OPEN ACCESS

Journal of Advances in Education and Philosophy

Abbreviated Key Title: J Adv Educ Philos
ISSN 2523-2665 (Print) |ISSN 2523-2223 (Online)
Scholars Middle East Publishers, Dubai, United Arab Emirates
Journal homepage: https://saudijournals.com

Original Research Article

Models and Structure of Competencies of Training of the Future Specialist Field of Information Protection in Globalization

Kymbat Saginbayeva[1]*, Alimbubi Aktayeva[2], Assiya Makatova[3], Dinara Zholamanova[4]

[1]PhD Student, Mongolian University of Science and Technology, Ulaanbaatar
[2]Ph.D., A. Myrzakhmetov Kokshetau University
[3]Senior Lecturer, Sh. Ualikhanov Kokshetau University
[4]Senior Lecturer, Sh. Ualikhanov Kokshetau University

DOI: https://doi.org/10.36348/jaep.2025.v09i12.003 | **Received:** 19.10.2025 | **Accepted:** 11.12.2025 | **Published:** 13.12.2025

***Corresponding author:** Kymbat Saginbayeva
PhD Student, Mongolian University of Science and Technology, Ulaanbaatar

Abstract

In the modern world, information security plays a key role in protecting data, financial transactions and personal information from cyber threats. Every year, the number and complexity of cyber-attacks grow, which requires information security specialists not only to have deep knowledge, but also to be able to quickly adapt to new challenges. Globalization leads to an expansion of the scale of interaction and data exchange, which, on the one hand, contributes to the development of technology and the economy, and on the other hand, creates new risks and threats. In the context of globalization, it is especially important to prepare students for future professional activities in the field of information security, providing them with relevant knowledge and skills. Educational institutions are faced with the task of developing and implementing effective training programmers that allow students to master advanced technologies and methods of information protection. An important aspect is the integration of innovative approaches into the educational process, such as the use of virtual reality, simulations, project-based learning and cooperation with industry. This article aims to study modern challenges in the field of information security, analyze existing programmers for training specialists and suggestions for their improvement. New methods and approaches to training, development and implementation of educational standards, as well as examples of successful integration of innovative technologies into educational programmers will be considered. The purpose of the article is to suggest ways to improve the training of students in the field of information security so that they can effectively counter cyber threats in the context of globalization

Keywords: Digital technologies, globalization, information security, professional competencies, professional training.

INTRODUCTION

In recent years, there has been a significant increase in the number of cyber threats, which is associated with the development of information technology and the increase in the number of users of digital devices. Cyber-attacks are becoming increasingly sophisticated and complex, which requires new approaches to ensuring security (see Fig. 1).

Traditional methods of protection, such as antivirus programs and firewalls, are no longer able to fully resist new types of threats. Globalization has a significant impact on information security, opening new opportunities for cybercriminals.

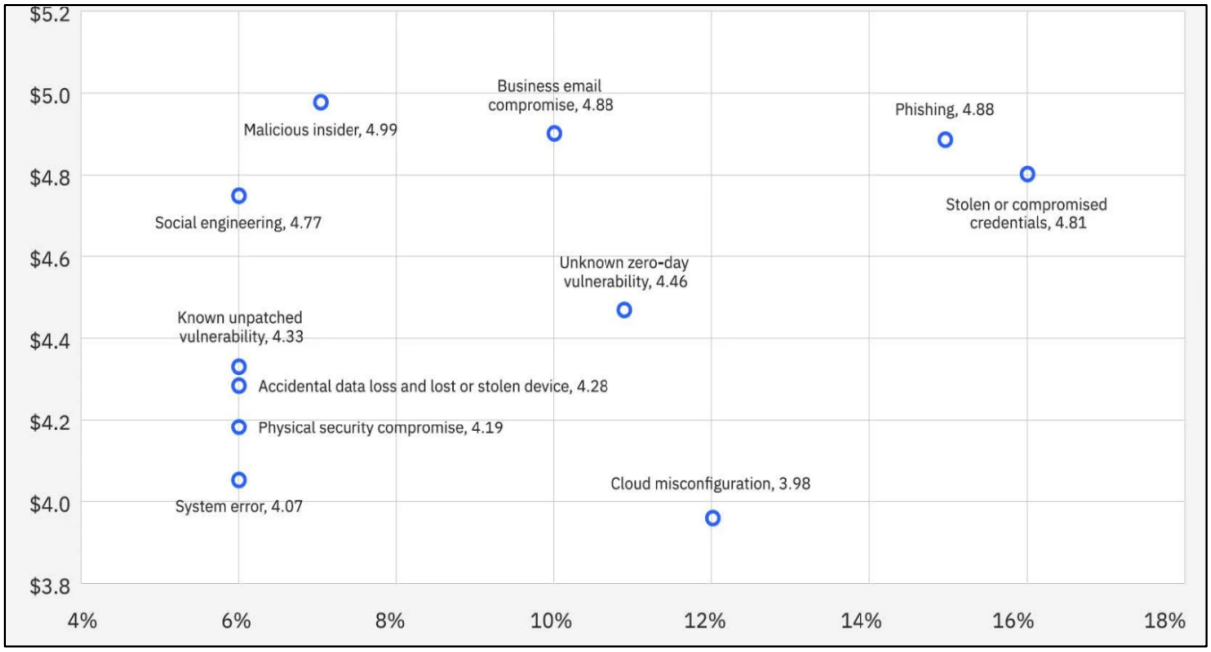

Fig. 1: The Impact of Globalization on Information Security [https://spycloud.com/blog/5-takeaways-from-ibms-cost-of-a-data-breach-report-2024/]

Increased international cooperation and cross-border transactions lead to an increase in the volume of data exchange and the complexity of managing information flows. Companies and organizations increasingly interact with partners and customers from different countries, which requires ensuring security at a global level.

In the context of globalization, there is a growing need to develop and implement international security standards and protocols. However, differences in legislation and approaches to ensuring security in different countries create additional complications. Cybercriminals can exploit weaknesses in security systems to carry out attacks, which requires joint efforts at the international level to counter these threats.

Information security is becoming an increasingly important topic on a global scale, and many countries are paying significant attention to developing educational programs aimed at preparing qualified specialists in this field. In the United States of America, for example, many universities and colleges offer both undergraduate and graduate programs in information security. Universities such as Carnegie Mellon University and the Massachusetts Institute of Technology are known for their extensive and advanced programs that include both theoretical and practical training [1].

There is also significant interest in training information security specialists in Europe. Universities such as the Darmstadt University of Technology in Germany and the University of Cambridge in the UK offer programs that emphasize an interdisciplinary approach that includes both technical and legal aspects of information security. In Asia, universities such as Japan and South Korea are actively developing educational programs aimed at studying advanced technologies and methods of ensuring information security [2].

Despite the challenges, there are many examples of successful programs and initiatives that can serve as models for other educational institutions. For example, the SANS Institute offers extensive courses and certification programs that help professionals develop their skills and gain up-to-date knowledge in the field of information security. SANS courses include both theoretical classes and practical exercises, allowing students to apply the acquired knowledge in practice [3,4].

In the UK, universities actively collaborate with government and private organizations to create programmed that meet modern requirements. Universities such as Cambridge and Oxford integrate real-life cases and projects into the curriculum, which helps students better understand and apply theoretical knowledge in practice [5].

In Japan, universities also offer programs that include practical training and collaboration with organizations such as the DETER Technology Research Center, allowing students to gain experience with advanced technologies and information security techniques. These programs demonstrate the importance of integrating theoretical training with practical skills to enhance the competence of future professionals [6,7].

Despite the efforts to create and develop educational programs in information security, there are a

number of problems and shortcomings that need to be addressed. One of the key shortcomings is the lack of qualified teachers with both theoretical knowledge and practical skills in the field of information security. This limits the ability of students to obtain relevant and practical knowledge necessary to work in a rapidly changing digital environment. Another problem is the lack of funding and resources for the development and updating of curricula. As a result, many programs do not have time to adapt to new challenges and threats arising in the field of cybersecurity. In addition, some educational institutions do not pay sufficient attention to practical classes and internships, which reduces the level of preparation of students for real work.

These examples show that successful information security training programs not only provide students with theoretical knowledge, but also actively engage them in practical activities, which allows them to develop the necessary skills and be better prepared for the challenges of today's digital environment. Undoubtedly, globalization and internationalization are processes that are interconnected in a certain way, but most likely they can be considered dialectically opposite, even though both are, in essence, forms of one phenomenon – international integration (see Fig. 2).

In the context of globalization, it is important to implement international standards and certifications in educational programs on information security. International standards, such as ISO/IEC 27001, establish uniform requirements for information security management and data protection. The implementation of these standards in educational programs helps to increase the competence and literacy of their students, which is necessary to ensure a more peaceful environment in the world, in which understanding of international problems and cooperation in their solution will be a very important condition for ensuring quality of life and maintaining economic, social and cultural development.

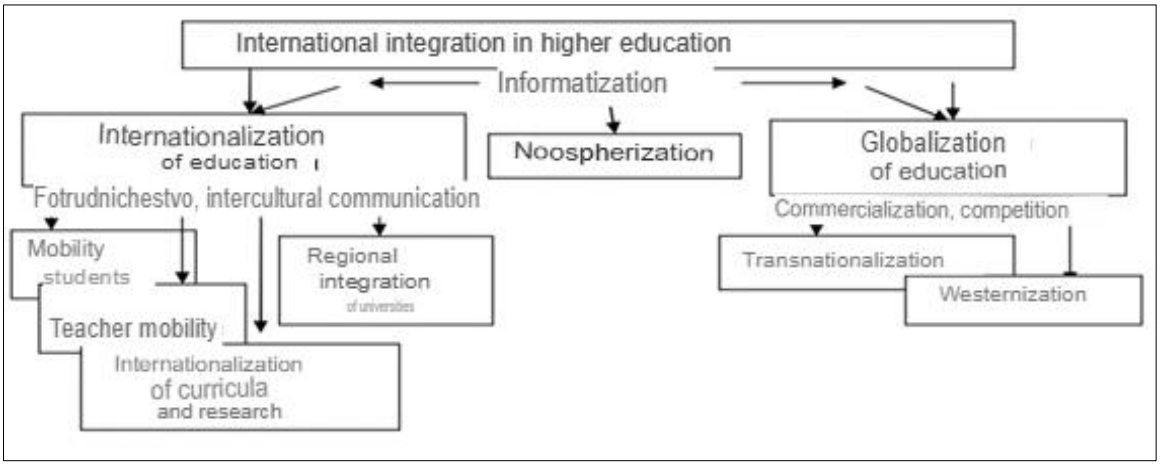

Fig. 2: Forms of international integration in the field of higher education

The problem of the competence-based approach in the system of higher education does not lose its significance in connection with the continuous process of improving the modern system of educational standards, the purpose of which is the formation of a competent specialist. Competency is vital to enable people and countries to thrive in an increasingly complex, interconnected and rapidly changing world. The OECD Learning Compass 2030 establishes a broad "learning framework", emphasizing the competencies essential for students to thrive by 2030 rather than focusing on measurable assessment criteria. While the notion that "what gets measured gets treasured" is common, this framework values aspects of learning that may not yet be quantifiable. Recognizing the intrinsic value of education, the framework incorporates diverse learning approaches within a flexible structure. It also serves as a reference for assessment initiatives, guiding discussions on prioritized learning areas for monitoring and supporting student progress. Importantly, the OECD Learning Compass 2030 is not a "curriculum framework". It acknowledges the significance of formal, non-formal, and informal education alongside traditional curricula. As 2030 approaches, understanding the multiple dimensions of learning—whether in schools, at home, or within communities—becomes increasingly crucial. Countries in which people develop strong competencies, engage in lifelong learning and use their competencies fully and effectively at work and in society are more productive, innovative and trustworthy, have better health outcomes and a higher quality of life (see Figure 3).

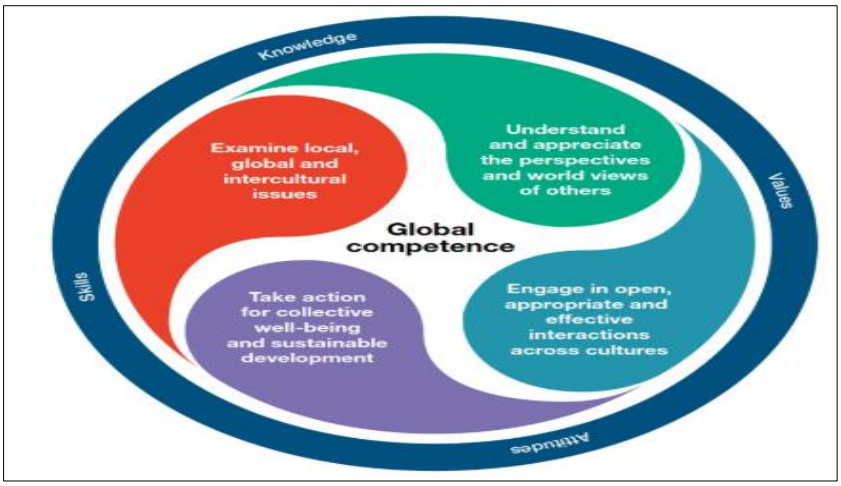

Fig. 3: OECD Framework for Competence Development

The integration of industry experts into the educational process also helps improve the quality of students' training. Joint projects, guest lectures and internships allow students to gain practical experience and better understand the real problems and challenges they may face in their professional activities. The problem of competence-based approach in the system of higher education emphasizes the importance of developing and implementing flexible and adaptive curricula, international standards and certifications, and training qualified teachers to ensure a high level of training for information security specialists in the context of globalization. This implies the ability to quickly update teaching materials and teaching methods in accordance with current challenges and new technologies.

The flexibility of the programs includes considering the diversity of threats and methods of their prevention, as well as the use of an interdisciplinary approach covering technical, legal and managerial aspects of information security. Flexible and adaptive programs enable students to gain up-to-date knowledge and skills needed to effectively counter modern cyber threats. This includes the use of innovative teaching methods such as project-based learning, simulations and virtual reality, which enable students to apply theoretical knowledge into practice and develop critical thinking.

The European Digital Competence Framework for Citizens, known as Dig Comp, offers a tool to improve the digital competence of citizens [6]. Digital competence is crucial in modern society, enabling successful integration into the digital economy, education, and social processes. Table 1 shows how Dig Comp 2.0 defines the key components of digital competence in 5 areas.

Table 1: Key components of digital competence in Dig Comp 2.0

Category	Description
Information and data literacy	Identifying information needs, retrieving and evaluating digital data, managing and organizing digital content.
Communication and collaboration	Interacting and collaborating through digital technologies, considering cultural and generational diversity, engaging in digital citizenship, managing digital identity and reputation.
Digital content creation	Creating and editing digital content, integrating information while respecting copyright and licenses, providing clear instructions for computer systems.
Safety	Protecting devices, data, and privacy, ensuring physical and psychological well-being, understanding digital technologies' impact on social inclusion and the environment.
Problem solving	Identifying and resolving issues in digital environments, utilizing digital tools for innovation, staying updated on technological advancements.

Developing digital skills enhances competitiveness, promotes social inclusion, and drives innovation. The Key Aspects of Digital Competence encompass information literacy, communication, content creation, safety, and problem-solving—elements defined in Dig Comp 2.0 and other international frameworks.

1. Economy and Employment: Digital skills are essential for career growth and competitiveness.
2. Education: Technology expands learning opportunities, providing access to information and new teaching methods.
3. Safety: Understanding cyber risks helps protect data and prevent digital threats.
4. Digital Citizenship: Participation in society through digital platforms facilitates access to services and interactions.

5. Innovation: Digital tools foster creativity and analytical thinking.

Comparing Dig Comp with Other Frameworks reveals that Dig Comp is widely used in the EU and focuses on digital skill development in both professional and everyday life. Other models emphasise technical aspects, pedagogy, or business innovations. Digital competence development is a key factor in sustainable social and economic progress, ensuring the effective use of technology and preventing digital divides. It was first published in 2013 and in 2016 the JRC published Dig Comp 2.0, updating the terminology and conceptual model and showing examples of its implementation at European, national and regional levels. The initial three qualification levels were expanded to eight levels. Dig Comp 2.0 includes 6 areas of digital competence (see Fig. 4).

Fig. 4: Areas of digital competence

In 2017, EU member states underlined their commitment to providing learners with the "best education". The European Council called for European education and training systems to be "fit for the digital age" [11]. Certifications such as the Certified Information Systems Security Professional (CISSP) and Certified Ethical Hacker (CEH) allow students to have their competencies recognized internationally. Including preparation for international certifications in curricula increases the competitiveness of graduates in the global labor market and promotes their professional growth, as well as facilitates international cooperation and exchange of experience. For each of the competencies, the qualification levels are substantiated, as well as the knowledge and skills corresponding to them (See Table 2).

Table 2: Skill levels

№	Skill levels
1	Basic levels (solving simple problems with instructions focusing on memorization)
2	Intermediate levels (solving specific and routine tasks and simple (hereinafter – non-standard) problems with an orientation towards understanding)
3	Advanced levels (solving various tasks and problems with a focus on applying knowledge and skills in practice)

The development of professional competence of future information security specialists requires the development of methodological and theoretical foundations that ensure a holistic approach to training. In our work, we considered and used the university specifications of the quality programs "6B01 - Computer Science, IS, ICT". When writing the article, we used the following scientific research methods: observation, information collection, processing of scientific literature, and secondary data analysis based on the information obtained.

MATERIALS AND METHODS

The methodological foundations include defining the goals and objectives of training, choosing methods and means, and assessing their effectiveness. The theoretical foundations are based on the fundamental principles of pedagogy and psychology, as well as specific knowledge in the field of information security. The main components of the formation of professional competence include:

Theoretical training: Study of basic information security concepts and techniques such as cryptography, data protection and risk management.

Practical training: Performing laboratory work, participating in projects and internships, which allows you to apply theoretical knowledge in practice and develop professional skills [18].

Critical Thinking and Problem Solving: Development of skills in analyzing and evaluating information, identifying threats and developing strategies to prevent them.

Interdisciplinary approach: Integration of knowledge from various fields such as law, management and information technology, which provides a comprehensive approach to learning.

Ethical aspects: Inclusion of issues of professional ethics and responsibility in the training program, which contributes to the formation of a high level of professional culture and awareness of the importance of the work of specialists for society.

The structure of the developed educational environment of the process of professional training of bachelor's in information security (Figure 5) includes the following blocks:

1. Technical means of teaching: network and multimedia systems, ICT.
2. Educational application programs and laboratory technical devices for ensuring information security.
3. Teaching aids: teaching aids, recommendations, instructions, system of test assignments.
4. Consulting and information: teacher-student interaction platform.
5. Interdisciplinary interaction: integration of academic disciplines into blocks, complexes and modules based on the interdisciplinary component.
6. Research into students' personal characteristics: a system of diagnostic tools for determining psychological characteristics of information perception.
7. Monitoring: a system of tools for continuous tracking and quantitative and qualitative interpretation of the level of development of professional competence.
8. Result-corrective: a system of tasks to determine the level of actual assimilation of educational content; corrective tasks.
9. Modeling of an individual educational learning trajectory: a system of tasks that considers the individual personal qualities and level of knowledge of the student, facilitating the creation of an individual educational trajectory along the path from "success to success".

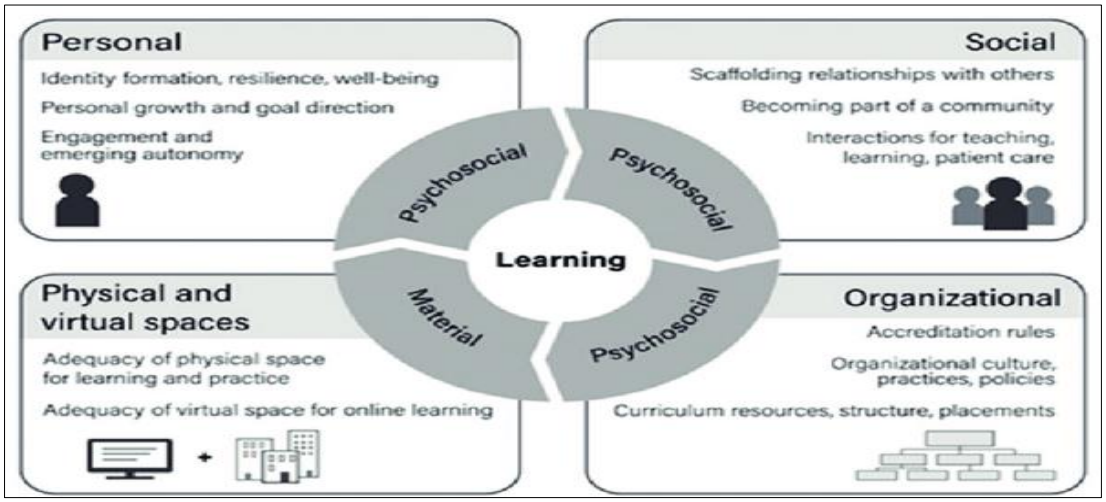

Fig. 5: Structure of the educational environment

The development of methodological and theoretical foundations allows us to create effective educational programs that ensure high-quality training of information security specialists and their compliance with modern labor market requirements.

Future research in the field of training information security specialists may focus on the following aspects:

1. Analysis of the effectiveness of integrating the latest technologies into educational programs: Research on the use of virtual reality, artificial intelligence and quantum computing in the learning process, as well as their impact on the quality of training specialists.
2. Development and evaluation of new teaching methods: Exploring different teaching methods such as project-based learning, simulations and gaming technologies and their impact on students' development of critical thinking and problem-solving skills.
3. Research of international cooperation and exchange of experience: Analysis of successful examples of international cooperation in the field of training information security specialists,

study of best practices and their adaptation for various educational systems.

4. Evaluation of long-term results of the implementation of international standards and certifications: A study of the impact of international standards and certifications on the career growth of specialists, their professional mobility and competitiveness in the global labor market.
5. Studying the impact of globalization on the requirements for information security specialists: Analysis of changes in the requirements for knowledge and skills of specialists in the context of globalization, study of new challenges and development of recommendations for educational institutions and governments.

RESULTS AND DISCUSSION

The study identified key aspects that influence the training of information security specialists in the context of globalization. Modern challenges and trends in cybersecurity require flexible and adaptive educational programs. The growth in the number and complexity of cyber threats, the changing nature of attacks, and the impact of globalization on information security highlight the need to integrate the latest technologies and teaching methods.

The implementation of the educational environment in the process of professional training of students in the field of information security allowed us to organize a holistic system of mediated management of training. The experimental implementation of groups of pedagogical conditions for the formation of the educational environment of the process of training Bachelor of Information Security was carried out in several stages. Figure 6 shows the general structure of the pedagogical experiment.

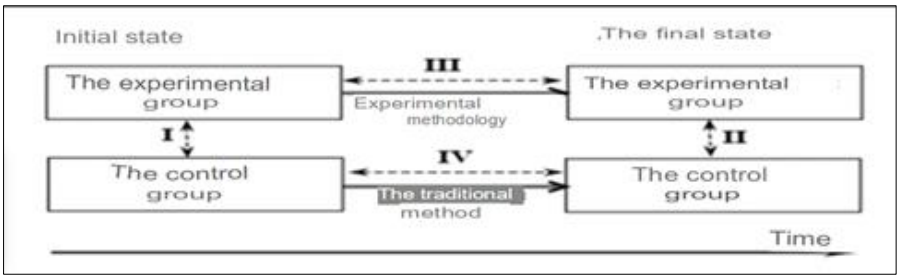

Fig. 6: Structure of the pedagogical experiment

At the stage of entrance testing, the level of professional competence is usually formed at the reproductive (minimum) level, then based on the system of diagnostic tools, the level of formation of components of professional competence was determined only by 4 criteria. Thus, the generalized coefficient of assimilation can be used to compare the results of training in different groups and streams of students. It can also be correlated with the usual 28ECTS scale of the point-rating system of academic performance assessment (see Table 3).

Table 3: Distribution of students by levels of development of components of professional competence of Bachelor of Information Security in control (CG) and experimental (EG) groups at the final stage of the experiment

Evaluation criteria	Groups		Level of development of professional competence			
			Reproductive	Reflexive	Heuristic	Creative
1	2	3	4	5	6	7
Motivational -value	EG	Number of students	28	54	35	33
		Percentage of students, %	19	36	23	22
	KG	Number of students	25	57	33	35
		Percentage of students, %	17	38	22	23
Cognitive	EG	Number of students	11	72	38	29
		Percentage of students, %	7	48	25	19
	KG	Number of students	70	13	45	22
		Percentage of students, %	47	9	30	15

Technological	EG	Number of students	35	35	38	42
		Percentage of students, %	23	23	25	28
	KG	Number of students	30	40	45	35
		Percentage of students, %	20	27	30	23
Organizational and communicative	EG	Number of students	24	43	55	28
		Percentage of students, %	16	29	37	19
	KG	Number of students	48	24	42	36
		Percentage of students, %	32	16	28	24
Resulting value	EG	Number of students	43	52	32	23
		Percentage of students, %	29	35	21	15
	KG	Number of students	48	60	19	23
		Percentage of students, %	32	40	13	15

Based on the results of the entrance control, diagrams were constructed of the distribution of students by levels of professional competence of future bachelors of information security in the control and experimental groups (Fig. 7).

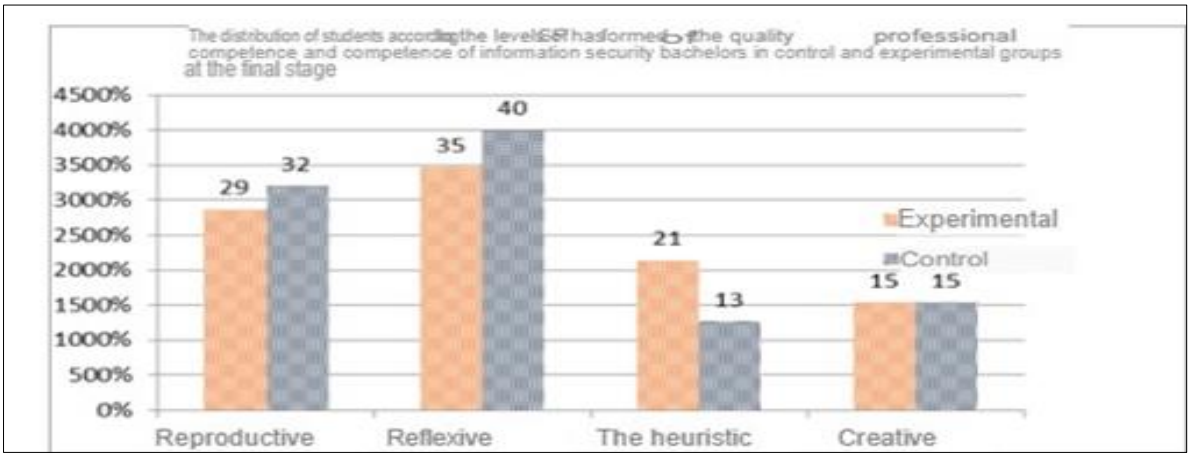

Fig. 7: Distribution of students by levels of development of professional competence of future Bachelor of Information Security in control and experimental groups at the ascertaining stage

One of the main findings of the study is the importance of introducing international standards and certifications into educational programs. This will standardize the knowledge and skills of specialists, increase their competitiveness in the global labor market and facilitate international cooperation. An example of successful integration of international standards can be certification preparation programs.

Cooperation with the industry and the integration of real cases and projects into the curriculum contribute to the development of students' skills in the practical application of theoretical knowledge and a better understanding of real problems and tasks. This interaction helps students gain the experience necessary to work in a rapidly changing digital environment. A necessary condition for ensuring the effectiveness of the implementation of the educational environment of the process of professional training of bachelor's in information security is a combination of the use of competency-based, differentiated and personality-oriented approaches using research and heuristic methods.

The use of a competency-based approach to training allows us to fulfill the target component of the requirements of the standard of the training direction "Information Security and Information Protection" for the level of development of students' general cultural, general professional and professional competencies. A differentiated approach, in turn, allows us to determine students' personal models of information perception, organize their effective interaction when working in small groups and performing research work.

The above conclusions indicate that the issues of the integrated use of training tools in the training of specialists in the field of information security are a promising area and require further scientific research. The conducted study does not exhaust all aspects of

creating conditions for the formation of an educational environment for the process of professional training of information security specialists

CONCLUSION

The future of information security education includes the integration of emerging technologies and teaching methods, such as virtual reality, artificial intelligence, and quantum computing. These innovative approaches will enable more effective and adaptive curricula that can respond quickly to changes in the cybersecurity landscape. Interdisciplinary approaches and collaboration with industry will play a key role in educational programs, providing students with access to real-world cases and practical experience.

The introduction of international standards and certifications will contribute to the standardization of knowledge and skills of specialists, facilitating their international mobility and cooperation. In future studies, it may be appropriate to expand our study on the importance of developing double degree programs and international internships, which will allow students to receive education in different countries and improve their qualifications at the global level, which contributes to the formation of a network of professional contacts and the exchange of best practices in the field of information security.

The study analyzed the importance of training information security specialists in the context of globalization. The study identified current challenges and trends related to the growth of cyber threats, changing nature of attacks, and the impact of globalization on information security. Particular attention was paid to the analysis of existing programs for training specialists in the context of globalization, identifying their shortcomings and problems, and reviewing the experience of successful programs and initiatives. Recommendations were offered for the creation of flexible and adaptive training programs, the implementation of international standards and certifications, and the training and advanced training of future specialists.

In conclusion, this study provides a comprehensive framework for the future development of modern education. focusing on the need to create flexible and adaptive curricula, implement international standards and certifications, and the importance of training future information security specialists in the context of globalization.

LIMITATION

The results emphasise the critical need for digital literacy in cybersecurity to develop skills and meta-cognitive capabilities, thereby supporting students' autonomy. The critical difficulties can impede their ability to engage in independent training, critical thinking and self-reflection. There is also a problem, as the content and training of the course are evaluated by students.

SUGGESTION

Further researchers should conduct a comparative analysis between various universities to find out how aspects of globalisation affect students' competence in cybersecurity. Student autonomy skills differ from institutional conditions. The variety of socioeconomic, cultural or educational origins can affect the level of autonomy and digital literacy in cybersecurity, which limited respondents cannot completely represent.

REFERENCES

1. E. V. Burkova, “Professional training of specialists in the field of information security”, Bulletin of the Orenburg State University, No. 2/190. 2016, pp. 3-8.
2. Yasenev, V. N., “Information Security: A Textbook”, Nizhny Novgorod: Nizhny Novgorod State University named after N. I. Lobachevsky, 2017, pp. 198.
3. Robert I.V., Mukhametzyanov I.Sh., Lopanova E.V., “Digital transformation of education: theory and practice. Monograph”, ed. E.V. Lopanova. - Omsk: Omsk State University Publishing House, 2022, pp. 190.
4. Skafa E.I., “Methodology and methods of scientific and pedagogical research: a tutorial”, Beau Bassin: LAP LAMBERT Academic Publishing RU, 2019, pp. 228.
5. O.A. Malykhina, Kazinets, V.A., “Improving the level of training of students at pedagogical universities and teachers in the field of information security”, Modern pedagogical education, No. 4, 2021, pp. 162-166.
6. Chvanova M.S., Anureva M.S., Lyskova V.Yu., Kotova N.A., “Molchanov A.A. Training specialists in the field of information security: an innovative approach to the formation of an educational environment”, Psychological and pedagogical journal Gaudeamus, No. 1 (25), 2015, pp. 18-31.
7. [7] Privalov, A. N., “Systemic aspects of organizing a secure information and educational environment of a university”, Bulletin of Tula State University. Technical Sciences, 2017, No. 2. - 2017, 2017, pp. 144-154.
8. [8] Mindzaeva, E. V., “Development of the concept of information security of the individual: information/cognitive approaches, Education Management: Theory and Practice, No. 2 (26). 2017, pp. 54-64.
9. [9] Kuzina, N. N., “The culture of information security of the teacher's personality and the process of its formation among students at a pedagogical university”, No. 2 (27). 2018, pp. 88-91.

10. Erina Yu. S., “Formation of information security culture among students - future teachers - in the process of professional training”, Bulletin of the Kemerovo State University of Culture and Arts, No. 41-2, 2017, pp. 186-193.
11. Arbuzov, S. S., “Formation of competencies in the field of computer networks among bachelors in the process of teaching computer science: abstract of dis. candidate of pedagogical sciences: 13.00.02”, Arbuzov Sergey Sergeevich; Ural state ped. university. - Ekaterinburg, 2016, pp. 23.
12. Belov E. B., “On professional standards in the field of information security”, Information counteraction to terrorist threats. - Taganrog: SFedU, Vol. 3, No. 25, 2015, pp. 5-13.
13. T. A. Polyakova, A. A. Streltsov, “Organizational and legal support for information security: textbook and practical training for bachelor's and master's degrees”, M.: Yurait Publishing House, 2016, pp. 325
14. Napalkov S. V., “Information security in the context of globalization: problems of modern educ
15. Azhmukhamedov, I. M., “Assessment of the quality of training specialists in the field of "Information Security", Astrakhan: Publishing house of ASTU, 2017, pp. 80-81.
16. Nosova, T. N., “Features of the formation of professional competencies of specialists in the field of computer security in teaching disciplines considering information systems”, Innovative projects and programs in psychology, pedagogy and education: collection of articles of the International scientific and practical conf. - Ufa: Aeterna., 2017, pp. 65-67.
17. Pomelnikova, E. A., “Validity of the structure of readiness for professional activity of information security specialists by the specifics of their activities”, Prospects for the development of science in the modern world: materials of the VIII international. scientific and practical. conf. - Ufa: Dendra, 2018, pp. 91-98.
18. Rudinsky, I. D., “Subject-specialized competence of a technical schoolteacher in the field of information security of automated systems”, Bulletin of the Immanuel Kant Baltic Federal University. Series: Philology, pedagogy, psychology. - Kaliningrad: Immanuel Kant Baltic Federal University, No. 4, 2018. pp. 102-110.
19. E.V. Dudina, L.A. Kolyvanova, E.N., “Chekanushkina Formation of professional competencies in the field of information security as a factor in the successful training of a future specialist”, Bulletin of the Samara Scientific Center of the Russian Academy of Sciences. Social, humanitarian, medical and biological sciences, vol. 23, no. 79(2), 2021, https://doi.org/10.37313/2413-9645-2021-23-79(2)-194-201
20. Kazinets, V. A., “Improving the level of training of students at pedagogical universities and teachers in the field of information security”, Modern pedagogical education, No. 4, 2021, pp. 162-166.
21. Solovieva S. A., “Specifics of the information security culture of students at a technical university, Development of education. Vol. 7, No. 2, 2024, pp. 50–56. https://doi.org/10.31483/r-110280. EDN DJMCMC.
22. Kozlov O. A., “Polyakov V. P., Information security of the individual: current pedagogical aspects”, Science of Man: Humanitarian Research, 2018, No. 3 (33). pp. 105-112, https://doi.org/10.17238/issn1998–5320.2018.33.105. EDN YBRQEX.