



"ZAMONAVIY TA'LIM VA TILSHUNOSLIK RIVOJI"

nomli respublika ilmiy-amaliy masofaviy konferensiyasi

VOLUME-1, ISSUE-2, 2026

THE USE OF GAMIFICATION AND INTERACTIVE LEARNING TECHNOLOGIES IN TEACHING CYBERSECURITY

KUTLIMURATOV ANVAR SABUROVICH

Computer Science Teacher, Specialized State General Secondary School No. 65,
Beruniy District

Abstract

This thesis analyzes the pedagogical potential of using gamification and interactive learning technologies in teaching cybersecurity. Gamification is considered a means of increasing students' engagement and motivation by incorporating game elements such as points, levels, badges, rankings, tasks, rewards, and narrative scenarios into the educational process. A 2026 systematic review analyzing 230 studies published between 2018 and 2024 demonstrates the widespread use of gamification and serious game approaches in cybersecurity education [1]. At the same time, studies published in 2025 indicate that game-based approaches can increase engagement, although their impact on learning outcomes is not always conclusive [2; 3]. The thesis proposes an approach that integrates gamification, interactive simulations, scenario-based learning, and immediate feedback into a unified methodological cycle.

Keywords

cybersecurity, gamification, interactive learning, serious games, game-based learning, simulation, CTF, feedback, digital competence.

KIBERXAVFSIZLIKNI O'QITISHDA GAMIFIKATSIYA VA INTERAKTIV TA'LIM TEXNOLOGIYALARIDAN FOYDALANISH

KUTLIMURATOV ANVAR SABUROVICH

*Beruniy tumani 65-ixtisoslashgan Davlat umumiy o'rta ta'lim makabi informatika
fani o'qituvichisi*

Annotatsiya





“ZAMONAVIY TA’LIM VA TILSHUNOSLIK RIVOJI”

nomli respublika ilmiy-amaliy masofaviy konferensiyasi

VOLUME-1, ISSUE-2, 2026

Mazkur tezisda kiberxavfsizlikni o‘qitishda gamifikatsiya va interaktiv ta’lim texnologiyalaridan foydalanishning pedagogik imkoniyatlari tahlil qilinadi. Gamifikatsiya ta’lim jarayoniga ball, daraja, badge, reyting, topshiriq, mukofot va hikoyaviy ssenariy kabi o‘yin elementlarini kiritish orqali o‘quvchilarning faolligi va motivatsiyasini oshirish vositasi sifatida qaraladi. 2026-yilgi tizimli sharh 2018–2024-yillarda chop etilgan 230 ta tadqiqotni tahlil qilib, kiberxavfsizlik ta’limida gamifikatsiya va serious games yondashuvlarining keng qo‘llanayotganini ko‘rsatadi [1]. Shu bilan birga, 2025-yilgi tadqiqotlar o‘yinli yondashuv engagementni oshirishi mumkinligini, biroq uning bilim natijalariga ta’siri har doim ham aniq emasligini ko‘rsatadi [2; 3]. Tezisda gamifikatsiya, interaktiv simulyatsiya, scenario-based learning va tezkor feedbackni yagona metodik siklga birlashtiruvchi yondashuv taklif etiladi.

Kalit so‘zlar: kiberxavfsizlik, gamifikatsiya, interaktiv ta’lim, serious games, game-based learning, simulyatsiya, CTF, feedback, raqamli kompetensiya.

Kirish

Kiberxavfsizlik mazmunining texnik murakkabligi va tahdidlarning tez o‘zgarishi an’anaviy ma’ruza va reproduktiv topshiriqlarga qo‘shimcha ravishda faol, interaktiv va tajribaga asoslangan o‘qitish usullaridan foydalanishni talab qiladi. 2025-yilgi tizimli sharhda boshlang‘ich kiberxavfsizlik ta’limiga oid 81 ta tadqiqot tahlil qilinib, game-based learning va storytelling eng ko‘p o‘rganilgan pedagogik strategiyalar qatorida qayd etilgan [4].

Gamifikatsiya o‘yin emas, balki o‘yin dizayni elementlarini o‘yin bo‘lmagan ta’lim faoliyatiga kiritishdir. Ball, badge, leaderboard, darajalar, challenge va feedback kabi elementlar o‘quvchini faol ishtirok etishga undashi mumkin [1]. Serious games esa ta’limiy yoki trening maqsadida maxsus ishlab chiqilgan o‘yinlar bo‘lib, kiberxavfsizlikdagi murakkab vaziyatlarni xavfsiz virtual muhitda mashq qilish imkonini beradi [3].





“ZAMONAVIY TA’LIM VA TILSHUNOSLIK RIVOJI”
nomli respublika ilmiy-amaliy masofaviy konferensiyasi
VOLUME-1, ISSUE-2, 2026

Gamifikatsiyaning kiberxavfsizlik ta’limidagi imkoniyatlari

Kiberxavfsizlikni o’qitishda gamifikatsiyaning asosiy didaktik afzalligi — murakkab tushunchalarni faol qaror qabul qilish vaziyatiga aylantirishdir. Masalan, phishing mavzusida o’quvchiga “phishing nima?” degan savolni berish o’rniga bir nechta elektron xabar namunalarini taqdim etib, xavfli xabarni aniqlash, sababini tushuntirish va to’g’ri harakatni tanlash topshiriladi. 2025-yilgi phishing bo’yicha tizimli sharh interaktiv simulyatsiyalar, serious games, reward systems va dynamic feedback kabi strategiyalarni eng ko’p uchraydigan gamifikatsion yondashuvlar sifatida ko’rsatadi [5].

Gamifikatsiya elementlarini quyidagi didaktik vazifalar bilan bog’lash mumkin:

Element	Didaktik vazifa	Misol
Ball	Natijani tezkor ko’rsatish	To’g’ri xavfsizlik qarori uchun ball
Daraja	Bosqichma-bosqich murakkablik	Beginner → Analyst
Badge	Erishilgan kompetensiyani belgilash	“Phishing Hunter”
Leaderboard	Ijtimoiy motivatsiya	Haftalik reyting
Challenge	Muammoli faoliyatni kuchaytirish	5 ta tahdidni aniqlash
Feedback	Xatoni darhol tushuntirish	Nima uchun havola xavfli?

Interaktiv ta’lim texnologiyalari

Gamifikatsiya interaktiv texnologiyalar bilan birlashtirilganda uning pedagogik samarasi kuchayishi mumkin. CTF (Capture the Flag) formatida o’quvchilar bosqichma-bosqich vazifalarni bajarib, yashirin “flag”larni topadilar; scenario-based learningda esa real hayotga yaqin vaziyatda qaror qabul qiladilar; simulyatsiyada esa



“ZAMONAVIY TA’LIM VA TILSHUNOSLIK RIVOJI”
nomli respublika ilmiy-amaliy masofaviy konferensiyasi
VOLUME-1, ISSUE-2, 2026

xatolarni real tizimga zarar yetkazmasdan sinab ko‘radilar. 2024-yilgi tadqiqotda non-cyber talabalarni jalb qilish uchun ochiq va hikoyaviy CTF formatlaridan foydalanilgan [6].

Interaktiv vositalarning muhim xususiyati — feedbackning tezkorligidir. O‘quvchi xato qilgan zahoti uning sababini ko‘rsa, keyingi urinishda qarorini tuzatishi mumkin. Biroq gamifikatsiya faqat ball va reyting bilan cheklanmasligi kerak. 2025-yilda ishlab chiqilgan steganografiya bo‘yicha narrative serious game tadqiqotida o‘yinli yondashuv engagementni sezilarli oshirgan, ammo qisqa muddatli bilim testi natijalarida matnli ta’limdan ustunlik aniqlanmagan [2]. Demak, o‘yin elementi o‘quv maqsadiga bevosita xizmat qilishi zarur.

Taklif etilayotgan interaktiv-gamifikatsion model

Kiberxavfsizlikni o‘qitish uchun quyidagi metodik sikl taklif etiladi: Muammo → Ssenariy → Challenge → Amaliy harakat → Feedback → Natija → Refleksiya. Dastlab o‘quvchiga real hayotga yaqin kiberxavfsizlik muammosi beriladi. Keyin ssenariy asosida bir nechta qaror variantlari taqdim etiladi. Challenge bosqichida topshiriq murakkabligi oshiriladi, feedback orqali xatolar tushuntiriladi va yakunda o‘quvchi o‘z qarorini refleksiya qiladi.

Modelni uch darajada qo‘llash mumkin: boshlang‘ich darajada phishing, parol va maxfiylik kabi kundalik xavfsizlik vaziyatlari; o‘rta darajada tarmoq, zararli dastur va ijtimoiy muhandislik ssenariylari; yuqori darajada esa CTF, attack–defence simulation va muammoli laboratoriya topshiriqlari. 2026-yilgi sharhda 172 ta tadqiqot tahlil qilinib, gamifikatsiyalangan platformalarda didaktika, UX va attack–defence simulation masalalarining birgalikda ko‘rib chiqilayotgani qayd etilgan [7].

Samaradorlik mezonlari

Gamifikatsion ta’limni baholashda faqat o‘yin davomida to‘plangan ballni natija deb qabul qilish noto‘g‘ri. Baholash kamida to‘rtta mezonni qamrab olishi kerak:



“ZAMONAVIY TA’LIM VA TILSHUNOSLIK RIVOJI”

nomli respublika ilmiy-amaliy masofaviy konferensiyasi

VOLUME-1, ISSUE-2, 2026

Mezon	Ko‘rsatkich	Baholash vositasi
Faollik	Ishtirok, topshiriqni yakunlash, takroriy urinish	Platforma loglari
Bilim	Tushunchalarni o‘zlashtirish	Pre-test/post-test
Amaliy kompetensiya	Xavfni aniqlash va to‘g‘ri qaror	Scenario/CTF
Motivatsiya	Qiziqish va davomiy ishtirok	So‘rovnoma
Xulq-atvor	Xavfsiz qarorni real vaziyatda qo‘llash	Kuzatuv/vaziyatli test

Kompleks samaradorlik indeksini metodik model sifatida quyidagicha ifodalash mumkin:

$$K_g = 0,20F + 0,25B + 0,30A + 0,15M + 0,10X$$

bu yerda F — faollik, B — bilim, A — amaliy kompetensiya, M — motivatsiya, X — xulq-atvor ko‘rsatkichi. Koeffitsiyentlar taklif etilayotgan metodik modelning boshlang‘ich parametrlari bo‘lib, tajriba-sinovda statistik va ekspert baholash orqali aniqlashtirilishi lozim.

Natijalar va muhokama

Tahlil shuni ko‘rsatadiki, gamifikatsiya kiberxavfsizlik ta’limida ayniqsa engagement va faol ishtirokni kuchaytirish uchun istiqbolli vositadir [1; 3]. Biroq o‘yin elementlari o‘quv maqsadidan uzilib qolsa, yuqori ball yoki reyting o‘quv mazmunining o‘zlashtirilishini anglatmasligi mumkin. Shu sababli har bir challenge aniq kompetensiya bilan, feedback esa o‘quv maqsadi bilan bog‘lanishi kerak [2].

Taklif etilayotgan modelda o‘yin mexanikalari pedagogik vosita sifatida ishlatiladi: challenge — muammoli vazifani, daraja — murakkablikning ortishini, feedback —



“ZAMONAVIY TA’LIM VA TILSHUNOSLIK RIVOJI”
nomli respublika ilmiy-amaliy masofaviy konferensiyasi
VOLUME-1, ISSUE-2, 2026

xatoni tuzatishni, badge — erishilgan natijani, CTF esa amaliy kompetensiyani ifodalaydi. Bunday yondashuv gamifikatsiyani “o‘yin o‘ynash”dan “maqsadli o‘rganish”ga aylantiradi.

2026-yilgi katta ko‘lamli sharhda 230 ta tadqiqot tahlil qilingan bo‘lsa, 2026-yilgi boshqa SLR 172 ta tadqiqotni ko‘rib chiqqan [1; 7]. Bu yo‘nalishning ilmiy faolligi yuqori ekanini ko‘rsatadi, biroq tadqiqotlar samaradorlikni turli mezonlar bilan o‘lchayotgani sababli standartlashtirilgan baholash vositalariga ehtiyoj saqlanib qolmoqda [1; 7].

Xulosa

Kiberxavfsizlikni o‘qitishda gamifikatsiya va interaktiv ta’lim texnologiyalaridan foydalanish ta’lim oluvchilarning faolligi, motivatsiyasi va amaliy vaziyatlarda qaror qabul qilish imkoniyatlarini kuchaytirishi mumkin. Eng samarali yondashuv gamifikatsiya elementlarini aniq o‘quv maqsadlari, ssenariy, simulyatsiya, CTF va tezkor feedback bilan uyg‘unlashtirishdan iborat.

Tadqiqotda Muammo → Ssenariy → Challenge → Amaliy harakat → Feedback → Natija → Refleksiya sikliga asoslangan interaktiv-gamifikatsion model taklif qilindi. Uning samaradorligini faollik, bilim, amaliy kompetensiya, motivatsiya va xulq-atvor mezonlari orqali kompleks baholash mumkin. Shu bilan birga, mavjud tadqiqotlar gamifikatsiyaning engagementga ijobiy ta’sirini ko‘rsatsa-da, bilim natijalaridagi ustunlik har doim ham bir xil emasligini ko‘rsatadi [2; 3]. Shuning uchun gamifikatsiya mustaqil maqsad emas, balki kiberxavfsizlik kompetensiyasini shakllantirishga xizmat qiluvchi pedagogik vosita sifatida qo‘llanishi lozim.

Foydalanilgan adabiyotlar

1. Weeratunge N. H., Hjelsvold R., Katt B. A systematic scoping review on game-based cybersecurity awareness education. International Journal of Information Security, 2026, 25, Article 71. DOI: 10.1007/s10207-026-01239-9.



"ZAMONAVIY TA'LIM VA TILSHUNOSLIK RIVOJI"

nomli respublika ilmiy-amaliy masofaviy konferensiyasi

VOLUME-1, ISSUE-2, 2026

2. Gamifying cybersecurity: A narrative-driven approach to teaching steganography. Computers and Education Open, 2025, 9, 100288. DOI: 10.1016/j.caeo.2025.100288.

3. Amjad M. et al. Unlocking Cybersecurity: A Game-Changing Framework for Training and Awareness—A Systematic Review. Human Behavior and Emerging Technologies, 2025. DOI: 10.1155/hbe2/9982666.

4. Liu N., Long S., Martin F. Systematic Review of Elementary Cybersecurity Education: Curriculum, Pedagogy, and Barriers. Journal of Cybersecurity Education, Research and Practice, 2025, Article 21.

5. Dominguez Aguila A. J., Ojeda Marchán R. S., Donayre Monteza F. A. Gamification in Education for Phishing Prevention: A Systematic Review. LACCEI, 2025. DOI: 10.18687/LEIRD2025.1.1.443.

6. Williams L., Anthi E., Cherdantseva Y., Javed A. Leveraging Gamification and Game-based Learning in Cybersecurity Education: Engaging and Inspiring Non-Cyber Students. Journal of The Colloquium for Information Systems Security Education, 2024, 11(1). DOI: 10.53735/cisse.v11i1.186.

7. From CTF to Competence: UX-Driven and Didactic Foundations for Gamified Cybersecurity Training Platforms. Applied Sciences, 2026, 16(12), 6100.