



O'QUVCHILARDA KIBERXAVFSIZLIK MADANIYATINI SHAKLLANTIRISH

Amirqulov Farrux Musurmon o'g'li

Annotatsiya. Ushbu maqolada zamonaviy raqamli muhitda o'quvchilarda kiberxavfsizlik madaniyatini shakllantirishning ahamiyati va samarali pedagogik usullari yoritilgan. Internet, ijtimoiy tarmoqlar, elektron pochta, mobil ilovalar va turli raqamli xizmatlardan foydalanish jarayonida o'quvchilar duch kelishi mumkin bo'lgan asosiy kiberxavflar tahlil qilingan. Shuningdek, kuchli parollardan foydalanish, shaxsiy ma'lumotlarni himoya qilish, fishing xabarlarini aniqlash, noma'lum havolalardan ehtiyot bo'lish, ikki bosqichli autentifikatsiyadan foydalanish va raqamli muloqot madaniyatini shakllantirish bo'yicha tavsiyalar berilgan. Maqolada informatika darslarida amaliy mashg'ulotlar, muammoli vaziyatlar va interfaol metodlardan foydalanish orqali o'quvchilarning kiberxavfsizlik bo'yicha bilim va ko'nikmalarini rivojlantirish masalalari ko'rib chiqiladi.

Kalit so'zlar: kiberxavfsizlik, axborot xavfsizligi, raqamli xavfsizlik, internet, shaxsiy ma'lumotlar, fishing, parol, autentifikatsiya, raqamli madaniyat, informatika ta'limi.

Bugungi kunda internet va raqamli texnologiyalar inson hayotining ajralmas qismiga aylanib bormoqda. Ta'lim olish, muloqot qilish, axborot izlash, elektron xizmatlardan foydalanish va turli topshiriqlarni bajarishda raqamli vositalardan keng foydalanilmoqda. Raqamli texnologiyalarning imkoniyatlari kengaygani sari kiberxavfsizlik masalasi ham tobora muhim ahamiyat kasb etmoqda. Ayniqsa, internetdan faol foydalanadigan o'quvchilar turli kiberxavflarga duch kelishi mumkin. Shaxsiy ma'lumotlarning oshkor qilinishi, firibgarlik xabarlar, zararli dasturlar, soxta internet sahifalari, noma'lum havolalar va ijtimoiy muhandislik kabi tahdidlar foydalanuvchidan yetarli darajadagi raqamli savodxonlik va ehtiyotkorlikni talab qiladi. Shu sababli maktab va akademik litsey ta'limida o'quvchilarga nafaqat



kompyuter va internetdan foydalanish ko'nikmalarini, balki xavfsiz raqamli xulq-atvorni ham o'rgatish zarur.

Kiberxavfsizlik madaniyati tushunchasi

Kiberxavfsizlik madaniyati — insonning raqamli muhitda xavfsiz, mas'uliyatli va ongli ravishda faoliyat yuritishi uchun zarur bo'lgan bilim, ko'nikma, odat va xulq-atvorlar majmuasidir.

O'quvchida kiberxavfsizlik madaniyati shakllangan bo'lsa, u:

- shaxsiy ma'lumotlarini himoya qiladi;
- kuchli va noyob parollardan foydalanadi;
- noma'lum havolalarni ochishda ehtiyotkor bo'ladi;
- shubhali xabarlarini taniy oladi;
- begona shaxslarga maxfiy ma'lumotlarni bermaydi;
- qurilmalar va dasturlarni yangilab boradi;
- internetdagi axborotga tanqidiy yondashadi;
- raqamli muloqot qoidalariga rioya qiladi;
- o'zining va boshqalarning raqamli huquqlarini hurmat qiladi.

Demak, kiberxavfsizlik madaniyati faqat texnik bilimlar bilan chegaralanmaydi. U o'quvchining raqamli muhitdagi kundalik xatti-harakatlarini ham qamrab oladi.

O'quvchilar duch kelishi mumkin bo'lgan asosiy kiberxavflar

O'quvchilar internetdan foydalanish jarayonida turli xavflarga duch kelishlari mumkin.

Fishing

Fishing — foydalanuvchini aldash orqali maxfiy ma'lumotlarni qo'lga kiritishga qaratilgan usullardan biridir. Masalan, foydalanuvchiga bank, ijtimoiy tarmoq, elektron pochta yoki boshqa xizmat nomidan soxta xabar yuborilishi mumkin.

O'quvchilarga fishing xabarlarini aniqlashning asosiy belgilarini tushuntirish muhim:



- noma'lum yoki shubhali jo'natuvchi;
- g'alati internet manzili;
- shoshilinch harakat qilishga undash;
- maxfiy ma'lumotlarni so'rash;
- imlo yoki grammatik xatolar;
- noma'lum fayl yoki havolani ochishga undash.

O'quvchi bunday xabarga duch kelganda, avvalo uning haqiqiyligini tekshirishi kerak.

Zaif parollar; Oddiy va bir nechta xizmatlarda takroran ishlatiladigan parollar foydalanuvchi xavfsizligi uchun jiddiy xavf tug'diradi. Shuning uchun o'quvchilarga har bir muhim hisob uchun imkon qadar uzun, noyob va taxmin qilish qiyin bo'lgan parol yaratish zarurligini tushuntirish kerak. Parolni do'stlar, tanishlar yoki begona shaxslar bilan ulashmaslik ham kiberxavfsizlik madaniyatining muhim qismidir.

Zararli dasturlar: Internetdan noma'lum dasturlar, o'yinlar yoki fayllarni yuklab olish qurilmaga zararli dasturlar tushishiga sabab bo'lishi mumkin. Shuning uchun o'quvchilar dasturlarni ishonchli manbalardan yuklab olish, shubhali fayllarni ochmaslik va qurilmadagi xavfsizlik vositalaridan foydalanish qoidalarini bilishlari kerak.

Ijtimoiy muhandislik: Kiberjinoyatchilar har doim ham murakkab texnik usullardan foydalanmaydi. Ba'zan ular insonning ishonuvchanligi, qo'rquvi yoki qiziqishidan foydalanib, kerakli ma'lumotni o'z ixtiyori bilan berishga undaydi. Masalan, "Siz sovrin yutdingiz", "Hisobingiz bloklanadi", "Tezda ushbu havolaga kiring" kabi xabarlar foydalanuvchini shoshilinch qaror qabul qilishga majbur qilishi mumkin. O'quvchilarga bunday vaziyatlarda to'xtash, o'ylash va tekshirish odatini shakllantirish muhim.

Shaxsiy ma'lumotlarni himoya qilish: Kiberxavfsizlik madaniyatining asosiy tarkibiy qismlaridan biri shaxsiy ma'lumotlarni himoya qilishdir. O'quvchilarga



internetda quyidagi ma'lumotlarni ehtiyotkorlik bilan baham ko'rish kerakligini tushuntirish lozim:

- telefon raqami;
- uy manzili;
- shaxsiy hujjatlarga oid ma'lumotlar;
- login va parollar;
- hisob ma'lumotlari;
- real vaqt rejimidagi joylashuv;
- shaxsiy fotosurat va videolar.

O'quvchi internetga joylashtirilgan ma'lumot keyinchalik keng tarqalib ketishi mumkinligini anglab yetishi kerak.

Ikki bosqichli autentifikatsiyaning ahamiyati

Hisoblarni himoya qilishda ikki bosqichli autentifikatsiya qo'shimcha xavfsizlik qatlamini yaratadi. O'quvchilarga imkon qadar muhim hisoblarida ushbu funksiyadan foydalanish, tasdiqlash kodlarini boshqa shaxslarga bermaslik va xavfsizlik sozlamalarini muntazam tekshirish tavsiya etilishi mumkin. Bunda o'quvchi autentifikatsiya kodi yoki tasdiqlash xabari ham maxfiy ma'lumot ekanini tushunishi kerak.

Informatika darslarida kiberxavfsizlikni o'rgatish

Kiberxavfsizlikni faqat nazariy ma'lumotlar asosida o'rgatish yetarli emas. O'quvchi real vaziyatlarda qanday harakat qilishni amaliy mashg'ulotlar orqali o'zlashtirishi kerak.

Informatika darslarida quyidagi topshiriqlardan foydalanish mumkin:

1-topshiriq. "Fishingni aniqlang". O'quvchilarga bir nechta elektron xabar namunalari beriladi. Ularning qaysi biri shubhali ekanini aniqlash va o'z qarorini asoslash so'raladi.



2-topshiriq. “Xavfsiz parol”. O‘quvchilar kuchli parolning asosiy xususiyatlarini aniqlaydilar va turli parollarni xavfsizlik nuqtayi nazaridan taqqoslaydilar.

3-topshiriq. “Ishonish mumkinmi?” O‘quvchilarga turli internet vaziyatlari beriladi. Masalan: “Notanish shaxs sizga sovrin yutganingiz haqida xabar yubordi va havolaga kirishingizni so‘radi. Nima qilasiz?” O‘quvchilar o‘z harakatlarining ketma-ketligini tushuntiradilar.

4-topshiriq. “Raqamli iz”. O‘quvchilar internetga joylashtirilgan ma’lumotlarning uzoq vaqt davomida saqlanib qolishi va tarqalishi mumkinligi haqida fikr yuritadilar. Bunday topshiriqlar nazariy bilimlarni amaliy ko‘nikmaga aylantirishga yordam beradi.

Muammoli ta’lim va kiberxavfsizlik

Kiberxavfsizlikni o‘rgatishda muammoli ta’lim metodidan foydalanish ayniqsa samarali. O‘qituvchi o‘quvchilarga tayyor qoidani berish o‘rniga muammoli vaziyatni taqdim etadi. Masalan: “Do‘stingizning ijtimoiy tarmoqdagi akkauntidan sizga pul so‘rab xabar keldi. Xabar odatdagidan boshqacha yozilgan. Siz qanday yo‘l tutasiz?” O‘quvchilar vaziyatni tahlil qilib, akkaunt egasi bilan boshqa aloqa vositasida bog‘lanish, xabarning haqiqiyligini tekshirish va shoshilinch harakat qilmaslik kabi yechimlarni taklif qilishlari mumkin. Bu usul o‘quvchining nafaqat bilimini, balki real vaziyatda to‘g‘ri qaror qabul qilish qobiliyatini ham rivojlantiradi.

Ota-ona va maktab hamkorligi

O‘quvchilarda kiberxavfsizlik madaniyatini shakllantirish faqat informatika o‘qituvchisining vazifasi emas. Bu jarayonda ota-onalar va ta’lim muassasasining hamkorligi muhim.

Ota-onalar farzandlari bilan:

- internetdan xavfsiz foydalanish;
- shaxsiy ma’lumotlarni himoya qilish;
- noma’lum shaxslar bilan muloqot;



- shubhali havolalar;
- ijtimoiy tarmoqlardagi xavfsizlik sozlamalari

haqida muntazam suhbatlashib turishlari maqsadga muvofiq. Bunda haddan tashqari taqiqlashdan ko'ra, o'quvchiga xavfni anglash va mustaqil ravishda to'g'ri qaror qabul qilishni o'rgatish samaraliroqdir.

Kiberxavfsizlik madaniyatini baholash

O'quvchilarning kiberxavfsizlik bo'yicha bilimlarini baholashda faqat testlardan foydalanish bilan cheklanmaslik kerak. Quyidagi mezonlardan foydalanish mumkin:

Ko'nikma Baholash mezonlari

Shubhali xabarni aniqlash Fishing belgilarini ajrata oladi

Parol xavfsizligi Kuchli va noyob parol tamoyillarini biladi

Shaxsiy ma'lumotlarni himoya qilish Qaysi ma'lumotlarni oshkor qilmaslik kerakligini biladi

Internetdagi muloqot Xavfsiz va mas'uliyatli muloqot qoidalariga rioya qiladi

Muammoli vaziyat Kiberxavf yuzaga kelganda to'g'ri harakatlar ketma-ketligini belgilaydi

Tanqidiy fikrlash Internetdagi axborotning ishonchliligini tekshira oladi

Bunday baholash o'quvchining real hayotdagi kiberxavfsizlik ko'nikmalarini aniqlashga yordam beradi.

Xulosa

Xulosa qilib aytganda, raqamli texnologiyalardan foydalanish ko'lami kengayib borayotgan sharoitda o'quvchilarda kiberxavfsizlik madaniyatini shakllantirish ta'limning muhim vazifalaridan biridir.

Kiberxavfsizlikni o'rgatish o'quvchiga faqat texnik qoidalarni yodlatishdan iborat bo'lmasligi kerak. Asosiy maqsad — o'quvchida xavfni oldindan anglash, ma'lumotni tekshirish, shoshilinch qaror qabul qilmaslik, shaxsiy ma'lumotlarni



himoya qilish va raqamli muhitda mas'uliyatli harakat qilish ko'nikmalarini shakllantirishdir.

Informatika darslarida muammoli vaziyatlar, amaliy topshiriqlar, rolli o'yinlar, real hayotiy misollar va interfaol metodlardan foydalanish kiberxavfsizlik bo'yicha bilimlarni amaliy ko'nikmalarga aylantirish imkonini beradi.

Shuningdek, maktab, o'qituvchi va ota-onalar o'rtasidagi hamkorlikni kuchaytirish o'quvchilarning xavfsiz raqamli muhitda faoliyat yuritishiga yordam beradi.

Demak, kiberxavfsizlik madaniyati — zamonaviy o'quvchining raqamli kompetensiyasining ajralmas qismi bo'lib, uni shakllantirish uzluksiz va tizimli pedagogik jarayon sifatida tashkil etilishi lozim.

FOYDALANILGAN ADABIYOTLAR

1. UNESCO. Guidance for Generative AI in Education and Research. — Paris: UNESCO, 2023.
2. NIST. Cybersecurity Framework (CSF) 2.0. — National Institute of Standards and Technology, 2024.
3. Council of Europe. Digital Citizenship Education Handbook.
4. European Union Agency for Cybersecurity (ENISA). Cybersecurity Education and Awareness Materials.
5. Axborot-kommunikatsiya texnologiyalari va kiberxavfsizlik bo'yicha ilmiy-uslubiy adabiyotlar.
6. Informatika fanini o'qitish metodikasiga oid o'quv-uslubiy materiallar.