KIBERXAVFSIZLIK VA MA'LUMOTLARNI HIMOYA QILISHNING ZAMONAVIY MUAMMOLARI VA YECHIMLARI

Mirvaliyeva Kamola Abdusattarovna,
Chilonzor tumani 1-son politexnikum,
Informatika va axborot texnologiyalari fani o'qituvchisi
kamolamirvaliyeva@gmail.com
998968671

Annotatsiya: *Mazkur ilmiy maqolada kiberxavfsizlik tushunchasi, ma'lumotlarni himoya qilishning dolzarbligi, zamonaviy kiberxavf-xatarlar, ularning turlari hamda axborot tizimlarini himoyalash usullari keng yoritilgan. Shuningdek, kriptografiya, autentifikatsiya, avtorizatsiya, tarmoq xavfsizligi va inson omilining kiberxavfsizlikdagi o'rni tahlil qilingan. Maqola raqamli texnologiyalar rivojlanayotgan hozirgi sharoitda axborot xavfsizligini ta'minlash muhimligini ilmiy asosda ochib beradi.*

Kalit so'zlar: *kiberxavfsizlik, axborot xavfsizligi, ma'lumotlarni himoya qilish, kiberhujum, kriptografiya, axborot tizimlari.*

Kirish

XXI asrda raqamli texnologiyalar jamiyat hayotining barcha sohalariga chuqur kirib bormoqda. Davlat boshqaruvi, ta'lim, sog'liqni saqlash, moliya, sanoat va kundalik hayotning aksariyat jarayonlari axborot texnologiyalariga bog'liq holda amalga oshirilmoqda. Shu bilan birga, raqamli muhitda ma'lumotlar hajmining keskin ortishi va ularning ochiq tarmoqlarda uzatilishi kiberxavfsizlik masalasini dolzarb muammoga aylantirmoqda.

Kiberxavfsizlik – bu axborot tizimlari, tarmoqlar va ma'lumotlarni ruxsatsiz kirish, buzish, o'zgartirish yoki yo'q qilishdan himoyalashga

qaratilgan chora-tadbirlar majmuasidir. Agar axborot yetarli darajada himoyalanmasa, bu katta moliyaviy zarar, maxfiy ma’lumotlarning oshkor bo‘lishi va jamiyat ishonchining yo‘qolishiga olib kelishi mumkin.

Shu sababli, kiberxavfsizlik va ma’lumotlarni himoya qilish masalalarini ilmiy jihatdan o‘rganish va samarali yechimlar ishlab chiqish bugungi kunda muhim vazifa hisoblanadi.

Kiberxavfsizlik tushunchasi va uning asosiy tamoyillari

Kiberxavfsizlik axborot xavfsizligining tarkibiy qismi bo‘lib, asosan raqamli muhitdagi tahdidlarga qarshi kurashishga qaratilgan. Axborot xavfsizligi uchta asosiy tamoyilga tayanadi:

1. **Maxfiylik (Confidentiality)** – ma’lumotlarga faqat ruxsat etilgan shaxslar kirishini ta’minlash.
2. **Butunlik (Integrity)** – ma’lumotlarning ruxsatsiz o‘zgartirilmasligi yoki buzilmasligini kafolatlash.
3. **Mavjudlik (Availability)** – axborot va tizimlardan kerakli vaqtda foydalanish imkoniyatini ta’minlash.

Ushbu tamoyillar buzilganda kiberxavfsizlik hodisalari yuzaga keladi. Masalan, maxfiylik buzilganda shaxsiy ma’lumotlar o‘g‘irlanadi, butunlik buzilganda ma’lumotlar soxtalashtiriladi, mavjudlik buzilganda esa tizimlar ishdan chiqadi.

Zamonaviy kiberxavf-xatarlar va ularning turlari

Bugungi kunda kiberxavf-xatarlar soni va murakkabligi ortib bormoqda. Ularning asosiy turlariga quyidagilar kiradi:

1. Zararli dasturlar (Malware)

Zararli dasturlar foydalanuvchi kompyuteriga yoki tarmog‘iga zarar yetkazish uchun yaratiladi. Ular viruslar, troyanlar, qurtlar (worm), josus dasturlar (spyware) va reklama dasturlarini (adware) o‘z ichiga oladi.

2. Fishing hujumlari (Phishing)

Fishing – foydalanuvchilarni aldash orqali ularning login, parol yoki bank ma’lumotlarini qo‘lga kiritishga qaratilgan hujum turi. Odatda soxta elektron pochta yoki veb-saytlar orqali amalga oshiriladi.

3. DDoS hujumlari

DDoS (Distributed Denial of Service) hujumlarida serverga juda ko‘p so‘rov yuborilib, uning ishlash qobiliyati izdan chiqariladi. Natijada tizim vaqtincha yoki butunlay faoliyatini to‘xtatadi.

4. Ichki tahdidlar

Kiberxavfsizlikka faqat tashqi hujumchilar emas, balki tashkilot ichidagi xodimlar ham tahdid solishi mumkin. Bilimsizlik, beparvolik yoki qasddan qilingan harakatlar jiddiy xavflarga olib keladi.

Ma’lumotlarni himoya qilish usullari

Ma’lumotlarni himoya qilish uchun turli texnik va tashkiliy choralar qo‘llaniladi. Ularning eng muhimlari quyidagilardan iborat:

Kriptografiya

Kriptografiya ma’lumotlarni shifrlash orqali himoyalash usulidir. Shifrlangan ma’lumotni faqat maxsus kalitga ega bo‘lgan shaxs o‘qishi mumkin. Bugungi kunda AES, RSA, SHA kabi kriptografik algoritmlar keng qo‘llaniladi.

Autentifikatsiya va avtorizatsiya

Autentifikatsiya – foydalanuvchining shaxsini tekshirish jarayoni bo‘lsa, avtorizatsiya – unga berilgan huquqlarni aniqlash jarayonidir. Kuchli parollar, ikki bosqichli autentifikatsiya (2FA) xavfsizlikni sezilarli darajada oshiradi.

Tarmoq xavfsizligi

Tarmoq xavfsizligi firewall, IDS/IPS tizimlari, VPN texnologiyalari yordamida ta’minlanadi. Bu vositalar tarmoq orqali ruxsatsiz kirishni cheklaydi va shubhali faoliyatni aniqlaydi.

Zaxira nusxalar (Backup)

Ma’lumotlarni muntazam zaxiralash kiberhujumlar yoki texnik nosozliklar oqibatida yo‘qotilgan ma’lumotlarni tiklash imkonini beradi.

Inson omili va kiberxavfsizlik

Ko‘plab tadqiqotlar shuni ko‘rsatadiki, kiberxavfsizlik hodisalarining katta qismi inson omili bilan bog‘liq. Foydalanuvchilarning xavfsizlik qoidalariga rioya qilmasligi, oddiy parollardan foydalanishi yoki shubhali havolalarni ochishi jiddiy muammolarga olib keladi.

Shu sababli, xodimlar va foydalanuvchilarni kiberxavfsizlik bo‘yicha muntazam o‘qitish, treninglar o‘tkazish va axborot madaniyatini oshirish muhim ahamiyatga ega.

Xulosa

Xulosa qilib aytganda, kiberxavfsizlik va ma’lumotlarni himoya qilish zamonaviy jamiyatning ajralmas qismi hisoblanadi. Raqamli texnologiyalar rivojlanishi bilan birga kiberxavf-xatarlar ham murakkablashib bormoqda. Shu sababli, axborot tizimlarini himoyalash uchun texnik, tashkiliy va huquqiy choralarni kompleks tarzda qo‘llash zarur.

Kriptografiya, autentifikatsiya, tarmoq xavfsizligi vositalari bilan bir qatorda inson omiliga alohida e’tibor qaratish kiberxavfsizlikni ta’minlashda muhim rol o‘ynaydi. Mazkur maqolada keltirilgan tahlillar kiberxavfsizlik sohasida ilmiy izlanishlar olib borish va amaliy yechimlar ishlab chiqishda foydali bo‘lishi mumkin.

FOYDALANILGAN ADABIYOTLAR

1. Stallings, W. **Cryptography and Network Security**. Pearson Education.
2. Anderson, R. **Security Engineering**. Wiley Publishing.
3. ISO/IEC 27001: Information Security Management Systems.
4. Pfleeger, C. P., Pfleeger, S. L. **Security in Computing**.
5. O‘zbekiston Respublikasi “Axborotlashtirish to‘g‘risida”gi Qonuni.