffrey Wayne Bennett Insider's Guide to Security Clearances: Get the Clearance and Land the Job (Security Clearances and Cleared Defense Contractors)

Сравнительный анализ применения платформы киберполигона для обучения в области кибербезопасности с помощью соревнований «Захват флага»

Алия Абдираман^{1*}, Лаура Алдашева¹, Бекжан Дарменов¹, Таалайбек Омурзаков¹,
Алма Закирова¹

¹ Astana IT University, Астана, Казахстан

Аннотация. Киберполигон – это платформа, предназначенная для обучения студентов в области кибербезопасности с целью получения профессиональных навыков. В связи с этим Astana I создал проект, направленный на разработку киберполигона с различными векторами использования кибератак. Этот проект позволяет более чем десяти студентам работать на платформе одновременно и приобретать навыки работы в команде Red/Blue. В этой статье представлена методология разработки платформы Cyberpolygon. Далее, в рамках Киберполигона было проведено экспериментальное обучение среди студентов второго года обучения в Astana IT University, которое позволяет решать реальные задачи с помощью киберполигона. Тестирование производительности и изучение платформы проводились методами сравнительного анализа.

Ключевые слова: киберполигон, уязвимости, redteam, blueteam, образовательная платформа, кибератаки, обучение кибербезопасности, практические навыки.

«Туды түсіру» жарысы арқылы Киберқауіпсіздік бойынша оқыту үшін киберполигон платформасының қолданылуын салыстырмалы талдау

Әлия Әбдіраман^{1*}, Лаура Алдашева¹, Бекжан Дарменов¹, Таалайбек Омурзаков¹,
Алма Закирова¹

¹Astana IT University, Астана, Қазақстан

Аннотация. Киберполигон – бұл студенттерге кәсіби дағдыларды қалыптастыру мақсатында Киберқауіпсіздік бойынша білім беруге арналған платформа. Осыған байланысты Astana I кибершабуылдарды пайдаланудың әртүрлі векторлары бар киберполигонды әзірлеуге бағытталған жоба құрды. Бұл жоба оннан астам студенттерге платформада бір уақытта жұмыс істеуге және Red/Blue командасында жұмыс істеу дағдыларын алуға мүмкіндік береді. Бұл мақалада cyberpolygon платформасын әзірлеу әдістемесі берілген. Әрі қарай, Киберполигон шеңберінде Astana IT University-де оқудың екінші жылының студенттері арасында эксперименттік оқыту өткізілді, бұл киберполигонның көмегімен нақты міндеттерді шешуге мүмкіндік береді. Өнімділікті тексеру және платформаны зерттеу салыстырмалы талдау әдістерімен жүргізілді.

Түйін сөздер: киберполигон, осалдықтар, қызыл бірлестік, көк бірлестік, білім беру платформасы, кибершабуылдар, киберқауіпсіздікке үйрету, практикалық дағдылар.

Сведения об авторах:

Рус.:

Әбдіраман Ә.С. – магистр, сеньор-лектор, Департамент интеллектуальных систем и кибербезопасности, Astana IT University, Проспект Мангилик ел 51, Астана, Казахстан, aliya.abdiraman@astanait.edu.kz

Алдашева Л.С. – кандидат технических наук, доцент, Департамент интеллектуальных систем и кибербезопасности, Astana IT University, Проспект Мангилик ел 51, Астана, Казахстан, laura.aldasheva@astanait.edu.kz

Дарменов Б. – студент, Департамент интеллектуальных систем и кибербезопасности, Astana IT University, Проспект Мангилик ел 51, Астана, Казахстан, 202199@astanait.edu.kz

Омурзаков Т.И. – Начальник цикла «Кибербезопасность» Военной кафедры, Astana IT University, Мәңгілік ел көшесі 51, Астана, Қазақстан, omurzakov.67@mail.ru

Закирова А.Б. – кандидат педагогических наук, доцент, Департамент интеллектуальных систем и кибербезопасности, Astana IT University, Проспект Мангилик ел 51, Астана, Казахстан, a.zakirova@astanait.edu.kz

Каз.:

Әбдіраман Ә.С. – магистр, аға оқытушы, Зияткерлік жүйелер мен киберқауіпсіздік Департаменті, Astana IT University, Мәңгілік ел көшесі 51, Астана, Қазақстан, aliya.abdiraman@astanait.edu.kz

Алдашева Л.С. – техникалық ғылымдар кандидаты, доцент, Зияткерлік жүйелер мен киберқауіпсіздік Департаменті, Astana IT University, Мәңгілік ел көшесі 51, Астана, Қазақстан, laura.aldasheva@astanait.edu.kz

Дарменов Б. – студент, Зияткерлік жүйелер мен киберқауіпсіздік Департаменті, Astana IT University, Мәңгілік ел көшесі 51, Астана, Қазақстан, 202199@astanait.edu.kz

Омурзаков Т.И. – Әскери кафедраның «Киберқауіпсіздік» циклі басшысы, Astana IT University, Мәңгілік ел көшесі 51, Астана, Қазақстан, omurzakov.67@mail.ru

Закирова А.Б. – педагогика ғылымдарының кандидаты, доцент, Зияткерлік жүйелер мен киберқауіпсіздік Департаменті, Astana IT University, Мәңгілік ел көшесі 51, Астана, Қазақстан, a.zakirova@astanait.edu.kz

Англ.:

Abdiraman A.S. – master, senior lecturer, Department of Intelligent Systems and Cybersecurity, Astana IT University, Mangilik Yel Avenue 51, aliya.abdiraman@astanait.edu.kz

Aldasheva L.S. – candidate of technical sciences, assistant professor, Department of Intelligent Systems and Cybersecurity, Astana IT University, Mangilik Yel Avenue 51, laura.aldasheva@astanait.edu.kz

Darmenov B. – student, Department of Intelligent Systems and Cybersecurity, Astana IT University, Mangilik yel avenue 51, 202199@astanait.edu.kz

Omurzakov T.I. – Head of the cycle “Cybersecurity” of the Military Department, Astana IT University, Mangilik Yel Avenue 51, omurzakov.67@mail.ru

Zakirova A.B. – Candidate of Pedagogical Sciences, assistant professor, Department of Intelligent Systems and Cybersecurity, Astana IT University, Mangilik Yel Avenue 51, a.zakirova@astanait.edu.kz