Online-Journals.org

iJEP International Journal of Engineering Pedagogy

iJEP | eISSN: 2192-4880 | Vol. 15 No. 4 (2025) | OPEN ACCESS

https://doi.org/10.3991/ijep.v15i4.53127

PAPER

Integration of Cybersecurity into Computer Science Teachers' Training: A Systematic Review

Meruyert Serik[1], Danara Tleumagambetova[1], Shyryn Tutkyshbayeva[2](✉), Alma Zakirova[1]

[1]L.N. Gumilyov Eurasian National University, Astana, Kazakhstan

[2]Astana IT University, Astana, Kazakhstan

sh.tutkyshbayeva@astanait.edu.kz

ABSTRACT

This paper addresses the integration of cybersecurity into the training programmes of computer science teachers in higher education institutions. Given the growing digital threats such as phishing, malware, and data leakages, attaining cybersecurity knowledge and skills becomes critical for educators. Based on a systematic review of 51 empirical studies selected from databases such as Scopus, Web of Science and Springer Link, different approaches to integrating cybersecurity into educational programmes and the results of such interventions are examined. This study shows that the systematic integration of cybersecurity topics and the use of interdisciplinary methods and tailored programmes contribute to the development of professional competencies, critical thinking and ethical skills. Key challenges include different levels of technological readiness among teachers and the need to regularly update curricula in response to rapidly changing cyber threats. The study also identifies the lack of practice-orientated training and specialised courses as significant barriers to effective integration. The results emphasise the importance of improving curricula to enhance the effectiveness of cybersecurity education and adapt to the requirements of today's digital environment.

KEYWORDS

cybersecurity, digital threats, higher education, teacher training

1 INTRODUCTION

Cybersecurity is an emerging and rapidly evolving field characterised by a growing body of research [1]–[3]. Rising dependence on the Internet and complex technological infrastructures in education have made cybersecurity a critical issue, as digital technology and cybersecurity are inextricably linked [3]. In such a context, the rapid development of digital environments creates new learning opportunities. Still, it increases the risks of cyber threats like phishing, malware and data leakages that require robust data and systems protection [4], [5]. Thus, cybersecurity should be integrated into the educational processes since it plays a key role in protecting educational institutions' data and digital systems [2], [5]. So, it is essential

Serik, M., Tleumagambetova, D., Tutkyshbayeva, S., Zakirova, A. (2025). Integration of Cybersecurity into Computer Science Teachers' Training: A Systematic Review. *International Journal of Engineering Pedagogy (iJEP)*, 15(4), pp. 57–75. https://doi.org/10.3991/ijep.v15i4.53127

Article submitted 2024-11-04. Revision uploaded 2025-01-27. Final acceptance 2025-01-27.

to consider what approaches to integrating cybersecurity into teacher training are most commonly used in higher education institutions and what results are achieved in training computer science teachers capable of transferring this knowledge to their students when integrating cybersecurity programs [6]–[10].

However, integrating cybersecurity into educational programmes has several challenges. Research indicates that the cybersecurity knowledge and skills level among computer science teachers is often insufficient, posing significant security risks for educational processes and students [3], [11]–[13]. Traditional teacher training programmes do not always cover all aspects of cybersecurity, resulting in knowledge and practical skills gaps. These gaps can significantly reduce teaching effectiveness and may even lead to vulnerabilities in educational institutions' cyber systems [11]–[14]. Besides, the varying levels of technological readiness among teachers hinder the implementation of unified standards and approaches to teaching cybersecurity, and the rapid growth and evolution of new digital threats necessitate continual updates to the curriculum, presenting an additional task for educational institutions [13], [15], [16]. Nevertheless, education focused on cybersecurity awareness leads to safe practices in cyberspace [9], [17]–[19]. For example, the level of education of an Internet user's immediate environment (family, friends, colleagues and others) can significantly influence his or her cybersecurity behaviour, i.e., an environment with a low level of ICT education can reduce the user's motivation to adhere to safe practices and attitude to data protection [9], [17]. It happens so since institutional and social contexts shape unique security practices depending on the engagement field [18], [19].

This highlights the need to develop educational programmes designed to improve teachers' cybersecurity awareness. After all, understanding the impact of the social environment and education helps to better integrate cybersecurity into the educational process of training computer science teachers. Such integration of cybersecurity differs significantly in approaches across various educational contexts. For instance, some universities integrate cybersecurity training into general computer science courses; meanwhile, other institutions develop specialised programmes and modules that focus on an in-depth study of the topic [2], [8]–[10], [20].

Also, approaches built on the integration of theoretical and practical elements are effective. For example, the use of experiential learning theory, which engages in real-life scenarios, allows learners to experience the complexities of cybersecurity [21]. Moreover, problem-based learning, which emphasises solving real-world networking problems and developing critical thinking, is valuable [21]. Such a comprehensive approach enables us to adapt practices to specific educational conditions and effectively prepare teachers for the challenges of the digital environment.

Given the importance of integrating cybersecurity in today's education and the necessity to increase cybersecurity awareness to achieve a higher level of security in the cyber environment, it has become relevant to examine the approaches to integrating cybersecurity into teacher training and understand the results of training computer science teachers when integrating cybersecurity into the curricula.

Thus, the following research questions have been developed to guide this study.

- What approaches to integrating cybersecurity into teacher training are most commonly used in higher educational institutions?
- What outcomes are achieved in training computer science teachers when integrating cybersecurity programmes?

To answer these questions, a systematic review of 51 empirical studies selected from databases such as Scopus, Springer Link and Web of Science was chosen as the

main method. This choice is justified based on the fact that a systematic review allows a large amount of data to be collected and analysed, which makes it possible to draw objective and valid conclusions. However, before exploring the applied method and other details of the methodology, it is worth introducing the background to this study.

2 CYBERSECURITY EDUCATION IN KAZAKHSTAN

Cybersecurity emerged as a discipline in response to rapid digitalisation and the ever-increasing amount of data that needed to be protected. With the expansion of the Internet and the introduction of complex information systems, the need to protect data has become a key challenge for educational institutions in Kazakhstan, especially during the COVID-19 and post-pandemic periods [22].

In Kazakhstan, cybersecurity has gained urgency as part of the Concept of Digital Transformation, Information and Communication Technology Industry Development and Cybersecurity for 2023–2029 (the Concept) [23], which aims to introduce advanced digital solutions into all spheres of life. However, despite such a demanding concept, educational programmes dedicated to cybersecurity training of teachers remain under-researched in the country.

In most universities, raising cybersecurity awareness is integrated into general cybersecurity and information technology courses, while specialised modules are rarely introduced [24]. It greatly limits the possibilities of training qualified specialists capable of working in the context of modern digital challenges. Thus, indicating the importance of integrating cybersecurity into educational processes to train computer science teachers, the study suggests adapting educational programmes to the challenging demands of the digital epoch [24], [25]. Besides, these authors highlight that along with such adaptations of programmes to train teachers together with students to be aware of today's cyber threats, higher education institutions should provide all the necessary technical support [24], [25]. However, although such statements remain simple as general suggestions, authors [24], [25] still emphasise the necessity of finding advanced educational solutions.

Overall, analysing the Scopus database showed that Kazakhstani researchers have been actively publishing papers on cybersecurity since 2017. To date, 46 academic publications have been registered in the database and this figure is gradually increasing every year. The publications are primarily in the Russian and Kazakh languages. However, there is a very small number of publications devoted to the study of cybersecurity in the educational sphere, especially in the English language.

Indeed, Kazakhstan attempts to develop approaches to cybersecurity education in line with global trends and national specifics to equip teachers with competencies to ensure cybersecurity. Integrating cybersecurity topics into general computer science and ICT courses is the most common approach. While this provides basic knowledge about data protection and attack prevention, it is limited by the depth of the subject matter [24]. Thus, it is suggested to strengthen the educational programmes on cybersecurity training to meet the market demands of the IT industry [26]. The Concept [23] specifies even attracting qualified industrial IT specialists to provide a case-based curriculum. Nevertheless, for a start, to achieve such demands, it is necessary to introduce practice-oriented and problem-orientated approaches to teaching cybersecurity to the teaching staff of higher education institutions to gain hands-on experience to explore cyber threats and apply them in real-life scenarios. This helps develop critical thinking skills to analyse complex situations and make informed decisions following cyber ethics [27]–[29].

3 METHODOLOGY

Understanding the necessity driven by today's rapid development of digitalisation along with the need to train specialists capable of addressing the challenging realities of cyber threats, higher education institutions need to introduce well-tailored curricula and specifically train their teaching staff to ensure that the transferred knowledge can help students adapt to the ever-changing cyber environment. Consequently, there is a growing need for systematic research design to examine the approaches to integrating cybersecurity into teacher training and understand the results of training computer science teachers when integrating cybersecurity into the curricula.

Thus, this study addressed two key research questions:

- What approaches to integrating cybersecurity into teacher training are most commonly used in higher educational institutions?
- What outcomes are achieved in training computer science teachers when integrating cybersecurity programmes?

To answer these two research questions, a systematic literature review was chosen as the primary method to achieve the study objectives and address the study questions. This choice is justified by the systematic review's capability to gather and analyse a large volume of data, enabling objective and valid conclusions [30]. Besides, systematic reviews can be conducted using various methods of data synthesis [30].

This study employed a qualitative content analysis, guided by the principles of an inductive approach to category creation based on the data [31]. The inductive approach was chosen because it aligns with the aim of this study to understand how these studies approached integrating cybersecurity into teacher training and because we did not want to mould these approaches into existing theories. The content analysis involved stages of open coding, category creation, and abstraction. Meaningful text fragments were identified as the unit of analysis for coding.

The assessment of data analysis quality and coding framework included verifying the coding process for consistency and reliability. In this study, a pilot coding was conducted, and the initial coding framework through a systematic process of coding classification and identification of themes and patterns from selected articles was modified. All authors participated in concluding coded data and discussing patterns, category interrelationships, and theoretical interpretations.

Thus, the conducted content analysis enabled the identification and classification of approaches to integrating cybersecurity and associated educational outcomes in training computer science teachers in higher education.

3.1 Search strategy

The study started with the stage of searching and selecting relevant articles. The primary data sources were the Scopus and Springer Link databases, providing access to a broad spectrum of scientific publications on cybersecurity topics. The search was conducted using the following keywords: "Computer Security in Education", "Cybersecurity in Higher Education", "Data Protection in Educational Institutions", "Cyber Threats in Education", and "IT Security Training for Educators". These keywords were chosen based on their relevance to the study questions

and contemporary challenges related to cybersecurity in educational institutions. To structure the selection processes and analyse the selected materials, the Excel spreadsheet was used since all other software required additional costs.

The search criteria for the articles were the following: (1) written in English; (2) based on empirical research; (3) focused on cybersecurity in the educational sphere; and (4) published in peer-reviewed scholarly journals.

As a result of the search, 409 (Springer Link-196, Scopus-145, Web of Science-68) articles were yielded, out of which 51 were selected for further analysis covering the period from 2010 to 2024.

These articles underwent rigorous selection based on the criteria of relevance, availability of empirical data, and publication quality. The final set of articles included publications that extensively examined issues such as integrating cybersecurity into educational programmes, analysed existing approaches to information and data protection in educational institutions, and outlined the results of training computer science teachers when integrating cybersecurity into the curricula. Figure 1 presents the search results structured into a flowchart. This figure reflects visually the keywords used in the search process, as well as the number of articles found and selected.

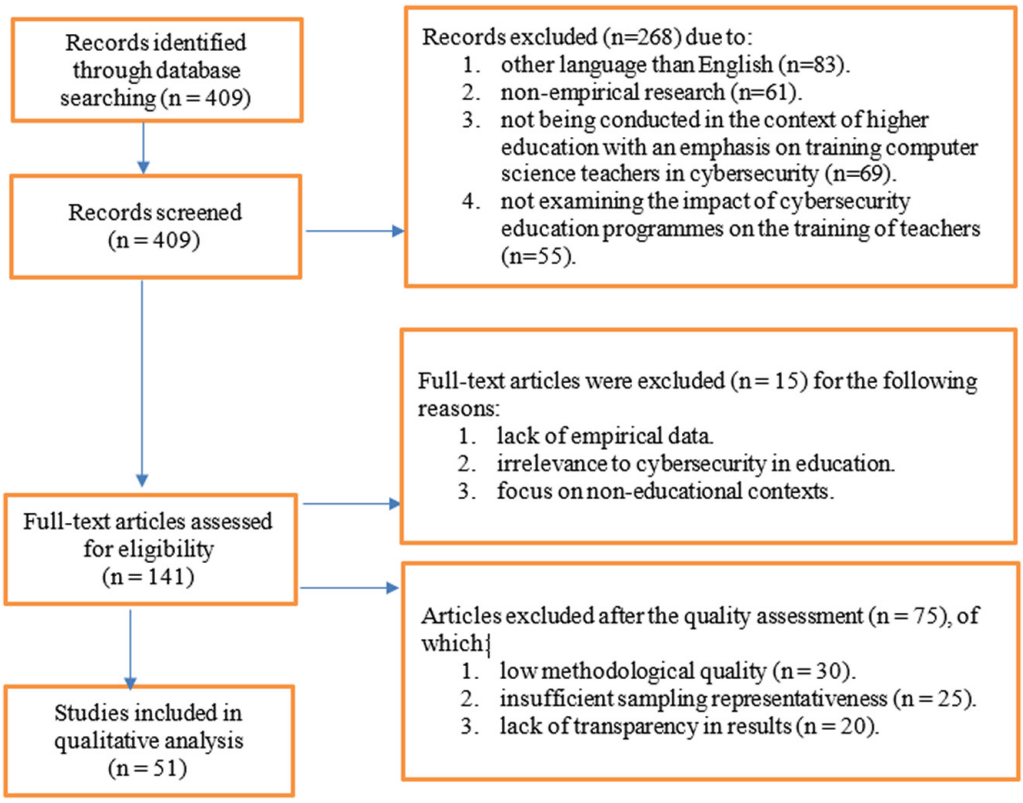

Fig. 1. Literature selection search results

3.2 Data extraction

The primary aim of the study was to include in the review only those articles that empirically studied the influence of integrating cybersecurity into educational programmes on teacher training. During the selection process, 268 articles

were excluded, mainly because they were written in languages other than English (n = 83) or were not empirical studies (n = 61). Also, many articles were not conducted in the context of higher education with a focus on training computer science teachers in cybersecurity (n = 69) and did not examine the impact of cybersecurity education programmes on the training of teachers (n = 55).

To extract key information from the remaining 141 articles, a data matrix was created including the following information for each study: author(s), year of publication, context and sample, study design, methods used to train teachers in cybersecurity, rationale for using these methods, and key findings related to teacher training. An additional 15 articles were excluded during the data analysis process. The main reasons for excluding at this stage were:

Firstly, the lack of empirical data (n = 5) made these studies inapplicable, as they did not provide the necessary framework to analyse the findings in the context of teacher training.

Second, several articles were irrelevant to cybersecurity in education (n = 6), reducing their relevance to this research topic.

Third, four articles were excluded due to a focus on non-educational contexts (n = 4), which again were incompatible with the aims of this analysis.

Besides, it should be mentioned that initially 75 articles were excluded after quality assessment, among which 30 articles had low methodological quality, 25 had insufficient sampling representativeness, and 20 had a lack of transparency in the results.

More than that, for example, the assessment revealed that the number of publications devoted to cybersecurity in educational institutions in Kazakhstan is significantly inferior to similar studies in countries such as the United States (173 publications), the United Kingdom (46 publications) and China (35 publications) (Figure 2). It indicates that, despite the existence of scientific interest in cybersecurity, this topic is still under-researched in Kazakhstan. More particularly, in the period from 2010 to 2024, the Scopus database recorded only three articles published by Kazakhstani authors on this topic in the English language. These articles were also excluded from the study due to their irrelevance to the research questions.

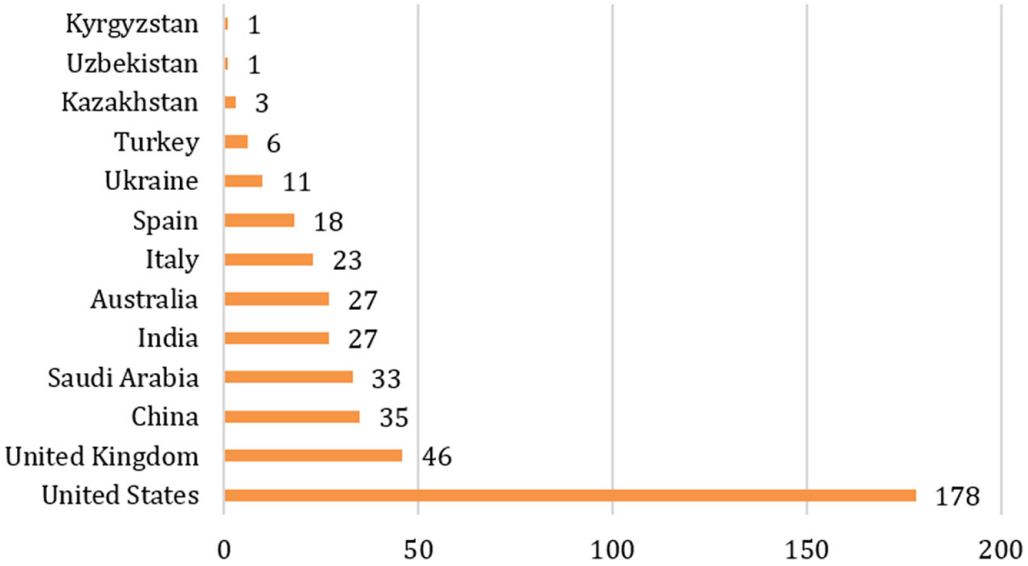

Fig. 2. Literature selection results by country (period 2010–2024)

4 ANALYSIS AND RESULTS

This study adopted a systematic search strategy that covers a wide range of original empirical research in the field of cybersecurity in educational institutions. The review incorporates both selective and representative search strategies, allowing the coverage of both narrowly focused and more general studies [30]. For this review, a systematic search strategy was applied, including recent and significant studies selected for inclusion in the search database on the L.N. Gumilyov Eurasian National University portal.

The Eurasian University portal provides access to hundreds of databases like Scopus, Web of Science and Springer Link (access through https://lib.enu.kz/ru/podpisnye-bazy-dannyh/), enabling a comprehensive analysis of existing literature on cybersecurity in education. Preliminary searches were conducted across various databases to compile a broad set of relevant sources. The final search was completed in early September 2024, including the most current and significant publications relevant to the research topic in the analysis.

The quality screening results included 51 studies with considerably varied sample sizes, ranging from small groups to larger cohorts. Some of these studies did not include important information such as the total number of participants or a description of the control groups. This lack of data made comparing results more difficult and required a more careful approach to interpreting the findings.

4.1 Examining the approaches to integrating cybersecurity into teacher training

During the initial categorisation stage, articles were classified into two main categories: those that included the definition of cybersecurity and those that did not. The latter category was further divided into two separate categories. In the abstraction phase, three mutually exclusive categories were conceptualised using content-characteristic words such as "cybersecurity defined as an integrated educational element", "cybersecurity not defined but considered as an integrated educational element", and "cybersecurity not defined but considered as a specialised teaching approach". These main categories were created to cover one aspect of the data, aiming for unidimensionality.

During the second stage, subcategories were formed based on qualitatively different descriptions of how cybersecurity is integrated into the educational programme. The unit of analysis was the textual description, allowing one study to be coded in multiple subcategories within one main category [32], [33]. Some difficulties in the levels of hierarchy coding were evident in the multidimensional subcategories and their relationship to the main categories. In this study, however, the decision was made to explore the diversity of descriptions of the concept of cybersecurity in original studies rather than the relationships between these descriptions.

This review examines the current use of the concept of integrating cybersecurity in the training of computer science teachers in higher education institutions, with particular attention to defining key concepts, approaches and arguments supporting their application. According to the findings, cybersecurity integration was found in 51 articles through three main approaches: (1) cybersecurity is considered an integral part of the educational process, (2) cybersecurity is not defined as a separate element but integrated into the overall educational process, and (3) cybersecurity is

viewed as a specialised approach to teaching. The overall analysis revealed that each of these three main categories consists of several subcategories. Table 1 illustrates these three categories of definitions with examples.

Table 1. Key categories of cybersecurity integration in training computer science teachers

Key Categories	Subcategory	Application Example	Total n*
Category 1: Cybersecurity as an integral part of the educational process	Systemic security integration	Including cybersecurity topics in every teacher training course	n = 45
	Regular training and practices	Ongoing seminars and laboratory work on data protection	n = 32
Category 2: Cybersecurity as an integrated element of the educational process	Integrating cybersecurity into other disciplines	Learning the principles of cybersecurity in programming courses	n = 40
	An interdisciplinary approach	Using cybersecurity as an example in different lessons	n = 35
Category 3: Cybersecurity as a specialised approach to education	Specialised courses	Developing and implementing individual cybersecurity courses	n = 27
	Advanced programmes	Creating training programmes entirely dedicated to cybersecurity	n = 20

Note: The term "n" may include multiple entries from the same study.

In this study, the definition of integrating cybersecurity into computer science teacher training (main category 1, n = 45) was grouped into subcategories like systemic security integration and regular training and practices. Specifically, systemic integration entails the inclusion of cybersecurity topics in every training course (n = 45), which promotes teachers' continuous awareness in this area. At the same time, regular training and practices (n = 32) serve as a practical component to reinforce data protection knowledge and skills.

The definition of integrating cybersecurity into computer science teacher training (main category 2, n = 40) was grouped into subcategories like integrating cybersecurity into other disciplines and an interdisciplinary approach. Integration of cybersecurity into other disciplines (n = 40) reflects incorporating cybersecurity principles into programming courses to enhance teachers' data protection skills in a broader educational context. The interdisciplinary approach (n = 35) demonstrates the use of cybersecurity as a case study in a variety of academic subjects, which promotes a holistic view of the topic.

The analysis of cybersecurity as a specialised approach to education in this study (main category 3, n = 27) focused on specialised courses and advanced programmes. Specialised courses (n = 27) involve the design and implementation of standalone courses entirely dedicated to cybersecurity, allowing the exploration of data protection and network security topics in depth. Advanced programmes (n = 20) are more detailed curricula focused entirely on cybersecurity, providing more thorough mastery of material and professional training in the field.

Moreover, Table 2 displays a summary of the 72 sources that were examined to analyse the rationales presented in the studies. The analysis revealed seven categories that justify the applied approaches to cybersecurity training: (1) empirical research-based justification for enhancing learning effectiveness, (2) commonly accepted justification for enhancing learning effectiveness, (3) policy-level recommendations,

(4) workplace expectations, (5) personal perceptions, (6) learning theories, and (7) general trends. The most common argument supporting the use of cybersecurity was that previous studies had demonstrated positive outcomes in promoting learning effectiveness (n = 17). The second most prevalent argument for using cybersecurity also relied on the belief in its benefit for learning, albeit without referencing specific research evidence (n = 14). Several studies justified the need for cybersecurity based on policy-level recommendations (n = 9) or requirements of the contemporary work environment (n = 9), often citing general skills that trainees should develop and can enhance through these methods. Some studies have posited the theories of learning as a basis for cybersecurity or portrayed cybersecurity as a prevailing trend displacing traditional teaching methods.

Table 2. Arguments for approaches applied in cybersecurity training of computer science teachers (n = 72)

Arguments	Examples
Empirical research-based rationale for improving learning effectiveness (n = 17)	The study shows that using case studies increases the trainees' interest in ethical issues and contributes to a better understanding of these aspects. Completing such a course ensures improvements in critical thinking skills and the ability to analyse ethical situations [34].
The generally accepted rationale for improving learning effectiveness (n = 14)	High-quality cybersecurity education enhances an institution's overall security and provides trainees with skills they can apply in their future careers. It improves the quality of learning and prepares for real-world information security threats [35].
Policy-level recommendations (n = 9)	It is recommended that appropriate AI techniques be selected based on specific tasks and criteria that can significantly improve the effectiveness of cybersecurity training [36].
Expectations of working environment (n = 9)	Based on the proposed educational framework, a dynamic modular design is incorporated, allowing modules to be replaced and modified during workflows. Such flexibility enables the creation of hybrid courses and customised learning programmes built on assessable learner profiles [36].
Own perceptions (n = 9)	Cybersecurity education through a hands-on approach creates unique opportunities. Working on real-world projects helps one learn better and develop critical thinking, reinforcing the importance of theory and practice. Partnerships between educational institutions and companies enrich the educational process, allowing one to gain hands-on experience in the rapidly changing field of cybersecurity [21].
Theory of learning (n = 8)	The emphasis in cybersecurity is on constructivism, which implies the active involvement of trainees in the learning process. Project-based and problem-based learning methods facilitate theoretical knowledge in practice and develop critical thinking. Integrating technology, such as simulations and laboratory work, helps build trainees' confidence and readiness for real security challenges [37].
General trends (n = 6)	The study demonstrates that the level of social education has a significant impact on cybersecurity awareness. Trainees with higher levels of social education exhibit better knowledge of cyber threats and take a more responsible approach to their online security. This highlights the importance of integrating cybersecurity education programmes into the curriculum and the need to raise awareness among professionals in the workplace to ensure a higher level of security in the digital environment [9].

4.2 Outcomes related to the integration of cybersecurity into training computer science teachers

The second aim of the analysis was to examine outcomes related to the integration of cybersecurity and how these outcomes were assessed in the studies reviewed. The analysis of the second research question focused exclusively on studies that treated cybersecurity as an educational element.

The analysis fell into two categories. The first category involved evaluating educational outcomes. Initially, the descriptions of educational outcomes were identified and categorised based on the specific outcomes studied (e.g., 'positive knowledge outcomes', 'improvement in teamwork skills'). These outcomes were then grouped into five final subcategories of educational outcomes.

The second category focused on analysing methods for assessing cybersecurity training outcomes. Primarily, these methods were identified and classified (e.g., 'survey', 'final exam'). These categories were then grouped into five final subcategories and appropriately labelled. Since the units of analysis were educational outcomes and assessment methods, each study could be included in multiple subcategories.

For the analysis of the first category, based on the analysis of 51 selected articles, five subgroups were identified describing how cybersecurity integration affects knowledge, skills, and professional readiness (refer to Table 3).

Table 3. Outcomes of integrating cybersecurity in the training of computer science teachers (n = 51)

Subcategories	Description	Application Example	Total n*
Subcategory 1: Positive knowledge outcomes	Improving theoretical understanding of cybersecurity concepts	Greater understanding of threat detection mechanisms	n = 35
Subcategory 2: Improving teamwork skills	Developing collaborative problem-solving skills through group activities	Teamwork on cybersecurity cases	n = 28
Subcategory 3: Application of practical skills	Improving the ability to apply cybersecurity knowledge in simulated or real-world scenarios	Practical laboratory work on safe programming	n = 31
Subcategory 4: Professional readiness for employment	Enhancing preparedness for work in the cybersecurity field	High rates of employment of graduates who have completed the training	n = 25
Subcategory 5: Ethical awareness in cybersecurity	Increasing awareness of ethical considerations in cybersecurity practices	Understanding the principles of ethical hacking and responsible use of data	n = 18

The first subcategory relates to positive knowledge outcomes. Trainees taking courses with cybersecurity integration demonstrate an improved theoretical understanding of core concepts such as threat detection mechanisms. These results, confirmed in 35 studies, suggest that integrating cybersecurity topics into educational programmes contributes to a significant increase in trainees' knowledge.

The second subcategory concerns improving teamwork skills. Integrating cybersecurity fosters collaborative problem-solving skills, which is particularly relevant in teamwork. For example, 28 studies indicate that group assignments, such as analysing real-world cyber threat cases, help students learn how to interact effectively with each other, find optimal solutions and assign responsibilities.

The third subcategory focuses on the application of practical skills. Programs with cybersecurity elements provide students with opportunities to apply theoretical knowledge in real or simulated environments. It may include laboratory work related to secure programming or vulnerability testing. 31 studies have shown that such practical assignments contribute to the development of trainees' confidence and professional competence.

The fourth subcategory indicates that trainees' professional readiness for employment is another important educational outcome. Graduates who have completed cybersecurity training demonstrate a high level of preparation and demand in the labour market. 25 surveys show that employers recognise the high professional readiness of graduates with cybersecurity training, which positively impacts their career prospects.

The latter subcategory emphasises the development of trainees' ethical awareness. This includes understanding the principles of ethical hacking and responsible data handling, which helps future professionals make informed and ethically sound decisions. 18 studies highlight the importance of such knowledge for successful cybersecurity careers.

The second category of the analysis explored methods for assessing cybersecurity training outcomes. These methods were identified and grouped into five final subcategories (refer to Table 4).

Table 4. Assessment methods of cybersecurity training outcomes (n = 117)

Assessment Methods	Examples
Subcategory 1: Surveys and questionnaires (n = 30)	The survey conducted helped identify that the students valued distance learning (92%), but satisfaction is lower in teacher training institutions due to the difficulty of laboratory classes. The study emphasises the importance of trust between teacher and student for effective knowledge and skills assessment and the application of necessary changes based on the feedback provided [7].
Subcategory 2: Final exams (n = 25)	In the study, the initial scores of the participants addressed the differences in their knowledge, and the final test scores assessed the success of the learning experience [38].
Subcategory 3: Practical assignments (n = 27)	The study shows that the focus was on presentations and discussions, but practical assignments significantly improved the application of theory and understanding of cybersecurity [39].
Subcategory 4: Laboratory works (n = 20)	Studies demonstrate that integrating cybersecurity into curricula significantly improves learners' career readiness. For example, the DETER project provides access to virtual labs where students practise skills to deal with real cyberattacks. Positive feedback from participants, especially during the COVID-19 pandemic, confirms the effectiveness of such formats. Virtual labs help students better absorb theory and delve into practice, creating an optimal environment for cybersecurity training [40], [41].
Subcategory 5: Case studies (n = 15)	Such a course helped develop the critical and interdisciplinary thinking necessary to analyse phishing attacks. The learners developed skills to evaluate information and make informed decisions, which are important for identifying phishing threats [42].

Assessing educational outcomes in higher education institutions is a crucial element that helps understand the effectiveness of integrating cybersecurity into the training of computer science teachers. A key aspect of this assessment is how learners acquire and apply the knowledge gained through such programmes, and how this knowledge impacts their readiness for professional activities.

The assessment of educational outcomes typically employs various tools such as final exams, projects, laboratory assignments, and student surveys. Some universities use the Moodle system, allowing instructors to track progress and analyse the achievements across different modules [43], [44]. This facilitates timely adjustments to educational programmes and adaptation to the needs of learners.

A successful example of outcome assessment can be seen in the report on graduates from Johns Hopkins University, demonstrating that students who completed cybersecurity courses exhibit high readiness for careers in this field, supported by employer feedback and strong employment rates [45].

Thus, the assessment of educational outcomes in higher education institutions, especially in the context of cybersecurity, should be comprehensive, considering both the academic and practical achievements. This approach not only enhances educational quality but also ensures the readiness to meet the challenges of the modern digital world.

5 DISCUSSION

Although cybersecurity has gained urgency as part of the Concept of Digital Transformation, Information and Communication Technology Industry Development and Cybersecurity for 2023–2029 in Kazakhstan [23]; Figure 2 shows the tremendous gap in this field in Kazakhstan as compared to other countries. Only three articles published in the English language were registered in Scopus, and even the publications in the Russian and Kazakh languages, if searched through Google Scholar, hardly cover the posed research questions.

Thus, given the importance of cybersecurity issues to Kazakhstan and not only, it was necessary to conduct a systematic review to examine the approaches to integrating cybersecurity into teacher training and understand the results of training computer science teachers when integrating cybersecurity into the curricula. This discussion of the study results highlights key points related to current cybersecurity education practices in higher education institutions, as well as their impact on educational outcomes and teacher training.

The systematic literature review confirms that the most common approach to teaching cybersecurity in higher education institutions is to integrate cybersecurity topics into general computer science and ICT courses. This approach, which is widely used in Kazakhstan, provides a basic level of knowledge and skills but limits opportunities for in-depth study and practical application of the topic [7], [26].

On the contrary, in international practice, an experiential learning theory that engages students in real-life cyber threat scenarios is actively used [21]. This promotes the development of analytical skills, critical thinking and the ability to make informed decisions. Thus, the findings of this study emphasise the effectiveness of practice-orientated learning, including laboratory exercises and case analysis, for training computer science teachers [27], [42].

Besides, considering that cybersecurity can be an integral part of the educational process, it is recommended to embed cybersecurity topics in every curriculum to increase the learners' awareness of cybersecurity issues [34]. Then, since cybersecurity can also be an integrated element of curricula, the results specify the use of interdisciplinary approaches and involve the application of such approach to training cybersecurity as an example across disciplines [9].

Results highlight applying the interdisciplinary approach to integrating cybersecurity into disciplines like law and social sciences. This allows the development of

the legal and ethical aspects of cybersecurity issues, e.g., understanding the principles of ethical hacking and responsible use of data. Indeed, such approaches help to form a more holistic view of cybersecurity [9], [10]. Such knowledge contributes to the development of responsible attitudes towards the use of technology and ethical decision-making, which is particularly important for the training of computer science teachers who pass these values on to their students. However, this approach to training is rarely used in Kazakhstan and remains limited, which creates a gap in preparing teachers for the modern challenges of the digital environment.

As for cybersecurity as a specialised approach, the results emphasise the need to develop specialised courses, which will ensure an in-depth study of cyber threats and professional training in this field [40]. Here, learning by applying case study methods may assist significantly. The learners can develop skills to evaluate information and make informed decisions, which are essential for identifying phishing and other cyber threats [42]. Another approach to reach the desired outcome is to include lecture sessions combined with practical assignments to allow learners to develop a deeper understanding of cybersecurity principles and their application in real-world scenarios [34].

Moreover, the study results demonstrate that integrating cybersecurity into educational programmes leads to positive changes in learners' knowledge, skills and professional readiness. These findings are consistent with those presented in Hong [9], which emphasises the importance of increased knowledge in building a culture of cybersecurity.

Working in teams can help build this culture of cybersecurity when teamwork can create a platform to build a shared understanding of issues. The results determine that group projects devoted to solving cases and modelling cyberattacks help learners demonstrate improved collaboration and collective decision-making skills. This is especially important for training computer science teachers who must not only understand the basic aspects of cybersecurity but also be able to work in interdisciplinary teams.

Laboratory work and real-world threat simulations can benefit learners as well, especially in developing their hands-on experiences. For instance, virtual labs play an important role in learning by allowing students to work with real-world threat scenarios [43]. Such formats indeed contribute not only to strengthening professional competencies but also allow students to better absorb theoretical materials, which is essential in distance learning environments. The progress can be tracked using the Moodle system, and based on the ongoing progress and assessment results, they can adapt their programmes of study according to the needs of learners and market demand.

Thus, based on the results of the analysis, it can be argued that effective cybersecurity training requires comprehensive and multifaceted approaches that combine theoretical knowledge and practical training. The application of various approaches may help improve the trainees' professional readiness for employment. Employers report that such graduates are better prepared to perform cybersecurity-related tasks, which contributes to their career advancement [45].

Overall, integrating cybersecurity into educational programmes in Kazakhstan has significant potential to improve the training of computer science teachers. However, insufficient attention to practical teaching methods and the lack of specialised programmes limit opportunities to achieve better educational outcomes. International experience shows that further development of laboratory exercises, case methods and ethical training can significantly improve the quality of cybersecurity training.

In other countries, cybersecurity is already being actively integrated into the educational process, including the use of experimental and problem-orientated approaches that have proven to be effective [21], [40]. Kazakhstan can use these approaches as a basis for developing localised educational programmes that will consider national characteristics and needs. This will be an important step to improve the level of training of teachers and students in the digital transformation of the educational environment.

6 CONCLUSION

Given the importance of cybersecurity issues for Kazakhstan and beyond, this study examines approaches to integrating cybersecurity into teacher training and explores the outcomes of training computer science teachers when incorporating cybersecurity into curricula. The findings highlight that the integration of cybersecurity is a critical aspect of modern educational practices, equipping teachers with the necessary skills to navigate the digital world.

The study demonstrates that effective integration of cybersecurity topics enhances professional competencies, critical thinking, teamwork, and ethical problem-solving skills among teachers. The analysis emphasises the importance of practice-orientated teaching methods, such as laboratory exercises, case studies, and interdisciplinary approaches. These methods, along with the adoption of innovative practices like real-life threat simulations and virtual labs, deepen learners' theoretical knowledge and practical skills, preparing them for real-world challenges.

This study contributes to the field by proposing structured and practice-orientated approaches to integrating cybersecurity into teacher training. It identifies barriers such as insufficient specialised courses and a lack of regular updates to teaching materials, offering actionable insights for curriculum improvement. The study also highlights the importance of a systematic approach that not only ensures educators are prepared for evolving digital threats but also fosters the development of a comprehensive skill set through interdisciplinary interaction.

To address existing gaps and further enhance cybersecurity training, future research could:

- Develop and test specialized cybersecurity courses tailored for teacher training programmes.
- Explore interdisciplinary frameworks that integrate cybersecurity education into broader educational contexts, such as social sciences and ethics.
- Focus on innovative teaching tools, including augmented reality and simulation-based learning, to enhance practical training in cybersecurity.
- Investigate localised strategies to balance global best practices with national education system requirements.

The analysis of existing programs demonstrates that successful integration of cybersecurity through building foundations of cybersecurity can significantly enhance learners' readiness for the challenges of the digital environment. Indeed, it is vital to ensure that teachers are prepared for the challenges of the digital world. The importance of a systematic approach to cybersecurity implementation emphasises the need to update educational materials regularly and the active participation of all stakeholders in the educational process. This approach not only adapts educational courses to modern requirements but also promotes the development of comprehensive skills among students through interdisciplinary interaction.

Overall, the results of this study confirm the necessity of a comprehensive approach to integrating cybersecurity into higher education programmes. Implementing modern educational practices focused on cybersecurity can significantly enhance the readiness of teachers and equip them with professional skills to meet the challenges of the contemporary professional environment.

6.1 Limitation of the research

This study has several limitations that need to be considered. Firstly, the search was aimed at identifying relevant research related to the research questions, but some important studies may have been missed, especially those published in languages other than English. The choice of databases and keywords adhered to principles of critical review; however, future research could focus on more specific approaches to integrating cybersecurity and utilise data from a broader range of sources to enhance coverage and depth of analysis.

During the analytical phase, certain methodological decisions-imposed limitations. For instance, the reliance on previously published research could introduce bias, as studies reporting statistically significant findings are more likely to be published. Despite these challenges, every effort was made to ensure the transparency and comprehensiveness of the methodology. Future research should address these limitations by incorporating diverse data sources and exploring more granular methods for evaluating cybersecurity integration in teacher training.

7 ACKNOWLEDGEMENTS

This paper is an output of the science project "Development educational portal on machine learning as an artificial intelligence's direction to improve the Informatic teacher's training in education globalisation". This study has been funded by the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant No. AP19677348 "Development educational portal on machine learning as an artificial intelligence's direction to improve the Informatic teacher's training in education globalisation").

8 REFERENCES

[1] Markets and Markets, "Cybersecurity market by offering, solution type, services (professional and managed), deployment mode (on-premises cloud, and hybrid), organization size (large enterprises and SMEs), security type, vertical and region – global forecast to 2028", *Markets and Markets*, 2015. http://www.marketsandmarkets.com/PressReleases/cyber-security.asp

[2] S. Syarova and S. Toleva-Stoimenova, "Cybersecurity issues in the secondary and higher education systems' curricula," in *Proceedings of the Informing Science and IT Education Conference*, M. Jones, Ed., 2023. https://doi.org/10.28945/5114

[3] J. Guaña-Moya, N. Salgado-Reyes, Y. Arteaga-Alcívar, and A. Espinosa-Cevallos, "Importance of cybersecurity education to reduce risks in academic institutions," in *2024 International Conference on Information and Communication Technology for Intelligent Systems (ICTIS)*, 2024, pp. 31–30. https://doi.org/10.1007/978-981-97-5799-2_4

[4] N. Q. Do, A. Selamat, O. Krejcar, E. Herrera-Viedma, and H. Fujita, "Deep learning for phishing detection: Taxonomy, current challenges and future directions," *IEEE Access*, vol. 10, pp. 36429–36463, 2022. https://doi.org/10.1109/ACCESS.2022.3151903

[5] M. D. Richardson, P. A. Lemoine, W. E. Stephens, and R. E. Waller, "Planning for cyber security in schools: The human factor," *Educational Planning*, vol. 27, no. 2, pp. 23–39, 2020. [Online]. Available: http://files.eric.ed.gov/fulltext/EJ1252710.pdf [Accessed: Aug. 28, 2024].

[6] E. C. K. Cheng and T. Wang, "Institutional strategies for cybersecurity in higher education institutions," *Information*, vol. 13, no. 4, pp. 1–14, 2022. https://doi.org/10.3390/info13040192

[7] S. Jacques, A. Ouahabi, and T. Lequeu, "Remote knowledge acquisition and assessment during the Covid-19 pandemic," *International Journal of Engineering Pedagogy (iJEP)*, vol. 10, no. 6, pp. 120–138, 2020. https://doi.org/10.3991/ijep.v10i6.16205

[8] D. Gormaz-Lobos, C. Calarce-Miranda, and H. Hortsch, "Online engineering education: A proposal for specialization of the teacher training in engineering," *International Journal of Engineering Pedagogy (iJEP)*, vol. 11, no. 5, pp. 105–120, 2021. https://doi.org/10.3991/ijep.v11i5.22427

[9] W. C. H. Hong *et al.*, "The influence of social education level on cybersecurity awareness and behaviour: A comparative study of university students and working graduates," *Education and Information Technologies*, vol. 28, pp. 439–470, 2023. https://doi.org/10.1007/s10639-022-11121-5

[10] G. Towhidi and J. Pridmore, "Aligning cybersecurity in higher education with industry needs," *Journal of Information Systems Education*, vol. 34, no. 1, pp. 70–83, 2023. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1998&context=jise

[11] E. Amankwa, "Relevance of cybersecurity education at pedagogy levels in schools," *Journal of Information Security*, vol. 12, no. 4, pp. 233–249, 2021. https://doi.org/10.4236/jis.2021.124013

[12] F. D. Guillén-Gámez, I. Martínez-García, E. Alastor, and Ł. Tomczyk, "Digital competences in cybersecurity of teachers in training. Computers in the schools," vol. 41, no. 3, pp. 281–306, 2024. https://doi.org/10.1080/07380569.2024.2361614

[13] R. Shillair, P. Esteve-González, W. H. Dutton, S. Creese, E. Nagyfejeo, and B. von Solms, "Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise," *Computers & Security*, vol. 119, p. 102756, 2022. https://doi.org/10.1016/j.cose.2022.102756

[14] S. Hina and P. D. D. Dominic, "Information security policies' compliance: A perspective for higher education institutions," *Journal of Computer Information Systems*, vol. 60, no. 3, pp. 201–211, 2018. https://doi.org/10.1080/08874417.2018.1432996

[15] J. Vain and V. Kharchenko, "Enhanced education for cybersecurity and resilience," *Information & Security*, vol. 35, no. 1, pp. 5–8, 2016. https://www.isij.eu/system/files/download-count/2023-01/3500_editorial.pdf

[16] S. Z. Salas-Pilco and Y. Yang, "Artificial intelligence applications in Latin American higher education: A systematic review," *International Journal of Educational Technology in Higher Education*, vol. 19, no. 21, pp. 1–20, 2022. https://doi.org/10.1186/s41239-022-00326-w

[17] Q. An, W. C. H. Hong, X. Xu, Y. Zhang, and K. Kolletar-Zhu, "How education level influences internet security knowledge, behaviour, and attitude: A comparison among undergraduates, postgraduates and working graduates," *International Journal of Information Security*, vol. 22, no. 2, pp. 305–317, 2023. https://doi.org/10.1007/s10207-022-00637-z

[18] S. Das, T. H. J. Kim, L. A. Dabbish, and J. I. Hong, "The effect of social influence on security sensitivity" in *10th Symposium on Usable Privacy and Security (SOUPS)*, 2014, pp. 143–157. Available: https://www.usenix.org/system/files/conference/soups2014/soups14-paper-das.pdf [Accessed: Sep. 27, 2024].

[19] H. J. Kam, T. Mattson, and S. Goel, "A cross-industry study of institutional pressures on organizational effort to raise information security awareness," *Information Systems Frontiers*, vol. 22, no. 5, pp. 1241–1264, 2020. https://doi.org/10.1007/s10796-019-09927-9

[20] B. D. Deebak and F. Al-Turjman, "Smart mutual authentication protocol for cloud-based medical healthcare systems using Internet of Medical Things," *IEEE Journal on Selected Areas in Communication*, vol. 39, no. 2, pp. 346–360, 2021. https://doi.org/10.1109/JSAC.2020.3020599

[21] T. Lowe and C. Rackley, "Cybersecurity education employing experiential learning," in *KSU Proc. On Cybersecurity Education, Research and Practice*, 2018. [Online]. Available: https://digitalcommons.kennesaw.edu/cgi/viewcontent.cgi?article=1077&context=ccerp [Accessed: July 8, 2024].

[22] B. Gulmira, M. Gulmira, O. Assel, O. Aigerim, Z. Altanbek, and S. Beibarys, "Aspects of digital transformation of higher education in the Republic of Kazakhstan," in *International Conference on Computational Science and Its Applications (ICCSA),* in Lecture Notes in Computer Science, O. Gervasi, B. Murgante, C. Garau, D. Taniar, A. M. A. C. Rocha, and M. N. Faginas Lago, Eds., Springer, Cham, 2024, pp. 111–123. https://doi.org/10.1007/978-3-031-65282-0_7

[23] Government of the Republic of Kazakhstan, "On approval of the concept of digital transformation, development of the information and communication technologies industry and cybersecurity for 2023–2029," 2023. [Online]. Available: https://adilet.zan.kz/rus/docs/P2300000269 [Accessed: June 1, 2024].

[24] Sh. B. Bekchonova, "The relevance of cybersecurity education in pedagogy," *Prosperity of Science*, vol. 2, no. 8, pp. 32–40, 2022.

[25] I. D. Alekperov, E. A. Alekperova, and A. I. Alekperova, "Cybersecurity in an era of digital education," *Intellectual Resources-Regional Development*, vol. 1, no. 1, pp. 16–19, 2020.

[26] K. Abdiyev, M. Zhassandykyzy, and G. Primbetova, "The alignment of university educational programs with the professional standards of the IT industry," *Journal of Social Studies Education Research*, vol. 14. no. 4, pp. 299–327, 2023.

[27] S. Petrenko, *Cyber Security Innovation for the Digital Economy: A Case Study of the Russian Federation*. New York, NY: River Publishers, 2022. https://doi.org/10.1201/9781003337782

[28] S. K. Muratbekova and Zh. A. Dzharaspayeva, "Problem-oriented education," *Medical Nurse*, vol. 4, no. 1, pp. 41–42, 2013.

[29] D. D. Dzhantasova, Zh. A. Azimbayeva, and V. V. Brtitvina, "Analysing key aspects of digital transformation of higher education system," *Pedagogy Vestnik of Karaganda Buketov University: Pedagogy Series*, vol. 29, no. 2, pp. 74–83, 2024. https://doi.org/10.31489/2024Ped2/74-83

[30] M. Imran and N. Almusharraf, "Digital learning demand and applicability of quality 4.0 for future education: A systematic review," *International Journal of Engineering Pedagogy (iJEP)*, vol. 14, no. 4, pp. 38–53, 2024. https://doi.org/10.3991/ijep.v14i4.48847

[31] S. Elo, M. Kääriäinen, O. Kanste, T. Pölkki, K. Utriainen, and H. Kyngäs, "Qualitative content analysis: A focus on trustworthiness," *SAGE Open*, vol. 4, no. 1, 2014. https://doi.org/10.1177/2158244014522633

[32] J. F. S. A. Ghezzi, E. F. R. Higa, M. A. Lemes, and M. J. S. Marin, "Strategies of active learning methodologies in nursing education: An integrative literature review," *Revista Brasileira de Enfermagem*, vol. 74, no. 1, pp. 1–10, 2021. https://doi.org/10.1590/0034-7167-2020-0130

[33] S. Tutkyshbayeva and A. Zakirova, "Analysing IoT digital education: Fostering students' understanding and digital literacy," *International Journal of Engineering Pedagogy (iJEP)*, vol. 14, no. 4, pp. 4–23, 2024. https://doi.org/10.3991/ijep.v14i4.45489

[34] J. Blanken-Webb, P. Imani, S. Deshaies, N. C. Burbules, R. H. Campbell, and M. Bashir, "A case study-based cybersecurity ethics curriculum," in *USENIX Workshop on Advances in Security Education (ASE 18)*, 2018, pp. 1–12. [Online]. Available: https://www.usenix.org/system/files/conference/ase18/ase18-paper_blanken-webb.pdf [Accessed: July 1, 2024].

[35] K. A. Yousif Yaseen, "Importance of cybersecurity in the higher education sector 2022," *Asian Journal of Computer Science and Technology*, vol. 11, no. 2, pp. 20–24, 2022. https://doi.org/10.51983/ajcst-2022.11.2.3448

[36] R. Trifonov, O. Nakov, S. Manolov, G. Tsochev, and G. Pavlova, "Possibilities for improving the quality of cyber security education through application of artificial intelligence methods," in *2020 International Conference Automatics and Informatics (ICAI)*, 2020, pp. 1–4. https://doi.org/10.1109/ICAI50593.2020.9311333

[37] A. Arabo and M. Serpell, "Pedagogical approach to effective cybersecurity teaching," in *Transactions on Edutainment XV.* in Lecture Notes in Computer Science, Z. Pan, A. Cheok, W. Müller, M. Zhang, A. El Rhalibi, and K. Kifayat, Eds., Springer, Berlin, Heidelberg, vol. 11345, 2019. https://doi.org/10.1007/978-3-662-59351-6_11

[38] M. D. Workman, J. Anthony Luévanos, and B. Mai, "A study of cybersecurity education using a present-test-practice-assess model," *IEEE Transactions on Education*, pp. 40–45, 2021. https://doi.org/10.1109/TE.2021.3086025

[39] C. Yue, "Teaching computer science with cybersecurity education built-in," USENIX Workshop on Advances in Security Education (ASE 16), pp. 1–8, 2016. https://www.usenix.org/system/files/conference/ase16/ase16-paper-yue.pdf

[40] R. Dopplick, "Experiential cybersecurity learning," *ACM Digital Library*, vol. 6, no. 2, p. 84, 2015. https://doi.org/10.1145/2743024

[41] I. Hassan, "Leveraging Apache Guacamole, Linux LXD and Docker containers to deliver a secure online lab for a large cybersecurity course," in *IEEE Frontiers in Education Conference (FIE)*, 2022, pp. 1–9. https://doi.org/10.1109/FIE56618.2022.9962510

[42] B. K. Payne, W. He, C. Wang, D. E. Wittkower, and H. Wu, "Cybersecurity, technology, and society: Developing an interdisciplinary, open, general education cybersecurity course," *Journal of Information Systems Education*, vol. 32, no. 2, pp. 134–149, 2021. [Online]. Available: https://jise.org/Volume32/n2/JISE2021v32n2pp134-149.pdf [Accessed: July 3, 2024].

[43] A. M. Alnajim, Sh. Habib, M. Islam, H. S. AlRawashdeh, and M. Wasim, "Exploring cybersecurity education and training techniques: A comprehensive review of traditional, virtual reality, and augmented reality approaches," *Symmetry*, vol. 15, no. 12, p. 2175, 2023. https://doi.org/10.3390/sym15122175

[44] D. Soylu, D. T. Medeni, R. Andekina, R. Rakhmetova, and R. Ismailova, "Identifying the cybercrime awareness of undergraduate and postgraduate students: Example of Kazakhstan," in *IEEE International Conference on Smart Information Systems and Technologies (SIST)*, 2021, pp. 1–7. https://doi.org/10.1109/SIST50301.2021.9465995

[45] Johns Hopkins, "Employment outcomes," 2023. https://sais.jhu.edu/student-experience/career-services/employment-outcomes

9 AUTHORS

Meruyert Serik is a Professor at the Department of "Informatics" at L.N. Gumilyov Eurasian National University. Her research interests include machine learning, big data, cloud technologies, neural networks, information security, quantum computing and robotics (E-mail: serik_meruerts@mail.ru).

Danara Tleumagambetova is a doctoral student in the educational program (8D01511 – Informatics) at L.N. Gumilyov Eurasian National University (E-mail: danara1310@gmail.com).

Shyryn Tutkyshbayeva is a Senior-Lecturer at the Department of Computer Engineering at Astana IT University. Her research IoT, information security, education, digital technologies and artificial intelligence (E-mail: sh.tutkyshbayeva@astanait.edu.kz).

Alma Zakirova is a Candidate of Pedagogical Sciences, an Associate Professor in the Department of Computer Science, Faculty of Information Technology, L.N. Gumilyov Eurasian National University (E-mail: alma_zakirova@mail.ru).