

RAQAMLI PEDAGOGIKADA MA'LUMOTLAR XAVFSIZLIGI MASALALARI

Fayzullayeva Dilnura Husan qizi

Shahrisabz davlat pedagogika instituti, Pedagogika yo'nalishi 2-bosqich talabasi

<https://doi.org/10.5281/zenodo.17786629>

Annotatsiya: Ushbu maqolada raqamli pedagogika jarayonida ma'lumotlar xavfsizligi masalalari yoritilgan. Raqamli ta'lim tizimlarining kengayishi bilan bog'liq kiberxavflar, xususan phishing, ransomware, ichki tahdidlar va shaxsiy ma'lumotlarning o'g'irlanishi kabi muammolar tahlil qilingan. Tadqiqotda xalqaro va mahalliy manbalar asosida ta'lim muassasalarida kiberxavfsizlik infratuzilmasining hozirgi holati, muammolari va ularni bartaraf etish yo'llari ko'rib chiqilgan. Shuningdek, O'zbekistonda kiberxavfsizlik bo'yicha mutaxassislarni tayyorlashga qaratilgan yangi tashabbuslarning ahamiyati ta'kidlangan.

Kalit so'zlar: Raqamli pedagogika, ma'lumotlar xavfsizligi, kiberxavfsizlik, ta'lim tizimi, phishing, ransomware, autentifikatsiya, ma'lumotlarni himoya qilish, raqamli ta'lim, kiber tahdidlar.

АННОТАЦИЯ

В данной статье рассматриваются вопросы безопасности данных в процессе цифровой педагогики. Проанализированы такие проблемы, как киберугрозы, связанные с расширением цифровых образовательных систем, в частности, фишинг, вымогательство, внутренние угрозы и кража персональных данных. В исследовании на основе международных и местных источников рассмотрены современное состояние инфраструктуры кибербезопасности в образовательных учреждениях, проблемы и пути их устранения. Также была отмечена важность новых инициатив, направленных на подготовку специалистов по кибербезопасности в Узбекистане.

Ключевые слова: Цифровая педагогика, безопасность данных, кибербезопасность, система образования, фишинг, ransomware, аутентификация, защита данных, цифровое образование, киберугрозы.

ANNOTATION

This article covers data security issues in the process of digital pedagogy. Problems related to the expansion of digital education systems, such as phishing, ransomware, internal threats, and the theft of personal data, were analyzed. The study examines the current state of cybersecurity infrastructure in educational institutions, problems, and ways to eliminate them based on international and domestic sources. The importance of new initiatives aimed at training cybersecurity specialists in Uzbekistan was also emphasized.

Keywords: Digital pedagogy, data security, cybersecurity, education system, phishing, ransomware, authentication, data protection, digital education, cyber threats.

KIRISH. Raqamli pedagogika yigirmanchi asrning boshlarida pochta orqali yuborilgan sirtqi kurslar shaklini olgan masofaviy o'qitishdan kelib chiqqan. 1858-yilda London universiteti tashqi dastur deb nomlanuvchi birinchi masofaviy o'qitish darajasini taklif qildi. Charlz Dikens muassasani "xalqlar universiteti" deb atagan, chunki u oliy ma'lumotga kengroq kirish imkonini bergan. Telekurslar 1970-yillarning boshlarida jamoat kollejlarning tarqalishi bilan qayta tiklandi. Ushbu masofaviy kurslar yigirmanchi asrning oxiridan boshlab Internetni ommalashtirish davrida keng tarqalgan onlayn ta'limga yo'l ochdi 1980-1990 yillarda kompyuterlar va gumanitar Fanlar assotsiatsiyasi raqamli gumanitar markazlar keng tarqalgani kabi, kompyuterlar va gumanitar fanlarni o'qitish bo'yicha seminarlar va

konferentsiyalar taklif qildi. 1965-yilda gumanitar Fanlar uchun Milliy jamg'arma (NEH) yaratildi. Bu tashkilot o'z vaqtidan ancha oldinda edi. Hatto raqamli gumanitar Fanlar ofisini ham ishga tushirdi. Endi har yili har yili boshqa mamlakatda bo'lib o'tadigan raqamli Pedagogika bo'yicha xalqaro konferentsiya mavjud. Vaterloo universiteti, Guelph universiteti, Brok universiteti, Ryerson universiteti va Toronto universiteti yaqinda qo'shma konferentsiya ishlab chiqish uchun birlashdilar.[1]

MAVZUGA OID ADABIYOTLAR TAHLILI. Adabiyotlarni tahlil qilish shuni ko'rsatadiki, raqamli pedagogika bo'yicha xalqaro tadqiqotlar asosan ta'limda raqamli texnologiyalarni qo'llash imkoniyatlari, onlayn ta'lim samaradorligi va raqamli savodxonlikka qaratilgan. Bret Hirsch va boshqa tadqiqotchilar raqamli pedagogikaning nazariy asoslari hamda uning gumanitar fanlarga ta'sirini o'rganadi. Cyber Security Breaches Survey (2024) esa ta'lim muassasalarida kiberhujumlarning oshib borayotganini, autentifikatsiya va parol siyosati yetarli emasligini ko'rsatadi. BD Emerson va boshqa xalqaro manbalar ta'lim sektorida ma'lumotlar buzilishi natijasida yuzaga keladigan moliyaviy yo'qotishlar va asosiy tahdidlar haqida aniq statistik ma'lumot beradi. Mahalliy adabiyotlarda Rustamov A. raqamli ta'limda kiberxavfsizlik madaniyati yetarlicha shakllanmaganini ta'kidlaydi. Tuxtayev O. esa O'zbekistonda kiberxavfsizlik infratuzilmasi zaifligi, ma'lumotlarni himoya qilish texnologiyalariga kam sarmoya ajratilishini ilmiy asosda tahlil qilgan. Ushbu adabiyotlar umumiy holda raqamli ta'limni modernizatsiya qilish uchun ma'lumotlar xavfsizligi strategiyalarini takomillashtirish zarurligini ko'rsatadi.

TADQIQOT METODOLOGIYASI. Nazariy, taqqoslash, statistik.

TAHLIL VA NATIJALAR. Raqamli pedagogika-bu o'qitish va o'qitishda zamonaviy raqamli texnologiyalarni o'rganish va ulardan foydalanish. Raqamli pedagogika onlayn, gibrid va yuzma-yuz ta'lim muhitida qo'llanilishi mumkin. Raqamli pedagogika konstruktivizm nazariyasida ham ildiz otgan. Raqamli pedagogika so'nggi yillarda ta'lim jarayonlarini modernizatsiya qilishda muhim rol o'ynamoqda. Onlayn platformalar, elektron darsliklar, virtual sinflar va turli o'quv dasturlari pedagogik jarayonlarni soddalashtiradi, lekin bu jarayonlarda ma'lumotlar xavfsizligi masalasi dolzarb bo'lib qolmoqda. Ta'lim muassasalari o'quvchilarning shaxsiy ma'lumotlari, baholar, test natijalari va boshqa elektron hujjatlarni himoya qilishga majburdir.

Raqamli ta'limda eng katta xavf shaxsiy ma'lumotlarning o'g'irlanishi va suiiste'mol qilinishidir. Onlayn platformalarga foydalanuvchi nomi va parol bilan kirish orqali, ruxsatsiz shaxslar o'quvchilarning shaxsiy ma'lumotlarini olishlari mumkin. Shuningdek, kiberhujumlar, masalan, phishing, malware va ransomware hujumlari orqali tizimga zarar yetkazilishi yoki ma'lumotlarning shifrlanishi ta'lim jarayonini to'xtatishi mumkin. Ma'lumotlarning noto'g'ri saqlanishi ham xavfni oshiradi; bulutli serverlarda shifrlash va autentifikatsiya tizimlarining yetarli emasligi ma'lumotlar xavfsizligiga tahdid soladi. Tashqi qurilmalar va internet resurslari orqali zararli dasturlar tizimga kirishi ham muammolardan biridir.[2]

Ma'lumotlar xavfsizligini ta'minlash uchun bir nechta asosiy choralar mavjud. Birinchidan, ma'lumotlarni shifrlash va foydalanuvchilarni ikki faktorli autentifikatsiya orqali himoya qilish muhimdir. Ikkinchidan, ma'lumotlarga kirish huquqlarini cheklash lozim, ya'ni faqat tegishli shaxslar ularga ega bo'lishi kerak. Uchinchidan, pedagoglar va o'quvchilarni kiberxavfsizlik bo'yicha o'qitish zarur, bu parolni himoya qilish, phishing hujumlaridan ehtiyot bo'lish va xavfsiz qurilmalardan foydalanishni o'z ichiga oladi. To'rtinchidan, muhim

ma'lumotlarning muntazam zaxira nusxasini yaratish va favqulodda vaziyatlarda tiklash mexanizmini yo'lga qo'yish lozim. Shuningdek, ta'lim muassasalarida ma'lumotlar xavfsizligi siyosati ishlab chiqilishi va unga rioya qilinishi kerak.

Raqamli ta'lim muassasalari kiberhujumlarning asosiy nishoniga aylanib borayapti. Masalan, 2025-yil ikkinchi choragida ta'lim sohasidagi tashkilotlar haftasiga o'rtacha 4 388 ta kiberhujumga uchragan, bu o'tgan yilga nisbatan 31% ga oshgan. Ushbu hujumlarning asosiy turi - phishing va ransomware'dir, ko'pincha ikki faktorli autentifikatsiya (MFA) va tizimdagi yangilanishlar bo'lmaganligi sababli hujumchilarga kirish imkonini beradi. [3] Ta'limda ma'lumotlar buzilishi juda yuqori moliyaviy yo'qotishlar keltirib chiqaradi. "BD Emerson" saytidagi ma'lumotlarga ko'ra, 2023-yilda ta'lim sektorida ma'lumot buzilishi o'rtacha 3,65 million dollar turadi. Shuningdek, kichik ta'lim muassasalari (K-12) o'tgan yillarda ransomware uchun talab qilingan pulning 115% ni to'lashi qayd etilgan. [4]

Bundan tashqari, Buyuk Britaniyada olib borilgan "Cyber Security Breaches Survey-2024" natijalariga ko'ra, maktablarning faqatgina 39% ikki faktorli autentifikatsiyadan (2FA) foydalanadi. Shu o'rinda, maktablarning 84% i fayllarni bulutda zaxiralab saqlaydi, lekin 2FA yoki kuchli parol siyosatiga rioya qilmaydigan muassasalar ham bor. [5] Raqamli ta'lim muhitida pedagoglar va talabalar ma'lumotlar xavfsizligiga nisbatan beparvolik qilishi ham katta muammo. Masalan, O'zbekiston ta'limida kiberxavfsizlik madaniyatini shakllantirish zarurligi yuzaga kelmoqda - Rustamov Alisher (Axborot texnologiyalari va menejment universiteti) bildirganicha, axborot xavfsizligi, shaxsiy ma'lumotlarni himoya qilish, raqamli etikaga oid bilimlar pedagogik strategiyalarda etarlicha integratsiyalashtirilmagan. [6] Ilmiy tadqiqotlar ham ichki tahdidlarni ko'rsatadi: masalan, "Understanding Cyber Threats Against the Universities, Colleges, and Schools" nomli maqolada 58 ta hujum tahlil qilingan — asosan ransomware tashqi hujumlar va talabalar ichki tahdid sifatida qayd etilgan. Shu bilan birga, ba'zi o'qituvchilar o'zlari tasdiqlanmagan texnologiyalar va ilovalardan foydalanadi, bu esa maxfiylik va ma'lumotlar xavfsizligiga katta xavf tug'diradi. [7]

O'zbekistonda ham raqamli ta'lim tizimlari kengayib borayapti, lekin kiberxavfsizlik infratuzilmasi va mutaxassislar tayyorlashda kamchiliklar mavjudligi ta'kidlanmoqda. Tuxtayev Ozodbekning tahliliga ko'ra, mamlakatda kiber tahdidlardan xabardorlik darajasi past va ma'lumotlarni himoya qilish texnologiyalariga yetarlicha sarmoya ajratilmaydi. [8] Shuning oqibatida ta'lim muassasalari, xususan maktablar va oliy ta'lim muassasalari, kiberhujumlarga nisbatan zaif bo'lib qolmoqda. Bu nafaqat shaxsiy ma'lumotlar — o'quvchilarning baholari, test natijalari va ro'yxatlari, balki o'quv materiallari va ilmiy ishlar xavfsizligini ham tahdid ostiga qo'yadi. Masalan, milliy ".uz" domenidagi veb-saytlarda 2024-yilning birinchi yarmida aniqlangan 63 ta axborot xavfsizligi hodisasi shuni ko'rsatadiki, tizimlar kiberxavflarga nisbatan yetarlicha himoyalanmagan. Shu jumladan, davlat tashkilotlarining saytlarida aniqlangan 22 ta hodisa ta'lim muassasalari uchun ham o'xshash xavflarning mavjudligini bildiradi.

Bunday sharoitda pedagoglar va talabalar o'zlarining raqamli faoliyatida xavfsizlik qoidalariga amal qilmasliklari ham qo'shimcha tahdidni yuzaga keltiradi. Kiberxavfsizlik bo'yicha yetarli malakaga ega bo'lmagan xodimlar va o'quvchilar shaxsiy ma'lumotlarni himoya qilish choralarini yetarlicha tushunmaydi, bu esa sistemaning butun xavfsizlik tizimini zaiflashtiradi. Shu sababli mamlakatda kiberxavfsizlik bo'yicha mutaxassislarni tayyorlash va axborot xavfsizligi madaniyatini shakllantirish bo'yicha chora-tadbirlar zarur. [9]

Mazkur ehtiyojni qondirish maqsadida, 2025/2026-yilda O'zbekiston Ichki ishlar vazirligi akademiyasida "Raqamli texnologiyalar sohasida jinoyatlarga qarshi kurashish (Kiberxavfsizlik)" yo'nalishi ochildi. Bu yo'nalish orqali ta'lim muassasalari uchun malakali kiberxavfsizlik mutaxassislarini yetishtirish va zamonaviy texnologiyalarni xavfsiz joriy etish imkoniyati yaratiladi. Shu bilan birga, kuchli autentifikatsiya tizimlari, zaxira mexanizmlari va muntazam xodim hamda talabalarni o'qitish orqali ma'lumotlar xavfsizligini ta'minlash mumkin.

Natijada, O'zbekistonda raqamli pedagogikani rivojlantirish bilan birga kiberxavfsizlik infratuzilmasini mustahkamlash, xodim va o'quvchilarni kiberxavfsizlik bo'yicha bilimli qilish ham muhim vazifa sifatida qaraladi. Bu esa nafaqat ta'lim jarayonining uzluksizligini ta'minlaydi, balki o'quvchilarning shaxsiy ma'lumotlari va ta'lim resurslarini himoya qilishni kafolatlaydi.[10]

XULOSA. Raqamli pedagogikaning tez rivojlanishi ta'lim jarayonini yengillashtirsa-da, ma'lumotlar xavfsizligini ta'minlash masalasini yanada dolzarb qiladi. Tadqiqot natijalariga ko'ra, ta'lim muassasalari uchun eng katta tahdidlar — phishing, ransomware, autentifikatsiya yetishmasligi, zaif infratuzilma va foydalanuvchilarning kiberxavfsizlik madaniyatining pastligi hisoblanadi. O'zbekistonda sohada olib borilayotgan islohotlar, jumladan kiberxavfsizlik yo'nalishlarining ochilishi, raqamli ta'limni xavfsiz rivojlantirish uchun muhim qadamdir.

Ma'lumotlar xavfsizligini ta'minlash uchun ta'lim muassasalarida kuchli autentifikatsiya, muntazam zaxiralash, xavfsizlik protokollariga rioya qilish, xodim va o'quvchilarni o'qitish kabi kompleks choralarni joriy etish zarur. Bu esa raqamli ta'limning barqarorligi, o'quvchilarning shaxsiy ma'lumotlari va ta'lim resurslarini himoya qilishni kafolatlaydi.

Adabiyotlar, References, Литературы:

1. Digital pedagogy - Wikipedia
2. Hirsch, Brett D. Hirsh, Brett D. "Raqamli gumanitar Pedagogika: amaliyot, tamoyillar va siyosat". 2012.
3. Data Breaches in Education 2025: Trends, Costs & Defense
4. Cybersecurity in Education Sector: Threats, Stats & Best Practices | BD Emerson
5. Cyber security breaches survey 2024: education institutions annex - GOV.UK
6. Rustamov A. "Raqamli ta'limda kiberxavfsizlik madaniyatini shakllantirishning pedagogik strategiyalari". Raqamli ta'limda kiberxavfsizlik madaniyatini shakllantirishning pedagogik strategiyalari | international journal of science
7. [2307.07755] Understanding Cyber Threats Against the Universities, Colleges, and Schools
8. Tuxtayev O. "Raqamli iqtisodiyotda ma'lumotlar xavfsizligini ta'minlashga ta'sir qiluvchi omillar tahlili". Raqamli iqtisodiyotda ma'lumotlar xavfsizligini ta'minlashga ta'sir qiluvchi omillar tahlili | ilm fan xabarnomasi
9. <https://csec.uz/?utm>
10. <https://bviib.uz/oz/news/zbekiston-respublikasi>