ELEKTRON RAQAMLI IMZO BILAN ISHLASH TEXNOLOGIYALARI

Zokirova Nargiza Sadriddin qizi
Namangan davlat universiteti
Raqamli ta’lim texnologiyalari kafedrasi o’qituvchisi
Nastinov Sadriddin Tojiddin o’g’li
Namangan davlat universiteti
Raqamli ta’lim texnologiyalari kafedrasi o’qituvchisi
E-mail: zokirovan99@gmail.com
Nastinovsadriddin290895@gmail.com

Annotatsiya: Ushbu maqolada elektron raqamli imzo (ERI) texnologiyalarining mohiyati, uning ishlash prinsiplari, huquqiy asoslari va amaliyotdagi o‘rni keng yoritilgan. Elektron raqamli imzo zamonaviy axborot-kommunikatsiya texnologiyalari bilan bog‘liq jarayonlarda ishonchli, xavfsiz va tezkor ma’lumot almashishni ta'minlovchi vosita sifatida ko‘riladi. Maqolada ERI qo‘llanilishining texnologik asoslari, algoritmlari, xavfsizlik masalalari va samaradorligi tahlil qilingan. Tadqiqot natijalariga ko‘ra, ERI texnologiyasi biznes, davlat xizmatlari va kundalik hayotda keng qo‘llanilayotgani aniqlangan.

Kalit so‘zlar: elektron raqamli imzo, axborot xavfsizligi, kriptografiya, autentifikatsiya, huquqiy asoslar, ma’lumotlarni himoya qilish.

ТЕХНОЛОГИИ РАБОТЫ С ЭЛЕКТРОННО-ЦИФРОВЫМИ ПОДПИСЯМИ

Закирова Наргиза Садриддинновна.
Наманганский государственный университет
Преподаватель кафедры цифровых образовательных технологий
Настинов Садриддина Таджиддинович.
Наманганский государственный университет
Преподаватель кафедры цифровых образовательных технологий
Электронная почта: zokirovan99@gmail.com
nastinovsadriddin290895@gmail.com

Абстрактный: В данной статье широко освещена природа технологии электронной цифровой подписи (ЭЦИ), ее принципы работы, правовая основа и роль на практике. Электронная цифровая подпись рассматривается как инструмент, обеспечивающий надежный, безопасный и быстрый обмен информацией в процессах, связанных с современными информационно-коммуникационными технологиями. В статье анализируются технологические основы, алгоритмы, вопросы безопасности и эффективности применения ERI.

По результатам исследования установлено, что технология ERI широко используется в бизнесе, государственных услугах и повседневной жизни.

Ключевые слова: электронная цифровая подпись, информационная безопасность, криптография, аутентификация, правовые основы, защита информации.

TECHNOLOGIES FOR WORKING WITH ELECTRONIC DIGITAL SIGNATURES

Zakirova Nargiza the daughter of Sadriddin
Namangan State University
Teacher of the Department of Digital Educational Technologies
Nastinov Sadriddin the son of Tajiddin
Namangan State University
Teacher of the Department of Digital Educational Technologies
E-mail: zokirovan99@gmail.com
nastinovsadriddin290895@gmail.com

Abstract: In this article, the nature of electronic digital signature (EDI) technologies, its principles of operation, legal basis and role in practice are widely covered. Electronic digital signature is seen as a tool that ensures reliable, safe and fast exchange of information in processes related to modern information and communication technologies. The article analyzes the technological bases, algorithms, security issues and efficiency of ERI application. According to the results of the research, it was found that ERI technology is widely used in business, public services and everyday life.

Key words: electronic digital signature, information security, cryptography, authentication, legal bases, data protection.

Kirish (Introduction)

Axborot-kommunikatsiya texnologiyalarining tezkor rivojlanishi zamonaviy jamiyat hayotiga bevosita ta’sir ko‘rsatmoqda. Hujjat almashish, shartnomalar tuzish va boshqa ma’lumotlarni elektron muhitda boshqarish jarayonida ma’lumotlarning xavfsizligi va ishonchliligini ta’minlash muhim ahamiyat kasb etmoqda. Shu jarayonda **elektron raqamli imzo (ERI)** texnologiyasi asosiy vositalardan biri sifatida e’tirof etiladi.

ERI — bu elektron hujjatga imzo qo‘yishning ishonchli va xavfsiz usuli bo‘lib, u hujjatning haqiqiyligini, imzolovchining shaxsini va taqdim etilgan hujjatga o‘zgartirish kiritilmaganligini kafolatlaydi. ERI texnologiyasi kriptografik asosda

ishlaydi va davlat xizmatlari, elektron tijorat, moliyaviy tranzaksiyalar kabi sohalarda keng qo‘llaniladi.

Mazkur maqolada elektron raqamli imzo bilan ishlash texnologiyalarining texnik va huquqiy asoslari, ishlash prinsiplari va amaliyotdagi ahamiyati batafsil ko‘rib chiqiladi.

Metodologiya (Methods)

Tadqiqot elektron raqamli imzoning texnologik va huquqiy jihatlarini o‘rganish uchun quyidagi metodlardan foydalanib amalga oshirildi:

Nazariy tahlil sifatida olib qaraydigan bulsak

ERI texnologiyalari va uning ishlash prinsiplari bo‘yicha ilmiy maqolalar, axborot xavfsizligi yuzasidan xalqaro standartlar (masalan, Xalqaro Elektron Aloqa Ittifoqi (ITU) standartlari) va O‘zbekiston Respublikasining qonunchilik hujjatlari o‘rganildi.

ERI algoritmlarini (RSA, DSA, va ECDSA) ishlash prinsiplari tahlil qilindi.

Amaliy kuzatuvlar natijasiga ko’ra

Elektron hujjat almashish jarayonida ERI texnologiyalarini qo‘llash bo‘yicha amaliy kuzatuvlar o‘tkazildi.

Davlat xizmatlari (my.gov.uz), tijorat banklari va boshqa xizmatlarda ERI qo‘llash tajribasi kuzatildi.

Eksperimental tadqiqot natijasiga ko’ra

Elektron raqamli imzo yordamida elektron hujjatlarni tasdiqlash jarayoni simulyatsiya qilindi. Bu jarayonda imzo yaratish, tasdiqlash va tekshirish bosqichlari o‘rganildi.

ERI algoritmlarining samaradorligi va xavfsizlik darajasi tahlil qilindi.

4. Huquqiy tahlil natijasiga ko’ra

O‘zbekiston Respublikasining **“Elektron raqamli imzo to‘g‘risida”gi qonuni** va xalqaro huquqiy standartlar o‘rganildi.

Elektron raqamli imzo bilan bog‘liq huquqiy masalalar va ularni hal qilish yo‘llari tahlil qilindi.

Natijalar (Results)

Tadqiqot davomida elektron raqamli imzo bilan ishlash jarayonining quyidagi asosiy natijalari aniqlandi:

ERI texnologiyasining ishlash prinsipi

Elektron raqamli imzo kriptografik algoritmlar (RSA, DSA, ECDSA va boshqalar) yordamida ishlaydi. Imzo yaratish jarayoni quyidagi bosqichlardan iborat:

Imzo yaratish: Imzo yaratuvchi dastur yordamida hujjatning xesh-funksiyasi hisoblanadi va maxfiy kalit yordamida shifrlanadi.

Imzo tekshirish: Ochiq kalit yordamida hujjatning haqiqiyligi va unga o‘zgartirish kiritilmaganligi tasdiqlanadi.

ERI qo‘llanilish sohalari

Davlat xizmatlari: O‘zbekistonda davlat xizmatlari portali (my.gov.uz) orqali ERI yordamida ariza topshirish, hujjatlarni tasdiqlash va soliq hisobotlarini yuborish amalga oshiriladi.

Elektron tijorat: Shartnomalar va bitimlarni masofadan turib imzolash imkonini beradi.

Moliyaviy xizmatlar: Banklar orqali tranzaksiyalarni himoyalashda keng qo‘llaniladi.

Xavfsizlik va muammolar

Elektron raqamli imzo ma’lumotlarning maxfiyligini va o‘zgarishsiz saqlanishini ta’minlasa-da, texnik va huquqiy masalalar mavjud. Masalan:

ERI kalitlarining buzilish xavfi (xususan, zaif parollar yoki noto‘g‘ri boshqaruv).

ERI sertifikatlarini boshqaruvchi markaziy tashkilotlarning (CA - Sertifikatlash markazi) mas’uliyati va ishonchliligi.

ERI samaradorligi

Tajribalar shuni ko‘rsatdiki, ERI ishlash algoritmlari (RSA, DSA) tezkor va samarali bo‘lib, ularning xavfsizlik darajasi kriptografik kalit uzunligiga bog‘liq.

O‘zbekiston sharoitida ERI texnologiyasi davlat xizmatlari va tijorat jarayonlarining avtomatlashtirilishini ta’minlashda yuqori samaradorlik ko‘rsatdi.

Tahlil va muhokama (Discussion)

Elektron raqamli imzo texnologiyasi elektron hujjatlar va ma'lumotlarni himoya qilishda muhim vosita hisoblanadi. Bu texnologiyaning afzalliklari quyidagilar:

1. **Axborot xavfsizligi**: ERI orqali hujjatlarning o‘zgartirilmaganligini kafolatlash mumkin. Bu esa, xususan, davlat xizmatlari va bank tizimlari uchun muhimdir.
2. **Ishonchlilik**: ERI orqali autentifikatsiya amalga oshiriladi, ya’ni hujjatni imzolagan shaxsning haqiqiyligi tasdiqlanadi.
3. **Tejamkorlik**: ERI hujjatlarni qog‘ozsiz boshqarish imkoniyatini beradi, bu esa vaqt va mablag‘ni tejaydi.

Biroq, ERI texnologiyasini keng qo‘llashda quyidagi muammolar mavjud:

Texnik muammolar: Ayrim foydalanuvchilar ERI yaratish va qo‘llash bo‘yicha yetarli bilimga ega emas.

Huquqiy masalalar: ERI bilan bog‘liq huquqiy nizolar, masalan, imzolovchining shaxsini soxtalashtirish xavfi dolzarbdir.

Texnologik zaifliklar: Kalitlarni boshqarish va saqlashda ehtiyotsizlik xavfsizlikni buzishi mumkin.

Shu sababli, ERI texnologiyalarini rivojlantirishda foydalanuvchilarni o‘qitish, huquqiy asoslarni mustahkamlash va texnologik infratuzilmani rivojlantirish lozim.

Xulosa (Conclusion)

Elektron raqamli imzo texnologiyasi zamonaviy axborot-kommunikatsiya tizimlarida xavfsizlikni ta'minlashning muhim vositasidir. Ushbu texnologiya hujjatlarning haqiqiyligini, imzolovchining shaxsini va hujjatga o‘zgartirish kiritilmaganligini kafolatlaydi. Tadqiqot natijalari shuni ko‘rsatadiki:

1. ERI texnologiyasi davlat xizmatlari, elektron tijorat va bank sohasida samarali qo‘llanilmoqda.
2. ERI orqali qog‘ozsiz hujjat aylanishi imkoniyati yaratilmoqda, bu esa vaqt va mablag‘ni tejashga xizmat qiladi.
3. Texnik va huquqiy muammolarni hal qilish orqali ERI texnologiyasining qo‘llanilishini yanada kengaytirish mumkin.

Kelgusida ERI texnologiyalarini rivojlantirish uchun quyidagilar tavsiya etiladi:

Foydalanuvchilarni ERI bilan ishlash bo‘yicha o‘qitish dasturlarini yaratish.

Sertifikatlash markazlarining xavfsizlik darajasini oshirish.

ERI texnologiyalarini yanada ommalashtirish uchun milliy va xalqaro hamkorlikni kuchaytirish.

Foydalanilgan adabiyotlar

1. O‘zbekiston Respublikasi qonuni: "Elektron raqamli imzo to‘g‘risida", 2003-yil.
2. O‘zbekiston Respublikasining "Elektron hukumat to‘g‘risida"gi qonuni, 2015-yil.
3. Stallings W. "Cryptography and Network Security", Pearson Education, 2020.
4. Rivest R., Shamir A., Adleman L. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM, 1978.
5. Xalqaro Elektron Aloqa Ittifoqi (ITU). "Public Key Infrastructure (PKI) Recommendations", 2022.
6. O‘zbekiston Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi. "Elektron raqamli imzo bo‘yicha metodik qo‘llanma", Toshkent, 2021.
7. Schneier B. "Applied Cryptography: Protocols, Algorithms, and Source Code in C", Wiley, 2015.