

PROCTORING.UZ: RAQAMLI TA'LIMDA KIBERXAVFSIZLIK VA AKADEMIK HALOLLIK TIZIMI

PROCTORING.UZ: CYBERSECURITY AND ACADEMIC INTEGRITY SYSTEM IN DIGITAL EDUCATION

Mo'minov Haydar Muhiddinovich

"Realsoft Academy" MChJ direktori (Ilmiy rahbar)

univorarsa@gmail.com

Ustenov Azizbek Jandar o'g'li

Toshkent amaliy fanlar universiteti, Axborot xavfsizligi yo'nalishi

ORCID: 0009-0008-3338-115X

azustenov@gmail.com

Zayniyev Ilhomjon Raxmatilla o'g'li

Toshkent amaliy fanlar universiteti, Axborot xavfsizligi yo'nalishi

ORCID: 0009-0000-1675-0429

ilhomjonzayniyev7@gmail.com

Annotatsiya: Ushbu maqolada Proctoring.uz platformasining texnik ishlash prinsiplari, uning O'zbekiston ta'im tizimidagi ahamiyati va kiberxavfsizlik mexanizmlari kompleks tarzda o'rganilgan. Masofaviy ta'limning kengayishi bilan birga yuzaga kelayotgan akademik halollik muammosi global ko'lamda jiddiy e'tibor talab etmoqda. Maqolada sun'iy intellekt (AI) va mashinali o'qitish (ML) asosidagi yuz tanish texnologiyalari, real vaqt rejimida monitoring, tarmoq nazorati va anomaliyalarni aniqlash usullari tahlil qilingan. Tizimning natijador jihatlari, xavfsiz imtihon muhitini shakllantirish mexanizmlari hamda ma'lu'motlar maxfiyligi, AI adolati va kiberxurujlardan himoya kabi axloqiy-huquqiy muammolar ko'rib chiqilgan. Tadqiqot natijalari shuni ko'rsatadiki, proktorlik tizimlari raqamli ta'limdagi ajralmas xavfsizlik standarti sifatida qaror topishi zarur bo'lib, texnologik innovatsiyalar bilan me'yoriy-huquqiy bazaning muvofiqlashtirilishi hal qiluvchi omil hisoblanadi.

Kalit so'zlar: proctoring, sun'iy intellekt, mashinali o'qitish, ma'lu'motlarni shifrlash, biometriya, raqamli nazorat, kiberxavfsizlik, axborot xavfsizligi, akademik halollik, Zero-Trust.

Abstract: This article provides a comprehensive examination of the technical operating principles of the Proctoring.uz platform, its significance within the Uzbekistan education system, and its cybersecurity mechanisms. The growing challenge of academic integrity in remote education demands serious attention at the global level. The study analyzes artificial intelligence (AI) and machine learning (ML)-based facial recognition technologies, real-time monitoring, network control, and anomaly detection methods. The productive aspects of the system and mechanisms for creating a secure examination environment are discussed, alongside ethical and legal issues including data confidentiality, AI fairness, and protection against cyberattacks. Research findings indicate that proctoring systems must be established as an indispensable security standard in digital education, with the alignment of technological innovation and regulatory frameworks serving as a decisive factor.

Keywords: proctoring, artificial intelligence, machine learning, data encryption, biometrics, digital monitoring, cybersecurity, information security, academic integrity, Zero-Trust.

1. Kirish

Bugungi kunda raqamli texnologiyalarning jamiyatning barcha jabhalariga jadal integratsiyalashuvi potentsial kiber tahdidlar manzarasini sezilarli darajada kengaytirdi. Ta'lim sohasida masofaviy imtihon topshirish jarayonida akademik halollikni saqlash eng katta muammolardan biriga aylanib bormoqda. Ko'chirib olish, begona shaxslar yordami va noqonuniy manbalardan foydalanish kabi tahdidlar tizimli xarakter kasb etgan bo'lib, an'anaviy nazorat usullari o'z samaradorligini yo'qotmoqda (Jumaev et al., 2023).

Proctoring.uz — bu nafaqat video kuzatuv vositasi, balki murakkab algoritmlar yig'indisidan tashkil topgan kiber-mudofaa tizimidir. Kiberxavfsizlik endilikda har bir raqamli tizimning ajralmas tarkibiy qismi bo'lib qolgani kabi, proktorlik tizimlari ham masofaviy ta'limning majburiy xavfsizlik standarti bo'lib bormoqda (Von Solms & Van Niekerk, 2013).

Ushbu maqolaning maqsadi Proctoring.uz platformasining texnik-metodologik asoslarini o'rganish, uning kiberxavfsizlik mexanizmlarini tahlil etish va raqamli ta'lim tizimida akademik halollikni ta'minlashdagi o'rnini yoritishdir.

2. Adabiyotlar sharhi va nazariy asos

Proktorlik tizimlari va raqamli ta'limda nazorat masalasi so'nggi yillarda keng muhokama qilinmoqda. Jumaev, Normuminov va Primbetov (2023) zamonaviy kiberxavfsizlik usullarini o'rganib, sun'iy intellekt asosidagi himoya tizimlarining samaradorligini tasdiqlagan. Jumaniyazova (2024) oliy ta'lim muassasalarida kiberxavfsizlik madaniyatini oshirish masalalarini ko'rib chiqib, xodimlar va talabalarning raqamli savodxonligini rivojlantirish zarurligini ta'kidlagan.

Von Solms va Van Niekerk (2013) axborot xavfsizligidan kiberxavfsizlikka o'tish jarayonini nazariy asoslagan. Mustaffaqulov, Eshturdiyeva va Abduraximova (2024) ta'lim jarayonida kiberxavfsizlikni ta'minlash mexanizmlarini tahlil qilib, proktorlik tizimlarini raqamli xavfsizlikning tarkibiy qismi sifatida ko'rib chiqqan.

Viola va Jones (2001) tomonidan ishlab chiqilgan yuz tanish algoritmlari zamonaviy proktorlik tizimlarining texnik asosini tashkil etadi. Ushbu adabiyotlar ko'rsatadiki, proktorlik va kiberxavfsizlik o'rtasidagi bog'lanadigan konseptual aloqa tobora mustahkamlanib bormoqda.

3. Tadqiqot metodologiyasi

Ushbu tadqiqotda sifatli tahliliy yondashuv qo'llangan bo'lib, quyidagi elementlar o'z ichiga olingan:

- Manba bazasi: Ilmiy jurnallar (IEEE, Computers & Security), sanoat hisobotlari, xalqaro tashkilotlar (BMT, WEF) nashrlari va O'zbekiston milliy platforma ma'lu'motlari.
- Davr chegarasi: 2001-yildan 2024-yilgacha, ayniqsa 2019-yildan keyingi — masofaviy ta'limning jadal rivojlangan davri — ustuvor hisoblanadi.
- Tahlil usullari: Texnologiyalarni qiyosiy tahlil qilish, amaliy tadqiqot (case study) metodologiyasi, tizimli umumlashtirish.
- Etik e'tirof: Maqolada hech qanday shaxsiy yoki maxfiy ma'lu'motlardan foydalanilmagan. Barcha manbalar tegishli ravishda ko'rsatilgan.

Tizim samaradorligini baholashda Proctoring.uz platformasining ochiq ma'lu'motlari va solishtirma ko'rsatkichlardan foydalanildi.

4. Natijalar va muhokama

4.1. Tizimning texnik metodologiyasi

Proctoring.uz bir necha bosqichli nazorat tizimiga ega bo'lib, ushbu metodlar to'rtta asosiy guruhga ajratiladi:

- Identifikatsiya (Face ID): Mashinali o'qitish modellari yordamida foydalanuvchi yuzini aniqlash va uni tizimdagi pasport ma'lumotlari bilan real vaqt rejimida solishtirish. Viola-Jones algoritmi asosida ishlaydi (Viola & Jones, 2001).
- Audio-vizual tahlil: Xonadagi ikkinchi shaxsning ovozi, shovqin darajasi va talabaning bosh harakatlarini real vaqt rejimida tahlil qilish. Anomal xatti-harakatlar avtomatik bayroqlanadi.
- Tarmoq va ekran nazorati (Safe Exam Browser): Talaba kompyuterida ruxsat etilmagan dasturlarni (masalan, Telegram, AnyDesk) bloklash va ekrandan nusxa olish imkoniyatini cheklash.
- Sun'iy intellekt asosidagi anomaliyalarni aniqlash: AI modellari imtihon davomida har bir talabaning xatti-harakatini o'rganib, normadan chetlanishlarni avtomatik aniqlaydi va tezkor choralar ko'radi (Jumaev et al., 2023).

1-jadval. Proctoring.uz tizimi samaradorligi ko'rsatkichlari

Ko'rsatkich	Izoh
Hujjatlarni tekshirish tezligi	Face ID orqali soniyalar ichida real vaqt rejimida amalga oshiriladi
Bir vaqtdagi qamrov hajmi	10 000 dan ortiq foydalanuvchini bir vaqtda nazorat qilish imkoniyati
Xarajatlar optimallasuvi	Qog'oz, transport va an'anaviy proktorlar xarajatlarini 70% gacha kamaytirish
Inson omili xatoligi	AI nazorati tufayli sub'yektiv xatoliklarni minimal darajaga tushirish
Natijalarga ishonch darajasi	Raqamli audit yozuvlari va blokcheyn integratsiyasi bilan ta'minlanadi

4.2. Kiberxavfsizlik va axloqiy muammolar

Proctoring tizimi rivojlanishi bilan birga axloqiy, huquqiy va maxfiylik muammolari ham paydo bo'lmoqda. Uch asosiy muammo belgilangan:

- Ma'lumotlar himoyasi: Talabalar yuz tasvirlari va shaxsiy ma'lumotlari kiberxurujlar nishoniga aylanishi mumkin. Shifrlangan saqlash (AES-256) va ma'lumotlarni minimallashtirish prinsipi joriy etilishi shart (Jabborov & Jabborova, 2024).
- AI adolati va tarafdashlik xavfi: Sun'iy intellekt modellari yetarli nur bo'lmagan xonada yoki boshqa shaxsiy xususiyatlarga ko'ra talabani noto'g'ri "shubhali" deb belgilashi mumkin. Bu muammo treningdagi ma'lumotlar xilma-xilligini oshirish orqali qisman hal qilinadi.
- Tashqi kiberhujumlardan himoya: Proktorlik platformasining o'ziga yo'naltirilgan DDoS hujumlari yoki ma'lumotlar o'g'irlash urinishlariga qarshi Zero-Trust arxitekturasini, ko'p faktorli autentifikatsiya (MFA) va real vaqt monitoring qo'llash zarur (Von Solms & Van Niekerk, 2013).

2-jadval. Proktorlik texnologiyalari taqqoslash tahlili

Texnologiya	Samaradorlik	Kuchli tomonlari	Cheklovlari
Face ID (Yuz tanish)	Yuqori	Tezkor, avtomatik identifikatsiya	Yoritish muammolari, AI tarafkashligi
Audio tahlil (ML)	O'rtacha-yuqori	Uchinchi shaxs ovozi aniqlash	Shovqinli muhitda xatolik darajasi oshadi
Safe Exam Browser	Yuqori	Ruxsatsiz dasturlarni bloklash	Texnik moslik muammolari
Anomaliya aniqlash (AI)	Juda yuqori	Real vaqt avtomatik monitoring	Katta hisoblash resurslari talab qiladi
Zero-Trust arxitekturas	Juda yuqori	Ichki va tashqi tahdidlardan himoya	Murakkab va qimmat joriy etish

4.3. Kelajak istiqbollari va innovatsiyalar

Proktorlik tizimlarini yanada takomillashtirish uchun quyidagi texnologik yo'nalishlar dolzarb hisoblanadi:

- Blokcheyn integratsiyasi: Imtihon natijalari, video-qaydlar va audit ma'lumotlarini o'zgartirib bo'lmaydigan blokcheyn bazasida saqlash — bu natijalarga ishonch darajasini oshiradi va manipulyatsiyani bartaraf etadi.
- Chuqur o'qitish algoritmlari: Deepfake va boshqa ilg'or aldov urinishlarini aniqlash uchun neyron tarmoqlar asosida ishlovchi tizimlarni joriy etish (Jumaev et al., 2023).
- Xalqaro standartlashtirilish: Global kiberxavfsizlik standartlariga muvofiq proktorlik platformalarini sertifikatlash va xalqaro tan olingan sertifikatlarni joriy etish.
- Kvantga chidamli shifrlash: Kelajakdagi kvant kompyuterlari hozirgi shifrlash algoritmlarini buzishi mumkinligi inobatga olinib, post-kvant kriptografik yechimlarni tadqiq qilish zarur.

5. Cheklovlar

Ushbu tadqiqotning bir qator cheklovlari mavjud. Birinchidan, tadqiqot asosan ochiq manbalar va umumiy ma'lumotlar asosida amalga oshirilgan bo'lib, Proctoring.uz platformasining ichki texnik me'morchiligi haqidagi batafsil ma'lumotlarga kirish imkoniyati cheklangan. Ikkinchidan, platformaning samaradorlik ko'rsatkichlari vaqt o'tishi bilan o'zgarishi mumkin va tadqiqot ma'lumotlari ma'lum bir davrni qamrab oladi. Uchinchidan, turli ta'lim muassasalari va mintaqalardagi real foydalanuvchi tajribasi to'g'risida keng qamrovli empirik so'rovnoma o'tkazilmagan. Kelajakdagi tadqiqotlarda talaba va o'qituvchilardan to'plangan birlamchi ma'lumotlar asosida tizimning ta'sirchanligini yanada chuqurroq baholash tavsiya etiladi.

6. Xulosa va takliflar

Proctoring.uz — O‘zbekiston ta’im tizimini raqamlashtirish yo‘lidagi strategik loyiha bo‘lib, u nafaqat imtihon o‘tkazish vositasi, balki yosh avlod bilimini adolatli baholash kafolati hamdir. Tadqiqot shuni ko‘rsatadiki, sun‘iy intellekt va mashinali o‘qitish texnologiyalari proktorlik samaradorligini sezilarli darajada oshirgan va an‘anaviy nazorat usullarining o‘rmini bosmoqda.

Quyidagi takliflar ishlab chiqildi:

- Proctoring.uz platformasida ma’lu’otlarni himoya qilish standartlarini (GDPR, ISO/IEC 27001) to‘liq joriy etish va foydalanuvchilar maxfiylikni kafolatlash.
- Sun‘iy intellekt modellarini xilma-xil demografik ma’lu’otlar bilan o‘qitish orqali AI tarafkashligini minimallashtirish va adolatli baholashni ta’minlash.
- Talaba va o‘qituvchilar uchun proktorlik tizimlari bilan ishlash bo‘yicha xabardorlik va o‘qitish tadbirlarini muntazam o‘tkazib borish.
- Zero-Trust arxitekturasini to‘liq joriy etish va platformaning o‘ziga qaratilgan kiberhujumlarga qarshi doimiy monitoring tizimini o‘rnatish.
- Blokcheyn texnologiyasini natijalarga ishonchlilikni oshirish uchun bosqichma-bosqich joriy etish va xalqaro hamkorlikni rivojlantirish.

Kiberxavfsizlik 21-asrda raqamli dunyoning barqarorligini ta’minlovchi asosiy vosita sifatida o‘z o‘rmini mustahkamlagan bo‘lib, proktorlik tizimlari ham ushbu global xavfsizlik ekotizimining ajralmas qismiga aylanib bormoqda.

Adabiyotlar ro‘yxati

- [1] Jabborov, Z. B., & Jabborova, N. B. (2024). O‘zbekistonda axborot xavfsizligi va kiberxurujlarning oldini olishga doir davlat siyosati. *Ilm-fan va innovatsiya*, 2(30), 120–122.
- [2] Jumaev, G., Normuminov, A., & Primbetov, A. (2023). Safeguarding the digital frontier: Exploring modern cybersecurity methods. *Journal of Multidisciplinary Bulletin*, 6(4). <https://doi.org/10.xxxxx/jomb.156>
- [3] Jumaniyazova, T. A. (2024). Oliy ta’im muassasalarida kiberxavfsizlik madaniyatini oshirish: o‘qituvchilar, xodimlar va talabalarning kiberxavfsizlik sohasidagi kompetensiyalarini rivojlantirish. *Journal of Academic Research and Trends in Educational Sciences*.
- [4] Mamatqulov, M. M. (2024). Kiber xavfsizlik muammolari va yechimlari. *Ilmiy Xabarlar*, 2(8).
- [5] Mustaffaqulov, M. A., Eshturdiyeva, Z. S., & Abduraximova, R. B. (2024). Ta’im jarayonida kiberxavfsizlikni ta’minlash. *Journal of Academic Research and Trends in Educational Sciences*.
- [6] Normo‘minov, A. A., Kendjaeva, D. X., & Primbetov, A. M. (2024). Kiberxavfsizlikning ta’im jarayonidagi roli. *Yevroosiyo akademik tadqiqotlar jurnali*, 4(12).
- [7] Sotvoldiyev, A. A., Isaxonov, X. M., & Siddiqov, M. Y. (2023). Kiberxavfsizlikni ta’minlashda axborot aktiv qiymatining o‘rni. *Yangi O‘zbekiston taraqqiyotida tadqiqotlarni o‘rni va rivojlanish omillari*, 2(2).
- [8] To‘xtasinov, A. R. (2023). O‘zbekiston kiberxavfsizlik taraqqiyoti. *PEDAGOGS jurnali*, 43(1), 180–185.
- [9] Viola, P., & Jones, M. (2001). Rapid object detection using a boosted cascade of simple features. *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 1. <https://doi.org/10.1109/CVPR.2001.990517>

- 
- [10] Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97–102. <https://doi.org/10.1016/j.cose.2013.04.004>
- [11] Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press.
- [12] Libicki, M. C. (2009). *Cyberdeterrence and Cyberwar*. RAND Corporation.
- [13] Muxammadjonov, X. Z. (2024). Madaniyatshunoslik yondashuvi asosida o'smirlarda kiberxavfsizlik tushunchalarini rivojlantirish mexanizmlari. *Universal xalqaro ilmiy jurnal*, 1(5).
- [14] International Telecommunication Union (ITU). (2023). *Global Cybersecurity Index 2023*. ITU Publications.
- [15] World Economic Forum (WEF). (2024). *Global Risks Report 2024*. WEF Publications. <https://www.weforum.org>