ISSN 3060-4567

KIBERXAVFSIZLIK VA MA’LUMOTLARNI HIMOYA QILISH USULLARI

Yo’ldasheva E’zoza Akramjon qizi

Namangan viloyati Chust tuman 3-son poletexnikum Informatika va axborot texnologiyalari fani o’qituvchisi

Annotatsiya: *Zamonaviy raqamli dunyoda axborot va ma'lumotlar har bir sohada asosiy resursga aylangan. Ularni himoya qilish, ruxsatsiz kirish va kiberhujumlardan asrash har qanday tashkilot va foydalanuvchi uchun dolzarb masala hisoblanadi. Shu sababli, kiberxavfsizlik tushunchasi va ma’lumotlarni himoya qilish usullari haqida bilimga ega bo‘lish har qachongidan ham muhimdir.*

Kiberxavfsizlikning asosiy yo‘nalishlari:

1.Tarmoq xavfsizligi – tarmoqlarni hujumlardan himoya qilish.

2.Axborot xavfsizligi – ma’lumotlarning maxfiyligi, yaxlitligi va mavjudligini ta’minlash.

3. Tizim xavfsizligi – kompyuter va server tizimlarining zaifliklarini himoya qilish.

4. Ilova xavfsizligi – dasturlardagi xatoliklar orqali kirishning oldini olish.

5. Bulutli xavfsizlik – bulut texnologiyalarida saqlanadigan ma’lumotlarni himoya qilish.

6. Foydalanuvchi xavfsizligi – oxirgi foydalanuvchilarni zararli dasturlardan va fishingdan himoya qilish.

Ma’lumotlarni himoya qilish usullari:

1. Shifrlash (Encryption) – ma’lumotlarni faqat ruxsat etilgan foydalanuvchi o‘qiy oladigan shaklga keltirish.

2. Avtentifikatsiya va avtorizatsiya – foydalanuvchini aniqlash va unga ruxsat berilgan resurslarga kirish huquqini berish.

3. Zaxira nusxalash – ma’lumotlarni yo‘qotilishining oldini olish uchun zaxira nusxalarini yaratish.

4. Antivirus va xavfsizlik devorlari – zararli dasturlarni aniqlash va to‘xtatish.

5. Tizimlarni yangilab borish – zaifliklarni bartaraf etish uchun doimiy yangilanishlar.

6. VPN – xavfsiz internet aloqasini ta’minlash.

7. Kirish huquqlarini cheklash – foydalanuvchilarga faqat kerakli resurslargina ruxsat berish.

Xulosa

Kiberxavfsizlik va ma’lumotlarni himoya qilish hozirgi texnologiyalar asrida eng muhim yo‘nalishlardan biri hisoblanadi. Ushbu sohada zamonaviy himoya choralari va yondashuvlarni to‘g‘ri qo‘llash, axborotning xavfsizligini ta’minlashga xizmat qiladi. Har bir foydalanuvchi va tashkilot ushbu bilimlarga ega bo‘lishi va amalda qo‘llashi zarur.

FOYDALANILGAN ADABIYOTLAR

1. Karimov, B. B. (2020). Axborot xavfsizligi asoslari. Toshkent: “Fan va texnologiya” nashriyoti.

2. Rakhimov, Sh. N. (2019). Kompyuter tarmoqlari va kiberxavfsizlik. Toshkent axborot texnologiyalari universiteti.

3. Stallings, W. (2021). Network Security Essentials: Applications and Standards (6th ed.). Pearson Education.

4. Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems (3rd ed.). Wiley.

5. ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements.

6. OWASP Foundation. (2024). Top 10 Web Application Security Risks. https://owasp.org

7. NIST. (2023). Cybersecurity Framework. https://www.nist.gov/cyb