

“KIBERXAVFSIZLIK VA AXBOROTNI HIMOYA
LASHNING ZAMONAVIY MUAMMOLARI”

QAHHOROVA NILUFAR QODIR QIZI

Qarshi davlat texnika universiteti raqamli

texnologiyalar va sun'iy intellekt fakulteti

kompyuter injiniringi 2-kurs talabasi

SHAHLO ULASHEVA

“Kompyuter tizimlarining dasturiy va texnika ta'minoti”

*Raqamli texnologiyalar va sun'iy intellekt fakultet, Xotin-qizlar masalalari
bo'yicha dekan maslahatchisi*

ANNOTATSIYA

Ushbu maqolada kiberxavfsizlik tushunchasi, uning axborot texnologiyalari rivojidadagi o'rni hamda axborotni himoyalashning zamonaviy usullari yoritib berilgan. Internet tarmog'ida yuzaga kelayotgan tahdidlar, kiberhujum turlari va ulardan himoyalalanish yo'llari tahlil qilinadi. Shuningdek, kiberxavfsizlik sohasida mutaxassislar tayyorlashning ahamiyati haqida fikr yuritiladi.

Kalit so'zlar:

kiberxavfsizlik, axborot xavfsizligi, zararli dasturlar, kiberhujumlar, ma'lumotlarni himoyalash, internet xavfsizligi, raqamli texnologiyalar.

KIRISH:

Axborot texnologiyalari jadal rivojlanayotgan hozirgi davrda kiberxavfsizlik masalasi dolzarb muammolardan biriga aylandi. Internet va raqamli texnologiyalardan

keng foydalanish axborot almashinuvi imkoniyatlarini oshirgan bo'lsa-da, bu bilan birga turli kiberxavflarni ham yuzaga keltirdi. Shu sababli axborotni himoyalash va kiberxavfsizlikni ta'minlash har bir tashkilot va foydalanuvchi uchun muhim vazifa hisoblanadi.

ASOSIY QISM

1. Kiberxavfsizlik tushunchasi va mohiyati

Kiberxavfsizlik — bu kompyuter tizimlari, tarmoqlar va ma'lumotlarni ruxsatsiz kirish, buzish yoki o'g'irlashdan himoyalashga qaratilgan chora-tadbirlar majmuasidir. Kiberxavfsizlik axborotning maxfiyligi, yaxlitligi va mavjudligini ta'minlashga xizmat qiladi.

2. Kiberxavflar va ularning turlari

Bugungi kunda eng ko'p uchraydigan kiberxavflarga quyidagilar kiradi:

- viruslar va zararli dasturlar
- fishing (soxta xabarlar orqali ma'lumot o'g'irlash)
- parollarni buzish
- ma'lumotlarni noqonuniy nusxalash
- xizmat ko'rsatishni rad etish hujumlari (DDoS)

Ushbu tahdidlar shaxsiy va korporativ ma'lumotlarga jiddiy zarar yetkazishi mumkin.

3. Axborotni himoyalash usullari

Axborotni himoyalash uchun bir qator texnik va tashkiliy choralar qo'llaniladi. Kuchli parollardan foydalanish, ikki bosqichli autentifikatsiya, antivirus dasturlar, shifrlash texnologiyalari va muntazam yangilanishlar kiberxavfsizlikni ta'minlashda muhim rol o'ynaydi.

4. Kiberxavfsizlik va jamiyat

Kiberxavfsizlik nafaqat tashkilotlar, balki oddiy foydalanuvchilar uchun ham muhimdir. Ijtimoiy tarmoqlar, onlayn to'lovlar va elektron xizmatlardan xavfsiz foydalanish axborot madaniyatini shakllantirishni talab qiladi. Yoshlar orasida kiberxavfsizlik bo'yicha bilimlarni oshirish dolzarb masaladir.

5. Kiberxavfsizlik sohasining kelajagi

Kelajakda raqamli texnologiyalar yanada rivojlanishi bilan kiberxavfsizlikka bo'lgan talab ham oshadi. Sun'iy intellekt asosidagi xavfsizlik tizimlari, avtomatik tahdid aniqlash vositalari keng qo'llanilishi kutilmoqda. Shu bilan birga, kiberxavfsizlik mutaxassislariga ehtiyoj ortib boradi.

XULOSA

Xulosa qilib aytganda, kiberxavfsizlik zamonaviy axborot jamiyatining ajralmas qismidir. Axborotni himoyalash, kiberxavflarning oldini olish va xavfsiz raqamli muhit yaratish bugungi kunning muhim vazifalaridan biridir. Kiberxavfsizlikni ta'minlash orqali axborot texnologiyalaridan samarali va ishonchli foydalanish mumkin.

FOYDALANILGAN ADABIYOTLAR:

1. Stallings, U. **Shifrlash va tarmoq xavfsizligi: prinsiplari va amaliyoti**. Pearson Education, 2017.
2. Whitman, M. E., & Mattord, H. J. **Axborot xavfsizligi prinsiplari**. Cengage Learning, 2018.
3. Anderson, R. **Xavfsizlik muhandisligi: ishonchli tarqatilgan tizimlarni yaratish bo'yicha qo'llanma**. Wiley, 2020.
4. Schneier, B. **Amaliy shifrlash**. John Wiley & Sons, 2015.
5. Kahn Academy. **Internet xavfsizligi va kiberxavfsizlik asoslari**.
6. Cisco Networking Academy. **Kiberxavfsizlikka kirish**.