*PEDAGOGIK TADQIQOTLAR JURNALI* *№ 4,Fevral, 2025*
*ISSN: 3060-4923, Impact Factor – 7,212* *worldly knowledge*
*Index: google scholar, research gate, research bib, zenodo, open aire.*
*https://scholar.google.com/scholar?hl=ru&as_sdt=0%2C5&q=wosjournals.com&btnG*
*https://www.researchgate.net/search/publication?q=worldly%20knowledge*
*https://journalseeker.researchbib.com/view/issn/3060-4923*

# KRIPTOGRAFIYA VA MA'LUMOTLARNI SHIFRLASH TEXNOLOGIYALARI

***Jalolov Tursunbek Sadriddinovich***

*Osiyo xalqaro universiteti Dotsenti p.f.f.d.(PhD)*

**Annotatsiya:** Ushbu maqolada kriptografiyaning nazariy asoslari, ma'lumotlarni shifrlash texnologiyalarining rivojlanishi va ularning amaliy qo'llanilishi, shuningdek, zamonaviy axborot xavfsizligidagi o'rni tahlil etiladi. Maqola davomida shifrlash usullarining tarixiy rivojlanishi, simmetrik va assimetrik shifrlash algoritmlari, kriptografik protokollar, raqamli imzo va sertifikatlar, shuningdek, kvant kriptografiyasi kabi yangi yo'nalishlar yoritiladi. Tadqiqot natijalari asosida ma'lumotlarni himoya qilishda innovatsion texnologiyalar, ularning samaradorligi va xavf-xatarlarni kamaytirish strategiyalari haqida mulohazalar bildiriladi.

**Kalit so'zlar:** kriptografiya, shifrlash, simmetrik algoritmlar, assimetrik algoritmlar, raqamli imzo, kvant kriptografiyasi, axborot xavfsizligi, kriptografik protokollar.

Kirish bosqichida, global axborot jamiyati va raqamli iqtisodiyotning tez sur'atlar bilan rivojlanishi sharoitida ma'lumotlarni himoya qilish muammosi dolzarb ahamiyat kasb etmoqda. Kriptografiya – bu axborotlarning sirligini ta'minlash, ma'lumotlar oqimini nazorat qilish va identifikatsiyalashda asosiy vosita sifatida paydo bo'lgan fan bo'lib, u tarixiy ildizlari qadimgi shifrlash usullaridan boshlanib, bugungi kunda murakkab matematik modellar va algoritmlar asosida amalga oshiriladi. Maqolamizda kriptografiyaning nazariy asoslari, shifrlash texnologiyalari va ularning real tizimlardagi qo'llanilish jarayoni, shuningdek, yangi tahdidlar va innovatsion yechimlar tafsilotlari yoritiladi.

Asosiy qismda, avvalo, kriptografiyaning tarixiy rivojlanishi haqida so'z yuritiladi. Qadimgi davrlarda yozma ma'lumotlarni himoya qilish uchun oddiy almashtirish (substitution) va transpozitsiya (transposition) usullari qo'llanilgan bo'lsa, hozirgi zamon kriptografiyasi matematik va kompyuter texnologiyalarining ilg'or yutuqlariga tayanadi. Simmetrik shifrlash algoritmlari, masalan, DES (Data Encryption Standard) va AES (Advanced Encryption Standard) kabi metodlar ma'lumotlarni tezkor va samarali himoya qilishda keng qo'llaniladi. Ushbu usullarda shifrlash va deshifrlash uchun bitta kalit ishlatiladi, bu esa tizimning tezligini ta'minlasa-da, kalitning maxfiyligini saqlash masalasida qo'shimcha choralarni talab qiladi.

Assimetrik shifrlash esa, boshqa tomonlama kalitlar – ochiq va yopiq kalitlar yordamida amalga oshiriladi. RSA algoritmi ushbu yondashuvning eng mashhur namunasi bo'lib, u ma'lumotlarni himoya qilish, raqamli imzo va elektron imzo tizimlarida keng qo'llaniladi. Assimetrik shifrlashning afzalligi shundaki, kalit almashinuvi jarayonida maxfiylik kafolati ta'minlanadi va bu usul ayniqsa elektron tijorat va onlayn bank ishlarida katta ahamiyatga ega. Shuningdek, kriptografik protokollar – SSL/TLS, IPSec va boshqalar orqali internet orqali uzatilayotgan ma'lumotlarning xavfsizligi ta'minlanadi. Ushbu protokollar internet tarmog'idagi axborot oqimlarini shifrlash va autentifikatsiya qilish orqali kiberhujumlar, ma'lumotlar buzilishi va identitet soxtalashtirish kabi tahdidlarga qarshi samarali himoya mexanizmlarini taqdim etadi.

Bugungi kunda raqamli imzo va sertifikatlar tizimi, elektron hujjatlarni himoya qilishda va huquqiy jihatdan tasdiqlashda muhim vosita sifatida qaralmoqda. Raqamli imzo algoritmlari

hujjatning haqiqiyligini, o‘zgarmasligini va yuboruvchining identifikatsiyasini ta’minlashda qo‘llaniladi. Ushbu texnologiyalar huquqiy ishonchlilikni oshirish bilan birga, elektron savdo va onlayn xizmatlar ishonchliligini ham ta’minlaydi.

Yaqinda paydo bo‘lgan kvant kriptografiyasi esa, an’anaviy shifrlash metodlariga nisbatan tubdan yangi yondashuvni ifodalaydi. Kvant mexanikasi tamoyillariga asoslangan bu usul, ayniqsa, kvant kompyuterlari kelgusi xavfi nazarda tutilganda dolzarb ahamiyat kasb etadi. Kvant kriptografiyasida kalitlarni tarqatish uchun kvant xususiyatlaridan foydalaniladi va bu orqali kalitlarni soxtalashtirish imkoniyati deyarli yo‘qoladi. Shu bilan birga, ushbu texnologiyaning amaliy qo‘llanilishi uchun hozirgi kunda murakkab tajriba va ilmiy-texnikaviy echimlar talab qilinadi, ammo kelajakda u keng ommalashishi kutilmoqda.

Kriptografiyaning nazariy jihatlari va amaliy qo‘llanilishida matematik modellar, ehtimollik nazariyasi, raqamli algoritmlar va hisoblash nazariyasi muhim o‘rin tutadi. Shifrlash algoritmlarining xavfsizligi matematik jihatdan ishonchli bo‘lishi kerak, ya’ni ularni buzish uchun ishlatiladigan usullar mavjud bo‘lmagan yoki ancha murakkab bo‘lishi lozim. Shu sababli, matematik tekshirish va kriptanaliz sohalarida olib borilayotgan ilmiy tadqiqotlar yangi va yanada mustahkam algoritmlarni yaratishda hal qiluvchi rol o‘ynaydi. Amaliy tomondan qaraganda, kriptografik tizimlar nafaqat axborotlarni himoya qilish, balki tizimlararo ishonchni shakllantirish, elektron to‘lovlar va shaxsiy ma’lumotlar almashinuvi kabi jarayonlarda ham asosiy o‘rinni egallaydi.

Zamonaviy raqamli iqtisodiyotda ma’lumotlarning xavfsizligini ta’minlash faqat texnologik yechimlar bilan chegaralanmaydi, balki tashkilotlar, davlat va butun jamoatchilik tomonidan qo‘llab-quvvatlanishi zarur bo‘lgan strategik yondashuvni talab qiladi. Kiberhujumlar, ma’lumotlar o‘g‘irlanishi va soxtalashtirish tahdidlari raqamli makonning ajralmas qismi bo‘lib, ushbu tahdidlarga qarshi kurashish uchun xalqaro hamkorlik, standartlar va qonunchilik hujjatlari ishlab chiqilmoqda. Shu munosabat bilan, axborot xavfsizligini ta’minlashda shifrlash texnologiyalari, xavfsizlik siyosati va inson resurslarini rivojlantirish hamkorlikda ko‘rilishi lozim.

Kriptografiya va ma’lumotlarni shifrlash texnologiyalari, shubhasiz, zamonaviy jamiyatda axborotlarning maxfiyligini saqlash, ishonchli kommunikatsiyani tashkil etish va raqamli tizimlarning barqarorligini ta’minlashda asosiy omil sifatida e’tirof etiladi. Ushbu texnologiyalar nafaqat ilmiy tadqiqotlar, balki kundalik hayotda ham qo‘llanilmoqda: bank tizimlaridan tortib, davlat ma’lumotlarini himoya qilish, shaxsiy qurilmalarda ma’lumotlarni shifrlashgacha keng doirada ishlatiladi. Shuningdek, internet orqali amalga oshiriladigan onlayn tranzaksiyalar va elektron tijorat jarayonlari xavfsizligini ta’minlashda kriptografiyaning o‘rni beqiyosdir. Bu boradagi innovatsiyalar kelajakda yanada rivojlanishi, yangi texnologik yechimlar va algoritmlarning amaliyotga tadbiq etilishi, shuningdek, kiberxavfsizlik sohasidagi yangi xavf-xatarlar va ularning oldini olish strategiyalarini yaratishda asosiy o‘rinni egallaydi.

Xulosa qilib aytganda, kriptografiya va ma’lumotlarni shifrlash texnologiyalari zamonaviy axborot xavfsizligining poydevorini tashkil etadi. Ushbu maqolada tarixiy rivojlanish, simmetrik va assimetrik shifrlash usullari, raqamli imzo, kvant kriptografiyasi va kriptografik protokollar asosida ma’lumotlarni himoya qilish mexanizmlari keng yoritildi. Axborot jamiyatining murakkab tahdidlari sharoitida, innovatsion texnologiyalar va matematik asosga tayanadigan

yechimlar orqali ma’lumotlarning maxfiyligi, butunligi va ishonchliligi ta’minlanishi lozim. Kelajakda olib boriladigan ilmiy tadqiqotlar va texnologik yangilanishlar ushbu sohani yanada mustahkam va samarali tizimlarga aylantirishga qaratilgan bo‘lib, shaxsiy, korporativ va davlat darajasida xavfsizlik strategiyalarining yagona tizim sifatida shakllanishiga xizmat qiladi.

Umuman olganda, kriptografiya nafaqat ilmiy fan sifatida, balki kundalik hayotning ajralmas qismiga aylangan texnologiya sifatida o‘z ahamiyatini saqlab qolmoqda. Ma’lumotlarni shifrlash, maxfiylikni ta’minlash va axborot oqimini ishonchli tarzda boshqarish bugungi kunda va kelajakda ham dolzarb masala bo‘lib, uning yechimida ilmiy izlanishlar, texnologik innovatsiyalar va xalqaro hamkorlik muhim rol o‘ynaydi. Shu sababli, ushbu yo‘nalishda olib borilayotgan izlanishlar va yangi texnologiyalar, raqamli dunyoning xavfsizligi va barqaror rivojlanishini ta’minlashda hal qiluvchi omil bo‘lib qolmoqda.

Natijada, kriptografiya va ma’lumotlarni shifrlash texnologiyalarining chuqur nazariy va amaliy jihatlari, ularning tarixi, bugungi kundagi qo‘llanilishi va kelgusidagi istiqbollari yoritildi. Ushbu yondashuv axborot xavfsizligini mustahkamlash, elektron tijorat, bank tizimlari va davlat ma’lumotlarini himoya qilishda innovatsion echimlarni ishlab chiqish uchun poydevor yaratadi. Kelajakda kriptografiya sohasida qo‘shimcha tadqiqotlar, yangi shifrlash algoritmlari va xavfsizlik protokollarining joriy etilishi orqali, axborotlarning butunligi va maxfiyligi yanada yuqori darajaga ko‘tariladi, bu esa raqamli jamiyatning barqarorligi va ishonchliligiga xizmat qiladi.

Ushbu maqola orqali kriptografiyaning nazariy asoslari, amaliy qo‘llanilishi va texnologik rivojlanishidagi dolzarb masalalar keng tahlil qilinib, axborot xavfsizligini ta’minlashda shifrlash texnologiyalarining o‘rni va ahamiyati aniqlandi. Umid qilamizki, mazkur yondashuv va tahliliy mulohazalar kelgusida kriptografiya sohasida yanada innovatsion yondashuvlar va xavfsizlik strategiyalarini ishlab chiqishga, shuningdek, raqamli muhitda ma’lumotlarning himoyasini ta’minlashga xizmat qiladi.

**Foydalanilgan adabiyotlar**

1. Jalolov, T. S. (2024). SOG ‘LIQNI SAQLASHDA SUN'IY INTELLEKTGA ASOSLANGAN DIAGNOSTIKA TIZIMLARINI YARATISH. Ensuring the integration of science and education on the basis of innovative technologies., 1(3), 13-18.
2. Jalolov, T. S. (2024). SUN'IY INTELLEKTNING IJTIMOIY TARMOQLARDAGI TASIRINI O ‘RGANISH: FOYDALANUVCHI XATTI-HARAKATLARINI TAHLIL QILISH. Ensuring the integration of science and education on the basis of innovative technologies., 1(3), 31-37.
3. Jalolov, T. S. (2024). TIBBIY TASVIRLARNI TAHLIL QILISH UCHUN CHUQUR O ‘QITISH ALGORITMLARINI QO ‘LLASH. Ensuring the integration of science and education on the basis of innovative technologies., 1(3), 19-24.
4. Jalolov, T. S. (2024). TA'LIM TIZIMIDA SUN'IY INTELLEKTNING BAHOLASH JARAYONLARIGA TA'SIRI: AVTOMATIK TEKSHIRISH TIZIMLARI. Ensuring the integration of science and education on the basis of innovative technologies., 1(3), 7-12.
5. Jalolov, T. S. (2024). INTELLEKTUAL DRON TIZIMLARIDA O ‘ZO ‘ZINI BOSHQARISH TEXNOLOGIYALARI. Ensuring the integration of science and education on the basis of innovative technologies., 1(3), 50-55.

6. Jalolov, T. S. (2024). KASALLIKLARNI ERTA ANIQLASHDA SUN'IY INTELLEKTNING QO ‘LLANILISHI: IMKONIYATLAR VA CHEKLOVLAR. Ensuring the integration of science and education on the basis of innovative technologies., 1(3), 38-43.
7. Jalolov, T. S. (2024). SUN'IY INTELLEKTGA ASOSLANGAN SHAXSIYLASHTIRILGAN O ‘QUV DASTURLARINI YARATISH. Ensuring the integration of science and education on the basis of innovative technologies., 1(3), 1-6.
8. Jalolov, T. S. (2024). IQTISODIY MODELLASHTIRISHDA SUN'IY INTELLEKT TEXNOLOGIYALARIDAN FOYDALANISH. Ensuring the integration of science and education on the basis of innovative technologies., 1(3), 44-49.
9. Jalolov, T. S. (2024). ПРИЛОЖЕНИЙ ДЛЯ ИЗУЧЕНИЯ ЯЗЫКА С ПОМОЩЬЮ АНАЛИЗА ТЕКСТА. Advanced methods of ensuring the quality of education: problems and solutions, 1(3), 106-111.
10. Jalolov, T. S. (2024). СРАВНЕНИЕ СИЛЬНЫХ И СЛАБЫХ МОДЕЛЕЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА. Advanced methods of ensuring the quality of education: problems and solutions, 1(3), 99-105.
11. Jalolov, T. S. (2024). ЗВУК РАБОТА АССИСТЕНТОВ ЭФФЕКТИВНОСТЬ УВЕЛИЧИВАТЬ ДЛЯ ПРЕПОДАВАНИЕ МЕТОДЫ. Advanced methods of ensuring the quality of education: problems and solutions, 1(3), 93-98.
12. Jalolov, T. S. (2024). ЭКОЛОГИЧЕСКИЙ СИСТЕМЫ ИСКУССТВЕННЫЙ В МОНИТОРИНГЕ ИНТЕЛЛЕКТ ТЕХНОЛОГИЙ ПРИЛОЖЕНИЕ. Advanced methods of ensuring the quality of education: problems and solutions, 1(3), 86-92.
13. Jalolov, T. S. (2024). НА ОСНОВЕ ИИ НАПАДЕНИЯ ПРОРОЧЕСТВО ДЕЛАТЬ И ЗАЩИЩАТЬ. Advanced methods of ensuring the quality of education: problems and solutions, 1(3), 60-65.
14. Jalolov, T. S. (2024). ОСНОВО МАШИННОГО ЯЗЫКА. Advanced methods of ensuring the quality of education: problems and solutions, 1(3), 46-52.
15. Jalolov, T. S. (2024). ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ С ИСПОЛЬЗОВАНИЕМ ФАЛЬШИВЫЙ ИНФОРМАЦИЯ ОПРЕДЕЛИТЬ МЕТОДЫ. Advanced methods of ensuring the quality of education: problems and solutions, 1(3), 53-59.
16. Jalolov, T. S. (2024). АЛГОРИТМЫ ПЛАНИРОВАНИЯ И ПРИНЯТИЯ РЕШЕНИЙ ДЛЯ РОБОТОТЕХНИКИ. Advanced methods of ensuring the quality of education: problems and solutions, 1(3), 73-79.
17. Jalolov, T. S. (2024). С ПОМОЩЬЮ ИИ СНОВА ПОДЛЕЖАЩИЙ ВОЗМЕЩЕНИЮ ЭНЕРГИЯ ИСТОЧНИКИ РАБОТА ЭФФЕКТИВНОСТЬ ОПТИМИЗАЦИЯ. Advanced methods of ensuring the quality of education: problems and solutions, 1(3), 80-85.
18. Jalolov, T. S. (2024). ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ КИБЕРБЕЗОПАСНОСТЬ В СИСТЕМАХ ПРИМЕНЯТЬ УГРОЗЫ. Advanced methods of ensuring the quality of education: problems and solutions, 1(3), 66-72.
19. Jalolov, T. S. (2024). AI YORDAMIDA QAYTA TIKLANUVCHI ENERGIYA MANBALARINI OPTIMALLASHTIRISH. Modern digital technologies in education: problems and prospects, 1(2), 72-77.
20. Jalolov, T. S. (2024). ATROF-MUHIT MONITORINGIDA SUN'IY INTELLEKT TEXNOLOGIYALARINING QO ‘LLANILISHI. Modern digital technologies in education: problems and prospects, 1(2), 78-84.

21. Jalolov, T. S. (2024). MATNNI QAYTA ISHLASH ORQALI TIL O ‘RGATISH ILOVALARINI RIVOJLANTIRISH. Modern digital technologies in education: problems and prospects, 1(2), 103-108.
22. Jalolov, T. S. (2024). OVOZLI KO ‘MAKCHILARNING SAMARADORLIGINI OSHIRISH UCHUN CHUQUR O ‘QITISH USULLARI. Modern digital technologies in education: problems and prospects, 1(2), 85-90.
23. Jalolov, T. S. (2024). SUN'IY INTELLEKTNI KIBERXAVFSIZLIK TIZIMLARIDA QO ‘LLASH: TAHDIDLARNI ERTA ANIQLASH USULLARI. Modern digital technologies in education: problems and prospects, 1(2), 54-59.
24. Jalolov, T. S. (2024). KUCHLI VA ZAIF SUN'IY INTELLEKT MODELLARI: ULARNING TAQQOSLANISHI VA RIVOJLANISH ISTIQBOLLARI. Modern digital technologies in education: problems and prospects, 1(2), 91-96.
25. Jalolov, T. S. (2024). MASHINA O ‘QITISH ALGORITMLARINI OPTIMALLASHTIRISH: SAMARADORLIK VA ANIQLIKNI OSHIRISH USULLARI. Modern digital technologies in education: problems and prospects, 1(2), 97-102.
26. Jalolov, T. S. (2024). SUN'IY INTELLEKT YORDAMIDA SOXTA MA'LUMOTLARNI ANIQLASH USULLARI. Modern digital technologies in education: problems and prospects, 1(2), 47-53.
27. Jalolov, T. S. (2024). AI ASOSIDA HUJUMLARNI BASHORAT QILISH VA HIMOYA STRATEGIYALARINI ISHLAB CHIQISH. Modern digital technologies in education: problems and prospects, 1(2), 66-71.
28. Jalolov, T. S. (2024). KUCHLI AI BILAN JIHOZLANGAN ROBOTOTEXNIKA UCHUN REJALASHTIRISH VA QAROR QABUL QILISH ALGORITMLARI. Modern digital technologies in education: problems and prospects, 1(2), 60-65.