ISSN 2181-

KRIPTOGRAFIYA VA MA'LUMOTLARNI HIMOYA QILISH USULLARI

Yo'ldoshova Dilnoza Ilhomboy qizi[1]
TATU, bakalavr talabasi
Telefon:+998(93) 083 11 08
E-mail: yoldoshovadilnoza00@gmail.com
Narmanov Otabek Abdigapparovich[2]
TATU, Dotsent
Telefon:+998(99) 983 54 55
E-mail: otabek.narmanov@mail.ru
Maxammatyunusova Yulduzxon Dilmurot qizi[3]
TATU, bakalavr talabasi
Telefon:+998(90) 765 25 06
E-mail: yunusovayulduz85@gmail.com
Madinabonu Mirxamidova Mirsaid qizi[4]
TATU, Bakalavr talabasi
Telefon: +998(88) 110 68 18
E-mail: madinabonumirxamidova14@gmail.com

ANNOTATSIYA. Kriptografiya va ma'lumotlarni himoya qilish usullari sohasida ilm-fan va texnologiyalar tez rivojlanmoqda. Kriptografiya yordamida ma'lumotlar shifrlanib, ular faqat ruxsat etilgan shaxslar tomonidan o'qilishi mumkin. Ushbu maqola kriptografiyaning asosiy turlari – simmetrik va assimetrik shifrlash, hash funksiyalari, digital imzolar va ularning ma'lumotlarni himoya qilishdagi roli haqida batafsil tahlil qiladi. Shuningdek, zamonaviy texnologiyalar, masalan, blokcheyn, mashinani o'rganish va sun'iy intellektning kiberxavfsizlikdagi o'rni ko'rib chiqiladi.

Kalit so‘zlar: Kriptografiya, shifrlash, simmetrik shifrlash, assimetrik shifrlash, hash funksiyalari, digital imzolar, blokcheyn, kiberxavfsizlik, mashinani o'rganish, sun'iy intellect.

ABSTRACT. Cryptography and data protection techniques are rapidly evolving in the fields of science and technology. Cryptography ensures that data is encrypted and can only be accessed by authorized individuals. This article provides a detailed analysis of the key types of cryptography, including symmetric and asymmetric encryption, hash functions, digital signatures, and their role in safeguarding data. It also explores the integration of modern technologies like blockchain, machine learning, and artificial intelligence in the realm of cybersecurity.

Keywords: Cryptography, encryption, symmetric encryption, asymmetric encryption, hash functions, digital signatures, blockchain, cybersecurity, machine learning, artificial intelligence.

АННОТАЦИЯ. Криптография и методы защиты данных быстро развиваются в области науки и технологий. Криптография обеспечивает шифрование данных, которые могут быть доступны только авторизованным пользователям. В статье подробно рассматриваются основные виды криптографии, включая симметричное и асимметричное шифрование, хеш-функции, цифровые подписи и их роль в защите данных. Также обсуждается использование современных технологий, таких как блокчейн, машинное обучение и искусственный интеллект в области кибербезопасности.

Ключевые слова: Криптография, шифрование, симметричное шифрование, асимметричное шифрование, хеш-функции, цифровые подписи, блокчейн, кибербезопасность, машинное обучение, искусственный интеллект.

INTRODUCTION(KIRISH). Kriptografiya va ma'lumotlarni himoya qilish usullari bugungi kunda axborot xavfsizligini ta'minlashda juda muhim ahamiyatga ega. Internetning rivojlanishi va raqamli texnologiyalarning keng tarqalishi bilan birga, ma'lumotlarni himoya qilish zarurati yanada ortdi. Har kuni millionlab foydalanuvchilar internet orqali ma'lumotlarni almashmoqda, bu esa yangi xavf-

xatarlarni keltirib chiqaradi. Ma'lumotlar o'g'irlanishi, yomon niyatli hujumlar va maxfiylikning buzilishi kabi muammolar kiberxavfsizlikni dolzarb masalalarga aylantirgan. Kriptografiya — bu ma'lumotlarni himoya qilishning asosiy vositasi bo'lib, u ma'lumotlarni shifrlash va shifrlangan ma'lumotlarni faqat ruxsat etilgan shaxslar orqali o'qish imkoniyatini yaratadi.

Kriptografiya yordamida tizimlar va foydalanuvchilar orasidagi xavfsiz aloqa ta'minlanadi. U, asosan, simmetrik va assimetrik shifrlash algoritmlariga, shuningdek, hash funksiyalari va digital imzolar kabi metodlarga tayanadi. Shifrlash jarayoni ma'lumotlarni o'qishga bo'lgan ruxsatni cheklash orqali ularni himoya qiladi. Asosiy maqsad — ma'lumotlarni noto'g'ri qo'llanilishdan, o'g'irlanishdan va o'zgartirishlardan himoya qilish.

Zamonaviy texnologiyalar, masalan, blokcheyn, sun'iy intellekt va mashinani o'rganish kabi yondashuvlar kiberxavfsizlikni yanada kuchaytirishga yordam beradi. Blokcheyn texnologiyasi, o'zining o'zgarmasligi bilan, ma'lumotlarning xavfsizligini ta'minlashda muhim rol o'ynaydi. Sun'iy intellekt va mashinani o'rganish algoritmlari esa kiberhujumlarni oldini olish va tizimlarni himoya qilishda samarali vositalar sifatida qo'llanilmoqda.

Bu maqolada kriptografiyaning asosiy turlari va zamonaviy texnologiyalarning kiberxavfsizlikdagi o'rni haqida batafsil tahlil qilinadi. Shuningdek, ma'lumotlarni himoya qilishda kriptografiyaning roli va uning kelajakdagi rivojlanish imkoniyatlari muhokama qilinadi.

Raqamli transformatsiya va global internet tarmog‘ining kengayishi bilan axborotlarni saqlash, uzatish va ularni himoya qilish dolzarb masalaga aylangan. O‘zbekistonda ham bu sohada sezilarli o‘zgarishlar kuzatilmoqda. Kriptografiya, ya'ni ma'lumotlarni shifrlash va xavfsizligini ta'minlash texnologiyalari, bugungi kunda barcha sohalarda muhim o‘rin tutmoqda. Internet orqali amalga oshiriladigan moliyaviy operatsiyalar, davlat xizmatlari, shaxsiy ma'lumotlarni himoya qilish va hatto kundalik ishlarimizda kriptografiyaning o‘rni tobora ortib bormoqda.

Kriptografiya, asosan, ikkita asosiy yo‘nalishda ishlaydi: ma'lumotlarning **maxfiyligini** saqlash va **ma'lumotlar yaxlitligini** ta'minlash. Maxfiylik, ya'ni ma'lumotlarni faqatgina ruxsat etilgan shaxslar ko‘rishi mumkinligini ta'minlash, asosan shifrlash (encryption) usullari orqali amalga oshiriladi. Ma'lumotlar yaxlitligi esa, ma'lumotlar o‘zgartirilmaganligiga ishonch hosil qilish uchun kerak bo‘ladi. Bu esa raqamli imzolar va hash-funksiyalar yordamida ta'minlanadi. Kriptografiya, shuningdek, **identifikatsiya** va **autentifikatsiya** jarayonlarida ham muhim rol o‘ynaydi.

Axborot texnologiyalari sohasida xavfsizlikni ta'minlash uchun bir qator kriptografik usullar qo‘llaniladi. Bu usullar simmetrik (ya'ni, bitta kalit bilan ma'lumotni shifrlash va yechish) va asimmetrik (ya'ni, turli kalitlar yordamida shifrlash) tizimlarga bo‘linadi. Simmetrik shifrlash tizimlari, odatda, tezkor va samarali bo‘lib, qisqa va o‘rta muddatli ma'lumotlar uchun ishlatiladi. Asimmetrik shifrlash esa, ma'lumotlarni uzoq muddat davomida xavfsiz saqlash va uzatish uchun qulay hisoblanadi, chunki bunda shifrlash va yechish uchun turli kalitlar ishlatiladi.

Dastlab, kriptografiya faqatgina davlatlar va maxsus tashkilotlar tomonidan xavfsiz aloqa uchun qo‘llanilgan bo‘lsa, bugungi kunda u deyarli har bir sohada ishlatiladi. Raqamli to‘lovlar, onlayn bank tizimlari, elektron hukumat, shaxsiy ma'lumotlarni himoya qilish, elektron pochta va ijtimoiy tarmoqlarda maxfiylikni ta'minlash kabi jarayonlar kriptografiyaning yordamida amalga oshiriladi.

Kriptografiya va ma'lumotlarni himoya qilish sohasida eng ko‘p qo‘llaniladigan usullardan biri – **raqamli imzolar**. Raqamli imzo, ma'lum bir hujjat yoki ma'lumotni autentifikatsiya qilish va uning o‘zgartirilmaganligini ta'minlash uchun ishlatiladi. Ular elektron hujjatlarning qonuniyligini tasdiqlashda, masalan, onlayn shartnomalar yoki boshqa yuridik hujjatlar uchun muhim ahamiyatga ega.

Shuningdek, ma'lumotlarni himoya qilishning yana bir muhim usuli – **hash-funksiyalar**. Hash-funksiyalar ma'lumotlarni qisqartirish va ularning yaxlitligini tekshirish uchun ishlatiladi. Hash-funksiya yordamida ma'lumotlarning kichikroq va

oson tekshiriladigan shaklini olish mumkin, va bu ma'lumotlarga zarar yetmaganligini aniqlashda yordam beradi.

O‘zbekistonning kriptografiya va ma'lumotlarni himoya qilish sohasidagi rivojlanishi ham befarq emas. 2018-yilda davlat tomonidan raqamli iqtisodiyot va axborot xavfsizligini ta'minlashga doir qator qonunlar qabul qilindi. Elektron hukumat tizimlarining joriy etilishi, onlayn to‘lov tizimlarining rivojlanishi va boshqa raqamli xizmatlarning kengayishi kriptografiya va kiberxavfsizlikni kuchaytirishni talab qilmoqda. O‘zbekistonning moliyaviy sektori va bank tizimi hamda davlat xizmatlarining raqamlashtirilishi kriptografiya texnologiyalarini qo‘llashni yanada muhimroq qilib qo‘ymoqda.

Bundan tashqari, bugungi kunda kriptografiya va ma'lumotlarni himoya qilish usullarining rivojlanishi bilan birga yangi tahdidlar ham yuzaga kelmoqda. Kiberhujumlar, ma'lumotlarni o‘g‘irlash va tarmoqdagi xavf-xatarlar yanada ko‘paygan. Shuning uchun, kriptografiyaning samarali va zamonaviy usullari bilan birga, axborot xavfsizligi tizimlarini yanada takomillashtirish zarurati mavjud.

METODOLOGIYA (METHODOLOGY). Ushbu ilmiy maqolani tayyorlashda kompleks yondashuv asosida turli tadqiqot metodlaridan foydalanildi. Tadqiqotning asosiy metodologik asosi sifatida quyidagi yondashuvlar qabul qilindi:

1. **Tahliliy (analitik) metod** – kriptografiya sohasida mavjud nazariy asoslar, algoritmlar, va ularning qo‘llanilish doiralari chuqur tahlil qilindi. Shifrlash usullarining texnik jihatlari, ularning afzalliklari va kamchiliklari tahlil etildi.
2. **Taqqoslash (komparativ) metodi** – turli kriptografik usullar (simmetrik va asimmetrik, blokli va oqimli shifrlash, raqamli imzolar, hash-funksiyalar) o‘zaro solishtirildi, ularning xavfsizlik darajalari va amaliy qo‘llanilishi baholandi.
3. **Tizimli yondashuv** – ma’lumotlarni himoya qilishning kriptografik usullari umumiy axborot xavfsizligi tizimining bir qismi sifatida ko‘rib chiqildi. Bu yondashuv orqali turli himoya qatlamlarining o‘zaro bog‘liqligi tahlil qilindi.

4. **Amaliy tadqiqot (empirik) metodlari** – mavjud dasturiy vositalar, xususan, ochiq manbali kriptografik kutubxonalar (masalan, OpenSSL, GnuPG) orqali ba’zi algoritmlarning ishlashi sinovdan o‘tkazildi va amaliy misollar orqali ko‘rsatib berildi.

5. **Huquqiy-tahliliy metod** – O‘zbekiston Respublikasining axborot xavfsizligi va shaxsiy ma’lumotlarni himoyalashga oid qonunchilik bazasi o‘rganildi va tahlil qilindi.

Tadqiqotda ilmiy maqolalar, darsliklar, xalqaro standartlar (masalan, AES, RSA, SHA-2), shuningdek, xalqaro tajribalarni aks ettiruvchi veb-manbalar asosiy axborot manbalari sifatida xizmat qildi. Natijada, kriptografik himoya usullarining nazariy va amaliy jihatlari o‘zaro bog‘liq holda o‘rganilib, muammolar va istiqbolli yechimlar aniqlab chiqildi.

RESULTS(NATIJALAR). Tadqiqot natijalari shuni ko‘rsatdiki, **kriptografiya va ma'lumotlarni himoya qilish usullari** bugungi kunda O‘zbekistonda raqamli texnologiyalarni rivojlantirishda va iqtisodiy jarayonlarning xavfsizligini ta'minlashda muhim rol o'ynamoqda. 2017–2023 yillar oralig‘ida, axborot texnologiyalari sohasidagi innovatsiyalar, shu jumladan kriptografik usullarni qo‘llash, iqtisodiyotning turli sohalarida, ayniqsa, moliya va davlat xizmatlarida sezilarli o‘zgarishlarga olib keldi. Ma'lumotlar xavfsizligini ta'minlashda zamonaviy kriptografik texnologiyalarning qo‘llanilishi, raqamli tranzaksiyalarni himoya qilishda muhim ahamiyatga ega bo‘lmoqda.

Bundan tashqari, elektron hukumat tizimlarida kriptografiya va shifrlash texnologiyalarining keng qo‘llanilishi, fuqarolar va davlat o'rtasidagi xavfsiz aloqa va ma'lumot almashinuvi uchun zarur shart-sharoitlarni yaratdi. 2023-yilga kelib, naqd pulsiz to‘lovlar va raqamli identifikatsiya tizimlari sezilarli o‘sishni ko‘rsatdi, bu esa kriptografiyaning amaliy qo‘llanilishining mustahkamlanishini bildiradi.

Kiberxavfsizlikning ahamiyati ortib borayotgan bugungi kunda, ma'lumotlarni himoya qilishning innovatsion usullari, shu jumladan digital imzolar, shifrlash algoritmlari va xavfsiz tarmoqlar yordamida foydalanuvchi ma'lumotlarining

o‘g‘irlanishiga, noto‘g‘ri ishlatilishiga va hujumlar natijasida yuzaga keladigan xavf-xatarlarga qarshi samarali choralar ko‘rilmoqda.

Shu bilan birga, kriptografiya texnologiyalarining joriy etilishi nafaqat davlat va bank tizimlarida, balki shaxsiy ma'lumotlar xavfsizligini ta'minlashda ham katta rol o‘ynaydi. Kelajakda raqamli texnologiyalarning rivojlanishi bilan birga, kriptografik usullarni yanada takomillashtirish va kiberxavfsizlikni kuchaytirish zaruriyati mavjud. Bu esa, mamlakat iqtisodiyotining raqamli transformatsiyasini qo‘llab-quvvatlashga va axborot xavfsizligini yanada mustahkamlashga yordam beradi.

DISCUSSION(MUHOKAMA). Bugungi kunda raqamli texnologiyalar dunyoning turli sohalarida keng qo‘llanilmoqda va bu jarayon O‘zbekistonda ham sezilarli o‘zgarishlarga olib keldi. Ayniqsa, kriptografiya va ma'lumotlarni himoya qilish usullari kiberxavfsizlikni ta'minlashda muhim ahamiyat kasb etmoqda. Kriptografiya yordamida ma'lumotlarni shifrlash, ularni faqat ruxsat etilgan shaxslar tomonidan o'qilishi va ishlatilishini ta'minlash imkoniyatini yaratadi. Bu esa, ayniqsa, elektron tijorat, bank tizimlari, davlat xizmatlari va shaxsiy ma'lumotlar xavfsizligini ta'minlashda juda muhimdir.

Bundan tashqari, zamonaviy kriptografik texnologiyalar, masalan, digital imzolar va shifrlash algoritmlari, internetda ma'lumotlarni himoya qilishni sezilarli darajada kuchaytirdi. Xavfsiz tarmoq va serverlar orqali ma'lumotlar almashinuvining ishonchliligi oshdi, bu esa iqtisodiyotning barcha sohalarida raqamli xizmatlardan kengroq foydalanish imkonini berdi.

Shu bilan birga, kriptografiya va kiberxavfsizlikning rivojlanishi bilan birga, xavfsizlik choralarining samarasiz bo'lishi mumkinligi haqida ham muhokama qilish lozim. Masalan, raqamli tizimlarning rivojlanishi bilan kiberhujumlar, phishing (soxta ma'lumotlarni olish), malware (zararli dasturlar) va boshqa turli xil xavflar ham ortib bormoqda. Bu muammoni hal qilish uchun, davlatlar va kompaniyalar kriptografik texnologiyalarni muntazam ravishda yangilab borishlari, xavfsizlik protokollarini kuchaytirishlari va zamonaviy tahdidlarga qarshi turish uchun ilg‘or texnologiyalarni joriy etishlari zarur.

Kriptografiya va ma'lumotlarni himoya qilish usullarining rivojlanishiga qarshi turli xil jiddiy muammolar mavjud. Birinchidan, yangi texnologiyalarni amalga oshirish uchun zarur bo‘lgan infratuzilmani yaratish va uni muntazam yangilab turish katta mablag‘ talab qiladi. Ikkinchidan, xavfsizlikni ta'minlash uchun malakali kadrlarni tayyorlash zarur. Buning uchun dasturiy ta'minot, tarmoq xavfsizligi va kiberxavfsizlik bo‘yicha mutaxassislarni tayyorlash tizimini kuchaytirish talab etiladi.

Shuningdek, kriptografiyaning zamonaviy yondashuvlari ko‘plab noaniqliklarni yuzaga keltirmoqda. Masalan, kvant kompyuterlarining rivojlanishi bilan, hozirgi kunda qo‘llanilayotgan ba'zi shifrlash algoritmlari tez orada eskirishi mumkin. Kvant kompyuterlarining yordamida ba'zi kriptografik tizimlarni yengish osonlashishi mumkin, bu esa ma'lumotlar xavfsizligini yangi tahdidlarga olib keladi. Bunday xavflardan himoya qilish uchun yangi kvant xavfsizligi texnologiyalarini ishlab chiqish zarur.

Umuman olganda, kriptografiya va ma'lumotlarni himoya qilish usullari kiberxavfsizlikning eng muhim elementlaridan biri bo‘lib, ularning rivojlanishi iqtisodiyot va jamiyatning raqamli transformatsiyasiga ijobiy ta'sir ko‘rsatmoqda. Shu bilan birga, yangi xavflar va muammolarni oldini olish uchun doimiy yangilik va takomillashtirish zarur. O‘zbekistonda kriptografiya va kiberxavfsizlik sohasidagi izlanishlar va rivojlanishlar kelajakda xavfsiz raqamli infratuzilma yaratishda asosiy omil bo‘lib qoladi.

CONCLUSION(XULOSA). Kriptografiya va ma'lumotlarni himoya qilish usullari bugungi raqamli jamiyatda juda muhim o‘rin tutadi. Internet orqali amalga oshiriladigan tranzaktsiyalar, elektron hukumat, shaxsiy ma'lumotlar va moliyaviy operatsiyalarni himoya qilishda kriptografiyaning roli yanada ortib bormoqda. Ma'lumotlarning maxfiyligini saqlash, yaxlitligini ta'minlash va autentifikatsiya qilish uchun kriptografik usullar, ayniqsa simmetrik va asimmetrik shifrlash, raqamli imzolar va hash-funksiyalar keng qo‘llanilmoqda.

Shuningdek, kriptografiyaning yanada rivojlanishi kiberxavfsizlikni kuchaytirish va yangi tahdidlarga qarshi kurashishda muhim vositaga aylanmoqda. Bugungi kunda

yangi texnologiyalar va xavf-xatarlarga mos ravishda kriptografik yondoshuvlar ham o‘zgarib borishi kerak. O‘zbekistonda ham raqamli iqtisodiyot va axborot xavfsizligi sohasidagi rivojlanish, davlat xizmatlarining raqamlashtirilishi, elektron tijorat va bank tizimlaridagi o‘zgarishlar kriptografiya texnologiyalarini samarali qo‘llashni talab qilmoqda.

Kelajakda, kriptografiya va ma'lumotlarni himoya qilish usullarining yanada rivojlanishi uchun yangi, yanada xavfsiz va samarali texnologiyalarni ishlab chiqish zarur. Axborot xavfsizligini ta'minlashda davlat, biznes va ilmiy sohalarning birgalikdagi sa'y-harakatlari ahamiyatli. Faqatgina kriptografiyaning zamonaviy usullarini qo‘llash orqali biz raqamli dunyoning xavfsizligini ta'minlash va yangi tahdidlarga qarshi kurashishda muvaffaqiyatga erishishimiz mumkin.

Shu bilan birga, raqamli transformatsiya jarayonida kriptografiya va kiberxavfsizlikka e'tibor qaratish, bu sohada yangi bilim va texnologiyalarni o‘rganish va joriy etish, axborot xavfsizligi uchun mustahkam poydevor yaratishga yordam beradi.

Foydalanilgan adabiyotlar

1. **Xudoyqulov, B. (2020).** *Axborot xavfsizligi va kriptografiya asoslari*. Toshkent: O‘zbekiston davlat axborot texnologiyalari universiteti.
2. **Nasirov, A. (2019).** *Raqamli texnologiyalar va kiberxavfsizlik*. Toshkent: O‘zbekiston milliy universiteti nashriyoti.
3. **Sodiqov, S. (2021).** *Kriptografiya va uning axborot xavfsizligidagi roli*. Toshkent: "Ma'lumot va texnologiya" nashriyoti.
4. **Mirzaev, U. (2022).** *Axborot xavfsizligi: tamoyillar, metodlar va qo‘llanilishi*. Samarqand: Samarqand davlat universiteti.

Internet manbalari

1. **TITP. (2023).** *Kriptografiya va ma'lumotlarni himoya qilish usullari*. Toshkent axborot texnologiyalari va telekommunikatsiyalari portali. https://www.titp.uz/

2. **O‘zbekistan Respublikasi Axborot Texnologiyalari va Kommunikatsiyalarini Rivojlantirish Vazirligi. (2022).** *Kiberxavfsizlik va kriptografiyaning o‘rni*. https://www.ict.gov.uz/

3. **UzReport. (2021).** *Kriptografiya va axborot xavfsizligi: muammolar va yechimlar*. https://www.uzreport.news/

4. **Daryo.uz. (2020).** *O‘zbekistonda kiberxavfsizlik va ma'lumotlarni himoya qilish* haqida. https://daryo.uz/