Date: 17th May-2026

KIBERXAVFSIZLIK: SHAXSIY MA'LUMOTLAR QANCHALIK HIMOYALANGAN?

Raximkulova Madina Istamovna
Norbo'tayeva Dildora Erkin qizi
Sharof Rashidov tuman 3-son texnikumi o'qituvchilari

Annotatsiya: Mazkur maqolada raqamli jamiyatda shaxsiy ma'lumotlarning himoyalanish darajasi, kiberxavfsizlik madaniyati va foydalanuvchi mas'uliyati masalalari yoritiladi. Bugungi kunda ta'lim, bank, sog'liqni saqlash, davlat xizmatlari va ijtimoiy tarmoqlarda shaxsga doir ma'lumotlardan keng foydalanilmoqda. Bu esa ma'lumotlarni saqlash, qayta ishlash va uzatishda xavfsizlik choralarini kuchaytirishni talab qiladi. Maqolada shaxsiy ma'lumotlarning huquqiy himoyasi, kiberhujumlar xavfi, inson omili, texnik himoya vositalari hamda texnikum o'quvchilarida axborot xavfsizligi madaniyatini shakllantirish masalalari tahlil qilinadi.

Kalit so'zlar: kiberxavfsizlik, shaxsiy ma'lumotlar, axborot xavfsizligi, raqamli savodxonlik, parol xavfsizligi, fishing, ma'lumotlar sizib chiqishi, texnikum, raqamli madaniyat.

Kirish. Raqamli texnologiyalar inson hayotining deyarli barcha sohalariga kirib keldi. Bugun oddiy foydalanuvchi mobil telefon, bank kartasi, ijtimoiy tarmoq, elektron pochta, davlat xizmatlari portali va turli ilovalar orqali doimiy ravishda shaxsiy ma'lumotlaridan foydalanadi. Ism-familiya, telefon raqami, pasport ma'lumotlari, yashash manzili, bank kartasi, surat, biometrik belgi va hatto kundalik harakatlar haqidagi ma'lumotlar ham raqamli tizimlarda saqlanadi. Shu bois "shaxsiy ma'lumotlar qanchalik himoyalangan?" degan savol bugungi kunda nafaqat mutaxassislar, balki har bir fuqaro uchun dolzarb masalaga aylandi.

O'zbekiston Respublikasining "Shaxsga doir ma'lumotlar to'g'risida"gi Qonunida shaxsga doir ma'lumotlarga ishlov berish va ularni himoya qilish bilan bog'liq munosabatlar tartibga solinishi belgilangan. Ushbu qonun shaxsiy ma'lumotlar bilan ishlashda huquqiy asos mavjudligini ko'rsatadi, ammo amaliy himoya faqat qonun bilan emas, balki foydalanuvchi madaniyati, tashkilot mas'uliyati va texnik xavfsizlik choralariga ham bog'liq [1].

Shaxsiy ma'lumot tushunchasi va uning raqamli qiymati

Shaxsiy ma'lumot — bu ma'lum bir jismoniy shaxsni aniqlashga xizmat qiladigan axborotdir. Bunga ism-familiya, tug'ilgan sana, telefon raqami, elektron pochta, pasport ma'lumotlari, bank kartasi, IP-manzil, biometrik ma'lumotlar va ijtimoiy tarmoqdagi faoliyat ham kirishi mumkin. Avvallari bunday ma'lumotlar ko'proq qog'oz hujjatlarda saqlangan bo'lsa, bugun ular elektron bazalarda, bulutli servislar va mobil ilovalarda jamlanmoqda.

Shaxsiy ma’lumotlarning qiymati shundaki, ular orqali insonning moliyaviy holati, qiziqishlari, kasbi, yashash joyi va kundalik odatlari haqida tasavvur hosil qilish mumkin. Shu sababli kiberjinoyatchilar uchun shaxsiy ma’lumotlar oddiy raqamlar yoki matn emas, balki noqonuniy foyda olish vositasiga aylanishi mumkin. Masalan, telefon raqami orqali fishing xabarlari yuboriladi, elektron pochta orqali soxta havolalar tarqatiladi, bank kartasi ma’lumotlari esa moliyaviy firibgarlik uchun ishlatilishi mumkin.

O‘zbekiston qonunchiligida shaxsga doir ma’lumotlarni yig‘ish, tizimlashtirish, saqlash, o‘zgartirish, foydalanish va uzatish jarayonlari huquqiy tartibga solinadi. Qonunda shaxsga doir ma’lumotlar bilan ishlovchi operator va mulkdorlarning majburiyatlari mavjudligi ko‘rsatiladi [1]. Bu holat shuni anglatadiki, shaxsiy ma’lumotni himoya qilish faqat foydalanuvchining vazifasi emas, balki ta’lim muassasasi, korxona, bank, xizmat ko‘rsatuvchi tashkilot va davlat organlarining ham mas’uliyatidir.

Kiberxavfsizlik va shaxsiy ma’lumotlar himoyasining dolzarbligi

Kiberxavfsizlik — bu axborot tizimlari, tarmoqlar, qurilmalar va ma’lumotlarni noqonuniy kirish, o‘zgartirish, yo‘q qilish yoki o‘g‘irlashdan himoya qilishga qaratilgan chora-tadbirlar majmuasidir. Shaxsiy ma’lumotlar himoyasi esa kiberxavfsizlikning eng muhim yo‘nalishlaridan biridir. Chunki har qanday raqamli tizim oxir-oqibat inson haqidagi ma’lumot bilan ishlaydi.

IBMning 2025-yilgi “Cost of a Data Breach Report” hisobotida ma’lumotlar buzilishi bilan bog‘liq global o‘rtacha xarajat 4,4 million AQSH dollari ekani qayd etilgan [2]. Bu raqam yirik tashkilotlar misolida keltirilgan bo‘lsa-da, mazmunan oddiy foydalanuvchi uchun ham muhim xulosa beradi: ma’lumot yo‘qolishi yoki o‘g‘irlanishi nafaqat texnik muammo, balki iqtisodiy, huquqiy va ijtimoiy oqibatlarga olib keladigan xavfdir.

Shaxsiy ma’lumotlar xavfsizligi ayniqsa ta’lim muassasalari uchun ham dolzarb. Chunki texnikum, maktab, kollej va oliy ta’lim muassasalarida o‘quvchi-talabalar, ota-onalar va xodimlar haqidagi ma’lumotlar saqlanadi. Elektron jurnal, onlayn platforma, test tizimi, elektron pochta va bulutli hujjatlar bilan ishlashda ma’lumotlarning noto‘g‘ri tarqalishi yoki begona shaxs qo‘liga tushishi salbiy oqibatlarga sabab bo‘lishi mumkin.

Shaxsiy ma’lumotlar qanday xavf ostida qoladi?

Shaxsiy ma’lumotlar ko‘pincha murakkab texnik hujumlar orqali emas, balki oddiy ehtiyotsizlik natijasida xavf ostida qoladi. Masalan, bir xil parolni bir nechta saytda ishlatish, telefonni parolsiz qoldirish, noma’lum havolani bosish, soxta ilovani o‘rnatish, ijtimoiy tarmoqlarda ortiqcha ma’lumot joylashtirish yoki begona Wi-Fi tarmoqlaridan himoyasiz foydalanish shaxsiy ma’lumotlar sizib chiqishiga olib kelishi mumkin.

Verizon kompaniyasining 2025-yilgi Data Breach Investigations Report ijroiy xulosasida 22 052 ta xavfsizlik hodisasi va 12 195 ta tasdiqlangan ma’lumotlar buzilishi tahlil qilingani ko‘rsatilgan [3]. Bunday katta hajmdagi tahlillar shuni ko‘rsatadiki, kiberxavfsizlik muammosi alohida tashkilot yoki alohida davlat doirasidagi masala emas, balki global miqyosdagi xavfdir.

Ko‘plab buzilishlarda inson omili muhim rol o‘ynaydi. Fishing xabarlariga ishonish, soxta saytga login-parol kiritish, zaif parol tanlash yoki xavfsizlik yangilanishlarini o‘z vaqtida o‘rnatmaslik kiberjinoyatchilar uchun qulay imkoniyat yaratadi. Shu sababli kuchli texnik himoya vositalari mavjud bo‘lsa ham, foydalanuvchi xatolari xavfsizlikni zaiflashtirishi mumkin.

Fishing va ijtimoiy muhandislik xavfi

Fishing — bu foydalanuvchini aldash orqali uning login, parol, bank kartasi yoki boshqa maxfiy ma’lumotlarini qo‘lga kiritishga qaratilgan kiberhujum turidir. Fishing xabarlari odatda bank, davlat xizmati, yetkazib berish xizmati, ijtimoiy tarmoq yoki tanish tashkilot nomidan yuborilgandek ko‘rinadi. Xabarda “hisobingiz bloklandi”, “mukofot yutdingiz”, “zudlik bilan tasdiqlang” kabi shoshiltiruvchi iboralar bo‘ladi.

Bunday hujumlarning xavfli tomoni shundaki, ular texnik jihatdan murakkab bo‘lmasligi mumkin, ammo psixologik jihatdan kuchli ta’sir qiladi. Inson qo‘rqadi, shoshiladi yoki qiziqadi va natijada havolani bosadi. Shu sababli kiberxavfsizlik madaniyatida “har qanday havolaga ishonmaslik”, “manzilni tekshirish”, “SMS-kodni hech kimga bermaslik”, “bank xodimi parol so‘ramasligini bilish” kabi oddiy qoidalar juda muhim.

Texnikumlarda bu mavzuni o‘rgatishda real hayotga yaqin vaziyatlardan foydalanish samarali. Masalan, o‘quvchilarga ikki xil xabar beriladi: biri haqiqiy, ikkinchisi soxta. Ular qaysi xabar fishing ekanini aniqlaydi, sabablarini tushuntiradi va xavfsiz harakat algoritmini ishlab chiqadi. Bu usul nazariy bilimni amaliy hushyorlikka aylantiradi.

Parol xavfsizligi va ikki bosqichli himoya

Shaxsiy ma’lumotlarni himoya qilishda parol xavfsizligi eng oddiy, lekin eng muhim omillardan biridir. Zaif parollar — “123456”, “password”, tug‘ilgan sana, ism yoki telefon raqamidan iborat parollar — kiberjinoyatchilar tomonidan tez topilishi mumkin. Bundan tashqari, bitta parolni barcha akkauntlarda ishlatish ham xavfli. Agar bitta sayt buzilsa, boshqa akkauntlar ham xavf ostida qoladi.

Kuchli parol uzun, harflar, raqamlar va maxsus belgilar aralashmasidan iborat bo‘lishi kerak. Eng muhimi, har bir muhim xizmat uchun alohida parol ishlatish lozim. Ikki bosqichli autentifikatsiya esa qo‘shimcha himoya beradi. Bunda foydalanuvchi parolni kiritgandan so‘ng SMS-kod, autentifikator ilovasi yoki biometrik tasdiq orqali kirishni yakunlaydi.

Bu yerda shaxsiy fikr sifatida aytish mumkinki, ko‘pchilik foydalanuvchilar xavfsizlikni murakkab texnik ish deb o‘ylaydi. Aslida esa shaxsiy ma’lumotlarni himoya qilish ko‘p hollarda oddiy intizomdan boshlanadi: kuchli parol tanlash, qurilmani bloklash, shubhali xabarga javob bermaslik va ma’lumotni keraksiz joyga kiritmaslik.

Ta’lim muassasalarida shaxsiy ma’lumotlarni himoya qilish

Texnikumlarda shaxsiy ma’lumotlar bilan ishlash jarayoni alohida e’tibor talab qiladi. O‘quvchilar ro‘yxati, baholar, ota-onalar bilan aloqa ma’lumotlari, xodimlar hujjatlari, elektron platformalarga kirish ma’lumotlari va ichki hujjatlar begona shaxslar

qo‘liga tushmasligi kerak. Buning uchun ta’lim muassasasida hujjat aylanishi, elektron fayllarni saqlash, ruxsat darajalari va parol siyosati aniq tartibga solinishi zarur.

Shaxsga doir ma’lumotlar to‘g‘risidagi qonunchilik shaxsiy ma’lumotlarni qayta ishlash va himoya qilish jarayonida operatorlar uchun mas’uliyatni belgilaydi [1]. Bu talab ta’lim muassasalariga ham tegishli bo‘lishi mumkin, chunki ular ham o‘quvchi va xodimlarga oid ma’lumotlarni yig‘adi, saqlaydi va ulardan foydalanadi. Demak, ta’lim muassasalarida axborot xavfsizligi faqat informatika o‘qituvchisining vazifasi emas, balki butun jamoaning madaniyati bo‘lishi kerak.

Amaliy jihatdan ta’lim muassasasida quyidagi qoidalarga rioya qilish foydali: shaxsiy ma’lumotlarni umumiy guruhlarga tashlamaslik, parollarni o‘quvchilar yoki begona shaxslarga bermaslik, hujjatlarni ochiq kompyuterda qoldirmaslik, bulutli fayllarga kirish huquqini cheklash, antivirus va tizim yangilanishlarini o‘z vaqtida amalga oshirish. Bu choralar oddiy ko‘rinsa-da, ko‘plab xavflarning oldini oladi.

Shaxsiy ma’lumotlar qanchalik himoyalangan?

Bu savolga bir tomonlama javob berish qiyin. Huquqiy jihatdan shaxsiy ma’lumotlarni himoya qilishga oid qonunlar va tartiblar mavjud. Texnik jihatdan esa ko‘plab tizimlarda shifrlash, parol, autentifikatsiya, antivirus, zaxira nusxa va monitoring kabi himoya vositalari qo‘llaniladi. Biroq amaliyotda himoya darajasi har doim ham bir xil emas. Tizim qanchalik kuchli bo‘lmasin, foydalanuvchi ehtiyotsiz bo‘lsa, xavf saqlanib qoladi.

IBM hisobotida ma’lumotlar buzilishi xarajatlari va xavflari yirik tashkilotlar uchun ham dolzarb ekani ko‘rsatiladi [2]. Bundan kelib chiqadigan xulosa shuki, shaxsiy ma’lumotlar hech qachon “to‘liq xavfsiz” holatda deb qaralmasligi kerak. Eng to‘g‘ri yondashuv — doimiy ehtiyotkorlik, muntazam yangilanish, foydalanuvchilarni o‘qitish va xavfsizlik madaniyatini shakllantirishdir.

Shaxsiy fikrimcha, bugungi kunda ma’lumotlar himoyasining eng zaif nuqtasi texnologiya emas, balki insonning beparvoligidir. Odamlar ko‘pincha xavfsizlikni faqat muammo yuz bergandan keyin eslaydi. Holbuki, kiberxavfsizlik yong‘in xavfsizligiga o‘xshaydi: hodisa bo‘lgandan keyin emas, oldindan tayyorgarlik ko‘rilganda foyda beradi.

Shaxsiy ma’lumotlar himoyasi uch asosiy omilga bog‘liq: huquqiy tartib, texnik himoya va foydalanuvchi madaniyati. Huquqiy tartib shaxsiy ma’lumotlar bilan ishlash chegaralarini belgilaydi. Texnik himoya ma’lumotlarga ruxsatsiz kirishning oldini olishga xizmat qiladi. Foydalanuvchi madaniyati esa har bir insonning o‘z ma’lumotiga mas’uliyat bilan munosabatda bo‘lishini ta’minlaydi.

Agar ushbu uch omildan biri zaif bo‘lsa, umumiy himoya darajasi pasayadi. Masalan, qonun mavjud, lekin tashkilotda parol siyosati bo‘lmasa, xavf ortadi. Yoki tizim kuchli himoyalangan, lekin foydalanuvchi fishing havolasiga kirsa, ma’lumotlar baribir xavf ostida qoladi. Shu sababli kiberxavfsizlikda “bitta yechim hammasini hal qiladi” degan qarash noto‘g‘ri.

Texnikum o‘qituvchilari uchun bu mavzuning tarbiyaviy ahamiyati ham katta. O‘quvchilarga shaxsiy ma’lumotlarni himoya qilishni o‘rgatish orqali ularda raqamli

mas’uliyat, ehtiyotkorlik va tanqidiy fikrlash ko‘nikmalari shakllanadi. Bugungi o‘quvchi ertaga bank xizmatidan, davlat portalidan, onlayn ta’limdan va ish joyidagi axborot tizimlaridan foydalanadi. Demak, kiberxavfsizlik bo‘yicha berilgan bilim uning kundalik hayotida bevosita kerak bo‘ladi.

Xulosa qilib aytganda, shaxsiy ma’lumotlar raqamli davrning eng muhim qadriyatlaridan biriga aylandi. Ularni himoya qilish faqat mutaxassislar yoki davlat tashkilotlarining vazifasi emas, balki har bir foydalanuvchining kundalik mas’uliyatidir. O‘zbekiston qonunchiligida shaxsga doir ma’lumotlarni himoya qilish huquqiy jihatdan tartibga solingan, xalqaro amaliyot esa ma’lumotlar sizib chiqishi global xavf ekanini ko‘rsatmoqda.

Shaxsiy ma’lumotlar qanchalik himoyalanganligi foydalanuvchining bilimiga, tashkilotning mas’uliyatiga va texnik vositalarning to‘g‘ri qo‘llanishiga bog‘liq. Kuchli parol, ikki bosqichli autentifikatsiya, ehtiyotkorlik, shubhali havolalardan saqlanish, qurilmalarni yangilab borish va axborot xavfsizligi qoidalariga amal qilish shaxsiy ma’lumotlarni himoya qilishning asosiy shartlaridir.

Texnikumlarda kiberxavfsizlik mavzusini amaliy misollar, real vaziyatlar va muammoli topshiriqlar orqali o‘rgatish o‘quvchilarda raqamli madaniyatni shakllantiradi. Bu esa nafaqat ta’lim jarayoni, balki jamiyatning umumiy axborot xavfsizligi uchun ham muhim ahamiyatga ega.

FOYDALANILGAN ADABIYOTLAR:

1. O‘zbekiston Respublikasining “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonuni. — O‘RQ-547-son, 02.07.2019. — Lex.uz.
2. IBM Security. **Cost of a Data Breach Report 2025**. — IBM, 2025.
3. Verizon. **2025 Data Breach Investigations Report: Executive Summary**. — Verizon Business, 2025.
4. IBM. **What Is a Data Breach?** — IBM Think, 2025.
5. O‘zbekiston Respublikasi qonunchilik ma’lumotlari milliy bazasi. **Shaxsga doir ma’lumotlar to‘g‘risida**. — Lex.uz.