KODLASH VA SHIFRLASH USULLAR

Respublika musiqa va san'at texnikumi
Informatika fani o'qituvchisi
Namozova Lubat Baxrilloyevna

Annotatsiya: *Axborot insoniyat hayotida o‘ziga xos ahamiyat kasb etib, uning asosiy boyliklaridan biriga aylangan. Zamonaviy dunyoda axborot almashinuvi, uzatilishi, saqlanishi va himoyalanishi jarayonlari yanada murakkablashib bormoqda. Bu jarayonlarning asosi sifatida kodlash va shifrlash usullari tobora muhim o‘rin egallamoqda. Kodlash va shifrlash usullari axborotni turli ko‘rinishda o‘zgartirish, uni boshqa manbalardan himoya qilish va uzatishning asosiy vositalaridan biri hisoblanadi. Ushbu maqolada zamonaviy kodlash va shifrlash usullarining nazariy asoslari, ularning axborot xavfsizligidagi ahamiyati, hozirgi kunda qo‘llaniladigan asosiy texnikalar, shuningdek, ularning istiqbollari batafsil yoritiladi.*

Kalit so‘zlar: *Kodlash, shifrlash, axborot xavfsizligi, kriptografiya, simmetrik shifrlash, assimmetrik shifrlash, axborotni himoyalash, axborotni uzatish, zamonaviy texnologiyalar.*

Kodlash o‘z ma’nosiga ko‘ra, axborotni bir ko‘rinishdan boshqa ko‘rinishga o‘zgartirish jarayonidir. Bu jarayon odatda axborotni uzatishda yoki saqlashda sodir bo‘ladi. Kodlash yordamida insonlar uchun mo‘ljallangan axborot texnik vositalar uchun yaroqli shaklga keltiriladi yoki aksincha, texnik vositalar uchun mo‘ljallangan ma’lumot inson anglay oladigan holatga o‘tkaziladi. Kodlash usullari asosida ma’lumotlarning maxsus alifbolar, kodlar va belgilar orqali ifodalanishi yotadi. Axborot xavfsizligi borasida, kodlash yordamida uzatilayotgan ma’lumotning mazmunini, agar zarur bo‘lsa, begona shaxslar tushunmaydigan qilib o‘zgartirish ham mumkin. Shifrlash, o‘z navbatida, axborotni maxfiylash, uni faqat belgilangan qabul qiluvchigina anglaydigan ko‘rinishga keltirish usulidir. Shifrlashda maxfiy

kalit yoki qoidalar orqali ma’lumot o‘zgartiriladi. Axborot shifrlanib, “ochiq matn”dan “shifrlangan matn”ga aylantiriladi. Uni qayta o‘qish uchun shifrlashda ishlatilgan maxfiy metodlar yoki kalitlar zarur bo‘ladi. Shifrlash asosan axborotni begona va ruxsatsiz shaxslardan himoya qilish, ma’lumot almashinuvida ishonchli muhiti yaratish uchun qo‘llaniladi. Shifrlash usullarining samaradorligi bevosita shifrlash algoritmlarining murakkabligi, kalitlarning uzunligi va ularning maxfiyligiga bog‘liq [1].

Zamonaviy texnologiyalar taraqqiyoti natijasida axborot xavfsizligini ta’minlashda kodlash va shifrlashning ahamiyati yanada ortib bormoqda. Bugun turli elektron pochta tizimlari, internet xizmatlari, mobil aloqa vositalarida axborotni shifrlash keng qo‘llanilmoqda. Elektron to‘lov xizmatlarida mijozlarning shaxsiy va moliyaviy ma’lumotlari yuqori darajada shifrlanadi. Shuningdek, davlat organlari va harbiy sohada ham axborot maxfiyligini ta’minlashning asosi sifatida shifrlashdan keng foydalaniladi. Axborot xavfsizligining asosiy tamoyillaridan biri axborotga ruxsatsiz kirishni cheklash va maxfiylikni ta’minlash hisoblanadi. Shuning uchun ham shifrlash usullari doimo takomillashtirilmoqda va yangi algoritmlar ishlab chiqilmoqda [2].

Kodlash usullari orasida klassik va zamonaviy yondashuvlar mavjud. Klassik usullarga morze kodi, binar kod tizimlari, askiy kod va boshqalar kiradi. Bunday kodlar axborotni aniq mantiqiy qonunlar asosida boshqa belgilar tizimiga aylantirish imkonini beradi. Masalan, harf va raqamlarni nol va birlardan iborat qatorlarga aylantirish binar kodlash asosini tashkil qiladi. Kodlashning zamonaviy usullari esa murakkab matnli va multimedia axborotini ixcham va tez uzatish imkonini beradi. Raqamli televidenie, video va audio fayllarni siqib kodlash (masalan, MPEG, MP3) zamonaviy kodlash usullarining amaliy namunasidir. Shuningdek, axborot almashinuvida axborot hajmini kamaytirishga xizmat qiladigan siqish (kompressiya) kodlash usullari ham keng tarqalgan. Shifrlash usullari esa dastlab simmetrik va assimmetrik turlarga bo‘linadi. Simmetrik shifrlashda axborot bir xil kalit yordamida shifrlanadi va shu kalit orqali teskari deshifrlanadi. Ushbu yondashuv juda tezkor va

samarali hisoblanadi, lekin kalitlarni almashish jarayonida noqulayliklar mavjud bo‘lishi mumkin. Simmetrik shifrlash algoritmlariga DES, AES kabi usullar kiritiladi. Assimmetrik shifrlashda esa ikki xil kalit qo‘llaniladi: biri – ochiq kalit (public key), ikkinchisi – maxfiy kalit (private key). Ma’lumotni ochiq kalit bilan shifrlash mumkin, ammo uni qayta ochish faqat maxfiy kalit bilan amalga oshiriladi. Bunday algoritmlar, jumladan, RSA, ElGamal va boshqalar, katta axborot tarmoqlarida xavfsiz axborot almashish uchun ayni muddao hisoblanadi [3].

Zamonaviy kriptografiyada shifrlash algoritmlarining xavfsizligi kishilarning va tashkilotlarning axborotga bo‘lgan ishonchini ta’minlash vositasidir. Axborotni shifrlash yordamida moliyaviy operatsiyalar, shaxsiy yozishmalar, tijorat va harbiy sirlar, davlatga taalluqli maxfiy ma’lumotlarni himoyalash bugungi kunda ham dolzarb hisoblanadi. Shifrlash algoritmlarini tanlashda, ularning zamonaviy talab va ehtiyojlarga javob berishi, samaradorligi va ishonchliligi alohida ahamiyatga ega. Axborot xavfsizligining kuchayishi bilan birga, kodlash va shifrlash sohasiga yangi ilmiy-texnik yondashuvlar ham kirib kelmoqda. Algoritmlar va protokollarning murakkablashuvi borasida raqamli imzo, autentifikatsiya, sertifikatlash kabi vositalar ham ahamiyat kasb etmoqda. Bu esa axborot almashinuvi va saqlashda nafaqat maxfiylik, balki ishonchlilik va yaxlitlikni ta’minlash imkonini beradi [4].

Ma’lumotlar bazasi, bulutli texnologiyalar va axborot xizmati platformalarida ham kodlash va shifrlash usullari muhim ahamiyatga esa. Internet tarmog‘idagi har bir foydalanuvchi va tashkilot o‘z axborotining xavfsizligini ta’minlash uchun ushbu zamonaviy yondashuvlardan samarali foydalanishi talab etiladi. Hozirgi kunda kriptografik texnologiyalarning tez rivojlanishi kodlash va shifrlash sohasida yangi algoritm va protokollarning paydo bo‘lishiga sabab bo‘lmoqda. Shu bois, har bir soha mutaxassisi, axborot xavfsizliga mas’ul shaxs va foydalanuvchi kodlash va shifrlash usullarining nazariy va amaliy jihatlarini yaxshi o‘rganishi, ulardan to‘g‘ri foydalanish qoidalarini puxta egallashi lozim. Bu nafaqat

texnik-texnologik rivojlanishda, balki axborot madaniyatining yuqori bo‘lishida ham muhim rol o‘ynaydi [5].

Xulosa:

Xulosa qilib aytganda, kodlash va shifrlash usullari – axborotni himoya qilish, uni tez va ishonchli, xavfsiz shaklda uzatish va saqlashning eng muhim vositalaridan biri hisoblanadi. Ularning rivojlanishi va takomillashuvi shubhasiz informatsion jamiyat taraqqiyotiga xizmat qiladi. Zamonaviy axborot markazlari, moliyaviy institutlar, davlat tashkilotlari va boshqa ko‘plab sohalar faoliyati kodlash va shifrlash usullarisiz tasavvur qilib bo‘lmaydi. Yangi algoritmlar va texnologiyalar rivojlansada, asosiysi – axborot almashuvi xavfsiz, ishonchli va yuqori samarali bo‘lishi zarur. Ana shu omillar jamiyat informatsion taraqqiyotining poydevoriga aylanadi.

FOYDALANILGAN ADABIYOTLAR:

1. Abdullayev, S. (2019). Pedagogika va psixologiya asoslari. Toshkent: O‘qituvchi.
2. Gulomov, A. (2020). Boshlang‘ich ta’limda kommunikativ kompetensiyani rivojlantirish metodlari. Toshkent: Fan va texnologiya.
3. Kovalev, S. Yu. (2018). Kriptografiya asoslari. Moskva: INFRA-M.
4. Kamilova, N. (2021). O‘quvchilarda kommunikativ kompetensiyani rivojlantirish: nazariy va amaliy yondashuvlar. Toshkent: O‘zbekiston Milliy Universiteti nashriyoti.
5. Vygotsky, L. S. (1978). Mind in Society: The Development of Higher Psychological Processes. Cambridge, MA: Harvard University Press.
6. Stallings, W. (2016). Cryptography and Network Security. Pearson Education Limited.