

TALABALARDA AXBOROT XAVFSIZLIGI MADANIYATINI SHAKLLANTIRISHNING ZAMONAVIY USULLARI

Tuxtabayeva Muxlisa Abbos qizi

O'zbekiston xalqaro islomshunoslik akademiyasi

Axborot xavfsizligi yo'nalishi 2-kurs talabasi

Email: muxlisatuxtabayeva@gmail.com

Ayitqulova Guliza Oqilbek qizi

O'zbekiston xalqaro islomshunoslik akademiyasi

Axborot xavfsizligi yo'nalishi 2-kurs talabasi

Email: ayitqulovaguliza@gmail.com

<https://doi.org/10.5281/zenodo.15869464>

Annotatsiya: Ushbu maqolada zamonaviy raqamli texnologiyalar va kiberxavfsizlik tahdidlari fonida talabalarda axborot xavfsizligi madaniyatini shakllantirish zarurati asoslab berilgan. Muallif axborot xavfsizligining nazariy asoslari, talabalar o'rtasida uchraydigan xavfsizlik xatolari va zamonaviy tahdidlar tahliliga asoslangan holda, ta'lim muassasalarida foydalanilishi mumkin bo'lgan interaktiv, diniy-ma'naviy va texnologik yondashuvlarni taklif qiladi. Xususan, gamifikatsiya, simulyatsiya, onlayn kurslar va diniy targ'ibot orqali talabalar ongida raqamli madaniyatni shakllantirish yo'llari yoritib berilgan.

Kalit so'zlar: axborot xavfsizligi, talabalar, zamonaviy texnologiyalar, raqamli madaniyat, diniy-ma'naviy yondashuv, gamifikatsiya, phishing, xavfsizlik xabardorligi.

MODERN METHODS OF FORMING INFORMATION SECURITY CULTURE AMONG STUDENTS

Abstract: This article substantiates the need to develop information security culture among students in the context of modern digital technologies and cybersecurity threats. The author analyzes theoretical foundations of information security, common security mistakes among students, and current threats. Based on this, the paper proposes interactive, spiritual-educational, and technological approaches applicable in educational institutions. In particular, the work discusses methods such as gamification, simulations, online training programs, and religious-moral awareness to improve digital literacy and culture among youth.

Keywords: information security, students, modern technologies, digital culture, religious-moral approach, gamification, phishing, security awareness.

Axborot xavfsizligi bugungi kunda nafaqat texnik, balki ijtimoiy va ma'naviy muammo sifatida qaralmoqda. Ayniqsa, talabalar orasida raqamli vositalardan noto'g'ri foydalanish, shaxsiy ma'lumotlarga e'tiborsizlik, phishing va zararli dasturlar bilan ehtiyotsiz muomala kabi holatlar tobora ko'paymoqda. Ushbu holat ta'lim tizimida axborot xavfsizligi madaniyatini shakllantirish zaruratini yuzaga keltirmoqda. Turli xalqaro tadqiqotlar asosida talabalarning axborot xavfsizligiga bo'lgan munosabati va bilim darajasini aniqlashga qaratilgan tahlillar shuni ko'rsatmoqdaki, hozirgi holatda an'anaviy ta'lim metodlari yetarli emas. Masalan, Majmaah Universiteti (Saudiya Arabistoni)da o'tkazilgan tadqiqotda talabalar axborot xavfsizligi bo'yicha o'rtacha darajada bilimga ega ekani, ayniqsa phishing va kriptografiyaga oid bilimlarning pastligi aniqlangan. Tadqiqotda ANOVA, Bartlett va KMO testlari yordamida

talabalar bilimini baholash metodikasi qo'llangan va natijalar asosida maqsadli tavsiyalar ishlab chiqilgan.

Shu bilan birga, interaktiv va amaliy mashg'ulotlar asosidagi yondashuvlar — xususan, gamifikatsiya va simulyatsiya — talabalar bilimini oshirishda samarali vosita bo'layotgani kuzatilmoqda. Tayvanda 110 nafar talabada olib borilgan quasi-eksperimental tadqiqotda gamifikatsiya asosida tashkil etilgan o'quv mashg'ulotlari orqali axborot xavfsizligi bo'yicha bilim darajasida sezilarli o'sish qayd etilgan. Shuningdek, SCORPION Cyber Range loyihasida 82,1% talabalar foydalanish qulayligini yuqori baholagan va foydalilik darajasi o'rtacha 4,57/5 ni tashkil qilgan. Bu kabi natijalar amaliy ko'nikmalarni shakllantirishda aniq metodlar mavjudligini ko'rsatadi.

Axborot xavfsizligi madaniyatini shakllantirishda faqat texnik yondashuvlar emas, balki diniy-ma'naviy qadriyatlarga tayanuvchi tushuntirishlar ham muhim o'rin tutadi. Jumladan, shaxsiy ma'lumotlarni asrash, yolg'on axborot tarqatmaslik, internetdagi odob va mas'uliyatli xatti-harakatlar Islom axloqiy tamoyillarida ham muhim sanaladi. Bu esa ta'lim jarayoniga integratsiyalangan holda axborot xavfsizligi ongini shakllantirish imkonini beradi.

Hozirgi holatda eng samarali yondashuvlar sifatida gamifikatsiyalashgan mashg'ulotlar, simulyatsiya asosida mashq qilish, phishingni tanish testlari va ijtimoiy muhandislikka qarshi treninglar taklif etiladi. Xalqaro tadqiqotlar natijasida gamifikatsiya o'qitish samaradorligini o'rtacha 15–30% ga oshirishi isbotlangan. Shuningdek, real tahdid ssenariylari asosidagi treninglar talabalar xotirasida uzoq saqlanadi va bu orqali xulq-atvor ham ijobiy tomonga o'zgaradi.

Shu asosda oliy ta'lim muassasalarida axborot xavfsizligi fanini zamonaviy metodikalar asosida qayta ishlab chiqish, interaktiv vositalarni (Cyber Range, gamifikatsiya, video treninglar) tatbiq etish, diniy-ma'naviy va axloqiy targ'ibotni kuchaytirish tavsiya etiladi. Bu bilan nafaqat talabalar, balki jamiyatda kengroq axborot madaniyatini shakllantirishga erishiladi.

Foydalanilgan adabiyotlarga tayanilsa, O'zbekiston Respublikasi Axborot xavfsizligi konsepsiyasi (2022) ushbu yo'nalishda davlat siyosatining ustuvorligini ko'rsatadi. Shuningdek, MDPI nashriyotining "Cybersecurity Awareness" maqolasi, SCORPION Cyber Range loyiha hisobotlari, OECD va NIST tomonidan taqdim etilgan metodikalar, CISA hamda ENISA tavsiyalari ilmiy va amaliy jihatdan ushbu yondashuvlarni asoslab beradi. Bu kabi aniq va ilmiy asoslangan manbalar orqali axborot xavfsizligini ta'lim tizimiga chuqur integratsiya qilish mumkinligi isbotlanadi.

References:

Используемая литература:

Foydalanilgan adabiyotlar:

1. O'zbekiston Respublikasi Axborot xavfsizligi konsepsiyasi. — Toshkent: 2022.
2. Xusanov B. *Axborot xavfsizligi asoslari*. — Toshkent: Ilm ziyo, 2020.
3. Alimova N. *Ta'lim tizimida raqamli madaniyatni rivojlantirish*. — O'zbekiston pedagogika jurnali, 2023.
4. National Institute of Standards and Technology (NIST). *Framework for Improving Critical Infrastructure Cybersecurity*. Version 1.1, April 2018.

5. European Union Agency for Cybersecurity (ENISA). *Cybersecurity Education and Awareness*. <https://www.enisa.europa.eu>
6. Cybersecurity & Infrastructure Security Agency (CISA). *Cybersecurity Awareness Programmes*. <https://www.cisa.gov>
7. Davis, J. (2021). *Gamification and Cyber Hygiene in Higher Education*. – *Journal of Cyber Ethics*, Vol. 6, No. 2.
8. Alenezi, A. et al. (2023). *Cybersecurity Awareness among University Students: A Study at Majmaah University*. – *Inventions*, 8(2), 45. <https://www.mdpi.com/2504-2289/8/2/45>
9. Wei, C.-W. & Lee, L. (2020). *A Gamified Learning Model for Information Security Awareness in Higher Education*. – *Interactive Learning Environments*. DOI: 10.1080/10494820.2020.1732515
10. Papamartzivanos, D. et al. (2024). *SCORPION Cyber Range for Security Training: Architecture and Evaluation*. – *arXiv:2401.12594*. <https://arxiv.org/abs/2401.12594>
11. OECD Digital Economy Papers. (2022). *Cybersecurity Policies for Students and Teachers*. <https://www.oecd.org>

INNOVATIVE
ACADEMY