DEVELOPING CYBERSECURITY SKILLS THROUGH GAMIFICATION: INTEGRATING THE CAPTURE-THE-FLAG METHODOLOGY INTO UNIVERSITY TRAINING

Khusenov Murodjon Zokhirovich

Associate Professor, Department of Artificial Intelligence and Information Security, Bukhara State University, Bukhara, Uzbekistan

E-mail: m.z.xusenov@buxdu.uz ORCID: 0000-0002-1533-3102

Abstract. Traditional lecture-based formats of cybersecurity instruction are repeatedly reported to produce low engagement and weak knowledge retention, while the labour market requires graduates with operational, practice-ready skills. Gamification — the use of game design elements in non-game contexts — and, above all, Capture-the-Flag (CTF) exercises have become the most widespread response to this problem. This article systematizes the empirical evidence on gamified cybersecurity training published in 2011–2026 and substantiates a didactic framework for the purposeful development of cybersecurity skills of university students on the basis of gamification. The framework is grounded in experiential learning theory and the concept of self-efficacy and consists of four interconnected blocks: target skills, game mechanics, scenario design, and assessment with feedback. A three-loop model of curricular integration (micro-challenges within classes, a semester-long gamified laboratory cycle, and annual CTF events) is proposed, and the conditions limiting the effectiveness of gamification — entry barriers for novices, fragmentary topic coverage and assessment validity — are analysed together with mitigation measures. The framework is intended for implementation in cybersecurity-related programmes of higher education institutions, including the universities of Uzbekistan.

Keywords: *gamification; capture the flag (CTF); cybersecurity skills; serious games; active learning; motivation; self-efficacy*

INTRODUCTION

Gamification is conventionally defined as “the use of game design elements in non-game contexts” [1]. In cybersecurity education this idea has acquired exceptional practical significance, because the discipline requires not only declarative knowledge but adversarial thinking, tool proficiency and the ability to act under uncertainty — qualities that passive instruction develops poorly. Practitioner reports describe a recurring pattern: lecture- and workshop-style security training fails to engage participants, leading to disinterest and low knowledge retention, whereas the transition to Capture-the-Flag (CTF) competitions noticeably improves both engagement and the ability to recall and apply the material [2].

CTF exercises are currently the dominant gamified format in the field. In jeopardy-style CTFs participants solve categorized puzzles (web exploitation, cryptography, reverse engineering, forensics and others) to obtain hidden text strings — “flags”; in attack–defence CTFs teams simultaneously protect their own services and attack those of opponents. CTF-based gamification has been deliberately introduced into undergraduate computer security laboratories [3], and large educational platforms — for example, picoCTF developed at Carnegie Mellon University for school and novice audiences — have made the format broadly accessible [4].

The empirical evidence is encouraging. A comparative study of university students in Finland and Czechia trained in a cyber range with a gamified CTF scenario found that the exercises increased knowledge and skill variables, self-efficacy and interest, with high satisfaction across student groups of different backgrounds, while gamification elements such as points and leaderboards supported engagement and motivation [5]. A structured CTF onboarding platform evaluated with 101 beta-test participants reported improved understanding, increased confidence and greater motivation to take part in jeopardy-style competitions [6]. Industry analyses likewise associate gamified security training with measurably higher completion rates and improved recognition of phishing attacks [7, 8].

At the same time, the adoption of gamification in curricula remains largely episodic: individual competitions are organized, but game elements are rarely linked systematically to target competencies and assessment. The aim of this study is to substantiate a didactic framework for the systematic development of cybersecurity skills of university students on the basis of gamification. The objectives are: (i) to systematize gamified formats and the empirical evidence of their effectiveness; (ii) to construct a framework linking game mechanics with skill formation and assessment; (iii) to propose a model of integration of gamified activities into the curriculum and to identify the conditions of their effective use.

MATERIALS AND METHODS

The study is based on the analysis of peer-reviewed publications, conference papers, preprints and documented practitioner reports on gamification in cybersecurity education published between 2011 and 2026, retrieved from IEEE Xplore, SpringerLink, Wiley, arXiv and recognized professional sources. Priority was given to works containing empirical measurements of learning-related variables (knowledge, skills, self-efficacy, motivation, satisfaction) or substantiated design recommendations.

The theoretical basis of the framework is formed by two complementary constructs. Experiential learning theory describes skill formation as a cycle of concrete experience, reflective observation, abstract conceptualization and active experimentation [9]; CTF exercises naturally instantiate the first and the last stages, while the framework must deliberately provide the middle, reflective ones. The concept of self-efficacy explains why successfully completed, appropriately difficult challenges increase the learner’s belief in their own capability and willingness to attempt harder tasks [10], which is directly confirmed by the growth of self-efficacy variables in CTF-based training [5].

The framework was constructed by the mapping method: game mechanics identified in the literature were related to the motivational mediators they activate and to the target skill domains structured according to the CSEC2017 curricular guidelines

[11]. Design requirements were additionally derived from empirically documented barriers — above all, unclear instructions, lack of foundational knowledge and navigation difficulties experienced by novice CTF participants [6]. The study is theoretical-synthetic in character; its own experimental verification is planned as the next stage and no original statistical results are reported here.

RESULTS

3.1. Taxonomy of gamified formats. Five basic formats are distinguished in the analysed corpus: (1) jeopardy-style CTFs with categorized independent challenges, best suited for differentiated skill development; (2) attack–defence CTFs, which add team coordination, monitoring and response under time pressure; (3) cyber escape rooms — time-boxed, team-based chains of interconnected puzzles oriented towards awareness and teamwork; (4) gamified defensive (blue-team) laboratories, in which realistic investigation scenarios are combined with points, leaderboards, titles and badges [7]; (5) micro-challenges embedded in ordinary classes. The formats differ in cost of preparation, required infrastructure and the balance between breadth of coverage and depth of immersion, and are therefore complementary rather than interchangeable.

3.2. Didactic framework. The framework consists of four blocks. Block 1 — target skills: technical domains (web security, cryptography, network analysis, digital forensics, reverse engineering) selected from CSEC2017 knowledge areas [11], cognitive skills (adversarial thinking, hypothesis testing under incomplete information) and social skills (team coordination, division of roles). Block 2 — game mechanics mapped to motivational mediators: points operationalize goal orientation; levels and badges mark milestones and sustain a sense of progress; leaderboards activate social comparison and must be applied selectively to avoid demotivating lower-ranked participants; narrative framing provides professional context; time-boxing trains action under pressure. Block 3 — scenario design: a graduated difficulty curve; scaffolded hints with progressive disclosure; preparatory briefings for novices, directly answering

the documented barriers of unclear instructions and missing foundations [6]; and deliberate alignment of every challenge with an intended learning outcome — since participants tend to learn precisely what is needed to solve the challenge, the challenge itself must embody the outcome [2]. Block 4 — assessment and feedback: flags serve as embedded evidence of task completion; attempt analytics reveal typical errors; and structured post-event reflection with visual feedback on the participant's path through the exercise is used to consolidate learning, in line with research on visual feedback in multi-level CTF games [12].

3.3. Model of curricular integration. Three nested loops are proposed. The micro-loop embeds 15–30-minute challenges into seminars and laboratory classes as formative practice. The meso-loop organizes a semester-long gamified cycle: laboratory works of a course are connected by a cumulative (preferably anonymized or team-based) leaderboard, badges for completed modules and an optional bonus track of harder tasks. The macro-loop comprises an annual university CTF and participation in external national and international competitions, performing motivational, diagnostic and career-orientation functions. Because CTFs are weaker than structured instruction at guaranteeing systematic coverage of a predetermined syllabus [2], the model is explicitly hybrid: gamified activities are paired with structured theoretical instruction, and the mapping of challenges to learning outcomes in Block 3 is used to monitor coverage.

DISCUSSION

The synthesized framework converts gamification from an occasional event into a managed didactic system. Its expected effects rest on convergent evidence: growth of knowledge, self-efficacy and interest in CTF-based training across heterogeneous student groups [5], improved retention reported by practitioners after replacing passive formats [2], positive experience of gamifying undergraduate security laboratories [3], and confidence gains produced by structured onboarding [6]. The finding that different

categories of students benefit in different ways [5] supports the differentiated design of difficulty and hint systems rather than a uniform competition for all.

The analysis also makes the boundary conditions explicit. First, entry barriers are the principal threat: without scaffolding, novices experience frustration instead of flow [6], which argues for preparatory tracks and platforms of the picoCTF type at the initial stage [4]. Second, competitive mechanics can backfire; leaderboards should be optional, team-based or anonymized for vulnerable groups. Third, assessment validity requires attention: flag sharing and surface strategies are countered by unique per-participant flags, write-up requirements and reflection reports, which simultaneously serve the reflective stage of the experiential cycle [9]. Fourth, the preparation of high-quality challenges is labour-intensive; the meso-loop is therefore realistic only if the institution accumulates a reusable scenario library, ideally shared between universities and connected to the institutional virtual laboratory infrastructure.

For the higher education institutions of Uzbekistan, where the demand for cybersecurity personnel is growing and practice-oriented infrastructure is being formed, the framework offers an implementable path that does not require expensive proprietary platforms at the start. The limitation of the study is its synthetic character: the framework aggregates external empirical evidence but has not yet been verified as a whole. A quasi-experimental evaluation in the educational process of Bukhara State University — with pre/post measurement of skill, self-efficacy and motivation indicators in experimental and control groups — is planned as the continuation of this work.

CONCLUSION

Gamification, and the CTF methodology in particular, is supported by consistent empirical evidence as a means of developing cybersecurity skills: it increases engagement, knowledge, self-efficacy and interest when challenges are well designed and appropriately scaffolded. The contribution of this article is a didactic framework that links game mechanics to target competencies, scenario design principles and

assessment instruments, and a three-loop model that integrates gamified activities into the curriculum in combination with structured instruction. The decisive conditions of effectiveness are graduated difficulty with support for novices, careful use of competitive elements, assessment procedures resistant to surface strategies, and the accumulation of reusable challenge libraries. Experimental verification of the framework and the development of a national inter-university CTF scenario repository constitute the directions of further research.

REFERENCES

1. Deterding S., Dixon D., Khaled R., Nacke L. From game design elements to gamefulness: Defining “gamification” // Proceedings of the 15th International Academic MindTrek Conference. ACM, 2011. P. 9–15.

2. Gamified Learning: Using Capture the Flag Challenges to Supplement Cybersecurity Training [Guest Diary] // SANS Internet Storm Center. 2024. [Online]. Available: https://isc.sans.edu/diary/30752

3. Beltran M., Calvo M., Gonzalez S. Experiences Using Capture The Flag Competitions to Introduce Gamification in Undergraduate Computer Security Labs // 2018 International Conference on Computational Science and Computational Intelligence (CSCI). IEEE, 2018. P. 574–579. DOI: 10.1109/CSCI46756.2018.00116.

4. picoCTF. Carnegie Mellon University. [Online]. Available: https://picoctf.org

5. Schafeitel-Tahtinen T. et al. Teaching and Learning Cybersecurity Using Capture the Flag: Effectiveness Comparison Between University Students in Finland and Czechia // Computer Applications in Engineering Education. 2025. Vol. 33. DOI: 10.1002/cae.70082.

6. Enhancing Cybersecurity Education Through Gamified Learning and Capture the Flag (CTF) Platform // Springer Nature book chapter. 2025. DOI: 10.1007/978-3-031-98003-9_6.

7. CloudShare. How Gamified Cybersecurity Labs Improve Skill Retention. 2025. [Online]. Available: https://www.cloudshare.com/blog/gamified-cybersecurity-labs-skill-retention/

8. TechClass. Gamification in Cybersecurity Awareness: Does It Really Work? 2026. [Online]. Available: https://www.techclass.com/resources/learning-and-development-articles/gamification-in-cybersecurity-awareness-does-it-really-work

9. Kolb D. A. Experiential Learning: Experience as the Source of Learning and Development. Englewood Cliffs: Prentice-Hall, 1984.

10. Bandura A. Self-efficacy: Toward a unifying theory of behavioral change // Psychological Review. 1977. Vol. 84, No. 2. P. 191–215.

11. Joint Task Force on Cybersecurity Education. Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. ACM / IEEE-CS / AIS SIGSEC / IFIP WG 11.8, 2017. DOI: 10.1145/3184594.

12. Visual Feedback for Players of Multi-Level Capture the Flag Games: Field Usability Study // arXiv preprint arXiv:1912.10781. 2019.