RAQAMLI IMZO VA UNING QO‘LLANILISHI

Anvarjonova Muhlisa Abdurahim qizi

Namangan davlat texnika universiteti talabasi

tel:+998956261405

e-mail muhlisam1403@gmail.com

Xayrillaxo‘jayev Ismoilxo’ja Islomxo‘ja o‘g‘li

Namangan davlat texnika universiteti talabasi

tel: 97-466-01-23

e-mailxayrillaxojayevismoilxoja@gmail.com

O’qituvchi: ***N.Sayidov***

Namangan davlat texnika universiteti

Annotation

This paper analyzes the concept of digital signature, its working mechanism, and its importance in ensuring information security. With the rapid development of digital technologies, electronic document exchange has become widespread. Ensuring authenticity, integrity, and non-repudiation of electronic documents is a critical issue today. Digital signature technology, based on public key cryptography and hash functions, plays a significant role in electronic government systems, banking, and e-commerce. The advantages, challenges, and future development prospects of digital signature systems are also discussed.

Key words: digital signature, cryptography, information security, electronic document, authentication, public key infrastructure.

Annotatsiya

Mazkur ilmiy ishda raqamli imzo tushunchasi, uning ishlash mexanizmi, axborot xavfsizligidagi o‘rni va turli sohalardagi amaliy qo‘llanilishi batafsil tahlil qilinadi. Zamonaviy axborot-kommunikatsiya texnologiyalari rivojlanishi natijasida elektron hujjat almashinuvi keng ommalashdi. Elektron hujjatlarning haqiqiyligini ta’minlash, ularni qalbakilashtirish va o‘zgartirishdan himoya qilish dolzarb masalaga aylandi. Raqamli imzo aynan shu vazifani bajaruvchi muhim kriptografik vosita hisoblanadi. Ishda ochiq kalitli kriptografiya, xesh funksiyalar, elektron hukumat tizimlari, bank sohasi va elektron tijoratda raqamli imzoning qo‘llanilishi yoritilgan. Shuningdek, tizimning afzalliklari, muammolari va rivojlanish istiqbollari ham ko‘rib chiqilgan.

Kalit so‘zlar: raqamli imzo, elektron hujjat, kriptografiya, axborot xavfsizligi, autentifikatsiya, xesh funksiya, ochiq kalit, PKI.

So‘nggi yillarda dunyo miqyosida raqamli transformatsiya jarayoni jadallashib bormoqda. Davlat boshqaruvi, moliya tizimi, ta’lim, sog‘liqni saqlash va savdo sohalarida elektron xizmatlardan foydalanish kengaymoqda. Qog‘oz hujjatlar o‘rnini elektron hujjatlar egallamoqda.

Bu esa axborot xavfsizligini ta’minlash, ma’lumotlarning yaxlitligini saqlash va foydalanuvchi shaxsini aniqlash kabi muhim vazifalarni keltirib chiqarmoqda. Elektron muhitda oddiy qo‘l imzosidan foydalanishning imkoni yo‘q. Shu sababli elektron hujjatlarni tasdiqlashning ishonchli mexanizmi zarur bo‘ldi. Raqamli imzo ana shunday mexanizm bo‘lib, u elektron hujjatning haqiqiyligini kafolatlaydi, muallifni aniqlaydi va hujjat mazmuni o‘zgarmaganligini tasdiqlaydi. Raqamli imzo bugungi kunda elektron hukumat tizimlari, bank operatsiyalari, elektron savdo maydonchalari va korporativ hujjat aylanish tizimlarining ajralmas qismiga aylangan.

Raqamli imzo tushunchasi va nazariy asoslari: raqamli imzo elektron hujjatga biriktiriladigan maxsus kriptografik kod bo‘lib, u hujjat muallifini aniqlash va hujjat mazmuni o‘zgarmaganligini tekshirish imkonini beradi. Raqamli imzo texnologiyasi ochiq kalitli kriptografiyaga asoslanadi. Ushbu tizimda har bir foydalanuvchi ikkita kalitga ega bo‘ladi. Yopiq kalit maxfiy saqlanadi va hujjatni imzolash uchun ishlatiladi. Ochiq kalit

esa imzoni tekshirish uchun xizmat qiladi. Ochiq kalit infratuzilmasi orqali kalitlarni boshqarish va sertifikatlash jarayoni amalga oshiriladi. Maxsus sertifikatlash markazlari foydalanuvchilarning ochiq kalitlarini tasdiqlaydi va ularga elektron sertifikat beradi. Ushbu sertifikat foydalanuvchining shaxsini tasdiqlovchi raqamli hujjat hisoblanadi.

Raqamli imzoning ishlash mexanizmi:raqamli imzo jarayonida avvalo imzolanadigan hujjat ustida xesh funksiyasi qo‘llaniladi. Xesh funksiya hujjatning qisqa raqamli ifodasini hosil qiladi. Agar hujjat mazmunining kichik bir qismi o‘zgarsa ham xesh qiymat butunlay o‘zgaradi. Bu esa hujjat yaxlitligini tekshirish imkonini beradi. Hosil qilingan xesh qiymat foydalanuvchining yopiq kaliti yordamida shifrlanadi va natijada raqamli imzo hosil bo‘ladi. Qabul qiluvchi tomon hujjatni qabul qilgach, xesh qiymatini qayta hisoblaydi hamda jo‘natuvchining ochiq kaliti yordamida imzoni tekshiradi. Agar ikkala xesh qiymat bir xil bo‘lsa, hujjat o‘zgarmagan va imzo haqiqiy deb topiladi. Raqamli imzo autentifikatsiya, yaxlitlik va inkor etib bo‘lmaslik kabi muhim xavfsizlik xususiyatlarini ta’minlaydi.

Raqamli imzoning qo‘llanilish sohalari: elektron hukumat tizimlarida fuqarolar turli davlat xizmatlaridan masofadan turib foydalanish imkoniyatiga ega bo‘lmoqda. Soliq hisobotlari, arizalar, litsenziyalar va boshqa rasmiy hujjatlar elektron tarzda yuboriladi va tasdiqlanadi. Bunday jarayonlarning huquqiy kuchga ega bo‘lishi aynan raqamli imzo orqali ta’minlanadi. Bank va moliya sohasida internet-banking operatsiyalarini tasdiqlash, kredit shartnomalarini rasmiylashtirish va onlayn to‘lovlarni amalga oshirishda raqamli imzo muhim rol o‘ynaydi. Bu moliyaviy operatsiyalarning xavfsizligini oshiradi hamda firibgarlik xavfini kamaytiradi. Elektron tijorat sohasida onlayn shartnomalar tuzish va hisob-fakturalarni rasmiylashtirish jarayonida ham raqamli imzo keng qo‘llaniladi. Korxonalarda ichki hujjat aylanish tizimlarini raqamlashtirish jarayonida buyruqlar, shartnomalar va hisobotlar elektron imzo orqali tasdiqlanadi. Bu vaqtni tejaydi va qog‘oz xarajatlarini kamaytiradi. Ta’lim tizimida diplom va sertifikatlarni elektron shaklda tasdiqlash jarayonida ham raqamli imzo muhim ahamiyat kasb etmoqda.

Afzalliklari va muammolari: raqamli imzo tizimi tezkorlik, ishonchlilik va yuqori darajadagi xavfsizlikni ta’minlaydi. U qog‘oz hujjatlar aylanishini kamaytiradi, xarajatlarni qisqartiradi va masofadan ishlash imkoniyatini yaratadi. Biroq yopiq kalitni yo‘qotish yoki o‘g‘irlanish xavfi, kiberhujumlar tahdidi, texnik savodxonlik yetishmasligi hamda infratuzilma xarajatlari muhim muammolar qatoriga kiradi. Shuning uchun kalitlarni ishonchli saqlash va zamonaviy himoya vositalaridan foydalanish zarur hisoblanadi.

Raqamli imzo va huquqiy asoslar: ko‘plab davlatlarda raqamli imzo qonun bilan tartibga solinadi. Elektron hujjat va elektron imzo to‘g‘risidagi qonunlar raqamli imzoning yuridik kuchini belgilaydi. Bu esa elektron hujjatlarni qog‘oz hujjatlar bilan tenglashtiradi va ularning huquqiy maqomini mustahkamlaydi. Huquqiy asoslarning mavjudligi elektron savdo va elektron hukumat tizimlarining rivojlanishiga ijobiy ta’sir ko‘rsatadi.

Kelajak istiqbollari: kelajakda raqamli imzo texnologiyalari yanada takomillashishi kutilmoqda. Biometrik autentifikatsiya, sun’iy intellekt asosidagi xavfsizlik tizimlari va blokcheyn texnologiyalari bilan integratsiya qilish orqali xavfsizlik darajasi yanada oshiriladi. Mobil qurilmalar orqali imzolash va bulutli sertifikatlash tizimlari raqamli imzoning qulayligini yanada kengaytirmoqda. Bu esa to‘liq raqamli iqtisodiyot shakllanishiga xizmat qiladi.

Xulosa qilganda:raqamli imzo zamonaviy axborot jamiyatining muhim tarkibiy qismi hisoblanadi. U elektron hujjatlarning haqiqiyligi va yaxlitligini ta’minlaydi, davlat va biznes jarayonlarini soddalashtiradi hamda axborot xavfsizligini mustahkamlaydi. Elektron xizmatlar hajmi ortib borayotgan sharoitda raqamli imzo texnologiyalarini takomillashtirish va ularni keng joriy etish dolzarb vazifa bo‘lib qolmoqda. Raqamli imzo kelajakda to‘liq raqamli iqtisodiyotning asosiy tayanch mexanizmlaridan biri sifatida xizmat qiladi.

Foydalanilgan adabiyotlar

1. Stallings, William. Cryptography and Network Security: Principles and Practice. Pearson, 2017.

2. Paar, Christof, and Jan Pelzl. Understanding Cryptography: A Textbook for Students and Practitioners. Springer, 2010.

3. Diffie, Whitfield, and Martin E. Hellman. New Directions in Cryptography. IEEE Transactions on Information Theory, 1976.

4. Menezes, Alfred J., Paul C. van Oorschot, and Scott A. Vanstone. Handbook of Applied Cryptography. CRC Press, 1996.

5. Kahn, David. The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet. Scribner, 1996.

6. Adams, Carlisle, and Steve Lloyd. Understanding PKI: Concepts, Standards, and Deployment Considerations. Addison-Wesley, 2003