IRSTI 14.35.07 https://doi.org/10.51889/2959-5762.2026.89.1.014

Amzeyeva A.,[1]* *Kazbay P.,*[2] *Kudaibergenova K.,*[1]

[1]*Korkyt Ata Kyzylorda University, Kyzylorda, Kazakhstan*
[2]*Al-Farabi Kazakh National University, Almaty*

INTEGRATING GAMIFICATION INTO CYBERSECURITY EDUCATION FOR PRE-SERVICE PRIMARY TEACHERS

Abstract

This study examines the effectiveness of using gamified instructional methods in teaching cybersecurity to pre-service primary school teachers. The research used a quasi-experimental design involving second- and third-year students from Korkyt Ata Kyzylorda University. Over three weeks, the experimental group participated in cybersecurity lessons enhanced with gamification elements such as points, badges, and missions, while the control group was taught through traditional methods. Digital tools such as Kahoot, Wordwall, Genially, and Google Forms were utilized during the sessions. Learning outcomes were assessed using pre- and post-tests, and data were analyzed with SPSS Statistics 29 software. Results showed a significant improvement in the experimental group's knowledge levels (Pre: M = 38.38, Post: M = 66.14, $p < 0.001$), whereas gains in the control group were limited.

Furthermore, students' perception and acceptance of gamification were measured using a structured questionnaire, revealing a moderate level of readiness to apply gamified tools in teaching. Descriptive statistics and t-tests were used to analyze the data. The findings align with previous research, confirming that gamification enhances motivation and facilitates understanding complex content. This study highlights the potential of gamification as an effective method to increase pre-service teachers' digital literacy and preparedness for managing cybersecurity in the classroom. Future research is recommended to explore long-term interventions and the integration of gamification in other subject areas.

Keywords: gamification, cybersecurity, pre-service teachers, digital literacy, quasi-experimental design.

А.А.Амзеева, [1]* *П.А.Қазбай,* [2] *К.Т.Құдайбергенова*[1]

[1] *Қорқыт Ата атындағы Қызылорда университет, Қызылорда қ., Қазақстан*
[2] *Әл-Фараби атындағы Қазақ ұлттық университет, Алматы қ., Қазақстан*

БОЛАШАҚ БАСТАУЫШ СЫНЫП МҰҒАЛІМДЕРІ ҮШІН ГЕЙМИФИКАЦИЯНЫ КИБЕРҚАУІПСІЗДІККЕ ОҚЫТУДА ҚОЛДАНУ

Аңдатпа

Бұл мақалада болашақ бастауыш сынып мұғалімдерін киберқауіпсіздікке оқытуда геймификация әдісінің тиімділігі қарастырылады. Зерттеу квазиэксперименттік дизайн негізінде жүргізілді және Қорқыт ата атындағы Қызылорда университетінің 2 және 3 курс студенттері қатысты. Үш аптаға созылған интервенция барысында эксперименттік топқа геймификация элементтерімен (ұпай, бейдж, миссиялар) толықтырылған киберқауіпсіздік сабағы өткізілді, ал бақылау тобы дәстүрлі әдіспен оқытылды. Сабақтарда Kahoot, Wordwall, Genially және Google Forms сияқты цифрлық құралдар қолданылды. Оқу нәтижелері Pre-test және Post-test арқылы бағаланды, ал деректер SPSS Statistics 29 бағдарламасында өңделді. Нәтижелерге сәйкес, эксперименттік топта білім деңгейі айтарлықтай артқаны байқалды (Pre: M = 38.38, Post: M = 66.14, $p < 0.001$), ал бақылау тобының өсімі шектеулі болды. Сондай-ақ, студенттердің геймификацияға қатысты қабылдауы орташа деңгейде екені анықталды. Талдау сипаттамалық статистика және t-тест арқылы жүргізілді. Зерттеу нәтижелері бұрынғы еңбектермен салыстырылып, геймификация әдісінің мотивацияны арттырып, күрделі мазмұнды игеруде тиімді құрал екені дәлелденді. Бұл жұмыс болашақ мұғалімдердің цифрлық сауаттылығы мен киберқауіпсіздікке дайындығын жетілдіруде геймификацияны тиімді әдіс ретінде ұсынуға негіз болады. Болашақта ұзақ мерзімді интервенциялар мен басқа пәндерге бейімделу арқылы зерттеуді кеңейту ұсынылады.

Түйінді сөздер: геймификация, киберқауіпсіздік, болашақ мұғалімдер, цифрлық сауаттылық, квазиэксперименттік дизайн.

Амзеева А.А.,[1]* *Қазбай П.А.,*[2] *Кудайбергенова К.Т.,*[1]
[1] *Кызылординский университет имени Коркыт Ата, г.Кызылорда, Казахстан*
[2]*Казахский национальный университет имени аль-Фараби, г.Алматы, Казахстан*

ИСПОЛЬЗОВАНИЕ ГЕЙМИФИКАЦИИ В ОБУЧЕНИИ КИБЕРБЕЗОПАСНОСТИ БУДУЩИХ УЧИТЕЛЕЙ НАЧАЛЬНЫХ КЛАССОВ

Аннотация

В данной статье рассматривается эффективность использования геймификации в обучении будущих учителей начальных классов основам кибербезопасности. Исследование было проведено в рамках квазиисперимента с участием студентов 2 и 3 курсов Кызылординского университета имени Коркыт Ата. В течение трёх недель экспериментальная группа обучалась с использованием геймифицированного модуля, включающего элементы баллов, значков и миссий, в то время как контрольная группа обучалась традиционными методами. В качестве цифровых инструментов использовались платформы Kahoot, Wordwall, Genially и Google Forms. Результаты обучения оценивались с помощью Pre-test и Post-test, а обработка данных осуществлялась в программе SPSS Statistics 29. Согласно результатам, уровень знаний студентов экспериментальной группы значительно повысился (Pre: M = 38.38, Post: M = 66.14, $p < 0.001$), тогда как рост у контрольной группы был ограничен. Кроме того, уровень принятия геймификации участниками оказался на среднем уровне. Для анализа использовались описательная статистика и t-критерий. Результаты исследования сопоставлены с предыдущими научными работами и подтверждают, что геймификация является эффективным инструментом для повышения мотивации и освоения сложного материала. Исследование демонстрирует потенциал геймификации как метода повышения цифровой грамотности и готовности будущих учителей к обеспечению кибербезопасности. В дальнейшем рекомендуется расширение исследования с учетом долгосрочных интервенций и адаптации в других учебных дисциплинах.

Ключевые слова: геймификация, кибербезопасность, будущие учителя, цифровая грамотность, квазиисперимент-альный дизайн.

Introduction. Integrating technology into the education system requires teachers to possess adequate cybersecurity knowledge. However, current teacher training programs lack sufficient content and motivation regarding cybersecurity, indicating that future teachers are not adequately prepared to handle digital threats. Cybersecurity is a rapidly evolving and complex field due to the fast-paced development of technology. Today, there is a global shortage of qualified professionals in this area. Therefore, cybersecurity education should be provided in technical university programs and other disciplines. Many cyberattacks happen due to user mistakes and a lack of cybersecurity awareness. Consequently, it is essential for every individual, whether an IT specialist or an average user, to understand the fundamentals of cybersecurity and how to protect themselves from digital threats. Security cannot be ensured solely through software and technical tools; human awareness is vital to protection . Educational institutions have become primary targets of cyberattacks such as phishing, malware, and data breaches. Teachers, who have direct access to student data and school networks, become vulnerable if inadequately trained [1]. Educators have adopted various pedagogical methods to teach cybersecurity literacy effectively, including the flipped classroom, project-based learning, serious games, and multimedia tools. These methods enhance student engagement, motivation, and comprehension of complex topics. Digital or computerized serious games are among the most effective instructional strategies for teaching cybersecurity awareness [2]. Serious games with constructivist principles foster active participation, collaboration, and experiential learning. Although proven effective, such games are time-consuming to develop and require significant resources for regular updates [3].

Gamification has emerged as a promising tool to make teaching and learning more engaging, especially in cybersecurity education. It involves applying game-like elements (e.g., points, badges, competition) in non-game contexts to make learning more interactive and motivating . This method has proven effective in enhancing motivation and engagement and improving learning outcomes in complex subjects. Although future teachers, raised in the digital age, are generally comfortable using technology, they often lack formal education in cybersecurity principles. Teaching them these principles during their initial teacher preparation stage is critical for ensuring a safe learning environment for future generations [4]. This study aims to evaluate the impact of a gamified cybersecurity module on developing

theoretical knowledge and practical skills among pre-service teachers. Traditional instruction sessions often require significant time and are less effective in motivation, engagement, and knowledge retention than gamified strategies. Therefore, the relevance of this study lies in assessing the effectiveness of gamified methods for improving future teachers' knowledge of cybersecurity and exploring their acceptance of such approaches.

Research Objective: To determine the effect of a gamified instructional module on pre-service primary teachers' knowledge of cybersecurity and their attitudes and acceptance toward gamification methods.

Research Tasks:

- To assess the initial level of cybersecurity knowledge among pre-service teachers (Pre-test);
- To develop and implement a gamified learning module;
- To measure the post-intervention level of knowledge (Post-test);
- To evaluate the effectiveness of gamification by comparing Pre-test and Post-test results;
- To analyze pre-service teachers' acceptance of gamification through descriptive statistics.
- To identify the benefits and limitations of gamified instruction.

Research Questions:

RQ1. How does gamification affect pre-service primary teachers' level of cybersecurity knowledge?

RQ2. What are pre-service primary teachers' perceptions and acceptance of gamified learning?

RQ3. Which gamification elements (points, badges, missions) are the most effective in cybersecurity instruction?

Basic Provisions. A modern teacher is expected to go beyond subject-specific knowledge and be equipped with digital safety skills that they can convey to children in a clear and accessible way. This study explores how gamification can be used to develop cybersecurity awareness among future primary school teachers.Gamification helps bridge academic content with real-life situations by increasing student engagement and motivation. Game-based tasks encourage active thinking and foster a shift from passive learning to practical action. In the context of digital safety, gamified elements play a crucial role in helping learners recognize online risks and develop strategies to stay safe.The training model proposed in this research combines theory with practice and provides an emotionally engaging, collaborative environment. This format supports not only the development of personal digital safety competencies but also strengthens the participants' ability to teach these concepts effectively to young learners. Rather than being passive recipients of knowledge, the participants took on active roles – making decisions, solving problems, and reflecting on their learning. Such an approach is a significant step toward building a conscious and responsible attitude to cybersecurity.

Literature Review. Although "gamification" was first introduced in 2002, it only began to gain widespread use around the 2010s. Gamification refers to using game-like features in settings outside of traditional games. In academic literature, gamification is widely discussed and frequently implemented by educators across various disciplines, particularly in STEM (science, technology, engineering, and mathematics). However, its use in improving cybersecurity literacy remains in the developmental stage. In cybersecurity education, gamification is traditionally understood as applying game elements in non-game environments to increase user engagement [5]. Researchers have identified multiple motivational aspects of gamification in cybersecurity learning, such as achievement, entertainment, knowledge acquisition, and teamwork.

Nevertheless, it remains unclear which aspects most effectively motivate students and their true intention when participating in gamified activities-whether to learn, win, or merely for fun. In addition to examining how gamification influences academic outcomes in cybersecurity, this research also explores lesser-known aspects of gamification. The study seeks to support a more effective and informed integration of gamified methods into cybersecurity education by uncovering these relatively unexamined elements.

Modern teaching strategies include various techniques to enhance student engagement and promote active participation. These techniques include the use of gamification [6], game-based instruction (GBL)

[7], learning through projects [8], flipped classroom models[9], and persuasive educational tools. Recently, gamification and game-based learning have become particularly widespread. Although related, they differ: gamification integrates game-like features such as points, rewards, or teamwork into educational environments, whereas game-based learning involves using educational games with specific learning goals [10]. A "serious game" is any game intended to teach or inform, distinct from games created solely for fun [11] . Within educational settings, games are seen as structured activities with rules and objectives designed to help learners reach specific goals or solve problems. While both game-based learning and serious games contribute to learning, this review emphasizes gamification as the primary focus.

Numerous studies have demonstrated the effectiveness of gamification in educational processes. Key mechanisms of gamification include increased intrinsic motivation, immediate feedback, and a safe environment that encourages learning through trial and error without fear of failure. In contrast, traditional methods for teaching cybersecurity often rely on lectures, text-based instruction, and rule-based learning. These methods promote passive learning and contribute to lower knowledge retention . Studies have indicated that active and experiential learning methods, such as labs, simulations, and scenario-based training, are more effective in developing cybersecurity skills. Teacher preparation programs typically include theoretical coursework, practical sessions, and microteaching. However, despite the recent emphasis on digital literacy, cybersecurity-specific training content is still either limited or inconsistently implemented. Therefore, there is a growing need to integrate innovative teaching methods into educational curricula to equip future teachers with essential technical knowledge, particularly in cybersecurity [12].

Considering the proven effectiveness of gamification in education and the urgent demand for cybersecurity competence among future teachers, this study proposes a novel approach that bridges both domains. Through a quasi-experimental design, we aim to present empirical evidence on the effectiveness of gamified cybersecurity instruction in pre-service teacher preparation.

Materials and Methods. This study was conducted over three weeks at Korkyt Ata Kyzylorda University. The research followed a quasi-experimental design grounded in a mixed-methods approach. It aimed to evaluate the effect of gamified instruction on pre-service primary teachers' cybersecurity knowledge. A total of 44 students participated in the experimental group and attended three 50-minute lessons. The sessions covered the following topics: cyber hygiene, phishing, social engineering, and classroom device and network security.

Gamification elements such as point accumulation, badges, leaderboards, and role-playing activities were integrated into the lessons. Digital platforms, including Kahoot, Wordwall, Genially, and Google Forms, were used as instructional tools. Students worked in small groups and completed game-based tasks, increasing their engagement. The intervention consisted of a three-week module delivered via two formats: the experimental group received gamified instruction, while the control group followed traditional teaching methods. Each week focused on a specific cybersecurity topic, with aligned lesson content, structure, and assessment tools, although pedagogical strategies differed across the groups.

Week 1: "Cyber Hygiene and Phishing" – The objective was to help students recognize phishing attacks and create secure passwords. The experimental group used Kahoot quizzes, badge rewards, and team games; the control group attended slide-based lectures and wrote notes. Assessment: mini-quiz via Google Form and Q&A.

Week 2: "Social Engineering and Fake Content" – The goal was to identify deception techniques and spot misinformation. The experimental group used simulations, case cards, and the "Phishing Detective" game; the control group read texts and listened to teacher explanations. Assessment: case analysis and written responses.

Week 3: "Safe Classroom: Devices and Networks"—The focus was on securing classroom Wi-Fi and digital devices—the experimental group engaged in role-playing games (as hackers and defenders) with point scoring. Students in the control group primarily relied on textbook-based tasks, such as completing tables and taking conventional tests. Their performance was evaluated using a final exam

and an individual task. This approach enabled a clear comparison of academic results between the experimental and control groups. The weekly assessments were carefully aligned with the learning objectives. Student progress was evaluated through observation checklists and reflective tasks *(Table 1).* The researcher delivered all lessons, ensuring consistent delivery and full participation. Initial qualitative findings suggest that gamification positively influenced students' motivation and increased their interest in cybersecurity topics.

Table 1- Three-Week Cybersecurity Training Module: Comparative Structure of Experimental (Gamified) and Control (Traditional) Groups

Week	*Topic*	*Objective*	*Experimental Group (Gamified)*	*Control Group (Traditional Method)*	*Assessment*
1	Cyber Hygiene and Phishing	Identify phishing, ensure password security	Kahoot quiz, badges, team-based games	Slide-based lecture, note-taking, oral explanation	Mini quiz (Google Forms), Q&A
2	Social Engineering and Fake Content	Recognize social deception, detect fake information	Simulation,case cards,"Phishing Detective" game	Reading texts, teacher explanation, questioning	Case analysis, explanation task
3	Safe Classroom: Devices and Networks	Device and Wi-Fi protection, classroom digital safety	Role-playing (defender and hacker), point scoring	Textbook activities, table filling, traditional test	Final test, individual assignment

The questionnaire developed for this research aimed to measure students' knowledge, confidence, and level of acceptance in cybersecurity and gamification pedagogy. The questionnaire's structure was adapted from the study by Ayanwale et al. (2023), titled "A gamified cyber safety education programme for pre-service teachers: development and evaluation" [13]. This study was designed to teach cybersecurity through gamification, and the questionnaire's content orientation aligns with the competencies under investigation.

The questionnaire included 15 statements, each evaluated using a 5-point Likert scale (1—strongly disagree, 5—strongly agree). The questions were divided into three main domains: cybersecurity knowledge, seven items; Teaching readiness and confidence, four items; and Gamification acceptance and intention, four items *(see Table 2).*

To ensure external validity of the questionnaire, the form was reviewed by two experts (a lecturer and a candidate of sciences) specializing in educational technologies and cybersecurity. The experts evaluated the items' formulation, topic relevance, and clarity and provided editorial suggestions. The final version was developed based on these suggestions. The experts highly rated the content validity of the questionnaire and confirmed that it was appropriate for comprehensively measuring the intended research dimensions.

Table 2- Structure of the Questionnaire Measuring Cybersecurity Knowledge, Teaching Readiness, and Gamification Acceptance

Section of the Questionnaire	Covered Topics	Number of Questions
Cybersecurity Knowledge	Phishing, passwords, social engineering, threats	7
Readiness to Teach	Teaching, explanation, confidence	4
Gamification Acceptance	Game elements, motivation, effectiveness	4

The collected data were processed using the SPSS Statistics 29 software. Several statistical methods were applied to analyze the quantitative data according to the research questions. First, a paired samples t-test was conducted to evaluate the variation in scores within the experimental group before and after the intervention. This method enabled analysis of how the students' knowledge changed over time due to the applied approach. According to the analysis results, the mean score difference between the Pre-test and Post-test was found to be statistically significant ($t(20) = 5.529$, $p < 0.001$). This study confirms

the positive influence of gamification on participants' knowledge acquisition in cybersecurity. Secondly, to evaluate the effectiveness of the instructional methods, an independent samples t-test was applied to analyze the post-test performance of the experimental and control groups. The test showed a meaningful difference in average scores ($t(42) = 2.451$, $p = 0.018$), suggesting that gamification resulted in better outcomes than the conventional teaching approach. Thirdly, descriptive statistical analysis was applied to the collected survey data. The mean, standard deviation, minimum, and maximum values were computed for each item to illustrate students' perceptions of gamification and cybersecurity topics. Finally, Cronbach's alpha coefficient was calculated to evaluate the internal consistency of the research instruments. This reliability analysis determined how well the survey items were correlated with the intended construct.

The alpha value calculated in the study was 0.930, which indicates a very high level of reliability (the acceptable threshold is 0.70). As shown in *Table 3*, this result confirms the internal consistency and measurement stability of the survey instrument used. Thus, the statistical analysis ensured the research findings' accuracy, reliability, and scientific validity.

Table 3- Reliability Statistics

Reliability Statistics	
Cronbach's Alpha	N
.930	19

Results. The demographic characteristics of the students who participated in the study are described as follows. A total of 44 participants, all female students aged 18–20, were enrolled in the Primary Education program at a higher education institution. The distribution by academic year was equal: 22 students (50%) were in their 2nd year, and 22 students (50%) were in their 3rd year. Additionally, the students were divided into two groups during the study: 21 students (47.7%) were assigned to the experimental group, and 23 (52.3%) to the control group. The nearly equal ratio between the groups ensured the relative fairness of the comparative analysis of the research results. (*Figure 1*)

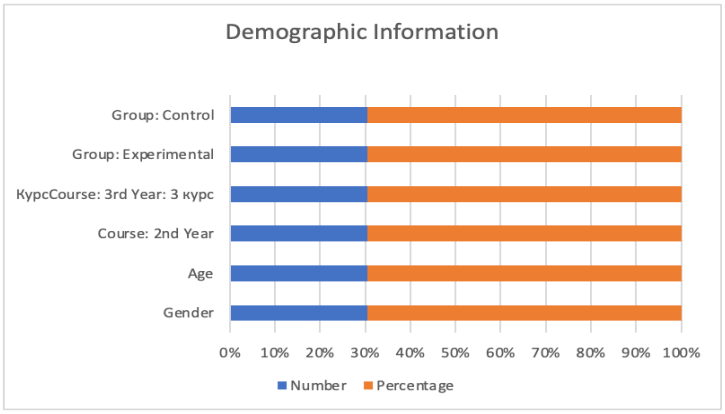

Figure 1. Percentage Diagram of Demographic Information

The first research question of this study was aimed at determining how the use of gamification affects the cybersecurity knowledge level of future primary school teachers. To evaluate the impact of the intervention, the experimental group completed identical tests before and after the program. The paired t-test analysis of these results confirmed the statistical validity of gamification's effectiveness. Specifically, during the Pre-test phase, the students' average score on cybersecurity knowledge was $M = 38.38$, with a standard deviation (SD) = 13.35. In the Post-test, this average score significantly increased to $M = 66.14$, $SD = 13.55$. (*Table 4)* Thus, as a result of a single intervention, participants' knowledge level increased by an average of 27.76 points.

Table 4- Paired Samples Statistics: Pre-test and Post-test Results of the Experimental Group

Paired samples statistics

		Mean	N	Standart deviation	Standart error of the mean
Pair 1	Pre_Total	38.38	21	13.351	2.913
	Post_Total	66.14	21	13.547	2.956

Table 5- Paired Samples t-Test Results Comparing Pre-Test and Post-Test Scores in the Experimental Group

Paired Samples Test

		Paired Differences					t	cdf	Significance	
		Mean	Standard Deviation	Standard Error of the Mean	95% Confidence Interval of the Difference				One-tailed p	Two-tailed p
					Lower	Upper				
	Pre_Total Post_Total	-27.762	23.008	5.021	-38.235	-17.289	5.529	0	<.001	<.001

The t-test results showed that the difference was statistically significant: $t(20) = -5.529$, $p < 0.001$. Furthermore, the 95% confidence interval for the difference ranged between [–38.24, –17.29], meaning the interval does not include zero, indicating that the result is not due to chance. *(Table 5)* These findings demonstrate that a learning process incorporating gamification elements (points, badges, missions) significantly improves pre-service teachers' cybersecurity knowledge. This approach has been confirmed to enhance learning motivation and facilitate mastery of educational content more effectively.

Table 6-Group Statistics for Post-Test Scores between Experimental and Control Groups

Group Statistics

	Group	N	Mean	Standard Deviation	Standard Error of the Mean
Post_Total	1	21	66.14	13.547	2.956
	2	23	56.96	11.292	2.354

Table 7-Independent Samples t-Test Results for Post-Test Scores between Experimental and Control Groups

Independent Samples Test											
		Levene's Test for Equality of Variances		t-test for Equality of Means							
		F	Sig.	т	df	Significance		Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
						One-tailed p	Two-tailed p			Lower	Upper
Post_ Total	Equal variances assumed	1.663	204	2.451	42	.009	.018	9.186	3.748	1.623	16.750
	Equal variances not assumed			2.431	39.113	.010	.020	9.186	3.779	1.543	16.830

During the educational experiment, the cybersecurity Post-test results of two groups using different instructional approaches — the experimental group taught with the gamification method and the control group trained with the traditional method — were compared. This comparison aimed to evaluate the effectiveness of the gamification approach. According to the results, students in the experimental group scored an average of 66.14 on the post-test, while the control group averaged 56.96. *(Table 6)*. This suggests that students taught through gamification had higher knowledge levels than those who learned through traditional methods. The number of participants in both groups was nearly equal (experimental – 21, control – 23), and the standard deviation values fell within the normal range. An independent samples t-test was conducted to assess the statistical significance of the difference between the two groups. The test revealed a t-value of 2.451 with 42 degrees of freedom and a p-value of 0.018. Since the p-value is below 0.05, the difference is statistically significant. In other words, the group taught using gamification performed significantly better than the group taught using traditional methods, and this difference is unlikely to be due to chance. The average score difference between the two groups was 9.19 points, with a 95% confidence interval ranging from [1.62 to 16.75], confirming the statistical reliability of the results (*Table 7)*.

Gamification proved an effective strategy for enhancing the cybersecurity knowledge of pre-service primary teachers. It increased students' cognitive engagement and fostered deeper, more active learning.

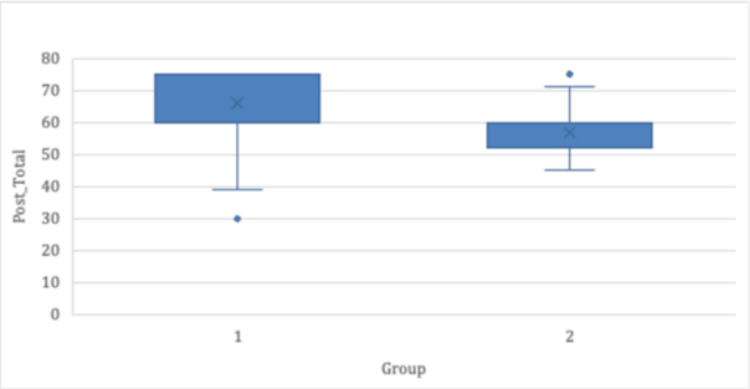

Figure 2. Boxplot Diagram of Post-Test Results for the Experimental and Control Groups

To help answer the first research question, a boxplot was used to visually compare the post-test scores of the experimental and control groups. The diagram shows that students in the experimental group performed better, with a median score around 70. This suggests they had a stronger understanding of cybersecurity. Meanwhile, the control group's median was about 60, which shows they had lower knowledge levels. In the control group, some students scored very low (36, 38, and 15), showing difficulties. Even though the experimental group had one low score (15), most scores were higher and

more consistent. This figure clearly shows the performance difference between the two groups. Combined with the t-test results, the visual data confirms that gamification positively affected students' learning in cybersecurity. Specifically, using game elements (points, badges, missions) improved future teachers' cybersecurity knowledge (*Figure 2).*

Answer to Research Question (RQ2): "What are pre-service teachers' perceptions and acceptance of gamified cybersecurity education?" The study results describe pre-service primary school teachers' self-assessment, confidence, and preparedness regarding cybersecurity and gamification. Responses from 44 students were analyzed using descriptive statistics, and the mean (M) and standard deviation (SD) were calculated for each statement.

The highest mean score was observed in the statement "I understand that sharing personal information online is risky" (M = 3.59, SD = 1.13). This indicates that future teachers have a basic understanding of online threats and pay attention to this topic. Similarly, the statement "I am aware of potential threats when using the internet" also had a high score (M = 3.52, SD = 1.13), suggesting their relatively high digital literacy.

However, the average scores were lower in other statements, particularly those related to practical application. For example, responses to "I know how to recognize phishing emails and links" (M = 2.30, SD = 1.13), "I know the basic rules of creating secure passwords" (M = 2.68, SD = 1.27), and "I know how to protect digital devices" (M = 2.66, SD = 1.24) indicate that future teachers have insufficient knowledge in these areas.

Students' attitudes toward gamification methods were also generally neutral. For example, the statements "I am ready to teach the topic of cybersecurity through games" (M = 2.93, SD = 1.23), "I can use gamification tools (e.g., Kahoot, Wordwall, etc.)" (M = 2.64, SD = 1.26), and "I can create game elements related to cybersecurity for my lessons" (M = 3.14, SD = 1.19) received average scores. These results suggest that while future teachers are interested in using gamification, they lack sufficient methodological preparedness.

Overall, the Pre_Total mean score was 43.80 (out of a possible maximum of 75), indicating that students' knowledge and confidence regarding cybersecurity and gamification are moderate. This highlights the need for additional practical training and well-structured instructional modules to support the effective use of gamification methods in the learning process *(Table 8).*

Table 8-Descriptive Statistics of Pre - and Post-Test Results on Cybersecurity Knowledge and Gamification Perceptions

Descriptive Statistics

	N	Minimum	Maximum	Mean	Standard Deviation
5. I know how to recognize phishing emails and links._Pre	44	1	5	2.30	1.133
6. I know the basic rules of creating secure passwords._Pre	44	1	5	2.68	1.272
7.I understand that sharing personal information online is risky._Pre	44	1	5	3.59	1.127
8. I can advise others on cybersecurity._Pre	44	1	5	2.80	1.268
9. I have heard about social engineering and understand what it is._Pre	44	1	4	2.52	1.110
10.I am aware of potential threats when using the internet._Pre	44	1	5	3.52	1.131
11. I know how to protect digital devices (e.g., antivirus, updates, etc.)._Pre	44	1	5	2.66	1.238
12.I think I can teach students about cybersecurity in the future._Pre	44	1	5	2.91	1.235
13.I am ready to teach cybersecurity through games._Pre	44	1	5	2.93	1.228

14.I can use gamification tools (e.g., Kahoot, Wordwall, etc.)._Pre	44	1	5	2.64	1.259
15.I believe gamification increases children's interest in cybersecurity._Pre	44	1	5	2.75	1.123
16.I can create game elements related to cybersecurity for my lessons._Pre	44	1	5	3.14	1.193
17. I think it is important to teach cybersecurity to primary school students._Pre	44	1	5	3.27	1.188
18. I believe gamification is effective in teaching students._Pre	44	1	5	3.02	1.171
19. I am ready to integrate cybersecurity knowledge into lesson planning._Pre	44	1	5	3.07	1.208
Pre_Total	44	15	65	43.80	13.678
ID	44	1	44	22.50	12.845
Post_Total	44	30	75	61.34	13.120
N valid (listwise)	44				

Discussion. This study shows that gamification can help future teachers improve their cybersecurity knowledge. The statistical difference between the pre-test and post-test scores of the experimental group ($p < 0.001$) indicates that the method had an apparent effect. These findings are in line with earlier research on similar topics. For example, the study by Figg & Jaipal-Jamani (2015) [14] , indicated the effectiveness of gamification in teacher preparation, particularly within the TPACK framework, and in mastering topics such as copyright and cybersecurity. Similarly, the research conducted by Yildiz et al. (2023) [15] found that gamification positively influences pre-service teachers' acceptance and use of technology in teaching. Furthermore, Guerrero Puerta (2024) [16] showed that teachers who experienced gamification were more inclined to use this method in the future.

Thus, this study's results align with previous findings and confirm that gamification is a practical approach to mastering complex and technical subjects such as cybersecurity.

The collected data and statistical analysis results indicate that the gamified method improves future primary school teachers' cybersecurity knowledge. Specifically, the average score difference between the pre- and Post-test was 27.76 points, which marked a significant improvement.

Gamification elements (points, badges, missions, etc.) enhance cognitive engagement by increasing motivation during the learning process. This is especially important in theoretical and technical subjects. Students' interest in learning through games encourages active participation and helps develop their ability to apply acquired knowledge in real-life situations.

Limitations of the study:

The study was conducted among only 44 students from a single higher education institution, limiting the generalizability of the results.

Participants' knowledge levels and perceptions were measured through self-assessment, which may lead to subjective responses.

The intervention duration was limited, so no data was collected on the long-term knowledge retention. Future studies should focus on how gamification affects students over time, especially regarding lasting results. It is also worth exploring how effective gamification is in different subjects. In addition, researchers can look into combining gamification with new technologies like augmented and virtual reality.

Conclusion. This study examined the effectiveness of gamified learning in improving the cybersecurity knowledge of future primary school teachers. The results showed a statistically significant improvement in the experimental group ($p < 0.001$), confirming the role of game mechanics (points, badges, missions) in increasing learning motivation, engagement, and successful mastery of complex

digital concepts. Gamification contributed not only to the growth of knowledge, but also to the formation of the ability to apply it in real online situations. Additional analysis of the perception of gamification showed a moderate level of confidence and readiness among respondents to implement this approach in their own teaching practice. This indicates the need to expand practice-oriented modules in teacher training programmes aimed at using digital tools and developing methodological competence. The pedagogical value of gamification lies in its focus on the principles of active and activity-based learning: creativity, collaborative problem solving, and modelling real digital threats. This approach shapes responsible behaviour among students online and promotes awareness of the importance of digital security in the school environment. The limitations of the study are related to the small sample size and the short duration of the intervention, which does not allow for an assessment of the long-term sustainability of the results. However, the data can serve as a reliable basis for further scientific work on expanding the use of gamification in teacher training. Prospects for further research include increased training duration, the involvement of different universities, the study of the effectiveness of hybrid formats, and the introduction of modern technologies (AR/VR, educational Escape Room). Thus, it has been established that gamification is an effective tool for developing digital literacy and the readiness of future teachers to ensure the cybersecurity of students, and should become an important component of modern teacher education.

References:

1. Hendrix M., Al-Sherbaz A., Bloom V. Game Based Cyber Security Training: are Serious Games suitable for cyber security training? // Int. J. Serious Games. *2016. T. 3, № 1.*

2. Schreuders Z. C., Butterfield E. Gamification for Teaching and Learning Computer Security in Higher Education. 2016.

3. Švábenský V.Enhancing Cybersecurity Skills by Creating Serious Games // Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education. 2018. C. 194–199. https://doi.org/10.1145/3197091.3197123

4. Hamari J., Koivisto J., Sarsa H. Does Gamification Work? – A Literature Review of Empirical Studies on Gamification // 2014 47th Hawaii International Conference on System Sciences. *2014. C. 3025–3034. https://doi.org/10.1109/HICSS.2014.377*

5. ((PDF) The role of gamification and game-based learning in authentic assessment within virtual environments [Electronic resource]. URL: https://www.researchgate.net/publication/279204307_The_role_of_gamification_and_game-based_learning_in_authentic_assessment_within_virtual_environments (дата обращения: 23.10.2025).

6. Villagrasa S. Teaching Case of Gamification and Visual Technologies for Education: // J. Cases Inf. Technol. *2014. T. 16, № 4. C. 38–57. https://doi.org/10.4018/jcit.2014100104*

7. Wiggins B.E. An Overview and Study on the Use of Games, Simulations, and Gamification in Higher Education: // Int. J. Game-Based Learn. 2016. T. 6, № 1. C. 18–29. https://doi.org/10.4018/IJGBL.2016010102

8. Nwokeji J. Panel: Integrating Requirements Engineering Education into Core Engineering Disciplines // 2018 IEEE Frontiers in Education Conference (FIE). San Jose, CA, USA: IEEE Press, 2018. C. 1–3. https://doi.org/10.1109/FIE.2018.8658590

9. Nwokeji J.C., Stachel R., Holmes T. Effect of Instructional Methods on Student Performance in Flipped Classroom // 2019 IEEE Frontiers in Education Conference (FIE). Covington, KY, USA: IEEE, 2019. C. 1–9. https://doi.org/10.1109/FIE43999.2019.9028670

10. Júnior E. S. Systematic literature review of Gamification and Game-based Learning in the context of Problem and Project Based Learning approaches2015

11. Clapper T.C. Serious Games Are Not All Serious // Simul. Gaming. 2018. T. 49, № 4. C. 375–377. https://doi.org/10.1177/1046878118789763

12. Legato P., Mazza R. M. A simulation optimisation-based approach for team building in cyber security.

13. Ayanwale M. A. A Structural Equation Approach and Modelling of Pre-service Teachers' Perspectives of Cybersecurity Education // Educ. Inf. Technol. 2024. T. 29, № 3. C. 3699–3727. https://doi.org/10.1007/s10639-023-11973-5

14. Jaipal-Jamani K., Figg C. A Case Study of a TPACK-Based Approach to Teacher Professional Development: Teaching Science With Blogs // Contemp. Issues Technol. Teach. Educ. *2015.*

15. Yildiz İ., Topçu E., İzmir E. The Effect Of Gamification On Pre-Service Teachers' Technology Acceptance // Ie Inq. Educ. 2023. T. 15, № 2.

16. Guerrero Puerta L. Exploring if Gamification Experiences Make an Impact on Pre-Service Teachers' Perceptions of Future Gamification Use: A Case Report // Societies. Multidisciplinary Digital Publishing Institute, 2024. T. 14, № 1. C. 11. https://doi.org/10.3390/soc14010011