

POST-KVANT KRIPTOGRAFIYA ALGORITMLARINING AXBOROT XAVFSIZLIGINI TA'MINLASHDAGI SAMARADORLIGINI TAHLIL QILISH

<https://doi.org/10.5281/zenodo.23433002>

Saparboy Feruzbek Zohidjon o'g'li

E-mail: feruzbeksaparboyev905@gmail.com +998942301788

Toshkent amaliy fanlar universiteti, Axborot texnologiyalari fakulteti KAX 23 01 talabasi

Anotatsiya

Yetarlicha quvvatli kvant kompyuteri RSA, Diffi–Hellman va elliptik egri chiziqlarga asoslangan hozirgi ochiq kalitli kriptografiyani buza oladi. Maqolada NIST 2024–2025 yillarda tasdiqlagan post-kvant algoritmlari (ML-KEM, ML-Dsa, SLH-Dsa, FN-Dsa va HQC) axborot xavfsizligini ta'minlash nuqtayi nazaridan baholanadi. Samaradorlik uchta mezon bo'yicha tahlil qilinadi: kvant hujumiga qarshi mustahkamlik, kalit va imzo o'lchamlari hamda amalda joriy etilganlik darajasi. Tahlil shuni ko'rsatadiki, kalit almashinuvi uchun ML-KEM allaqachon real trafikda keng qo'llanilmoqda, imzolar uchun esa o'lcham va sertifikatlar muammosi saqlanib qolmoqda. Maqola oxirida o'tish strategiyasi (inventarizatsiya, gibrid sxemalar, kripto-chaqqonlik) bo'yicha tavsiyalar beriladi.

Kalit so'zlar

post-kvant kriptografiya, ML-KEM, ML-Dsa, SLH-Dsa, FN-Dsa, HQC, Shor algoritmi, "hozir yig', keyin shifrn och" hujumi, kripto-chaqqonlik.

Аннотация

Достаточно мощный квантовый компьютер способен взломать современную криптографию с открытым ключом (RSA, Диффи–Хеллман, эллиптические кривые). В статье оценивается эффективность постквантовых алгоритмов, стандартизированных NIST в 2024–2025 гг. (ML-KEM, ML-Dsa, SLH-Dsa, FN-Dsa, HQC), по трём критериям: стойкость к квантовым атакам, размеры ключей и подписей, степень практического внедрения. Показано, что ML-KEM уже широко используется в реальном трафике, тогда как для подписей остаются проблемы размера и сертификатов. Даны рекомендации по миграции: инвентаризация, гибридные схемы, криптоагильность.

Ключевые слова

постквантовая криптография, ML-KEM, ML-Dsa, SLH-Dsa, алгоритм Шора, «собери сейчас, расшифруй потом», криптоагильность.

Abstract

A sufficiently powerful quantum computer can break today's public-key cryptography (RSA, Diffie-Hellman, elliptic curves). The article evaluates the post-quantum algorithms standardised by NIST in 2024-2025 (ML-KEM, ML-DSA, SLH-DSA, FN-DSA, HQC) against three criteria: resistance to quantum attacks, key and signature sizes, and degree of real-world deployment. ML-KEM is already widely used in live traffic, while signatures still face size and certificate problems. Migration recommendations are given: inventory, hybrid schemes and crypto-agility.

Keywords

post-quantum cryptography, ML-KEM, ML-DSA, SLH-DSA, Shor's algorithm, harvest now decrypt later, crypto-agility.

Kirish

Internetdagi deyarli har bir himoyalangan ulanish – bank ilovasi, elektron pochta, davlat xizmatlari – ikkita ishga tayanadi: tomonlar umumiy maxfiy kalitni xavfsiz kelishib olishi va o‘zaro haqiqiy ekanini tekshirishi kerak. Buning uchun bugun RSA, Diffi-Xellman va elliptik egri chiziqli algoritmlar ishlatiladi. Ularning xavfsizligi katta sonlarni ko‘paytuvchilarga ajratish va diskret logarifmni topishning qiyinligiga asoslangan. Piter Shor 1994 yilda kvant kompyuterida bu ikkala masalani ham polinomial vaqtda yechish mumkinligini ko‘rsatdi [1]. Demak, yetarlicha quvvatli kvant kompyuteri paydo bo‘lsa, hozirgi ochiq kalitli kriptografiya butunlay yaroqsiz bo‘ladi.

Muammo "kvant kompyuteri hali yo‘q" degan fikr bilan hal bo‘lmaydi. Hujumchi bugun shifrlangan trafikni yozib olib, kelajakda, kvant kompyuteri paydo bo‘lganda ochishi mumkin. Bu "hozir yig‘, keyin shifrnı och" (harvest now, decrypt later) hujumi deb ataladi; CISA, NSA va NIST birgalikda chiqargan hujjatda ham aynan shu xavf sabab sifatida ko‘rsatilgan, ayniqsa uzoq yillar maxfiy qolishi kerak bo‘lgan ma‘lumotlar uchun [2]. Maqolaning maqsadi – post-kvant kriptografiya (PQC) algoritmlarining samaradorligini xavfsizlik, o‘lcham va joriy etilganlik bo‘yicha baholash hamda amaliy tavsiyalar berish.

1. Kvant tahdidining real ko‘lami

Kvant kompyuteri kriptografiyaning turli qismlariga turlicha ta‘sir qiladi (1-jadval). Shor algoritmi ochiq kalitli tizimlarni (RSA, DH, ECC) to‘liq sindiradi, shuning uchun ularni almashtirish shart. Grover algoritmi esa qidiruvni faqat kvadratik tezlashtiradi [3]: simmetrik shifr va xesh funksiyalarda bu xavfsizlik darajasini taxminan ikki baravar kamaytiradi, xolos. Shuning uchun ular uchun

kalit va xesh uzunligini oshirish yetarli: masalan, NSA o'zining CNSA 2.0 to'plamida AES-256 va SHA-384/SHA-512 ni talab qiladi [4].

1-jadval. Kvant hujumining kriptografik algoritmlarga ta'siri

Algoritm sinfi	Misol	Kvant hujumi	Chora
Ochiq kalitli shifrlash va kalit almashinuvi	RSA, Diffi-Hellman, ECDH	Shor algoritmi: to'liq buziladi	ML-KEM (FIPS 203) ga o'tish
Raqamli imzo	RSA, ECDSA	Shor algoritmi: to'liq buziladi	ML-DSA, SLH-DSA, FN-DSA
Simmetrik shifr	AES	Grover algoritmi: mustahkamlik taxminan ikki baravar kamayadi	AES-256 dan foydalanish
Xesh funksiya	SHA-2, SHA-3	Grover algoritmi: mustahkamlik kamayadi	SHA-384/512 dan foydalanish

Manba: Muallif tomonidan [1, 3, 4] asosida umumlashtirilgan.

"Kvant kompyuteri qachon paydo bo'ladi?" degan savolga aniq javob yo'q, lekin hisob-kitoblar yildan yilga qisqarmoqda. 2019 yilda Gidney va Ekerå 2048 bitli RSA ni taxminan 8 soatda sindirish uchun 20 million shovqinli kubit kerak, deb baholagan edi [5]. 2025 yil may oyida Gidney yangilangan baho e'lon qildi: 2048 bitli RSA ni bir haftadan kamroq vaqtda, 1 milliondan kam shovqinli kubit bilan sindirish mumkin [6]. Bu hisob-kitob nazariy va muayyan faraz (0,1% xato darajasi va boshqalar) ostida bajarilgan, bugungi qurilmalar undan juda uzoq. Lekin kubitlar soniga qo'yiladigan talabning yigirma barobar kamayishi ko'chishni kechiktirib bo'lmasligini ko'rsatadi.

2. NIST standartlari va ularning asosiy g'oyasi

2024 yil 13 avgustda NIST dastlabki uchta post-kvant standartni tasdiqladi: FIPS 203 (ML-KEM, ilgari CRYSTALS-Kyber), FIPS 204 (ML-DSA, ilgari CRYSTALS-Dilithium) va FIPS 205 (SLH-DSA, ilgari SPHINCS+) [7]. ML-KEM kalit almashinuvi uchun asosiy standart bo'lib, kichik kalitlar va yuqori tezlik bilan ajralib turadi; ML-DSA imzo uchun asosiy standart; SLH-DSA esa imzo uchun zaxira, chunki u boshqa matematik g'oyaga – xesh funksiyalarga – tayanadi. ML-KEM xavfsizligi modul panjaralarda xatolar bilan o'rganish (Module-LWE) masalasining qiyinligiga asoslangan [8]; LWE masalasini Regev 2005 yilda kiritgan [9].

2025 yil 11 martda NIST kalit almashinuvi uchun beshinchi algoritm sifatida HQC ni tanladi. HQC panjaralarga emas, xatolarni tuzatuvchi kodlarga asoslangan, ya'ni ML-KEM buzilib qolsa, ikkinchi himoya chizig'i bo'ladi. U ML-KEM dan kattaroq va ko'proq hisoblash talab qiladi; uning standart loyihasi 2026 yil atrofida, yakuniy varianti 2027 yilga kutilgan edi [10]. Falcon asosidagi FN-DSA (FIPS 206) esa mavjud sharhlarda hali qoralama sifatida ko'rsatilgan: u eng kichik imzo va

kalitlarni beradi, lekin imzolash suzuvchi nuqtali Gauss tanlashga tayanadi va uni xavfsiz, doimiy vaqtda amalga oshirish qiyin [11]. Hozirgi holatini NIST saytidan alohida tekshirish kerak.

2-jadval. NIST tanlagan post-kvant algoritmlari

Algoritm	Vazifasi	Matematik asosi	Holati
ML-KEM (FIPS 203)	Kalit almashinuvi	Modul panjaralar (Module-LWE)	Tasdiqlangan, 2024
ML-DSA (FIPS 204)	Raqamli imzo (asosiy)	Modul panjaralar	Tasdiqlangan, 2024
SLH-DSA (FIPS 205)	Raqamli imzo (zaxira)	Xesh funksiyalar	Tasdiqlangan, 2024
FN-DSA (FIPS 206)	Ixcham imzo	NTRU panjaralari (Falcon)	Qoralama (sharhlar bo'yicha)
HQC	Kalit almashinuvi (zaxira)	Xatolarni tuzatuvchi kodlar	2025 yilda tanlangan, standart ishlab chiqilmoqda

Manba: NIST ma'lumotlari asosida muallif tuzgan [7, 10, 11].

3. Samaradorlikni baholash

3.1. Xavfsizlik. Yangi algoritmlarning kvant hujumiga mustahkamligi isbotlanmagan, u faqat "hozircha hech kim buza olmadi" degan ishonchga tayanadi. Buni 2022 yildagi ikkita voqea yaxshi ko'rsatadi. Avgustda Castryck va Decru SIKE algoritmini (NIST dagi finalga yaqin nomzod) bir oddiy protsessorda taxminan bir soatda buzdi [12]. Shundan oldin Beullens Rainbow imzo sxemasini noutbukda bir hafta oxiri ichida sindirgan edi [13]. Ikkala holda ham algoritm yillar davomida o'rganilgan, ammo yangi matematik g'oya uni bir zumda yaroqsiz qildi. Shuning uchun NIST turli matematik asoslarga tayangan zaxira algoritmlarni (SLH-DSA, HQC) tanladi, amaliyotda esa tizimni algoritmni tez almashtira oladigan qilib qurish (kripto-chaqqonlik) zarur.

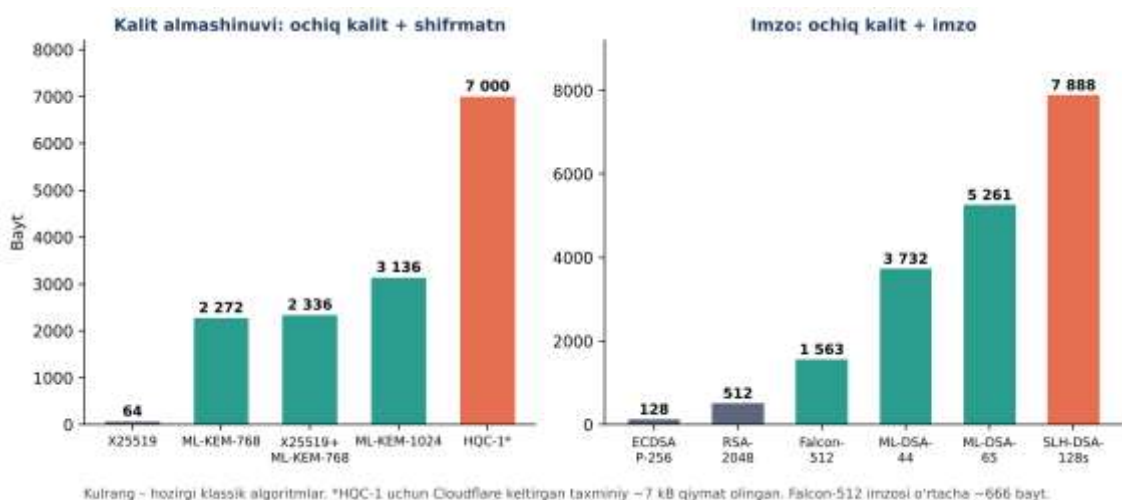
3.2. Kalit va imzo o'lchamlari. Post-kvant algoritmlarining asosiy narxi – hajm. ML-KEM-768 da ochiq kalit 1 184 bayt, shifrmtn 1 088 bayt; hozirgi X25519 da esa har biri 32 bayt [8]. Imzolar da farq yanada katta: ML-DSA-65 imzosi 3 309 bayt, ochiq kaliti 1 952 bayt; ECDSA P-256 imzosi esa atigi 64 bayt [14]. SLH-DSA imzolari variantga qarab 7 856 dan 49 856 baytgacha yetadi [15]. Bu 3-jadval va 1-rasmda ko'rsatilgan. Kalit almashinuvi uchun bu oshish kam sezilarli (taxminan 2 kB), imzolar uchun esa sertifikat zanjirlari kattalashib, handshake sekinlashishi mumkin.

3-jadval. Ba'zi algoritmlarning o'lchamlari (bayt)

Algoritm	Ochiq kalit	Shifrmtn / imzo	Izoh
X25519 (klassik)	32	32	Hozirgi kalit almashinuvi
ML-KEM-512	800	768	Eng past daraja

Algoritm	Ochiq kalit	Shifratn / imzo	Izoh
ML-KEM-768	1 184	1 088	Fuqarolik uchun asosiy
ML-KEM-1024	1 568	1 568	CNSA 2.0 talabi
ECDSA P-256 (klassik)	64	64	Hozirgi imzo
ML-DSA-44	1 312	2 420	Eng past daraja
ML-DSA-65	1 952	3 309	Fuqarolik uchun asosiy
ML-DSA-87	2 592	4 627	CNSA 2.0 talabi
SLH-DSA (variantlar)	32-64	7 856 – 49 856	Zaxira, eng katta imzolar

Manba: FIPS 203, 204, 205 hujjatlari asosida [8, 14, 15]. ML-KEM-512 va ML-DSA-44 qiymatlari ham shu standartlardan olingan; ularni yakuniy matndan qayta tekshirish tavsiya etiladi.



1-rasm. Klassik va post-kvant algoritmlarda uzatiladigan ma'lumot hajmi (bayt).

3.3. Amalda joriy etilganlik. Kalit almashinuvi bo'yicha o'tish allaqachon boshlangan. Cloudflare ma'lumotiga ko'ra, 2025 yil oktabr oyining oxirgi haftasida uning tarmog'idagi insonlar yaratgan trafikning ko'pchiligi X25519MLKEM768 gibril kalit almashinuvidan foydalangan; bu sxema klassik X25519 ni ML-KEM-768 bilan birlashtiradi, shuning uchun biror qismi buzilsa ham ikkinchisi himoyani saqlaydi [16]. Zamonaviy brauzerlar, OpenSSL, Go va yangi Apple tizimlarida u sukut bo'yicha yoqilgan. Imzolar bo'yicha esa holat boshqacha: o'sha manbaga ko'ra 2025 yil oktabrida birorta ham ommaviy post-kvant sertifikatini ishlatilmagan, birinchi sertifikatlar 2026 yilda kutilgan, lekin ular 2027 yilgacha barcha brauzerlarda keng ishonchli bo'lishi ehtimoldan yiroq deb baholangan [16]. Shunday qilib, "hozir yig', keyin shifrn och" xavfiga qarshi (kalit almashinuvi) himoya sezilarli darajada oldinga siljigan, autentifikatsiya (imzolar) esa ortda.

Umuman olganda, samaradorligi bo'yicha ML-KEM ni eng muvaffaqiyatli post-kvant algoritmi deb atash mumkin: u kichik, tez va allaqachon keng sinovdan o'tgan. ML-DSA qabul qilinadigan, lekin hajm jihatidan qimmatroq; SLH-DSA ishonchli, ammo eng og'ir; FN-DSA ixcham, lekin amalga oshirish murakkab; HQC esa zaxira vazifasini bajaradi va eng ko'p resurs talab qiladi. Bu xulosa bevosita

ko'rsatilgan o'lchamlar va manbalardagi sifat baholariga asoslangan; unumdorlikni (tezlik, energiya) aniq qurilmada alohida o'lchash kerak.

4. O'tish strategiyasi va tavsiyalar

Davlat darajasidagi muddatlar o'tishni shoshilinch qiladi. NSA CNSA 2.0 bo'yicha milliy xavfsizlik tizimlari uchun ML-KEM-1024 va ML-DSA-87 ni, ko'rsatilgan dasturiy ta'minot imzolari uchun esa LMS yoki XMSS ni talab qiladi; 2027 yil 1 yanvardan yangi xaridlar CNSA 2.0 ga mos bo'lishi shart, 2030 yil oxirigacha mos kelmaydigan uskunalar chiqarilishi, 2031 yil oxiriga kelib esa talab majburiy bo'lishi kerak, 2035 yilgacha barcha tizimlar kvantga chidamli bo'ladi [4] (2-rasm). Bu AQSh davlat tizimlariga tegishli, ammo xalqaro bozordagi mahsulot va xizmatlar ham shu jadvalga moslashadi.



2-rasm. Post-kvant o'tishdagi asosiy voqealar va CNSA 2.0 muddatlari. Manba: [4, 7, 10, 6, 16] asosida.

Bu ma'lumotlardan tashkilot uchun bir necha amaliy qadam kelib chiqadi. Birinchi qadam – kriptografik inventarizatsiya: ochiq kalitli kriptografiya qayerda ishlatilishini (tarmoq, ilovalar, firmware) aniqlash va har bir tizim himoya qilayotgan ma'lumotning qancha yil maxfiy qolishi kerakligini yozib chiqish; CISA, NSA va NIST ham aynan shuni tavsiya qiladi [2]. Ikkinchi qadam – ustuvorlik: uzoq muddat maxfiy qolishi kerak bo'lgan ma'lumotlar uchun kalit almashinuvini birinchi o'rinda gibrid sxemaga (klassik + ML-KEM) o'tkazish. Uchinchi qadam – tizimni kripto-chaqqon qilish, ya'ni algoritmnin kodning ichiga qotirib qo'ymasdan, sozlama orqali almashtira oladigan qilish: SIKE tajribasi buning nega kerakligini ko'rsatdi. To'rtinchi qadam – ta'minotchilar bilan ishlash: sotib olinadigan uskuna va dasturlar uchun post-kvant yo'l xaritasini shartnomaga kiritish. Beshinchi qadam – imzolar va sertifikatlar uchun hajm sinovi: kattalashgan sertifikat zanjirlari kechikishni oshirishi mumkin, shuning uchun uni ishga tushirishdan oldin o'z tarmog'ida o'lchash kerak.

O'zbekiston sharoitida bu ishlar "Kiberxavfsizlik to'g'risida"gi qonun va unga asoslangan kritik axborot infratuzilmasini himoya qilish talablari doirasida amalga oshirilishi kerak [17]. Milliy kriptografik standartlarga post-kvant algoritmlarini kiritish masalasi tegishli organlar bilan kelishilishi zarur; maqola mualliflari bu bo'yicha rasmiy hujjat topa olmadi, shuning uchun bu yerda faqat umumiy yondashuv keltirilgan.

Xulosa

Tahlil quyidagi xulosalarga olib keldi. Birinchidan, kvant tahdidi ochiq kalitli kriptografiyaga (RSA, DH, ECC) to'liq, simmetrik kriptografiyaga esa qisman ta'sir qiladi; 2025 yilgi hisob-kitoblar 2048 bitli RSA ni sindirish uchun kerakli kubitlar sonini 20 milliondan 1 milliondan kamgacha tushirdi. Ikkinchidan, NIST ning ML-KEM, ML-DSA va SLH-DSA standartlari mavjud va ishlatishga tayyor, HQC va FN-DSA esa to'ldiruvchi sifatida kutilmoqda. Uchinchidan, samaradorlikda asosiy qiymat - hajm: ML-KEM kichik qo'shimcha yuk bilan allaqachon real trafikda ishlayapti, imzolar esa o'nlab baravar kattaroq (ECDSA P-256 da 64 bayt, ML-DSA-65 da 3 309 bayt) va ommaviy sertifikatlarda hali qo'llanilmayapti. To'rtinchidan, SIKE va Rainbow ning sindirilishi yangi algoritmlarga ham ehtiyotkorlik bilan, gibrid sxema va kripto-chaqqonlik bilan yondashish kerakligini ko'rsatadi. Tashkilotlar uchun eng arzon va eng muhim birinchi qadam - kriptografik inventarizatsiya va uzoq muddat maxfiy ma'lumotlar uchun gibrid kalit almashinuviga o'tishdir.

ADABIYOTLAR RO'YXATI:

1. Shor, P. W. (1997). Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM Journal on Computing, 26(5), 1484-1509.
2. CISA, NSA, NIST. (2023). Quantum-Readiness: Migration to Post-Quantum Cryptography (qo'shma axborot varaqasi, 2023 yil avgust; PostQuantum.com sharhi orqali). <https://postquantum.com/quantum-policy/cisa-quantum-readiness/>
3. Grover, L. K. (1996). A Fast Quantum Mechanical Algorithm for Database Search. Proc. ACM STOC, 212-219.
4. NSA. (2022). Commercial National Security Algorithm Suite 2.0 - Cybersecurity Advisory FAQ. https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/0/CSI_CNSA_2.0_FAQ_.PDF

5. Gidney, C., & Ekerå, M. (2021). How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. *Quantum*, 5, 433.
6. Gidney, C. (2025). How to factor 2048 bit RSA integers with less than a million noisy qubits. arXiv:2505.15917. <https://arxiv.org/abs/2505.15917>
7. NIST. (2024, 13 avgust). NIST Releases First 3 Finalized Post-Quantum Encryption Standards. <https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards>
8. NIST. (2024). FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard. <https://csrc.nist.gov/pubs/fips/203/final>
9. Regev, O. (2009). On Lattices, Learning with Errors, Random Linear Codes, and Cryptography. *Journal of the ACM*, 56(6), 34.
10. NIST. (2025, 11 mart). NIST Selects HQC as Fifth Algorithm for Post-Quantum Encryption. <https://www.nist.gov/news-events/news/2025/03/nist-selects-hqc-fifth-algorithm-post-quantum-encryption>
11. Encryption Consulting. FN-DSA (FIPS 206): holati va Falcon amalga oshirish muammolari (sharh). <https://www.encryptionconsulting.com/education-center/fn-dsa-fips-206/>
12. Castryck, W., & Decru, T. (2023). An Efficient Key Recovery Attack on SIDH. EUROCRYPT 2023 (Cryptomathic sharhi, 2022 yil avgust orqali). <https://www.cryptomathic.com/blog/nist-post-quantum-cryptography-standardization-sike-bites-the-dust>
13. Beullens, W. (2022). Breaking Rainbow Takes a Weekend on a Laptop. CRYPTO 2022; IACR ePrint 2022/214.
14. NIST. (2024). FIPS 204: Module-Lattice-Based Digital Signature Standard. <https://csrc.nist.gov/pubs/fips/204/final>
15. NIST. (2024). FIPS 205: Stateless Hash-Based Digital Signature Standard. <https://csrc.nist.gov/pubs/fips/205/final>
16. Cloudflare. (2025, 28 oktabr). Post-quantum cryptography bo'yicha 2025 yil sharhi (blog yozuvi). <https://blog.cloudflare.com/pq-2025/>
17. O'zbekiston Respublikasining "Kiberxavfsizlik to'g'risida"gi Qonuni, ZRU-764, 15.04.2022. <https://lex.uz/uz/docs/-5960604>