

**RAQAMLI TA'LIM MUHITLARIDA KIBERXAVFSIZLIK MASALALARI****Urimbetova Gʻulshad Abdirazakovna**

Nukus shahri 1-sonli politexnikumi maxsus fani o'qituvchisi

Annotatsiya: Mazkur maqolada raqamli ta'lim muhitlarining jadal rivojlanish i sharoitida yuzaga kelayotgan kiberxavfsizlik muammolari chuqur o'rganiladi. Bugungi kunda ta'lim jarayonida internet-resurslardan keng foydalanilayotganligi, masofaviy va onlayn o'qitish tizimlarining keng qo'llanilishi, elektron hujjatlar aylanmasi, raqamli baholash vositalari va bulutli texnologiyalarning joriy etilishi raqamli xavfsizlikni ta'minlashni dolzarb masalaga aylantirmoqda. Ayniqsa, oliy ta'lim muassasalarida talabalar va pedagoglarning shaxsiy ma'lumotlari, o'quv resurslari va elektron tizimlarning himoyalani sh darajasi past bo'lsa, bu butun ta'lim jarayoniga salbiy ta'sir ko'rsatishi mumkin. Maqolada kiberxavfsizlik tahdidlarining asosiy turlari–phishing, social engineering, zararli dasturlar, parol siyosatidagi zaifliklar, ma'lumotlar sızdirilishi, tarmoq hujumlari – ilmiy nuqtai nazardan tahlil qilinadi.

Kalit so'zlar: kiberxavfsizlik, raqamli ta'lim muhitlari, axborot xavfsizligi, uzluksiz ta'lim, onlayn ta'lim platformalari, kibergigiyena, parol siyosati, phishing va social engineering, TryHackMe, HackTheBox, akademik halollik, raqamli texnologiyalar, kiberxavfsizlik madaniyati.

Annotation: This article explores in depth the cybersecurity issues arising in the context of the rapid development of digital learning environments. Today, the extensive use of internet resources in the educational process, the widespread implementation of remote and online learning systems, electronic document circulation, digital assessment tools, and the integration of cloud technologies have made ensuring digital security a pressing issue. In particular, if the level of protection for the personal data of students and educators, educational resources, and electronic systems in higher education institutions is low, it can negatively affect the entire educational process. The article provides a scientific analysis of major cybersecurity threats such as phishing, social engineering, malware, password policy vulnerabilities, data breaches, and network attacks.

Keywords: cybersecurity, digital learning environments, information security, lifelong learning, online learning platforms, cyber hygiene, password policy, phishing and social engineering, TryHackMe, HackTheBox, academic integrity, digital technologies, cybersecurity culture.

Kirish

Raqamli transformatsiya jarayoni ta'lim sohasida tub o'zgarishlarga sabab bo'ldi. An'anaviy o'qitish usullaridan raqamli platformalar, onlayn darslar, elektron darsliklar, www.innovativepublication.uz



bulutli texnologiyalar va sun'iy intellektga asoslangan vositalarga o'tilmoqda. Bunday o'zgarishlar bilan birga ta'lim muhitida kiberxavfsizlikni ta'minlash zarurati ham ortib bormoqda[1]. O'quvchilarning shaxsiy ma'lumotlari, o'quv resurslarining muhofazasi, akademik halollik va o'quv jarayonining texnik xavfsizligi bugungi kunda eng dolzarb muammolardan biri hisoblanadi [2][4].

Bugungi ta'lim muassasalari – ayniqsa, oliy ta'lim tizimi–o'z infratuzilmasida keng ko'lamli internet resurslar, elektron axborot bazalari, raqamli kutubxonalar va masofaviy o'qitish tizimlaridan foydalanadi. Shu bilan birga, turli tahdidlar, xususan, phishing hujumlari, kiberfiribgarlik, ma'lumotlar sızdirilishi, kompyuter viruslari va tarmoq hujumlari kabi xavflar ham bu tizimlarning ajralmas qismiga aylangan.

Asosiy masalalar va muammolar

1. **Shaxsiy ma'lumotlar xavfsizligi** – Talaba, o'qituvchi va xodimlar haqidagi ma'lumotlarning maxfiyligi va xavfsizligini ta'minlash[6][7].
2. **Elektron platformalarga ishonchlilik** – Masofaviy o'qitish tizimlarining doimiy ishlashini ta'minlash va ularga hujumlar xavfini kamaytirish[4][9].
3. **Kiber gigiyena madaniyati yetishmasligi** – Talaba va o'qituvchilarning raqamli savodxonlik va xavfsizlik bo'yicha bilimlari yetarli emasligi[6][8].
4. **Zararli dasturlar va viruslar** – O'quv resurslariga kirishda viruslar va zararli ilovalar orqali tizimga zarar yetkazish ehtimoli.
5. **Akademik halollikni buzuvchi vositalar** – Imtihon va topshiriqlarda sun'iy intellekt yoki boshqa vositalar yordamida taqlid qilish holatlari[10].

Raqamli ta'lim muhitlarida kiberxavfsizlikni ta'minlash uchun quyidagi chora-tadbirlar muhim ahamiyatga ega:

Parol siyosatini takomillashtirish: Har bir foydalanuvchi kuchli va noyob parollar bilan tizimga kirishini ta'minlash;

Antivirus va himoya tizimlarini yangilash: Raqamli qurilmalarda doimiy nazorat va himoya tizimlarini ishga solish[3][4];

Kiberxavfsizlik bo'yicha o'quv mashg'ulotlari: O'quvchi va o'qituvchilarga maxsus treninglar tashkil etish;

Simulyatsion mashqlar: HackTheBox, TryHackMe kabi platformalarda amaliy mashg'ulotlar orqali bilimlarni mustahkamlash;

Raqamli etikani o'rgatish: Onlayn xulq-atvor, axborotni tekshirish va akademik halollik qoidalarini tushuntirish[2][8][10].

Xulosa. Raqamli ta'lim muhitida kiberxavfsizlikni ta'minlash nafaqat texnik, balki ijtimoiy va pedagogik yondashuvlarni ham talab qiladi. Bu yo'nalishda keng qamrovli strategiyalar, uzluksiz o'quv dasturlari va muntazam monitoring asosida ish olib borish zarur. Ayniqsa, yosh avlodda raqamli xavfsizlik madaniyatini shakllantirish orqali, kelajakdagi kibertahdidlarning oldini olishga katta hissa qo'shiladi. Ta'lim muassasalari bu borada faqat



texnik vositalar bilan emas, balki axborot xavfsizligi bo'yicha zamonaviy metodikalar bilan ham qurollanishi lozim.

FOYDALANILGAN ADABIYOTLAR:

1. Касымов, А.К. *Kiberxavfsizlik asoslari*. 2022. Toshkent: Fan va texnologiya nashriyoti.
2. Tariq, A., & Niazi, M. *Cybersecurity in Digital Education: Risks, Prevention, and Policies*. Springer. 2021.
3. Kaspersky Security Bulletin. *Threat predictions for education systems*. [https://www.kaspersky.com], 2023.
4. Cisco Networking Academy. *Cybersecurity Essentials Course*. [https://www.netacad.com]
5. TryHackMe & HackTheBox – Kiberxavfsizlikni amaliy mashg'ulotlar orqali o'qitish uchun interaktiv platformalar.
6. Bobokalonov, M.M. *Axborot xavfsizligi va raqamli madaniyat*. 2023. Samarqand davlat universiteti nashriyoti.
7. ISO/IEC 27001 – *Information Security Management Systems (ISMS)* standarti, xalqaro axborot xavfsizligi normalari.
8. Qodirov, Z.X. *Oliy ta'limda raqamlashtirish va uning xavfsizlik talablari*. 2021. O'zbekiston Milliy universiteti ilmiy to'plami.
9. National Institute of Standards and Technology (NIST).2020. *Framework for Improving Critical Infrastructure Cybersecurity*.
10. UNESCO IITE 2021. *Cybersecurity and privacy for online and blended learning environments*. [https://iite.unesco.org]