

TALABALARDA KIBERXAVFSIZLIK MADANIYATINI SHAKLLANTIRISHNING PSIXOLOGIK-PEDAGOGIK XUSUSIYATLARI

Muxammadjonov Xojiakbar Zafarjon o'g'li

Qori Niyoziy nomidagi Tarbiya pedagogikasi milliy instituti mustaqil izlanuvchisi

Annotatsiya. Mazkur maqolada talabalarda kiberxavfsizlik madaniyatini shakllantirishning psixologik-pedagogik xususiyatlari ilmiy-nazariy jihatdan tahlil qilingan. Raqamli texnologiyalarning jadal rivojlanishi sharoitida yoshlarning axborot xavfsizligini ta'minlash, ularni kiberxavflardan himoyalash hamda xavfsiz raqamli xulq-atvorni shakllantirish oliy ta'lim tizimining ustuvor vazifalaridan biri sifatida yoritilgan. Maqolada kiberxavfsizlik madaniyatining tarkibiy komponentlari, kompetensiyalari, pedagogik qo'llab-quvvatlash mexanizmlari hamda psixologik omillari tahlil qilinadi.

Kalit so'zlar: kiberxavfsizlik, kiberxavfsizlik madaniyati, pedagogik qo'llab-quvvatlash, psixologik omillar, raqamli ta'lim, kompetensiya, axborot xavfsizligi, interfaol metodlar, refleksiya, talaba.

Аннотация. В данной статье с научно-теоретической точки зрения проанализированы психолого-педагогические особенности формирования культуры кибербезопасности у студентов. В условиях стремительного развития цифровых технологий обеспечение информационной безопасности молодежи, их защита от киберугроз и формирование безопасного цифрового поведения освещены как одна из приоритетных задач системы высшего образования. В статье анализируются компоненты, компетенции, механизмы педагогической поддержки и психологические факторы культуры кибербезопасности.

Ключевые слова: кибербезопасность, культура кибербезопасности, педагогическая поддержка, психологические факторы, цифровое образование, компетенция, информационная безопасность, интерактивные методы, рефлексия, студент.

Abstract. This article analyzes the psychological and pedagogical characteristics of developing cybersecurity culture among university students. In the context of rapid digital transformation, ensuring students' information security and developing safe digital behavior have become one of the priority tasks of higher education institutions. The study examines the structural components of cybersecurity culture, key competencies, pedagogical support mechanisms, and psychological factors affecting cybersecurity awareness.

Keywords: cybersecurity, cybersecurity culture, pedagogical support, psychological factors, digital education, competence, information security, interactive learning, reflection, students.

Kirish. Bugungi kunda jamiyatning barcha sohalarida raqamlashtirish jarayonlari jadal sur'atlarda rivojlanmoqda. Sun'iy intellekt, bulutli texnologiyalar, mobil ilovalar, ijtimoiy tarmoqlar va elektron ta'lim platformalarining keng qo'llanilishi natijasida axborot almashinuvi misli ko'rilmagan darajada tezlashdi. Shu bilan birga, kiberjinoyatchilik, fishing hujumlari, zararli dasturlar, shaxsiy ma'lumotlarning o'g'irlanishi keng tarqalishi kiberxavfsizlikni zamonaviy ta'limning eng dolzarb yo'nalishlaridan biriga aylantirmoqda.

Oliy ta'lim muassasalari talabalari internet va raqamli texnologiyalardan eng faol foydalanuvchilar hisoblanadi. Shu sababli ularda kiberxavfsizlik madaniyatini shakllantirish nafaqat texnik bilimlarni o'rgatish, balki psixologik tayyorgarlik, axborotga tanqidiy yondashuv hamda mas'uliyatli raqamli xulq-atvorni rivojlantirishni ham talab etadi.

Kiberxavfsizlik madaniyati shaxsning bilimlari, amaliy ko'nikmalari, qadriyatlari, motivatsiyasi va mas'uliyatli xatti-harakatlari yig'indisini ifodalaydi. Aynan ushbu madaniyat talabalarning axborot muhitidagi xavf-xatarlarni to'g'ri baholashiga, ularning oldini olishiga hamda xavfsiz qarorlar qabul qilishiga xizmat qiladi.

Asosiy qism

Kiberxavfsizlik madaniyatini rivojlantirish zamonaviy pedagogika, psixologiya, axborot xavfsizligi hamda axborot-kommunikatsiya texnologiyalari sohalarining kesishgan nuqtasida shakllanayotgan dolzarb ilmiy yo'nalishlardan biri hisoblanadi. Raqamli transformatsiya jarayonlarining jadallashuvi, sun'iy intellekt texnologiyalarining keng qo'llanilishi, masofaviy ta'limning rivojlanishi hamda internet xizmatlaridan foydalanish ko'lamining ortishi natijasida kiberxavfsizlik masalalari alohida ilmiy va amaliy ahamiyat kasb etmoqda. Ayniqsa, oliy ta'lim muassasalari talabalari raqamli texnologiyalardan eng faol foydalanuvchilar qatoriga kirganligi sababli ular kiberxavfsizlik madaniyatini shakllantirish pedagogik jarayonning ustuvor yo'nalishlaridan biri sifatida qaralmoqda.

Kiberxavfsizlik madaniyatining nazariy asoslari ko'plab xorijiy va mahalliy olimlarning ilmiy izlanishlarida o'z aksini topgan. Xususan, A. V. Belous, G. V. Grachev va A. A. Malyuk axborot-psixologik xavfsizlikni milliy xavfsizlik tizimining muhim tarkibiy elementi sifatida e'tirof etib, uning huquqiy, tashkiliy, texnologik va psixologik jihatlarini kompleks ravishda tahlil qilganlar. Ularning ilmiy qarashlariga ko'ra, zamonaviy axborot makonidagi eng katta tahdid faqat texnik hujumlar emas, balki shaxs ongiga yo'naltirilgan psixologik manipulyatsiyalar, dezinformatsiya, yolg'on axborot tarqatish, ijtimoiy tarmoqlar orqali amalga oshiriladigan yashirin ta'sirlar ham hisoblanadi. Shu sababli axborot xavfsizligini ta'minlashda texnik himoya vositalari bilan bir qatorda shaxsning tanqidiy fikrlashi, media savodxonligi hamda axborotni tahlil qilish kompetensiyalarini rivojlantirish zarurligi asoslab berilgan.

A. A. Sterxov tomonidan ishlab chiqilgan pedagogik qo'llab-quvvatlash modeli esa talabalarda xavfsiz xulq-atvorni shakllantirishning samarali mexanizmlaridan biri sifatida e'tirof etiladi. Mazkur model motivatsion-maqсадli, mazmun-faoliyat va natijaviy-refleksiv bloklardan iborat bo'lib, ta'lim jarayonining barcha bosqichlarida talabaning shaxsiy rivojlanishiga yo'naltirilgan pedagogik ta'sirni nazarda tutadi. Olimning fikricha, pedagog, oila, jamoatchilik hamda ta'lim muassasasi o'rtasidagi uzviy hamkorlik shaxsning axborot xavfsizligiga oid mas'uliyatli pozitsiyasini shakllantirishda muhim omil hisoblanadi.

M. Z. Xusenov oliy ta'lim muassasalarida kiberxavfsizlik madaniyatini rivojlantirishning metodik asoslarini tadqiq etib, interfaol ta'lim metodlari, muammoli vaziyatlar, amaliy laboratoriya mashg'ulotlari, virtual simulyatorlar hamda raqamli ta'lim platformalaridan foydalanishning pedagogik samaradorligini ilmiy jihatdan asoslab bergan. Tadqiqot natijalariga ko'ra, talabalarning nazariy bilimlarini amaliy mashg'ulotlar bilan uyg'unlashtirish ularning kiberxavflarni aniqlash, baholash va ularga qarshi to'g'ri choralar ko'rish kompetensiyalarini sezilarli darajada rivojlantiradi.

Mazkur ilmiy tadqiqotlar shuni ko'rsatadiki, kiberxavfsizlik madaniyatini shakllantirish faqat axborot texnologiyalariga oid bilimlarni o'rgatish bilangina cheklanmaydi. Ushbu jarayon psixologik tayyorgarlik, pedagogik texnologiyalar, axloqiy qadriyatlar, huquqiy madaniyat hamda shaxsning ijtimoiy mas'uliyatini uyg'un ravishda rivojlantirishni talab etadigan murakkab pedagogik tizim hisoblanadi. Shuning uchun ham zamonaviy oliy ta'limda kiberxavfsizlik madaniyatini kompetensiyaviy yondashuv asosida rivojlantirish alohida dolzarblik kasb etmoqda.

Talabalarda kiberxavfsizlik madaniyati ko'p komponentli pedagogik hodisa bo'lib, u shaxsning raqamli muhitda xavfsiz, mas'uliyatli va ongli faoliyat yuritishini ta'minlaydigan bilim, ko'nikma, qadriyat, xulq-atvor hamda refleksiv kompetensiyalar majmuasidan iborat.

Mazkur madaniyatning shakllanishi talabalarning axborot-kommunikatsiya texnologiyalaridan samarali foydalanishi bilan bir qatorda, yuzaga kelishi mumkin bo'lgan kiberxavflarni oldindan baholash, ularning oqibatlarini anglash hamda himoyalanih strategiyalarini to'g'ri tanlay olish qobiliyatini ham rivojlantiradi. Pedagogik nuqtai nazardan kiberxavfsizlik madaniyati quyidagi asosiy komponentlarni o'z ichiga oladi:

1. Bilim komponenti. Bilim komponenti talabaning kiberxavfsizlik sohasidagi nazariy tayyorgarligini ifodalaydi. Mazkur komponent orqali talabalar axborot xavfsizligining asosiy tamoyillari, ya'ni maxfiylik (Confidentiality), yaxlitlik (Integrity) va mavjudlik (Availability) tamoyillari (CIA triadasi), axborot aktivlari, tahdid, zaiflik, xavf va risk tushunchalari o'rtasidagi bog'liqlikni anglaydi. Bundan tashqari, ular fishing, spear-phishing, ransomware, botnet, DDoS hujumlari, zararli dasturlar, zararli kodlar, ijtimoiy muhandislik, sun'iy intellekt yordamida amalga oshirilayotgan kiberhujumlar, shaxsiy ma'lumotlarni himoya qilish usullari, kriptografik himoya vositalari hamda xalqaro va milliy axborot xavfsizligi standartlari haqida chuqur bilimlarga ega bo'ladilar. talabalarda raqamli etikaga oid bilimlar, mualliflik huquqi, intellektual mulkni himoya qilish, shaxsiy ma'lumotlar bilan ishlash qoidalar, kiberjinoyatlar uchun javobgarlik hamda axborot xavfsizligi bo'yicha amaldagi qonunchilikka oid tushunchalar ham shakllanadi. Mazkur bilimlar talabaning har qanday vaziyatda ilmiy asoslangan va oqilona qaror qabul qilishiga xizmat qiladi.

2. Amaliy ko'nikmalar komponenti. Amaliy ko'nikmalar komponenti nazariy bilimlarning real hayotdagi qo'llanilishini tavsiflaydi. Ushbu komponent doirasida talabalar kuchli parollar yaratish va ularni boshqarish, parol menejerlaridan foydalanish, ko'p bosqichli autentifikatsiyani yoqish, elektron pochta xavfsizligini ta'minlash, zararli havolalarni aniqlash, antivirus dasturlarini sozlash, operatsion tizimlarni muntazam yangilash, VPN texnologiyalaridan foydalanish, Wi-Fi tarmoqlarini himoyalash, bulutli xizmatlarda xavfsiz ishlash, mobil qurilmalar xavfsizligini ta'minlash hamda ma'lumotlarning zaxira nusxalarini yaratish ko'nikmalarini egallaydilar. talabalar amaliy mashg'ulotlar davomida kiberinsidentlarni aniqlash, ularga tezkor javob berish, xavfsizlik siyosatini qo'llash, xavf darajasini baholash va kiberxavflarning oldini olish bo'yicha algoritmlarni ishlab chiqishni ham o'rganadilar. Ushbu kompetensiyalar kelgusidagi kasbiy faoliyatda muhim ahamiyat kasb etadi.

3. Qadriyat va munosabat komponenti. Qadriyat va munosabat komponenti shaxsning axborot xavfsizligiga nisbatan ongli va mas'uliyatli munosabatini aks ettiradi. Mazkur komponent orqali talabalarda axborotdan foydalanish madaniyati, internet etikasi, raqamli fuqarolik, akademik halollik, shaxsiy va jamoaviy mas'uliyat, boshqalarning huquq va manfaatlarini hurmat qilish kabi fazilatlar rivojlanadi.

Talabalar axborotdan noqonuniy foydalanish, plagiat, noqonuniy dasturiy ta'minotdan foydalanish, yolg'on axborot tarqatish, kiberbulling va boshqa salbiy holatlarning jamiyat taraqqiyotiga salbiy ta'sirini anglay boshlaydilar. Natijada ularda axborot xavfsizligi talablariga ixtiyoriy va ongli ravishda amal qilish ehtiyoji shakllanadi.

4. Mas'uliyatli xulq-atvor komponenti. Mazkur komponent kiberxavfsizlik madaniyatining amaliy ifodasini tashkil etadi. Talaba internet va axborot tizimlaridan foydalanishda xavfsizlik qoidalariga rioya qiladi, noma'lum havolalarni ochmaydi, shubhali fayllarni yuklab olmaydi, boshqalarning shaxsiy ma'lumotlariga ehtiyotkorlik bilan munosabatda bo'ladi hamda axborot tizimlarida yuzaga kelishi mumkin bo'lgan tahdidlarni oldindan baholashga harakat qiladi. Mas'uliyatli xulq-atvor talabaning raqamli makondagi huquqiy madaniyatini ham namoyon etadi. U axborot xavfsizligi siyosatiga amal qiladi, noqonuniy dasturlarni tarqatmaydi, kiberjinoyatlarga qarshi murosasiz pozitsiyani egallaydi, axborot resurslaridan faqat qonuniy maqsadlarda

foydalanadi hamda jamiyatning umumiy kiberxavfsizlik darajasini oshirishga o'z hissasini qo'shadi.

5. Refleksiv baholash komponenti. Refleksiv baholash komponenti talabani o'z bilimlari, ko'nikmalari va xatti-harakatlarini muntazam ravishda tahlil qilishga yo'naltirilgan. Talaba o'zining kiberxavfsizlik bo'yicha tayyorgarlik darajasini baholaydi, mavjud kamchiliklarni aniqlaydi, ularni bartaraf etish strategiyalarini ishlab chiqadi hamda yangi bilimlarni egallashga intiladi. Refleksiya jarayoni shaxsning uzluksiz kasbiy rivojlanishini ta'minlaydi. Chunki kiberxavflar doimiy ravishda o'zgarib borayotganligi sababli mutaxassis muntazam ravishda yangi himoya texnologiyalari, zamonaviy dasturiy vositalar hamda xalqaro tajribalarni o'zlashtirib borishi zarur. Aynan refleksiv yondashuv shaxsning o'z-o'zini rivojlantirish kompetensiyasini shakllantiradi.

Yuqorida tavsiflangan komponentlar o'zaro uzviy bog'liq bo'lib, ularning har biri ikkinchisini to'ldiradi. Nazariy bilim amaliy ko'nikmalarni rivojlantirish uchun asos bo'lsa, qadriyat va munosabatlar mas'uliyatli xulq-atvorni shakllantiradi, refleksiya esa ushbu jarayonlarning uzluksiz takomillashishini ta'minlaydi. Shu bois kiberxavfsizlik madaniyatini alohida fan doirasida emas, balki uzluksiz pedagogik jarayon sifatida tashkil etish maqsadga muvofiqdir.

Tahlillar shuni ko'rsatadiki, bugungi kunda oliy ta'lim muassasalarida kiberxavfsizlik bo'yicha berilayotgan bilimlar asosan texnik yo'nalishga ega bo'lib, dasturiy ta'minot, tarmoq xavfsizligi va axborotni himoyalash vositalariga ko'proq e'tibor qaratiladi. Biroq axborot manipulyatsiyasiga qarshi psixologik immunitetni shakllantirish, media savodxonlikni rivojlantirish, tanqidiy fikrlashni kuchaytirish, raqamli etikani singdirish, shaxsning axborot iste'moli madaniyatini rivojlantirish kabi masalalar o'quv jarayonida yetarli darajada integratsiyalashmagan.

Kiberxavfsizlikka oid mashg'ulotlarda real hayotiy vaziyatlar, kiberinsidentlar tahlili, virtual laboratoriyalar, simulyatsiyalar, keys-stadi texnologiyalari, gamifikatsiya elementlari hamda loyiha asosida o'qitish metodlari imkoniyatlaridan to'liq foydalanilmayotganligi kuzatiladi. Bu esa talabalarning nazariy bilimlarini amaliy faoliyat bilan bog'lash imkoniyatlarini cheklaydi.

Shu munosabat bilan oliy ta'lim tizimida kiberxavfsizlik madaniyatini rivojlantirishning integrativ modelini ishlab chiqish zarur. Mazkur model barcha fanlar mazmuniga kiberxavfsizlik elementlarini kiritish, interfaol pedagogik texnologiyalarni qo'llash, raqamli ta'lim resurslaridan samarali foydalanish, talabalarni real kiberxavf vaziyatlarini modellashtirish orqali o'qitish, ularning media savodxonligi, tanqidiy fikrlashi va refleksiv kompetensiyalarini rivojlantirishga yo'naltirilishi lozim. Bunday yondashuv talabalarning nafaqat texnik tayyorgarligini, balki ularning ma'naviy, huquqiy, psixologik va kasbiy kompetentligini ham kompleks ravishda rivojlantirish imkonini beradi. Natijada raqamli transformatsiya sharoitida xavfsiz, mas'uliyatli va raqobatbardosh mutaxassislarni tayyorlash uchun mustahkam pedagogik asos yaratiladi.

Xulosa. Talabalarda kiberxavfsizlik madaniyatini shakllantirish murakkab psixologik-pedagogik jarayon bo'lib, u bilim, ko'nikma, motivatsiya, mas'uliyat va xavfsiz xulq-atvorning uzviy birligiga asoslanadi. Pedagogik qo'llab-quvvatlash, interfaol metodlar, muammoli vaziyatlar hamda refleksiv faoliyat ushbu jarayonning samaradorligini sezilarli oshiradi. Oliy ta'lim muassasalarida kiberxavfsizlik madaniyatini rivojlantirish bo'yicha kompleks metodik tizimni yaratish zamonaviy ta'limning muhim ustuvor yo'nalishlaridan biri hisoblanadi.

Foydalanilgan adabiyotlar

Bekmuratov T. F., G'aniyev S. K., Karimov M. M., Tashayev K. A. Axborot xavfsizligi: oliy o'quv yurtlari talabalari uchun o'quv qo'llanma. – Toshkent: «Fan va texnologiya», 2016. – B. 125–126.

Akbarov Bahodir Akbarovich. Kiberxavfsizlik madaniyati va ta'lim jarayonida axborot xavfsizligi kompetensiyalarini rivojlantirish. – Toshkent: Fan, 2023. – 256 b. – B. 200.



Мелников Д. А. Информационная безопасность открытых систем: учебник / Д. А. Мелников. – М.: Флинта, 2013. – 448 с.

F. M. Muxtarov, “Kiberxavfsizlik asoslari” Darslik. Farg‘ona 2023. 339 b.

Qodirov N., Raqamli xavfsizlik asoslari, “Fan va texnologiya” nashriyoti, Toshkent, 2022, 250 bet.

Ganiev S. K., Karimov M. M., Toshev BA Kiberxavfsizlik asoslari: o‘quv qo‘llanma. – Toshkent: TATU, 2021. – 320 b.