



TA'LIM JARAYONIDA KIBERXAVFSIZLIK MADANIYATINI SHAKLLANTIRISH METODLARI

Subanova Go'zal O'ktamovna

Jizzax viloyati Paxtakor tumanidagi

1-sonli politexnikum

Informatika va axborot texnologiyalari fan o'qituvchisi

Annotatsiya: Ushbu maqolada ta'lim jarayonida kiberxavfsizlik madaniyatini shakllantirishning zamonaviy yondashuvlari, metodlari va pedagogik asoslari keng yoritiladi. Raqamli transformatsiya sharoitida o'quvchi va talabalarning internetdan xavfsiz foydalanish ko'nikmalarini rivojlantirish, shaxsiy ma'lumotlarni himoya qilish, kiberxavflarni tanish va ularga to'g'ri munosabat bildirish kabi kompetensiyalarni shakllantirish ta'lim tizimi oldidagi eng dolzarb vazifalardan biri ekanligi asoslab beriladi. Maqolada kiberxavfsizlik madaniyatining tarkibiy qismlari, yosh xususiyatlariga mos pedagogik metodlar, gamifikatsiya, amaliy treninglar, simulyatsiyalar, interaktiv mashg'ulotlar hamda sun'iy intellekt asosida yaratilgan o'quv vositalaridan foydalanishning afzalliklari tahlil qilinadi. Shuningdek, informatika fanini o'qitishda kiber gigiyena qoidalarini o'rgatish, raqamli xavflarni oldini olish bo'yicha profilaktik ishlari, kiberhujumlarga qarshi ongli immunitetni shakllantirish strategiyalari batafsil ko'rib chiqiladi. Tadqiqot natijalari ta'lim muassasalarida kiberxavfsizlik madaniyatini tizimli va bosqichma-bosqich rivojlantirish uchun samarali metodik tavsiyalarni taklif etadi.

Kalit so'zlar: kiberxavfsizlik madaniyati, kiber gigiyena, raqamli xavflar, ta'lim jarayoni, informatika ta'limi.

Kirish

Hozirgi globallashuv va raqamli transformatsiya jarayonlari inson faoliyatining barcha sohalariga, xususan ta'lim tizimiga chuqur kirib bormoqda. Internet tarmoqlarining keng qo'llanilishi, axborot texnologiyalarining jadal rivoji, elektron platformalar va masofaviy o'qitishning keng tarqalishi ta'lim jarayonida yangi imkoniyatlar bilan birga turli darajadagi kiberxavflarni ham yuzaga keltirmoqda. Bugungi kunda raqamli axborot muhitida duch kelinadigan phishing, zararli dasturlar, shaxsiy ma'lumotlarni o'g'irlash, virtual firibgarlik, ijtimoiy muhandislik kabi tahdidlar o'quvchi va talabalarning raqamli xavfsizligi uchun jiddiy xatar hisoblanadi. Shu bois ta'lim tizimida kiberxavfsizlik madaniyatini shakllantirish dolzarb pedagogik vazifalardan biriga aylanmoqda.



Kiberxavfsizlik madaniyati nafaqat texnik bilim va ko'nikmalarni, balki raqamli muhitda ongli, ehtiyotkor, mas'uliyatli va xavfsiz xulq-atvorni shakllantirishga qaratilgan kompleks kompetensiyalar majmuasini anglatadi. Bu jarayon shaxsiy ma'lumotlarni himoya qilish, kuchli parollardan foydalanish, noma'lum havolalarni ochmaslik, internet etikasi, kiberhujumlarga nisbatan ogohlik kabi kundalik amaliy ko'nikmalarni qamrab oladi. O'quvchilar yoshligidan to'g'ri raqamli odatlarni o'zlashtirsa, kelajakda ular kiber tahdidlarga nisbatan ancha barqaror, mas'uliyatli va ongli foydalanuvchilarga aylanishi mumkin. Shu nuqtai nazardan, o'qituvchilarning vazifasi faqat kiberxavfsizlik bo'yicha nazariy ma'lumot berish bilan cheklanmaydi.

Kiberxavfsizlik madaniyatining nazariy asoslari va ta'limdagi ahamiyati

Kiberxavfsizlik madaniyati — bu shaxsning raqamli muhitda ongli, mas'uliyatli va xavfsiz faoliyat yuritish qobiliyatini belgilovchi bilim, ko'nikma, malaka va qadriyatlar majmuasidir. Uning asosiy maqsadi insonni internetdagi tahdidlar, virtual firibgarlik, zararli dasturlar, feyk axborot, shaxsiy ma'lumotlarning tarqalishi kabi xavflardan himoyalay oladigan darajaga yetkazishdir. Ta'lim jarayonida ushbu madaniyatni shakllantirish o'quvchilarning nafaqat texnik bilimlarini, balki mas'uliyatli axborot madaniyatini rivojlantiradi. Kiberxavfsizlik madaniyati, shuningdek, raqamli etikaga amal qilish, xushmuomalalik, intellektual mulkka hurmat, internetda iz qoldirish oqibatlarini anglash kabi ijtimoiy jihatlarni ham qamrab oladi.

Bugungi kunning dolzarb muammosi shundaki, o'quvchilar internetdan faol foydalanishsa-da, ko'pchiligida raqamli xavflarni oldindan sezish va ulardan himoyalalanish kompetensiyasi yetarli darajada shakllanmagan. Axborot texnologiyalari rivojlangan sari yangi turdagi kiberhujumlar paydo bo'lmoqda, bu esa ta'lim tizimini ushbu sohada muntazam yangilanib borishga majbur qiladi. Kiberxavfsizlik madaniyati ta'limning turli bosqichlari — boshlang'ich sinflardan oliygohgacha — izchil shakllantirilishi kerak bo'lgan uzluksiz jarayondir. Har bir yosh guruhiga mos, bosqichma-bosqich bilim berish o'quvchilarda ongli raqamli xulq-atvorni barqaror shakllantiradi.

Nazariy jihatdan, kiberxavfsizlik madaniyatini shakllantirishni o'quvchining axborot kompetensiyasini rivojlantirish bilan to'g'ridan-to'g'ri bog'lash mumkin. Raqamli kompetensiya — bu zamonaviy ta'limning ajralmas qismi bo'lib, uning tarkibiy elementlari axborotni izlash, tahlil qilish, saralash, xavfsiz saqlash va to'g'ri ulash ko'nikmalaridan iborat. Shunday ekan, kiberxavfsizlik faqat texnik bilim emas, balki funksional savodxonlik, tanqidiy fikrlash va ma'lumotlar bilan ongli muomala qilish madaniyatidir. Shu nuqtai nazardan, kiberxavfsizlik madaniyatining ta'limdagi o'rni strategik ahamiyatga



ega bo‘lib, yoshlarni kelajakdagi raqamli jamiyatga moslashtirishning hal qiluvchi omillaridan biridir.

Kiber gigiyena ko‘nikmalarini shakllantirishda pedagogik metodlar

Kiber gigiyena — bu internetdan foydalanishda kundalik xavfsiz xatti-harakatlar majmuasi bo‘lib, o‘quvchilarda uni shakllantirish o‘qituvchidan maxsus metodik yondashuvlarni talab qiladi. Amaliy o‘rgatish — eng samarali pedagogik metodlardan biri hisoblanadi. Masalan, o‘quvchilarga kuchli parollar yaratish, ikki bosqichli autentifikatsiyani yoqish, shubhali fayllarni ochmaslik, noma’lum havolalarni tekshirish kabi asosiy ko‘nikmalarni real misollar asosida o‘rgatish ularda mustahkam amaliy bilimgacha olib keladi. Bu jarayonda instruksion mashg‘ulotlar, laboratoriya topshiriqlari va mini-treninglar muhim rol o‘ynaydi.

Interaktiv metodlar — kiber gigiyena bo‘yicha ta’limni yanada jonli va qiziqarli qilish imkonini beradi. Munozara, aqliy hujum, klaster, “Case-study” (muammoli vaziyat tahlili) kabi metodlar orqali o‘quvchilar kiber tahdidlarni mustaqil aniqlaydi, ularning oqibatlarini baholaydi va o‘z xulosalarini chiqaradi. Masalan, real hayotga o‘xshash kiberhujum stsenariysi taqdim etilib, o‘quvchilardan uni tahlil qilish, tahdidni aniqlash va qanday himoyalaniшни taklif qilish so‘raladi. Bu esa ularda tanqidiy va mantiqiy fikrlashni rivojlantiradi.

Zamonaviy pedagogik yondashuvlardan yana biri — gamifikatsiya (o‘yinlashtirish) asosida o‘qitishdir. Kiber gigiyenani o‘yin shaklida o‘rgatish, masalan, missiyalar bajarish, ball yig‘ish, xavfsizlik darajasini oshirish orqali o‘quvchilarning qiziqishini keskin kuchaytiradi. O‘yinlashtirilgan darslar nafaqat motivatsiya beradi, balki murakkab axborotni tez va samarali o‘zlashtirishga yordam beradi. Bu metod yoshlar psixologiyasiga mos keladi, ular jarayonni o‘yin kabi qabul qilib, oson va samarali o‘rganadilar. Natijada, kiber gigiyena ko‘nikmalari ongli ravishda shakllanadi va kundalik odatga aylanadi.

Amaliy mashg‘ulotlar va simulyatsiyalar orqali kiber tahdidlardan himoyalaniش

Kiberxavfsizlikni nazariy o‘rgatish yetarli emas, chunki o‘quvchilar real vaziyatlarda duch keladigan tahdidlarni amalda his qilishlari zarur. Shu bois simulyatsiya mashg‘ulotlari — eng samarali metodlardan biridir. Simulyatsiya o‘quvchini virtual, ammo realga juda yaqin holatlarga qo‘yadi va uning qanday qaror qabul qilishini sinaydi. Masalan, phishing (soxta xabar) simulyatsiyasi orqali o‘quvchilarga turli elektron xatlar yuboriladi va ularning reaksiyasi kuzatiladi. Bu usul o‘quvchining ongli ogohligini oshirib, real hayotdagi xatolarning oldini olishga xizmat qiladi.



Amaliy laboratoriya mashg'ulotlari orqali o'quvchilar real kiberhujumlar qanday ishlashini va ular qanday himoyalaniishi mumkinligini o'rganadilar. Masalan, zararli dasturlar qanday tarqalishi, kompyuter tizimiga qanday kirib borishi va qanday aniqlanishi mumkinligi bo'yicha kichik tajribalar o'tkazish mumkin. Bu orqali o'quvchilar "xavf qanday paydo bo'ladi?" degan savolga chuqurroq javob oladi. Amaliy mashg'ulotlar orqali o'rganilgan bilimlar uzoq muddat saqlanadi va hayotiy vaziyatlarda qo'llash osonlashadi.

Kiber poligonlar (cyber range) yoki virtual xavfsizlik maydonlaridan foydalanish ta'lim jarayonining zamonaviy shaklidir. Bu texnologiya orqali o'quvchilar real tizimlarga zarar yetkazmagan holda haqiqiy hujum stsenariylarini sinab ko'rishi mumkin. Ular kiberhujumni aniqlash, to'xtatish, himoya devori (firewall) sozlash, zararli trafikni aniqlash kabi ko'nikmalarni mashq qiladilar. Simulyatsiya asosidagi o'qitish nafaqat texnik savodxonlikni oshiradi, balki tezkor qaror qabul qilish, muammoni hal qilish, jamoada ishlash ko'nikmalarini ham rivojlantiradi.

Sun'iy intellekt va raqamli platformalardan foydalanishning didaktik afzalliklari

Sun'iy intellekt (AI) kiberxavfsizlik madaniyatini rivojlantirishda yangi pedagogik imkoniyatlarni yaratmoqda. AI asosida ishlaydigan o'quv tizimlari o'quvchilarning bilim darajasini avtomatik tahlil qilib, ularga mos individual topshiriqlarni taklif etishi mumkin. Masalan, o'quvchi phishing xabarini tanishda qiynalgan bo'lsa, tizim unga qo'shimcha misollar beradi, xatolarni tushuntiradi va individual o'quv yo'nalishini shakllantiradi. Bu yondashuv o'quvchilarning o'zlashtirish jarayonini tezlashtiradi va bilimdagi bo'shliqlarni aniq to'ldirishga xizmat qiladi.

Raqamli o'quv platformalari — virtual laboratoriyalar, multimedia darsliklar, videodarslar, interaktiv topshiriqlar — kiberxavfsizlikni o'rgatishda samaradorlikni oshiradi. Multimedia vositalari murakkab tushunchalarni soddalashtiradi, masalan, zararli dastur algoritmini animatsiya ko'rinishida ko'rsatish o'quvchilarning tushunishini ancha osonlashtiradi. Interaktiv testlar, onlayn viktorinalar, virtual mashqlar o'quvchilarni faol o'qishga undaydi va bilimni darhol mustahkamlaydi.

AI yordamida xavfli kontentni aniqlash va filtratsiya qilish jarayonlari ham ta'lim muassasalarida muhim ahamiyatga ega. Masalan, sun'iy intellekt noto'g'ri havolalarni aniqlaydi, zararli saytlarni bloklaydi, o'quvchilarning onlayn faoliyatini xavfsiz muhitga yo'naltiradi. Bu o'z navbatida nafaqat himoya vositasi, balki o'quvchilarga real misollar orqali "nima xavfli, nima xavfsiz" ekanini o'rgatadigan ta'limiy mexanizmga aylanadi. Shuningdek, AI yordamida yaratilgan o'quv chat-botlari o'quvchilarga 24/7 rejimda yordam



beradi, savollariga javob beradi va mustaqil o'rganish jarayonini qo'llab-quvvatlaydi.

Xulosa

Raqamli transformatsiya jarayonlari jadal sur'atlarda rivojlanayotgan hozirgi zamonda ta'lim tizimida kiberxavfsizlik madaniyatini shakllantirish dolzarb va strategik ahamiyatga ega masalaga aylanib bormoqda. O'quvchilar va talabalar internetdan foydalanish jarayonida turli kiber tahdidlarga duch kelishi tabiiy hol bo'lib, ularning bunday vaziyatlarda to'g'ri qaror qabul qilishi, shaxsiy ma'lumotlarini himoya qilishi va xavfsiz xulq-atvorni namoyon etishi uchun maxsus pedagogik yondashuvlar talab etiladi. Tadqiqot davomida ko'rib chiqilgan metodlar — interaktiv o'qitish, gamifikatsiya, amaliy mashg'ulotlar, simulyatsiyalar va sun'iy intellekt texnologiyalaridan foydalanish — o'quvchilarda kiberxavfsizlik madaniyatini bosqichma-bosqich va samarali shakllantirish imkonini berishi aniqlandi.

Tahlillar shuni ko'rsatadiki, kiberxavfsizlik bo'yicha faqat nazariy bilimlarni berish yetarli emas, balki o'quvchilarning real vaziyatlarda duch keladigan tahdidlarni amalda tushunishi, ularga ongli ravishda munosabat bildira olishi va xavfsiz strategiyalarni qo'llay bilishi muhimdir. Simulyatsiya texnologiyalari, virtual kiber poligonlar va amaliy laboratoriya mashg'ulotlari o'quvchilarning texnik savodxonligini oshirish bilan birga ularning muammoli vaziyatni tahlil qilish, tanqidiy fikrlash va tezkor qaror qabul qilish qobiliyatlarini rivojlantiradi.

FOYDALANILGAN ADABIYOTLAR

1. Abdullayev, A. Kiberxavfsizlik asoslari. – Toshkent: Innovatsiya, 2021.
2. Karimova, M. Axborot madaniyati va xavfsizligi. – Toshkent: O'zbekiston Milliy universiteti nashriyoti, 2020.
3. Soliyev, R. Raqamli ta'lim texnologiyalari. – Toshkent: Fan va texnologiya, 2022.
4. National Institute of Standards and Technology (NIST). Cybersecurity Framework, 2020.
5. ENISA. Cybersecurity Education and Awareness Report, 2021.
6. OECD. Digital Literacy Skills for the Future, 2022.
8. Krotov, V. Informatsionnaya bezopasnost v obrazovanii. – Moskva: Akademkniga, 2019.
9. Shor, K. Cyber Hygiene for Students. – London: Routledge, 2021.
10. UNESCO. Digital Citizenship Competencies, 2020.