Kiberxavfsizlik, Onlayn ma’lumotlaringizni qanday himoya qilish mumkin?

Nazarov Farhod O‘sar o’g’li
Toshkent transport universiteti
Transportda axborot tizimlari va texnologiyalari kafedirasi asistenti

Annotatsiya: *Ushbu maqola kiberxavfsizlikning raqamli texnologiyalardagi o‘rni va ahamiyatini ko‘rib chiqadi. Kiberxavfsizlik ma’lumotlarni himoya qilish, ish faoliyatini davom ettirish va iste’molchilar ishonchini oshirishga xizmat qiladi. Maqolada internet, bulutli xizmatlar va mobil qurilmalar doirasida xavfsizlikni ta’minlash usullari muhokama qilinadi. Kiberxavfsizlikni ta’minlash uchun zarur bo’lgan qadamlar, jumladan xavfsizlik siyosatini ishlab chiqish va xodimlarni o‘qitish taklif etiladi. Xulosa qilib, maqola kiberxavfsizlikning raqamli muhitda muvaffaqiyat uchun muhim ekanligini ta’kidlaydi.*

Abstract: *This article examines the role and importance of cybersecurity in digital technologies. Cybersecurity serves to protect data, maintain business continuity, and increase consumer confidence. The article discusses methods for ensuring security within the Internet, cloud services, and mobile devices. It suggests steps to ensure cybersecurity, including developing a security policy and training employees. In conclusion, the article emphasizes that cybersecurity is essential for success in the digital environment.*

Kalit so’zlar: *Kiberxavfsizlik, raqamli texnologiyalar, ma’lumotlarni himoya qilish, internet, bulutli xizmatlar, mobil qurilmalar, xavfsizlik siyosati, xodimlarni o’qitish, kiberhujumlar, tarmoq xavfsizligi, iste’molchilar ishonchi, antivirus dasturlari, shifrlash texnologiyalari.*

Keywords: *Cybersecurity, digital technologies, data protection, internet, cloud services, mobile devices, security policy, employee training, cyberattacks, network security, consumer trust, antivirus software, encryption technologies.*

Kirish

Raqamli texnologiyalarning keng tarqalishi bilan birga, internet foydalanuvchilari uchun axborot xavfsizligi tobora dolzarb masalaga aylanmoqda. Bugungi kunda odamlar shaxsiy ma’lumotlari, moliyaviy axborotlari, tibbiy yozuvlari va professional faoliyatiga oid hujjatlarni turli onlayn platformalarda saqlamoqdalar. Ushbu ma’lumotlarning xavfsizligini ta’minlash, ularni ruxsatsiz kirish, o‘g‘irlash, buzish yoki yo‘q qilishdan himoya qilish kiberxavfsizlikning asosiy vazifasidir. Ushbu maqolada kiberxavfsizlik tushunchasi, tahdid turlari, himoyalanish usullari, xalqaro va mahalliy tajriba, hamda kiberxavfsizlik madaniyatining ahamiyati tahlil qilinadi.

Ushbu maqolada kiberxavfsizlik onlayn ma’lumotlaringizni qanday himoya qilishi mumkin mavzusi ko’rib chiqiladi. Maqola kiberxavfsizlik masalalariga to’g’ri yondashish, bu masalalarning dolzarbligini va raqamli muhitda xavfsiz

hayot kechirish uchun zarur choralarni ko’rish muhimligini ta’kidlaydi. Kiberxavfsizlik bo’yicha ogohlikni oshirish, zamonaviy texnologiyalarni qo’llash va samarali xavfsizlik siyosatini ishlab chiqish kiberhujumlarning oldini olishda muhim ahamiyatga ega.

Kiberxavfsizlik tushunchasi

Kiberxavfsizlik — bu raqamli tizimlar, tarmoqlar, foydalanuvchi qurilmalari va ularning ma’lumotlarini himoya qilishga qaratilgan chora-tadbirlar majmuasidir. Bu soha nafaqat texnik vositalarni o‘z ichiga oladi, balki ijtimoiy, psixologik va huquqiy omillarni ham qamrab oladi. Kiberxavfsizlik uchta asosiy tamoyilga tayanadi: maxfiylik (confidentiality), butunlik (integrity) va mavjudlik (availability). Mazkur tamoyillar asosida har qanday axborotni himoya qilish strategiyasi ishlab chiqiladi.

Kiberxavflar turlari

Zamonaviy tahdidlar turli shakllarda namoyon bo‘ladi. Ular quyidagilardan iborat:

- Zararli dasturlar (malware): viruslar, trojanlar, spyware va ransomware kabi dasturlar qurilmalarga zarar yetkazish yoki ma’lumotlarni o‘g‘irlash maqsadida ishlatiladi.
- Fishing: foydalanuvchini aldash orqali maxfiy ma’lumotlarni (parol, bank rekvizitlari) olishga qaratilgan soxta elektron pochta yoki veb-sahifalardan foydalaniladi.
- DDoS hujumlar: serverlarga ortiqcha so‘rov yuborib, ularning faoliyatini izdan chiqaradi.
- Ijtimoiy muhandislik: inson psixologiyasidan foydalanib, foydalanuvchini o‘z ma’lumotlarini oshkor qilishga undash.
- Tarmoqqa ruxsatsiz kirish: zaif parollar yoki xavfsizlik teshiklaridan foydalanib, foydalanuvchi tizimlariga kirish.
- Shifrlash asosidagi tovlamachilik: muhim fayllar shifrlanadi va ularni qayta ochish uchun foydalanuvchidan pul talab qilinadi.

Parollar va autentifikatsiya

Kiberxavfsizlikning birinchi darajadagi himoyasi — bu kuchli va xavfsiz parol tizimidir. Parollar kamida 12 belgidan iborat bo‘lishi, katta va kichik harflar, raqamlar va maxsus belgilarni o‘z ichiga olishi lozim. Har bir xizmat uchun alohida parol ishlatish, parol menejerlaridan foydalanish va har 3-6 oyda yangilash tavsiya etiladi. Shuningdek, ikki faktorli autentifikatsiya (2FA) orqali tizimga kirish yanada xavfsizlashtiriladi.

Shaxsiy ma’lumotlarni himoya qilish

Foydalanuvchilar o‘z shaxsiy ma’lumotlarini faqat ishonchli veb-saytlar yoki ilovalarda kiritishlari kerak. Ijtimoiy tarmoqlarda ortiqcha ma’lumot joylashtirmaslik, profil maxfiylik sozlamalarini ehtiyotkorlik bilan tanlash zarur. Geolokatsiya, telefon raqami yoki manzil kabi axborotlar oshkoralik xavfini oshiradi. Ma’lumotlarni shifrlash, foydalanuvchi ruxsatlarini nazorat qilish va ilovalarni doimiy yangilab borish muhimdir.

Jamoaviy tarmoqlarda xavfsizlik

Ochiq Wi-Fi tarmoqlari, masalan, aeroport, kafelarda mavjud internetga ulanish tarmoqlari ko‘pincha himoyasiz bo‘ladi. Bunday tarmoqlarda maxfiy ma’lumotlar almashish tavsiya etilmaydi. VPN (Virtual Private Network) texnologiyasi yordamida internet aloqasi shifrlanadi va foydalanuvchining IP manzili yashiriladi, bu esa xavfsizlikni oshiradi.

Mobil qurilmalar xavfsizligi

Mobil qurilmalar bizning kundalik hayotimizda muhim rol o‘ynaydi. Ularni himoyalash quyidagicha amalga oshiriladi:

- Qurilmani parol, barmoq izi yoki yuzni tanish orqali himoyalash.
- Ilovalarni faqat rasmiy manbalardan yuklab olish.
- Antivirus dasturlarini o‘rnatish.
- Ilova ruxsatlarini doimiy tekshirib turish.
- Bluetooth va geolokatsiyani ishlatilmaganda o‘chirib qo‘yish.

Kiberxavfsizlikda xalqaro va mahalliy tajriba

Xalqaro miqyosda ko‘plab qonunlar va me’yorlar mavjud. Masalan:

- GDPR — Yevropa Ittifoqida shaxsiy ma’lumotlarni himoya qilish qonuni.
- CCPA — Kaliforniyada qabul qilingan iste’molchilarning maxfiylik huquqlarini mustahkamlovchi qonun.
- ISO/IEC 27001 — axborot xavfsizligi boshqaruv tizimi standarti.

O‘zbekistonda ham ushbu yo‘nalishda muhim ishlar amalga oshirilmoqda. “Shaxsiy ma’lumotlar to‘g‘risida”gi Qonun qabul qilingan. “Raqamli O‘zbekiston — 2030” strategiyasi doirasida axborot xavfsizligini mustahkamlash choralari ko‘rilmoqda. CERT O‘zbekistan — bu kompyuter insidentlariga tezkor javob beruvchi milliy guruh bo‘lib, tahdidlarga qarshi chora-tadbirlarni amalga oshiradi.

Kiberxavfsizlik madaniyatini shakllantirish

Texnologik vositalardan tashqari, kiberxavfsizlik madaniyati ham muhim ahamiyatga ega. Har bir foydalanuvchi o‘zining onlayn xatti-harakatlariga e’tiborli bo‘lishi, xavfsizlik qoidalariga amal qilishi kerak. Maktab, kollej va universitetlarda kiberxavfsizlik asoslarini o‘rgatish, korxonalarda treninglar tashkil etish va xodimlar xabardorligini oshirish orqali jamiyatda umumiy xavfsizlik darajasi oshiriladi.

Xulosa

Zamonaviy raqamli muhitda kiberxavfsizlik nafaqat texnik muammo, balki ijtimoiy, huquqiy va madaniy masaladir. Har bir foydalanuvchi o‘z raqamli hayotini xavfsiz yuritish uchun shaxsiy mas’uliyatni his qilishi kerak. Kuchli parollar, ehtiyotkorlik, yangilanishlar, autentifikatsiya va foydalanuvchi madaniyati — bu xavfsizlikning asosiy unsurlaridir. Shaxsiy ma’lumotlaringizni himoya qilish orqali siz o‘zingizni va jamiyatni raqamli tahdidlardan asraysiz.

Tashkilotlar va individual foydalanuvchilar kiberxavfsizlikni ta’minlash uchun o’zaro hamkorlikda ishlashlari lozim. Kiberxavfsizlikni oshirishda har bir shaxs va tashkilotning roli muhimdir, chunki bu nafaqat texnologik masala, balki ijtimoiy va iqtisodiy barqarorlikni ta’minlash uchun zaruriy shartdir. Kiberxavfsizlik sohasida

amalga oshirilgan tadqiqotlar, mavjud muammolarni hal qilishga va raqamli muhitda xavfsizlikni ta’minlashga xizmat qiladi.

FOYDALANILGAN ADABIYOTLAR:

1. Abdullayeva. G. (2020). “Kiberxavfsizlik: Dolzarb muammolar va yechimlar”.
O’zbekiston Respublikasi Xalq ta’limi vazirligi nashrlari.
2. Buxoriy. I. (2021). “Raqamli dunyoda xavfsizlikni ta’minlash”. *Xavfsizlik va muhofaza* jurnali, 4(2), 34-45.
3. Khalilov. R. (2019). “Kiberxavfsizlik va uning ahamiyati”. *Zamonaviy texnologiyalar* jurnali, 3(1), 12-20.
4. Mirzayeva. D. (2022). “Raqamli texnologiyalarda kiberhujumlar”.
O’zbekiston ilm-fan va texnologiyalar jurnali, 5(3), 56-63.
5. Saidov. A. (2023). “Kiberxavfsizlikni ta’minlashda innovatsion yechimlar”.
Ma’lumotlar xavfsizligi jurnali, 6(1), 22-30.
6. Toshpulatov.S. (2020). “Kiberhujumlar va ularga qarshi kurash usullari”.
Iqtisodiyot va xavfsizlik jurnali, 4(2), 18-25.
7. Xudoyberganov.A. (2021). “Kiberxavfsizlik siyosati va uning amalga oshirilishi”. *O’zbekiston ta’lim tizimi* jurnali, 2(1), 40-48.