KOMPYUTER TARMOQLARIDA SHIFRLASH VA AUTENTIFIKATSIYA USULLARI

Jo’rabekova Xumora Muzaffar qizi
Toshkent davlat iqtisodiyot universiteti talabasi
jurabekovaxumora@gmail.com

Annotatsiya: *Ushbu tezisda kompyuter tarmoqlarida axborot xavfsizligini ta'minlashda qo‘llaniladigan asosiy texnologiyalar — **shifrlash** (kriptografiya) va **autentifikatsiya** usullari haqida batafsil ma'lumot beriladi. Shifrlash ma’lumotlarni uchinchi shaxslardan himoya qilish uchun kodlashni, autentifikatsiya esa foydalanuvchi yoki qurilmaning haqiqiyligini aniqlashni nazarda tutadi. Taqdimotda simmetrik, assimetrik va gibrid shifrlash usullari, shuningdek, parol asosidagi, ikki bosqichli va biometrik autentifikatsiya turlari tushuntirilgan. Xesh funksiyalar, MAC va raqamli imzolar kabi qo‘shimcha xavfsizlik mexanizmlari ham ko‘rib chiqilgan. Amaliyotda bu texnologiyalar bank, davlat idoralari, internet xizmatlari va tibbiyot tizimlarida keng qo‘llaniladi. Taqdimot oxirida ushbu texnologiyalarning zamonaviy axborot xavfsizligidagi ahamiyati ta'kidlanadi.*

Kalit so‘zlar: *shifrlash, autentifikatsiya, kompyuter tarmoqlari, axborot xavfsizligi, simmetrik shifrlash, assimetrik shifrlash, gibrid shifrlash, AES, RSA, parol autentifikatsiyasi, ikki bosqichli autentifikatsiya, biometrik autentifikatsiya, raqamli sertifikat, PKI, xesh funksiyalar, SHA-256, MAC, raqamli imzo, foydalanuvchi identifikatsiyasi, tarmoq xavfsizligi, PGP, HTTPS, OWASP, NIST*

Raqamli texnologiyalar rivoji bilan bir qatorda kompyuter tarmoqlari orqali axborot almashinuvi hajmi va tezligi ortmoqda. Bu esa o‘z navbatida axborotni himoyalash masalasini dolzarb qilmoqda. Axborot xavfsizligini ta’minlashda ikki muhim tushuncha – **shifrlash (kriptografiya)** va **autentifikatsiya (tasdiqlash)** markaziy o‘rinni egallaydi. Mazkur tezisda ushbu texnologiyalar mazmuni, turlari, qo‘llanilish sohalari va amaliy ahamiyati o‘rganiladi.

Shifrlash - bu axborotni faqat ruxsat etilgan shaxslar o‘qiy oladigan shaklga keltirish jarayoni bo‘lib, u ma’lumotlar uzatilishida yoki saqlanishida ishlatiladi. Shifrlash algoritmlari matematik asosda ishlab chiqilgan bo‘lib, ularning asosiy turlari quyidagilardir:

- Simmetrik shifrlash - bir xil kalit yordamida ma’lumotni shifrlash va yechish amalga oshiriladi. Bu usul tez ishlasa-da, kalitni uzatishda xavfsizlik muammosi yuzaga chiqadi. Misollar: AES, DES.
- Assimetrik shifrlash — ikkita kalit (ochiq va maxfiy) ishlatiladi. Ochiq kalit bilan shifrlangan ma’lumot faqat maxfiy kalit yordamida ochiladi. Bu usul yuqori xavfsizlik darajasini ta’minlaydi. Misol: RSA algoritmi.

- Gibrid shifrlash — simmetrik va assimetrik yondashuvlarni birlashtiradi. Avval kalitlar assimetrik tarzda almashiladi, keyin ma’lumot simmetrik tarzda shifrlanadi. Bu usul yuqori xavfsizlik va tezlikni birgalikda ta’minlaydi.

Autentifikatsiya — foydalanuvchi yoki qurilmaning shaxsini aniqlash va tasdiqlash jarayonidir. U quyidagi asosiy ko‘rinishlarda amalga oshiriladi:

- **Parol asosidagi autentifikatsiya** — foydalanuvchi login va parol orqali tizimga kiradi. Bu eng sodda usul bo‘lib, zaif himoya vositasidir.
- **Ikki bosqichli autentifikatsiya (2FA)** — paroldan tashqari telefon orqali yuborilgan kod yoki maxsus ilovadagi token orqali tasdiqlash. Bu xavfsizlikni sezilarli darajada oshiradi.
- **Biometrik autentifikatsiya** — foydalanuvchining barmoq izi, yuz ifodasi, ovozi yoki ko‘z qorachig‘i asosida aniqlash. Eng yuqori ishonchlilik darajasiga ega.
- **Raqamli sertifikatlar va PKI tizimi** — elektron identifikatsiya va xavfsiz aloqani ta’minlaydigan usul. U veb-saytlar, hukumat tizimlari va banklarda keng qo‘llaniladi.

Identifikatsiya va autentifikatsiya o‘rtasidagi farq shundaki, ko‘p hollarda bu ikki atama aralashtiriladi. Identifikatsiya — bu shunchaki foydalanuvchining kimligini bildirish (masalan, login kiritish), autentifikatsiya esa ushbu foydalanuvchining asl shaxs ekanini isbotlashdir (masalan, parol kiritish, SMS-kod orqali tasdiqlash). Autentifikatsiya identifikatsiyadan keyin keladi va xavfsizlik darajasini oshiradi.

Qo‘shimcha xavfsizlik texnologiyalari:

Xesh funksiyalar (hashing) — parollarni saqlashda ishlatiladi. Bu usul parollarni maxsus matematik formulalar orqali kodlab, orqaga qaytarilmas shaklda saqlash imkonini beradi.

MAC (Message Authentication Code) — xabar o‘zgarmaganini tekshiradi.

Raqamli imzolar — yuboruvchining haqiqiyligini va ma’lumotning yaxlitligini isbotlaydi.

Shifrlash va autentifikatsiya texnologiyalari quyidagi sohalarda keng qo‘llaniladi:

- Bank tizimlarida (internet-banking, to‘lov tizimlari)
- Davlat xizmatlarida (my.gov.uz, elektron hukumat)
- Onlayn ta’lim, sog‘liqni saqlash, tibbiy ma’lumotlar bazasida
- Mobil ilovalar, ijtimoiy tarmoqlar, elektron pochtalarda

Bu texnologiyalarsiz zamonaviy internet xizmatlarining xavfsizligi ta’minlanishi mumkin emas.

Xulosa. Shifrlash va autentifikatsiya texnologiyalari zamonaviy axborot xavfsizligi tizimining ajralmas bo‘lagidir. Ular yordamida foydalanuvchi va tizimlar o‘rtasidagi ma’lumotlar almashinuvi xavfsiz, ishonchli va nazorat ostida bo‘ladi. Shu bois har bir tashkilot, muassasa va alohida foydalanuvchi ushbu vositalardan foydalanishni o‘z odatiga aylantirishi zarur. Axborotning muhofazasi — bu raqamli xavfsizlikning kalitidir.

Foydalanilgan adabiyotlar:

1. S.K.Ganiyev, M.M.Karimov, K.A.Tashev, “*Axborot xavfsizligi*” - Nashriyot: Fan va texnologiya, Nashr yili: 2017
2. Yusupov T.A., Karimov R.A. *Axborot texnologiyalari va axborot xavfsizligi asoslari.* – Toshkent: Iqtisodiyot, 2020.
3. Ubaydullayev A.N. *Kompyuter tarmoqlari va ularning xavfsizligi.* – Toshkent: TDYU nashriyoti, 2019.
4. Ibragimov Sh.T. *Axborot xavfsizligi: nazariyasi va amaliyoti.* – Toshkent: Innovatsiya, 2022.
5. Xasanov O.K. *Kriptografiya asoslari.* – Toshkent: Fan va texnologiya, 2021.
6. Maxmudov A.B. *Kompyuter xavfsizligi va ma'lumotlarni himoyalash.* – Samarqand: SamDCHTI, 2020.