Ilmiy tadqiqotlar va ularning yechimlari jurnali
Aoka guvohnoma № 323759 ISSN: 3060-4818

INFORMATIKA DARSLARIDA KIBERXAVFSIZLIK MADANIYATINI SHAKLLANTIRISHNING ZAMONAVIY YONDASHUVLARI

Akobirov Hasan Alixonovich
Jizzax viloyati Zafarobod tumani
6-umumiy o‘rta ta’lim maktabining
informatika fani o'qituvchisi
https://doi.org/10.5281/zenodo.24276466

ANNOTATSIYA: Mazkur maqolada informatika darslarida o‘quvchilarning kiberxavfsizlik madaniyatini shakllantirishning zamonaviy pedagogik yondashuvlari, samarali metodlari va amaliy imkoniyatlari yoritilgan. Raqamli texnologiyalardan foydalanish jarayonida uchraydigan kiberxavflar, shaxsiy ma’lumotlarni himoya qilish, kuchli parollardan foydalanish, fishing hujumlarini aniqlash, internetdagi axborotlarni tanqidiy baholash kabi masalalarning ta’lim jarayonidagi ahamiyati tahlil qilingan. Shuningdek, muammoli ta’lim, loyiha asosida o‘qitish, gamifikatsiya, vaziyatli topshiriqlar va interaktiv mashg‘ulotlar orqali o‘quvchilarda xavfsiz raqamli xulq-atvorni rivojlantirish yo‘llari taklif etilgan. Maqolada kiberxavfsizlikni faqat texnik bilim sifatida emas, balki kundalik hayotda zarur bo‘lgan mas’uliyatli raqamli madaniyat sifatida o‘rgatish zarurligi asoslab berilgan.
Kalit so‘zlar: kiberxavfsizlik, raqamli madaniyat, informatika ta’limi, axborot xavfsizligi, shaxsiy ma’lumotlar, fishing, raqamli savodxonlik, internet xavfsizligi, interaktiv metodlar, tanqidiy fikrlash.

KIRISH

Bugungi kunda raqamli texnologiyalar inson hayotining deyarli barcha sohalariga chuqur kirib bormoqda. Ta’lim, tibbiyot, iqtisodiyot, davlat boshqaruvi va kundalik muloqot jarayonlarida internet hamda axborot-kommunikatsiya texnologiyalaridan foydalanish imkoniyatlari kengaymoqda. Biroq raqamli imkoniyatlarning ortishi bilan bir qatorda, internetdagi firibgarlik, shaxsiy ma’lumotlarning o‘g‘irlanishi, zararli dasturlar, soxta havolalar, kiberbulling va boshqa xavfsizlik muammolari ham kuchaymoqda.

Ayniqsa, o‘quvchilarning ijtimoiy tarmoqlar, mobil ilovalar, onlayn o‘yinlar va turli raqamli platformalardan faol foydalanishi ularda kiberxavfsizlik bo‘yicha yetarli bilim va ko‘nikmalarni shakllantirish zaruratini yuzaga keltirmoqda. Chunki internetdan foydalanish imkoniyatiga ega bo‘lishning o‘zi xavfsiz raqamli xulq-atvorni anglatmaydi. O‘quvchi shaxsiy ma’lumotlarini himoya qilish, shubhali xabarlarni farqlash, ishonchsiz manbalarga murojaat qilmaslik va internetdagi muloqot odobiga rioya qilishni bilishi kerak.

O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi Qonunida kiberxavfsizlik sohasidagi munosabatlarni tartibga solishning huquqiy asoslari belgilangan [1]. Mazkur yo‘nalishning ta’lim bilan bog‘liq jihati shundaki, yosh avlodda axborot resurslaridan ongli, mas’uliyatli va xavfsiz foydalanish ko‘nikmalarini shakllantirish muhim vazifaga aylanmoqda.

Shu nuqtayi nazardan, informatika darslarida kiberxavfsizlik mavzusini faqat nazariy ma’lumotlar bilan cheklamasdan, hayotiy vaziyatlar, amaliy mashqlar, muammoli topshiriqlar va interaktiv metodlar asosida o‘rgatish maqsadga muvofiqdir. Maqolaning asosiy maqsadi informatika ta’limida kiberxavfsizlik madaniyatini shakllantirishning zamonaviy yondashuvlarini tahlil qilish hamda dars jarayonida qo‘llash mumkin bo‘lgan amaliy tavsiyalarni ishlab chiqishdan iborat.

METODLAR

Tadqiqot jarayonida pedagogik tahlil, qiyosiy o‘rganish, umumlashtirish, kuzatish va metodik modellashtirish usullaridan foydalanildi. Kiberxavfsizlikka oid ilmiy-metodik qarashlar hamda ta’limda raqamli xavfsizlikni rivojlantirishga qaratilgan yondashuvlar o‘rganildi.

Maqolada kiberxavfsizlik madaniyatini shakllantirish quyidagi asosiy yo‘nalishlar bo‘yicha ko‘rib chiqildi:

1. Muammoli ta’lim yondashuvi. O‘quvchilarga real hayotda uchrashi mumkin bo‘lgan kiberxavfli vaziyatlar taqdim etiladi. Masalan, noma’lum shaxsdan “Siz sovrin yutdingiz, havolaga bosing” mazmunidagi xabar kelganida qanday yo‘l tutish kerakligi muhokama qilinadi. O‘quvchilar vaziyatni tahlil qilib, xavfni aniqlash va to‘g‘ri qaror qabul qilishga o‘rganadilar.

2. Amaliy faoliyatga asoslangan yondashuv. O‘quvchilar kuchli parol yaratish, ikki bosqichli autentifikatsiya mohiyatini tushunish, maxfiylik sozlamalarini o‘rganish va shubhali havolalarni aniqlash bo‘yicha mashqlar bajaradilar. Bu jarayonda nazariy bilimlar amaliy ko‘nikmalarga aylanadi.

3. Gamifikatsiya yondashuvi. Kiberxavfsizlik mavzulari o‘yin elementlari, musobaqalar, maxsus kartochkalar va ball to‘plash tizimi orqali o‘rgatiladi. Masalan, “Fishingni aniqlang”, “Xavfsiz parol detektivi” va “Kiberxavfsizlik bilimdoni” kabi topshiriqlar o‘quvchilarning qiziqishini oshiradi.

4. Loyiha asosida o‘qitish. O‘quvchilar guruhlarda ishlagan holda “Xavfsiz internet qoidalari”, “Mening raqamli izim” yoki “Kiberxavfsiz maktab” kabi loyihalarni tayyorlaydilar. Loyihalar orqali ular mustaqil izlanish, axborotni saralash, hamkorlikda ishlash va o‘z fikrlarini taqdim etish ko‘nikmalarini rivojlantiradilar.

5. Vaziyatli tahlil va rolli o‘yinlar. O‘quvchilar internet foydalanuvchisi, kiberxavfsizlik mutaxassisi, moderator yoki mas’uliyatli raqamli fuqaro rollarida turli vaziyatlarni tahlil qiladilar. Bunda o‘quvchilarga zararli harakatlarni bajarish emas, balki xavfni tanib olish va undan himoyalanish vazifasi beriladi.

NATIJALAR

Tahlil natijasida informatika darslarida kiberxavfsizlik madaniyatini shakllantirish uchun o‘quvchilarga faqat xavfsizlik qoidalarini yodlatish yetarli emasligi aniqlandi. Ular turli raqamli vaziyatlarda xavfni mustaqil aniqlay olishi, to‘g‘ri qaror qabul qilishi va o‘z harakatlari uchun javobgarlikni his qilishi lozim.

Kiberxavfsizlik madaniyatini shakllantirishda quyidagi bilim va ko‘nikmalar muhim o‘rin tutadi:

Shaxsiy ma’lumotlarni himoya qilish. O‘quvchilar telefon raqami, yashash manzili, parol, bank kartasi ma’lumotlari, shaxsiy suratlar va boshqa maxfiy axborotlarni internetda tarqatish qanday xavf tug‘dirishini tushunishlari kerak. Shuningdek, ijtimoiy tarmoqlardagi maxfiylik sozlamalaridan foydalanishni bilishlari zarur.

Kuchli parollardan foydalanish. O‘quvchilarga oddiy va taxmin qilish oson bo‘lgan parollardan voz kechish, har bir muhim hisob uchun alohida parol tanlash hamda imkon mavjud bo‘lsa, ko‘p omilli autentifikatsiyani yoqish o‘rgatiladi. AQSH Kiberxavfsizlik va infratuzilma xavfsizligi agentligi ham kuchli parollar, ko‘p omilli autentifikatsiya, fishingni aniqlash va dasturiy ta’minotni yangilashni internetda xavfsiz bo‘lishning asosiy amaliy choralaridan deb ko‘rsatadi [3].

Fishing xabarlarini aniqlash. O‘quvchilar soxta xabarlar, shubhali havolalar va yolg‘on sovrin takliflarini farqlashni o‘rganadilar. Masalan, noma’lum manbadan kelgan “Hisobingiz bloklandi, darhol havolaga kiring” mazmunidagi xabarni tekshirmasdan ochmaslik kerakligi tushuntiriladi.

Raqamli iz va internet odobi. O‘quvchilarga internetga joylashtirilgan ma’lumotlar uzoq vaqt saqlanib qolishi va ularning kelajakdagi obro‘siga ta’sir qilishi mumkinligi anglatiladi. Boshqalarning suratlari yoki shaxsiy ma’lumotlarini ruxsatsiz tarqatmaslik, haqoratli izohlar yozmaslik va internetdagi muloqot madaniyatiga rioya qilishga alohida e’tibor qaratiladi.

Axborotni tanqidiy baholash. Internetdagi barcha ma’lumotlar ham ishonchli emas. Shu bois o‘quvchilar axborot manbasini tekshirish, shubhali xabarlarni boshqa ishonchli manbalar bilan solishtirish va yolg‘on axborotni tarqatmaslik ko‘nikmalarini egallashlari lozim.

Ushbu yo‘nalishlarni dars jarayoniga tizimli kiritish natijasida o‘quvchilarda kiberxavflarni tanish, ulardan himoyalanish, raqamli muhitda mas’uliyatli faoliyat yuritish va zarur holatlarda kattalar yoki tegishli mutaxassislardan yordam so‘rash ko‘nikmalarini rivojlantirish mumkin.

Kiberxavfsizlikni o‘rgatishda qo‘llash mumkin bo‘lgan amaliy topshiriqlar

Topshiriq nomi	Mazmuni	Kutiladigan natija
“Fishingni aniqlang”	Haqiqiy va soxta xabarlarni taqqoslash	Shubhali xabarlarni farqlaydi
“Parol detektivi”	Turli parollarning mustahkamligini baholash	Kuchli parol yaratishni o‘rganadi
“Raqamli izim”	Internetda qoldiriladigan ma’lumotlarni tahlil qilish	Shaxsiy axborotga ehtiyotkor munosabat shakllanadi
“Xavfsizmi yoki xavfli?”	Turli internet vaziyatlariga yechim topish	Mustaqil qaror qabul qilish rivojlanadi
“Kiberhimoya loyihasi”	Sinf uchun xavfsiz internet qoidalarini ishlab chiqish	Hamkorlik va ijodkorlik rivojlanadi

MUHOKAMA

Kiberxavfsizlik madaniyatini shakllantirish jarayonida o‘quvchilarning yosh xususiyatlari, raqamli tajribasi va bilim darajasini hisobga olish muhimdir. Chunki boshlang‘ich bosqichdagi o‘quvchiga internetda shaxsiy ma’lumotlarni oshkor qilmaslik va begonalarning xabarlariga ehtiyotkor munosabatda bo‘lish o‘rgatilsa, yuqori sinf o‘quvchilari bilan fishing, zararli dasturlar, akkaunt xavfsizligi, raqamli iz va ijtimoiy muhandislik kabi murakkabroq mavzularni muhokama qilish mumkin.

NIST tomonidan ishlab chiqilgan Cybersecurity Framework 2.0 tizimida kiberxavfsizlik risklarini boshqarish “Govern, Identify, Protect, Detect, Respond, Recover” — boshqarish, aniqlash, himoyalash, kuzatish, javob berish va tiklash yo‘nalishlari orqali yoritilgan [2]. Ushbu yondashuvni ta’lim jarayoniga moslashtirish o‘quvchilarga xavfsizlikni bir martalik harakat emas, balki doimiy davom etadigan jarayon sifatida tushunishga yordam beradi.

Masalan, o‘quvchi noma’lum havolani olganida, avvalo uning manbasini aniqlashi, havolaning ishonchliligini tekshirishi, shubha tug‘ilganda uni ochmasligi va zarur bo‘lsa, mas’ul shaxsga xabar berishi kerak. Agar akkaunt xavfsizligi buzilgan bo‘lsa, parolni almashtirish, faol seanslarni tekshirish va tegishli yordamga murojaat qilish kabi choralarni bilishi lozim.

Muammoli ta’lim bu jarayonda alohida ahamiyat kasb etadi. O‘quvchiga tayyor qoida berish o‘rniga, uni fikrlashga undaydigan vaziyat taqdim etiladi. Masalan: “Do‘stingiz ijtimoiy tarmoq orqali sizga noma’lum fayl yubordi va uni darhol ochishingizni so‘radi. Siz qanday yo‘l tutasiz?” O‘quvchilar vaziyatni muhokama qilib, xavfni aniqlaydilar va asoslangan qaror chiqaradilar. Bunday mashg‘ulotlar nazariy bilimlarni kundalik hayot bilan bog‘lash imkonini beradi.

Shuningdek, gamifikatsiya metodidan foydalanish ham samarali hisoblanadi. “Kiberxavfsizlik bilimdoni” musobaqasida o‘quvchilarga turli vaziyatlar berilib, ular xavfsiz va xavfli harakatlarni ajratadilar. Har bir to‘g‘ri javob uchun ball beriladi. Bu jarayon o‘quvchilarni faol ishtirok etishga undaydi va mavzuni qiziqarli o‘zlashtirishga yordam beradi.

Loyiha asosida o‘qitishda esa o‘quvchilar “Xavfsiz internet — mening tanlovim” mavzusida plakat, buklet, taqdimot yoki qisqa videorolik tayyorlashlari mumkin. Bunda ular nafaqat o‘z bilimlarini mustahkamlaydilar, balki tengdoshlari orasida ham kiberxavfsizlik madaniyatini targ‘ib qilish imkoniyatiga ega bo‘ladilar.

Muhokama natijalari shuni ko‘rsatadiki, kiberxavfsizlikni o‘qitishning samaradorligi texnik vositalar soni bilan emas, balki o‘quvchining real vaziyatlarda xavfsiz qaror qabul qila olish darajasi bilan belgilanadi. Shu sababli informatika o‘qituvchisi darslarda nazariy tushuntirish, amaliy mashq, muammoli vaziyat va refleksiyani o‘zaro uyg‘unlashtirishi maqsadga muvofiq.

XULOSA

Xulosa qilib aytganda, informatika darslarida kiberxavfsizlik madaniyatini shakllantirish zamonaviy ta’limning muhim yo‘nalishlaridan biridir. Raqamli muhitda faoliyat yuritayotgan o‘quvchi nafaqat texnologiyalardan foydalanishni, balki ulardan xavfsiz, ongli va mas’uliyatli foydalanishni ham bilishi zarur.

Maqolada ko‘rib chiqilgan muammoli ta’lim, gamifikatsiya, loyiha asosida o‘qitish, amaliy mashqlar va vaziyatli tahlil kabi yondashuvlar o‘quvchilarning kiberxavfsizlikka oid bilimlarini hayotiy ko‘nikmalarga aylantirish imkonini beradi. Ayniqsa, shubhali xabarlarni aniqlash, kuchli parol yaratish, shaxsiy ma’lumotlarni himoya qilish va raqamli izni nazorat qilishga qaratilgan topshiriqlar darsning amaliy ahamiyatini oshiradi.

Kiberxavfsizlik madaniyatini shakllantirishda o‘qituvchi, ota-ona va ta’lim muassasasi hamkorligi ham muhim o‘rin tutadi. O‘quvchilarga xavfli vaziyatlarda muammoni yashirmasdan, ishonchli kattalarga murojaat qilish zarurligini tushuntirish lozim. Bunda jazolashdan ko‘ra, ogohlik, tushuntirish va to‘g‘ri yo‘l-yo‘riq ko‘rsatish ustuvor bo‘lishi kerak.

Demak, informatika ta’limida kiberxavfsizlikni izchil va amaliy yo‘naltirilgan holda o‘rgatish orqali raqamli savodxon, tanqidiy fikrlaydigan, shaxsiy ma’lumotlarini himoya qila oladigan hamda internetda mas’uliyat bilan faoliyat yuritadigan yoshlarni tarbiyalash mumkin. Xavfsiz raqamli kelajak, avvalo, bugun shakllanayotgan bilim va odatlardan boshlanadi.

FOYDALANILGAN ADABIYOTLAR

1. G‘aniyev S.K., G‘aniyev A.A., Xudoyqulov Z.T. Kiberxavfsizlik asoslari. – Toshkent, 2020. – 221 b.
2. G‘aniyev S.K., Karimov M.M., Tashev K.A. Axborot xavfsizligi. – Toshkent: Fan va texnologiya, 2017. – 372 b.
3. Whitman M.E., Mattord H.J. Principles of information security. – Cengage Learning, 2018. – 656 p.
4. Stallings W., Brown L. Computer security: Principles and practice. – Pearson, 2018. – 880 p.
5. Anderson R. Security Engineering: A guide to building dependable distributed systems. – Wiley, 2020. – 1232 p.
6. Moallem A. Cybersecurity awareness among students and faculty. – CRC Press, 2019. – 104 p.