RAQAMLI TA’LIM MUHITIDA KIBERXAVFSIZLIK MASALALARI: ASOSIY TAHDIDLAR VA ULARNI BARTARAF ETISH USULLARI

Muallif: ***Raximov Ravshonbek***
Osiyo xalqaro universiteti magistranti

Annotatsiya: Ushbu maqolada raqamli ta’lim tizimiga o‘tish davrida oliy ta’lim muassasalari, o‘qituvchilar va talabalar duch kelayotgan kiberxavfsizlik muammolari keng qamrovli tahlil qilinadi. Tadqiqot davomida ta’lim platformalaridagi (LMS) tizimli zaifliklar, zararli dasturlar ta’siri va foydalanuvchilarning kibergigiyena madaniyati o‘rganildi. Natijalar shuni ko‘rsatadiki, ta’lim muassasalarida ijtimoiy injeneriya, fishing va axborot sizib chiqishi kabi xavflar yuqori darajada saqlanib qolmoqda. Maqolada “Nol ishonch” (Zero Trust) arxitekturasini joriy etish va ma’muriy-tashkiliy choralarni ko‘rish orqali ushbu tahdidlarni kamaytirish bo‘yicha aniq amaliy tavsiyalar ishlab chiqilgan.

Kalit so‘zlar: Raqamli ta’lim, kiberxavfsizlik, masofaviy o‘qitish, fishing, kibergigiyena, ma’lumotlar maxfiyligi, zararli dasturlar (malware), Zero Trust.

Аннотация: В данной статье проводится всесторонний анализ проблем кибербезопасности, с которыми сталкиваются высшие учебные заведения, преподаватели и студенты в период перехода к цифровому образованию. В ходе исследования изучены системные уязвимости образовательных платформ (LMS), влияние вредоносного программного обеспечения, а также уровень кибергигиены пользователей. Результаты показывают, что такие угрозы, как социальная инженерия, фишинг и утечка данных, остаются на высоком уровне в образовательных учреждениях. В статье разработаны конкретные практические рекомендации по снижению данных рисков посредством внедрения архитектуры «Нулевого доверия» (Zero Trust), а также применения административных и организационных мер.

Ключевые слова: цифровое образование, кибербезопасность, дистанционное обучение, фишинг, кибергигиена, конфиденциальность данных, вредоносное ПО (malware), Zero Trust.

Abstract: This article provides a comprehensive analysis of cybersecurity challenges faced by higher education institutions, teachers, and students during the transition to digital education. The study examines system vulnerabilities in Learning Management Systems (LMS), the impact of malicious software, and the level of users’ cyber hygiene. The results indicate that threats such as social engineering, phishing, and data breaches remain highly prevalent in educational environments. The paper proposes specific practical recommendations to mitigate these risks through the

implementation of a Zero Trust architecture, along with administrative and organizational measures.

Keywords: digital education, cybersecurity, distance learning, phishing, cyber hygiene, data privacy, malware, Zero Trust.

1. Kirish

So‘nggi yillarda, xususan, global pandemiya sababli ta’lim tizimining raqamli platformalarga (LMS - Learning Management Systems, HEMIS, Zoom, Moodle va boshqalar) keskin o‘tishi ta’lim uzluksizligini saqlab qolish imkonini berdi. Biroq, bu o‘tish jarayoni axborot xavfsizligi borasida kutilmagan va jiddiy muammolarni yuzaga keltirdi [2]. An’anaviy ta’lim dan farqli o‘laroq, raqamli makon doimiy ravishda global tarmoqqa ulangan bo‘lib, har bir foydalanuvchi potentsial hujum nishoniga aylanadi.

Ta’lim muassasalari katta hajmdagi shaxsiy ma’lumotlar, jumladan, talabalarning pasport ma’lumotlari, professor-o‘qituvchilarning ilmiy ishlanmalari (intellektual mulk) hamda moliyaviy hisobotlar bazasiga ega. Aynan shu sababli oliygohlar kiberhujumchilar uchun jozibador moliyaviy va strategik nishonga aylandi [5]. Mamlakatimizda ta’limni raqamlashtirish jadal davom etayotgan bir paytda, iqtisodiy va axborot xavfsizligi masalalari davlat miqyosidagi dolzarb masalaga aylanmoqda [1]. Ushbu tadqiqotning asosiy maqsadi - O‘zbekiston va xalqaro tajriba misolida raqamli ta’lim muhitidagi eng xavfli kiber-tahdidlarni tahlil qilish va ta’lim ishtirokchilarining axborot xavfsizligini ta'minlash bo‘yicha kompleks mexanizmlarni taklif etishdir.

2. Metodologiya

Ushbu ilmiy-amaliy tadqiqotni amalga oshirishda miqdoriy va sifat tahlili (quantitative and qualitative analysis) usullaridan foydalanildi. Tadqiqot 2023-2024 o‘quv yili davomida amalga oshirildi:

- Adabiyotlar va qonunchilik tahlili: Raqamli ta’lim da xavfsizlik mavzusida chop etilgan ilmiy nashrlar hamda O‘zbekiston Respublikasining kiberxavfsizlikka oid me’yoriy-huquqiy hujjatlari o‘rganildi.
- So‘rovnoma usuli: Mahalliy oliy ta’lim muassasalarining 300 nafar ishtirokchisi (220 nafar talaba, 80 nafar professor-o‘qituvchi va xodimlar) o‘rtasida anonim onlayn so‘rovnoma o‘tkazildi. So‘rovnoma qatnashchilarning raqamli savodxonligi, parollarni boshqarish amaliyoti va xakerlik hujumlariga uchrash tajribasini baholashga qaratildi.
- Tizimli xavfsizlik auditi (System audit): Eng ko‘p ommalashgan masofaviy ta’lim platformalarining (Moodle bazasidagi tizimlar) autentifikatsiya, tarmoq protokollari (HTTP/HTTPS) va ma’lumotlar ni shifrlash darajasi yuzasidan dastlabki audit o‘tkazildi [3].

3. Natijalar

Tadqiqot, tahlil va so‘rovnoma natijalari ta’lim tizimining raqamli infratuzilmasida bir nechta zaif nuqtalar mavjudligini ko‘rsatdi. Asosiy tahdidlar asosan inson omili va texnik kamchiliklar atrofida shakllangan.

Quyidagi jadvalda tadqiqot davomida aniqlangan eng ko‘p uchraydigan kiberxavflar va ularning tarqalish darajasi keltirilgan:

1-jadval. Raqamli ta’lim muhitida aniqlangan asosiy kiber-tahdidlar tahlili

Tahdid turi	Uchrash darajasi (%)	Asosiy sababi / Zaiflik	Oqibati
Zaif parollar va takroriylik	68%	Foydalanuvchi kiber-savodxonligi pastligi	Shaxsiy kabinetga ruxsatsiz kirish
Fishing (Phishing)	45%	Elektron pochtadagi soxta havolalarga ishonish	Ma’lumotlar ni o‘g‘irlash
Zararli dasturlar (Malware)	32%	Litsenziyasiz ta’lim iy dasturlarni yuklab olish	Qurilmaning zararlanishi, shifrlanishi
Ochiq Wi-Fi tarmoqlari (MitM)	27%	VPN ishlatmasdan jamoat joylarida darsga ulanish	Tarmoq trafigini tutib olish

Batafsil tahlil natijalari:

1. Foydalanuvchilarning past kiber-xabardorligi: So‘rovnoma ishtirokchilarining aksariyati kiberxavfsizlik qoidalarini e'tiborsiz qoldirishi aniqlandi. Ayniqsa, o‘qituvchilarning shaxsiy kompyuterlarida talabalarning baholari va test savollari yetarlicha himoyalanmagan holda saqlanadi.

2. Ijtimoiy injeneriya va Fishing hujumlari: Kiberjinoyatchilar ko‘pincha “LMS tizimi parolini yangilash” yoki “Grant yutib oldingiz” degan mazmundagi soxta

xabarlarni yuborish orqali ta’lim muassasasi tarmog‘iga kirish huquqini (credentials) qo‘lga kiritmoqda [4].

3. Ikki bosqichli autentifikatsiya (2FA) muammosi: Tahlil qilingan tizimlarning qariyb 70 foizida zamonaviy xavfsizlik standarti hisoblangan 2FA tizimi to‘liq joriy etilmagan yoxud foydalanuvchilar ixtiyoriga tashlab qo‘yilgan [3]. Bu esa akkauntlarni buzishni osonlashtiradi.

4. Qurilmalar va litsenziyasiz dasturlar (Piracy): Talabalar va o‘qituvchilar tomonidan pullik darsliklar yoki o‘quv dasturlarining noqonuniy (“krak” qilingan) versiyalaridan foydalanishi ta’lim tizimi tarmog‘iga troyan va to‘lov talab qiluvchi dasturlar (Ransomware) tushishiga asosiy sabab bo‘lmoqda.

4. Muhokama

Olingan natijalar shuni ko‘rsatmoqdaki, ta’lim tizimidagi kiberxavfsizlik faqatgina IT bo‘limlarining texnik muammosi emas, balki inson omili bilan bevosita bog‘liq bo‘lgan kompleks jarayondir. O‘quv muassasalarida markazlashgan kuchli himoya tizimlari (Firewall, Antivirus) o‘rnatilgan bo‘lishiga qaramay, bitta ehtiyotsiz talaba yoki xodimning xatosi butun tizimni xavf ostiga qo‘yishi mumkin [4].

Xalqaro miqyosda (masalan, Educause hisobotlarida) oliy ta’lim tizimi “Nol ishonch” (Zero Trust) arxitekturasiga o‘tishi kerakligi ta'kidlanmoqda. Ya'ni, tarmoq ichidagi hech bir foydalanuvchiga yoki qurilmaga avtomatik tarzda ishonib bo‘lmaydi va har bir ulanish qat'iy tekshirilishi shart [7]. O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi Qonunida ham muhim axborot infratuzilmasi obyektlarining xavfsizligini ta'minlash qat'iy belgilab qo‘yilgan [6]. Shunga qaramay, ko‘plab mahalliy ta’lim muassasalarida moliyaviy cheklovlar va malakali kiberxavfsizlik mutaxassislarining yetishmasligi muammoni chuqurlashtirmoqda.

Muammolarni hal qilish bo‘yicha kompleks tavsiyalar:

- Ma’muriy-tashkiliy choralar: O‘quv yurtlarida ichki axborot xavfsizligi siyosatini (Information Security Policy) ishlab chiqish va qabul qilish. Unda ma’lumotlar ni saqlash, uzatish va zaxiralash (back-up) tartib-qoidalari aniq belgilanishi lozim.
- Ta’limiy yondashuv (Kibergigiyena): Barcha talabalar o‘quv dasturining birinchi kursiga axborot savodxonligi va kibergigiyena bo‘yicha majburiy qisqa muddatli kredit-modulni kiritish. Xodimlar uchun yiliga kamida bir marta fishing-simulyatsiya testlarini o‘tkazish.
- Texnik himoyani modernizatsiya qilish: - Ta’lim platformalariga (LMS, elektron jurnallar) kirishda Ikki bosqichli autentifikatsiyani (2FA/MFA) majburiy etib belgilash.
  - Universitet hududidagi ochiq Wi-Fi tarmoqlarini segmentatsiyalash va ta’lim ma’lumotlar bazasidan ajratish.

- **Maxfiylik va qonunchilik mosligi:** Milliy qonunchilik talablariga mos ravishda talaba va professor-o‘qituvchilarning shaxsiy ma’lumotlar ini uchinchi shaxslarga o‘tib ketishining oldini oluvchi yuridik mexanizmlarni joriy etish [6].

Xulosa

Raqamli ta’lim texnologiyalari zamonaviy ta’lim ning ajralmas ustuniga aylanib ulgurdi. Biroq, bu taraqqiyot kiber-tahdidlarning ham xuddi shunday tezlikda o‘sishiga olib kelmoqda. Tadqiqot shuni ko‘rsatadiki, ta’lim muassasalari shaxsiy va intellektual ma’lumotlar ni himoya qilish uchun mudofaa strategiyalarini qayta ko‘rib chiqishlari kerak. Faqatgina qimmatbaho xavfsizlik dasturlarini sotib olish bilan cheklanib qolmasdan, balki ta’lim ishtirokchilarining ongli kiber-madaniyatini shakllantirish orqaligina xavfsiz va ishonchli raqamli ta’lim muhitini yaratish mumkin [1, 5]. Kelgusidagi tadqiqotlar ta’lim tizimida Sun’iy intellekt (AI) yordamida kiberhujumlarni oldindan aniqlash texnologiyalarini joriy etish masalalariga bag‘ishlanishi maqsadga muvofiqdir.

Foydalanilgan adabiyotlar ro‘yxati

1. G‘ulomov, S. S., & Shermuhamedov, A. T. (2021). Raqamli ta’lim va iqtisodiyotda kiberxavfsizlik masalalari. Iqtisodiyot va ta’lim jurnali, 4(2), 15-22.

2. Al-Zoubi, A. M., & Alqatawna, J. (2022). Cyber Security Challenges in E-Learning Systems during the Digital Transition. International Journal of Advanced Computer Science and Applications (IJACSA), 13(4), 112-119.

3. Xolmatov, T. H., & Qodirov, M. R. (2022). Oliy ta’lim muassasalarida masofaviy o‘qitish platformalarining (LMS) axborot xavfsizligini ta’minlash. Axborot texnologiyalari va kommunikatsiyalari ilmiy-amaliy jurnali, 5(3), 45-51.

4. Bandara, I., Ioras, F., & Maher, K. (2020). Cyber Security Concerns in E-Learning Education: Phishing and Social Engineering. Journal of Information Security and Applications, 55, 102-110.

5. Kaspersky Lab. (2023). Ta’lim sohasidagi kiber-tahdidlar: Yillik tahliliy hisobot. Kiberxavfsizlik hisobotlari portali.

6. O‘zbekiston Respublikasining Qonuni. (2022). “Kiberxavfsizlik to‘g‘risida”gi O‘RQ-764-son qonuni. Qonunchilik ma'lumotlari milliy bazasi, 16.04.2022-y., 03/22/764/0306-son.

7. Educause. (2023). Higher Education Trend Watch: Information Security Strategy in Digital Learning. Educause Research Publications.