ISSN 2181-3187

ELEKTRON RAQAMLI IMZO VA UNING ZAMONAVIY TURLARI

G‘allarol 1-son Politextnukumi
Axborot xavfsizligi fani o‘qtuvchisi
Xayitboyev Sardor Keldiyor o‘gli

ANNOTATSIYA Ushbu maqola elektron raqamli imzolar (ERI) va ularning zamonaviy turlari haqida batafsil ma'lumot beradi. Maqola, elektron imzoning asosiy tushunchalari, uning ishlash prinsiplari va xavfsizlik texnologiyalari haqida umumiy ma'lumotni o‘z ichiga oladi. Shuningdek, zamonaviy texnologiyalar yordamida yaratib ishlatilayotgan elektron imzolar turlari, jumladan, asimmetrik kriptografiya (PKI), biometrik imzolar, blockchain texnologiyasi va hashing metodlari haqida muhokama qilinadi. Maqolada, elektron raqamli imzolarni turli sohalarda, ayniqsa, **elektron tijorat**, **moliyaviy operatsiyalar**, **hukumat xizmatlari** va boshqa axborot texnologiyalarida qanday keng qo‘llanilishi va qanday xavfsizlikni ta'minlashga xizmat qilishi haqida tahlil qilinadi. Shuningdek, elektron imzolarni kelajakda rivojlantirish imkoniyatlari va yangi texnologiyalar yordamida xavfsizlikni kuchaytirish va tizimlarni yanada samarali qilish masalalari yoritiladi. Maqola, elektron imzo texnologiyalarining hujjatlarni tasdiqlash, tranzaktsiyalarni xavfsiz qilish va axborot almashinishdagi o‘rnini ko‘rsatib, raqamli iqtisodiyotda ishonchli va xavfsiz muhitni yaratishga yordam berishini ta'kidlaydi. Maqola, elektron raqamli imzolar va ularning turlari bo‘yicha ta'lim olish yoki ularni amaliyotda qo‘llashni xohlagan mutaxassislar va talabalar uchun foydali bo‘ladi.

Kalit so‘zlar Elektron imzo, zamonaviy, dastur, taklif, axborot, texnalogiya, xavfsizligi;

ANNOTATION This article details electronic digital signatures (ERI) and their modern types. The article contains an overview of the basic concepts of electronic signature, its principles of operation and security technologies. It also discusses the

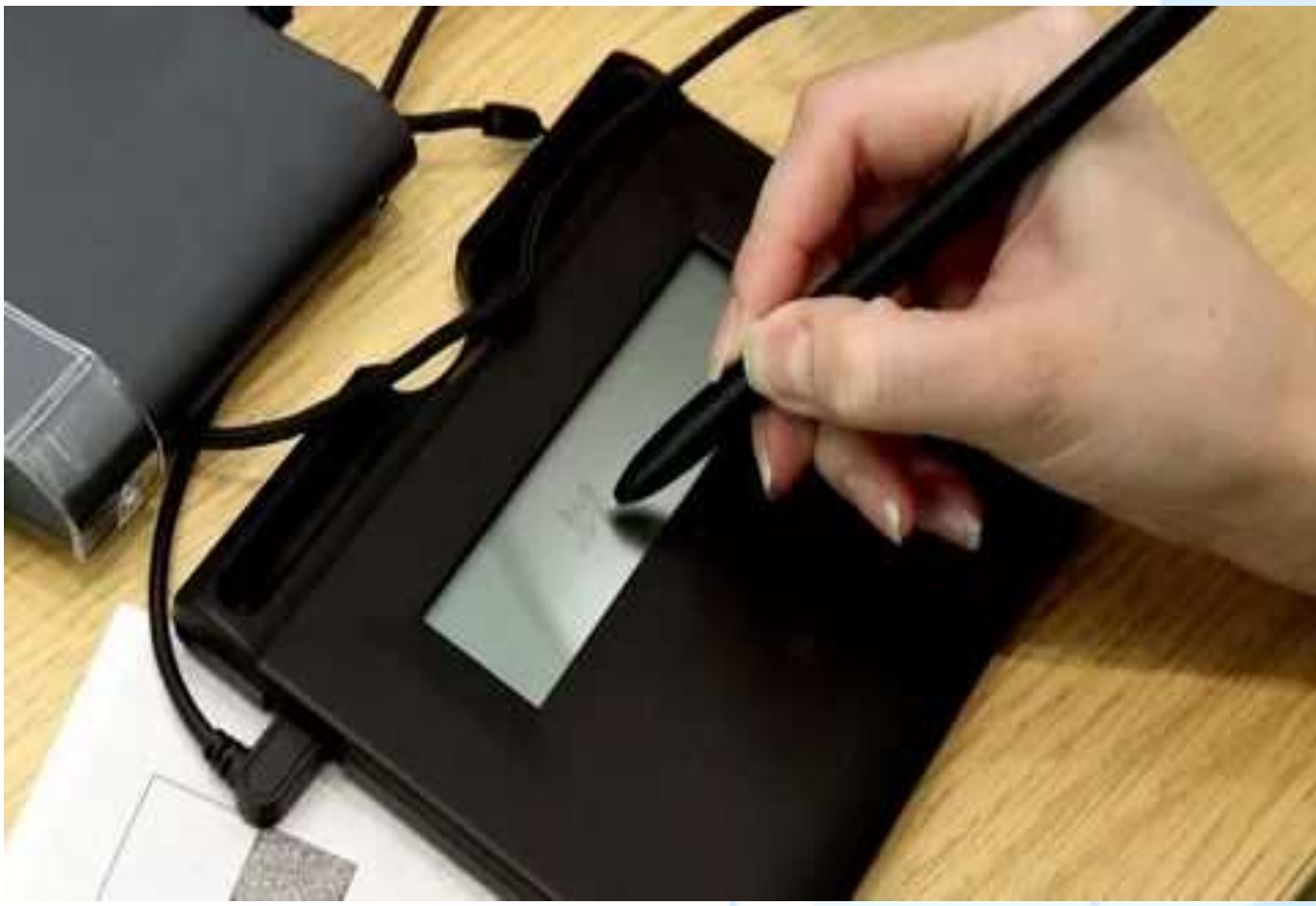
ISSN 2181-3187

types of electronic signatures that are being created and used using modern technologies, including asymmetric cryptography (PKI), biometric signatures, blockchain technology, and hashing techniques. The article will analyze how electronic digital signatures are widely used and serve to ensure security in various fields, especially in e-commerce, financial transactions, government services and other information technologies. The issues of strengthening security and making systems more efficient will also be covered by the possibilities of future development of electronic signatures and new technologies. Article, document approval of electronic signature technologies

Key words Electronic signature, modern, application, offer, information, technology, security;

KIRISH Axborot xavfsizligi bugungi kunda har bir sohada, xususan, raqamli texnologiyalarning jadal rivojlanishi bilan tobora muhim ahamiyatga ega bo‘lib bormoqda. Ma'lumotlar xavfsizligi, maxfiylikni saqlash, integritetni ta'minlash va tizimlarning uzluksiz ishlashini nazorat qilish – bularning barchasi axborot xavfsizligi sohasining asosiy vazifalaridir. Elektron raqamli imzo (ERI) aynan shu vazifalarni amalga oshirishda muhim rol o‘ynaydi. Elektron raqamli imzo — bu elektron hujjatlarning haqiqiyligini tasdiqlovchi va uning o‘zgartirilmaganligini kafolatlovchi raqamli vosita hisoblanadi. Elektron imzo, hujjatlar yoki tranzaktsiyalarni himoya qilish va tasdiqlash uchun zarur bo‘lib, foydalanuvchining haqiqiyligini aniqlash va ma'lumotlar yaxlitligini tekshirish uchun ishlatiladi.

ISSN 2181-3187



Yuqori xavfsizlikni talab qiladigan sohalarda, masalan, elektron tijorat, davlat xizmatlari, bank tizimlari, tibbiyot va huquq sohalarida elektron raqamli imzolar kundalik hayotning ajralmas qismiga aylangan. Elektron imzoning o‘rni juda kengaygan: oddiy hujjatlardan tortib murakkab shartnomalar va transaksiyalarni tasdiqlashgacha bo‘lgan jarayonlarda ishonchli va xavfsiz imzo ta'minlash uchun qo‘llaniladi. Bugungi kunda, axborot texnologiyalarining tez rivojlanishi va global bozorlarning o‘sishi bilan birga, elektron raqamli imzolar nafaqat hujjatlarni raqamli shaklda tasdiqlashning eng ishonchli vositasi sifatida, balki yangi texnologiyalar yordamida yanada kompleks xavfsizlik choralari yaratish imkoniyatlarini taqdim etadi.

ISSN 2181-3187

Elektron raqamli imzolar, asosan, asimmetrik kriptografiya (Public Key Infrastructure, PKI) va biometrik tizimlar yordamida yaratiladi. Ularning yordamida hujjatlarning autentifikatsiyasi va yaxlitligi ta'minlanadi, shuningdek, tizimlar o‘rtasidagi elektron tranzaktsiyalar va aloqalar xavfsizligi mustahkamlanadi. Elektron raqamli imzolarni zamonaviy texnologiyalar bilan birgalikda qo‘llash, axborot xavfsizligi sohasida yangi imkoniyatlar yaratadi. Ma'lumotlarni uzatishda va saqlashda

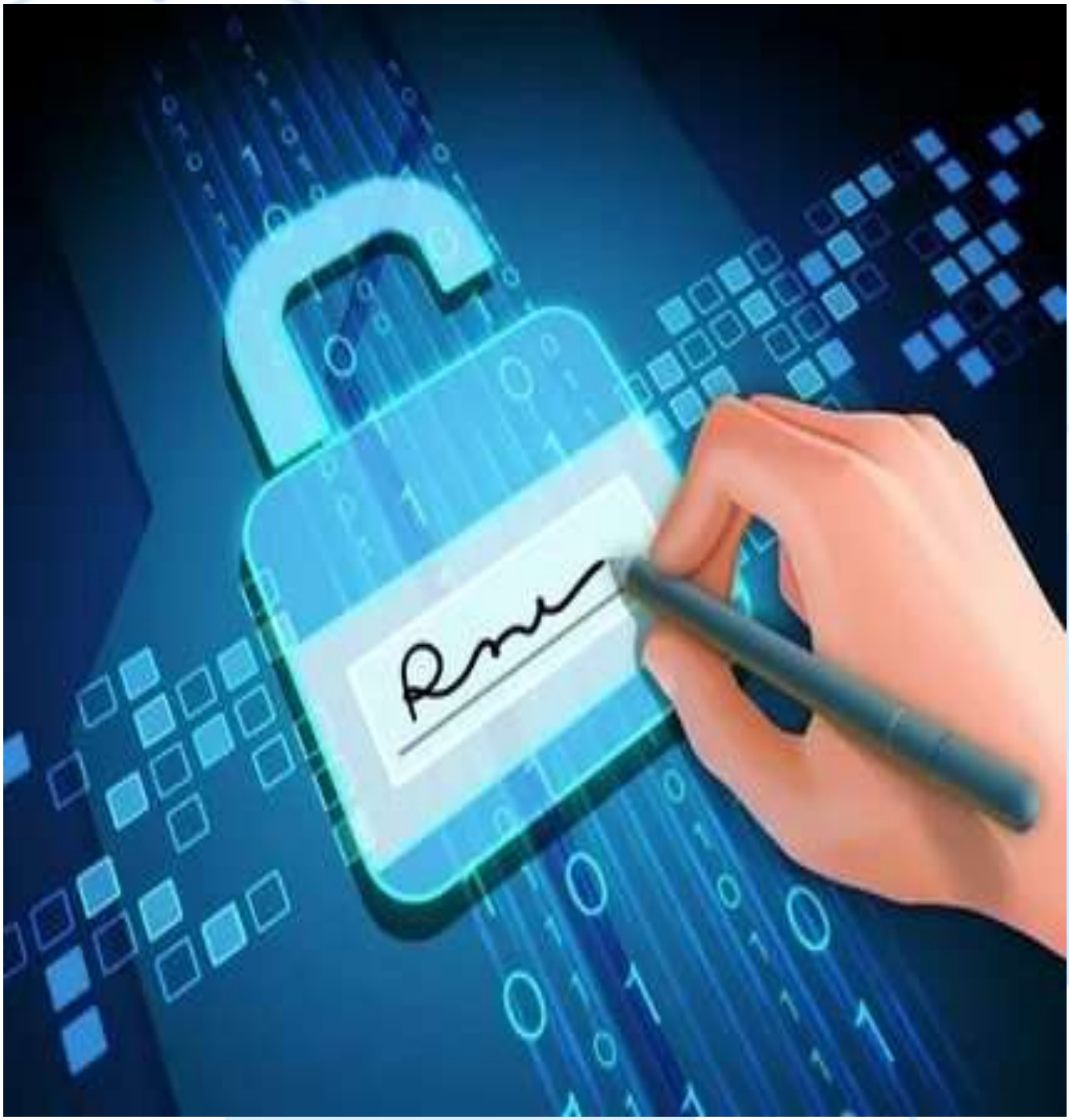
ISSN 2181-3187

yuqori xavfsizlikni ta'minlash uchun ilg‘or texnologiyalar, xususan, blockchain texnologiyasi, biometrik autentifikatsiya va boshqa innovatsion yechimlar, elektron imzolarni zamonaviy va ishonchli tizimlarga aylantirmoqda. Ushbu maqolada elektron raqamli imzoning asosiy tushunchalari, uning yaratilish jarayoni, zamonaviy turlari, shuningdek, axborot xavfsizligini ta'minlashdagi ahamiyati va foydalari haqida so‘z yuritiladi. Maqolada shuningdek, texnologiyalarning rivojlanishi bilan birgalikda elektron imzolarni qo‘llashda yuzaga keladigan yangi xavfsizlik choralari va metodologiyalarni ham tahlil qilamiz.

TADQIQOT METODOLOGIYASI Elektron Raqamli Imzo: Umumiy Tushuncha Elektron raqamli imzo (ERI) – bu raqamli hujjatlar va tranzaktsiyalarni autentifikatsiya qilish uchun ishlatiladigan kriptografik vosita bo‘lib, uni imzolovchining o‘ziga xos xususiyatlarini aks ettiradi. Elektron imzo, foydalanuvchining raqamli kaliti yordamida hujjatni imzolash jarayonini o‘zgartirish va buzilishlardan himoya qilishga xizmat qiladi. Elektron imzo, aslida, an'anaviy qo‘l imzosining raqamli shakli bo‘lib, uning maqsadi va funktsiyasi bir xil – hujjatning haqiqiyligini, yaxlitligini va imzolovchining kimligini tasdiqlash. Elektron raqamli imzo asosan asimmetrik kriptografiya yordamida yaratiladi. Bu yerda ikkita kalit ishlatiladi: xususiy kalit (private key) va ommaviy kalit (public key). Xususiy kalit yordamida hujjatning raqamli imzosi yaratiladi, bu esa imzolovchining maxfiy kalitini faqat o‘zi bilishiga imkon yaratadi. Ommaviy kalit esa, hujjatni tekshirishda foydalaniladi va barcha foydalanuvchilar uchun ochiq bo‘ladi. Imzo yaratilgandan so‘ng, uni tekshirish jarayonida ommaviy kalit yordamida hujjatni tasdiqlash mumkin. Agar hujjatning matni yoki tarkibi o‘zgargan bo‘lsa, uning hashing kodi ham o‘zgaradi va imzo noaniqligini ko‘rsatadi. Shunday qilib, elektron imzo, hujjatning yaxlitligini va haqiqiyligini kafolatlashda muhim vosita hisoblanadi. **Elektron Raqamli Imzoning Zamonaviy Turlari.** Elektron raqamli imzolar, texnologiya va xavfsizlik talablarining o‘sishi bilan birga, doimiy ravishda yangilanib va takomillashib boradi. Hozirgi kunda elektron imzolarni yaratish va ularni boshqarishda turli texnologiyalar va metodlar qo‘llaniladi. Ushbu turlar va metodlar quyidagicha tasniflanishi mumkin:

ISSN 2181-3187

Asimmetrik Kriptografiya (Public Key Infrastructure - PKI). Asimmetrik kriptografiya, ya'ni PKI tizimi – bu elektron imzo tizimlarining asosini tashkil etuvchi texnologiyadir.



ISSN 2181-3187

PKI tizimi ikkita kalitdan iborat: xususiy kalit va ommaviy kalit. Har bir foydalanuvchi o‘zining xususiy kalitini sir tutishi kerak, chunki u faqat o‘ziga tegishli hujjatlarni imzolash uchun ishlatiladi. Ommaviy kalit esa, uni barcha foydalanuvchilar bilan bo‘lishish mumkin bo‘lgan kalit bo‘lib, imzo haqiqiyligini tekshirishda ishlatiladi. PKI tizimi, shuningdek, Sertifikatlashtirish Markazi (CA) tomonidan tasdiqlangan sertifikatlarni taqdim etadi, bu esa tizimda ishtirok etayotgan tomonlarning ishonchli ekanligini kafolatlaydi. Elektron imzolar orqali, har bir hujjatni yoki elektron tranzaktsiyani ishonchli va xavfsiz ravishda tasdiqlash mumkin bo‘ladi.

Biometrik Elektron Imzolar. Biometrik autentifikatsiya texnologiyalari, foydalanuvchining biologik xususiyatlarini aniqlash va tekshirish uchun ishlatiladi. Bular orasida barmoq izlari, yuzni tanish, ko‘z tarmog‘ini skaner qilish, va ovozi kabi tizimlar mavjud. Biometrik tizimlar xavfsizlikni yanada kuchaytiradi, chunki har bir insonning biometrik xususiyatlari o‘ziga xos bo‘lib, bu ma'lumotlarni boshqalar tomonidan taqlid qilish yoki o‘zgartirish mumkin emas. Biometrik elektron imzolarni qo‘llash, ayniqsa yuqori xavfsizlikni talab qiluvchi tizimlarda, masalan, moliyaviy muassasalar, davlat xizmatlari, yuridik tizimlarda juda samarali bo‘ladi. Biometrik texnologiyalar yordamida, hujjatlarni imzolashda ishonchli va aniq autentifikatsiya jarayonini yaratish mumkin.

Hashing texnologiyasi, ma'lumotlarni yoki hujjatlarni xavfsiz tarzda himoya qilish uchun ishlatiladi. Hashing yordamida hujjatlarning o‘zgarmas raqamli izini yaratish mumkin. Bu raqamli iz yoki hash har bir hujjatga xos bo‘ladi va uning tarkibiga qo‘shimchalar kiritilganida darhol o‘zgaradi. Elektron imzo tizimi, hujjatni imzolashdan oldin uning hashing kodini yaratadi, va bu kod keyinchalik xususiy kalit yordamida imzolanadi. Bu tizim, hujjatlarning yaxlitligini ta'minlashda muhim o‘rin tutadi, chunki har qanday o‘zgartirish yoki buzilish, hujjatning asl imzosining yaroqsizligini keltirib chiqaradi. Shunday qilib, hujjatlarning xavfsizligini ta'minlashda hashing metodologiyasi elektron imzolar bilan birgalikda ishlaydi. Elektron sertifikatlar, foydalanuvchilar yoki tashkilotlarning haqiqiyligini va ishonchliligini tasdiqlovchi maxsus raqamli hujjatlardir. Elektron raqamli sertifikatlar

ISSN 2181-3187

Sertifikatlashtirish Markazi (CA) tomonidan chiqariladi va ular ommaviy kalitni tasdiqlash uchun ishlatiladi. Sertifikatlar orqali foydalanuvchining identifikatsiyasi amalga oshiriladi va ular orqali elektron hujjatlar tasdiqlanadi. Elektron sertifikatlar, odatda, shaxsiy identifikatsiya raqami (PIN) bilan himoyalangan bo‘lib, ularni faqat ma'lum ruxsatga ega bo‘lgan shaxslar ishlata oladi. Bu texnologiya, ayniqsa, davlat organlarining, bank tizimlarining va xalqaro moliyaviy tashkilotlarning elektron tranzaktsiyalarida qo‘llaniladi. Blockchain texnologiyasi, ma'lumotlarni xavfsiz tarzda saqlash va ularni o‘zgartirilmasligini ta'minlash uchun yaratilgan tizimdir. Hujjatlar yoki tranzaktsiyalar bloklar shaklida saqlanadi va har bir blok, oldingi blokni o‘zining raqamli imzosi bilan tasdiqlaydi. Bu tizimda, har qanday o‘zgarish yoki noto‘g‘ri ma'lumot, barcha bloklarni tekshirish orqali aniqlanishi mumkin. Blockchain texnologiyasi, ayniqsa elektron tijorat, moliya va boshqa yuqori xavfsizlikni talab qiluvchi sohalarda elektron imzolarni qo‘llashda keng tarqalgan. Ma'lumotlar o‘zgartirilmasligi va xavfsizligi blockchain tizimi orqali kafolatlanadi, bu esa elektron imzolarni ishonchli va xavfsiz qilishga yordam beradi. Elektron raqamli imzolarni qo‘llash, nafaqat elektron hujjatlarni xavfsiz tarzda imzolash, balki quyidagi sohalarda ham keng qo‘llaniladi: Elektron Tijorat: Elektron tijoratda, xaridlarni tasdiqlash, shartnomalarni raqamli shaklda imzolash va to‘lovlarni xavfsiz amalga oshirishda elektron imzolar keng qo‘llaniladi. Masalan, onlayn xaridlar, shartnoma tuzish, va boshqa tijorat operatsiyalari elektron imzo yordamida amalga oshiriladi. Bank tizimi: Banklarda elektron raqamli imzolar, moliyaviy operatsiyalarni, tranzaktsiyalarni va hisob-kitoblarni xavfsiz va ishonchli ravishda tasdiqlash uchun qo‘llaniladi. Shuningdek, xalqaro pul o‘tkazmalari, kredit shartnomalari va depozit hisobvaraqlari uchun elektron imzolar keng tarqalgan.

Hukumat xizmatlari: Elektron raqamli imzolar, davlat xizmatlarida fuqarolik holati haqidagi ma'lumotlarni

XULOSA VA TAKLIFLAR Elektron raqamli imzo (ERI) — bu zamonaviy axborot texnologiyalarida xavfsizlikni ta'minlash va elektron hujjatlarni imzolashning muhim vositasidir. U elektron hujjatlarning yaxlitligini, haqiqiyligini va ishonchliligini

ISSN 2181-3187

tasdiqlashda katta rol o‘ynaydi. Elektron imzo, shuningdek, hujjatlar o‘rtasidagi o‘zgarishlarni aniqlash va tizimlar o‘rtasida ishonchli ma'lumot almashinuvini ta'minlashda asosiy instrument hisoblanadi. Zamonaviy texnologiyalar yordamida, masalan, asimmetrik kriptografiya, biometrik autentifikatsiya, blockchain texnologiyasi, va hashing metodlari kabi innovatsion yondoshuvlar elektron raqamli imzolarni yaratishda va ularni boshqarishda ishlatilmoqda. Bu metodlar, hujjatlarning xavfsizligini ta'minlashda, hujjatlarni soxtalashtirishning oldini olishda, va har qanday o‘zgarishlarni aniqlashda juda samarali bo‘ladi. Elektron raqamli imzo texnologiyasi butun dunyo bo‘ylab keng qo‘llaniladi. U elektron tijorat, moliyaviy sektorda, hukumat xizmatlarida, boshqaruv tizimlarida, va boshqa ko‘plab sohalarda muhim ahamiyatga ega. Elektron imzolar orqali shartnomalar, to‘lovlar, va boshqa hujjatlar xavfsiz va qonuniy tarzda amalga oshiriladi. Hujjatlarning elektron shaklda saqlanishi va tasdiqlanishi jarayonida, elektron raqamli imzo texnologiyasi ishonchlilikni ta'minlab, tizimlar o‘rtasida muammosiz hamkorlikni davom ettirishga imkon beradi.

Elektron Imzolarni Kelajakda Rivojlantirish. Elektron raqamli imzolarni yanada rivojlantirish uchun bir qator imkoniyatlar mavjud. Avvalo, **biometrik autentifikatsiya** texnologiyalarining yanada takomillashishi, foydalanuvchilarning haqiqiyligini tasdiqlashda yanada ishonchli va qulay usullarni taqdim etadi. **Blockchain** texnologiyasining rivojlanishi, esa raqamli hujjatlar va imzolarni xavfsiz va o‘zgartirilmas tarzda saqlash imkoniyatlarini kengaytiradi. Shuningdek, **sun'iy intellekt** va **kengaytirilgan analizlar** yordamida, imzolangan hujjatlarni va ularning o‘zgarishlarini avtomatik ravishda kuzatish va tahlil qilish imkoniyatlari ham mavjud. Bu texnologiyalar nafaqat xavfsizlikni ta'minlaydi, balki hujjatlarni boshqarish jarayonlarini samarali va tezlashtirilgan holda amalga oshirishga yordam beradi. Elektron raqamli imzolar va ular asosidagi texnologiyalar rivojlanishi bilan, dunyo bo‘ylab elektron tizimlarda ishlov berish va tranzaktsiyalarni bajarish yanada xavfsiz, tez va samarali bo‘ladi. Kelajakda, elektron imzo texnologiyalari nafaqat davlat va yirik tijorat sohalarida, balki kichik va o‘rta biznesda ham keng qo‘llanilishi kutilmoqda. Xulosa qilib aytganda, elektron raqamli imzo texnologiyasining

rivojlanishi va zamonaviy turlarining kengayishi, axborot xavfsizligini ta'minlashda, hujjatlarning o‘zgartirilmasligini nazorat qilishda, va ishonchli elektron tranzaktsiyalarni amalga oshirishda asosiy vosita bo‘lib xizmat qilmoqda. Elektron imzo tizimlarining kelajagi, innovatsiyalarni o‘z ichiga olgan holda, ko‘plab yangi imkoniyatlar yaratadi va elektron hujjatlar bilan ishlashni yanada xavfsiz, tezkor va samarali qiladi.

FOYDALANILGAN ADABIYOTLAR:

1. Aripov X.K. va boshq. “Elektronika” O.F.M.J.N. T. 2012 y.400 b.

2. Fraiden_Dzh. Handbook of “Modem sensors”, Sovremennbie datchiki. 2004, New-York,470 p.

3. Гусев В.Г., Гусев Ю.М. Электроника - Москва.: Высшая школа, 2006г. 342 с.

4. N.R.Yusupbekov va boshq. Texnologik jarayonlami nazorat qilish va avtomatlashtirish. T.2011,576 c. 5.Бохан Н.И. и др. Средства автоматики и телемехеники. - М.: Агропромиздат, 1992,

6. Faxriddin B., No‘monbek A. ABS SISTEMASI BILAN JIHOZLANGAN M1 TOIFALI AVTOMOBILLARNING TORMOZ SAMARADORLIGINI MATEMATIK NAZARIY TAHLILI //International journal of scientific researchers (IJSR) INDEXING. – 2024. – Т. 4. – №. 1. – С. 333-337.

7.Qurbonazarov S. et al. ANALYSIS OF THE FUNDAMENTALS OF MATHEMATICAL MODELING OF WHEEL MOVEMENT ON THE ROAD SURFACE OF CARS EQUIPPED WITH ABS //Multidisciplinary Journal of Science and Technology. – 2024. – Т. 4. – №. 8. – С. 45-50.

8.Xuzriddinovich B. F. et al. ABS BILAN JIHOZLANGAN AVTOMOBILNI TORMOZ PAYTIDA O ‘ZO ‘ZIDAN VA MAJBURIY TEBRANISHLARINI TORMOZ SAMARADORLIGIGA TA’SIRINI TAHLIL QILISH //ОБРАЗОВАНИЕ НАУКА И ИННОВАЦИОННЫЕ ИДЕИ В МИРЕ. – 2024. – Т. 47. – №. 4. – С. 81-87.

9. Xusinovich T. J., Ro‘zibayevich M. N. M1 TOIFALI AVTOMOBILLARNI TURLI MUHITLARDA TORMOZLANISHINI TAHLIL QILISH VA PARAMETRLARINI O ‘RGANISH.

10. Karshiev F. U., Abduqahorov N. ABS BILAN JIHOZLANГAN M1 TOIFALI AVTOMOBILLAR TORMOZ TIZIMLARINING USTIVORLIGI //Academic research in educational sciences. – 2024. – Т. 5. – №. 5. – С. 787-791. 11.Каршиев Фахридин Умарович, Н.Абдуқаҳоров ИЗУЧЕНИЕ МИКРОСТРУКТУРЫ СТАЛИ В МАТЕРИАЛОВЕДЕНИ//https://www.iupr.ru/6-121-2024 https://www.iupr.ru/_files/ugd/b06fdc_15c4798c874a4ddab326a52bd3af34ea.pdf?index=true

12. Xusinovich T. J., Ro‘zibayevich M. N. M1 TOIFALI AVTOMOBILLARNI TURLI MUHITLARDA TORMOZLANISHINI TAHLIL QILISH VA PARAMETRLARINI O ‘RGANISH.

13. Farxadjonovna, Bekimbetova Elmira, and Abduqahorov No‘monbek. "STARTING ENGINES AT LOW TEMPERATURES." Multidisciplinary Journal of Science and Technology 5.2 (2025): 83-87.

14. Xusinovich, Turdialiyev Jonibek, and Mo‘minov Nurali Ro‘zibayevich. "M1 TOIFALI AVTOMOBILLARNI TURLI MUHITLARDA TORMOZLANISHINI TAHLIL QILISH VA PARAMETRLARINI O ‘RGANISH."

15. В. Я. Бочкарев. Новые технологии и средства измерений, методы организации водоучета на оросительных системах. Новочеркасск, 2012,227 с

16.В.А.Втюрин.Автоматизированные системы управления технологичес-кими процессами .Основы АСУТП. Санкт-Петербург 2006,154 с.

17.Рачков М.Ю. Технические средства автоматизатсии.- Москва: МГИУ, 2006,-347 с. 9.Vohidov A.X. Abdullaeva D.A. Avtomatikanmg texnik vositalari. T..TIMI, 2011.180 b.