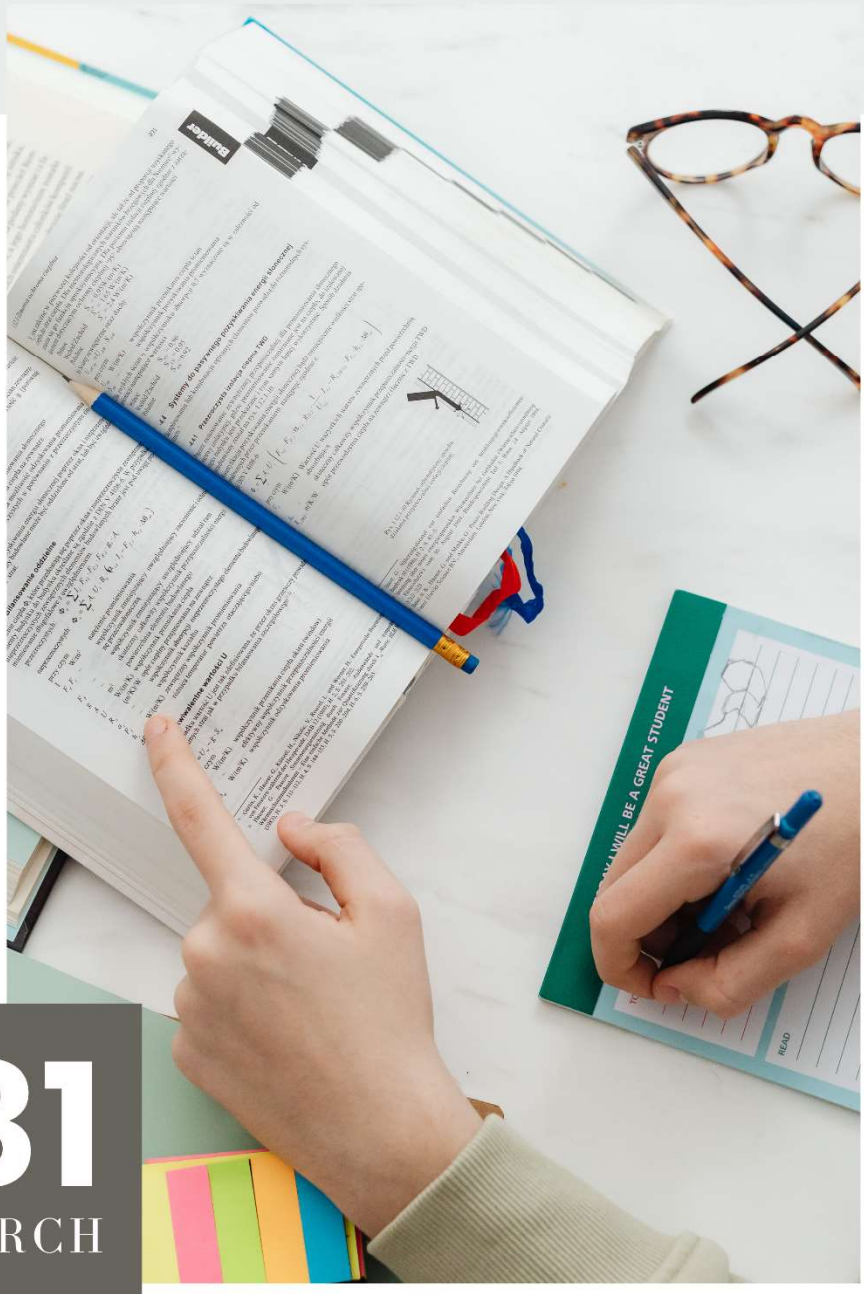
III INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE 2026

COLLECTION

Innovation, integration and modern problems in the scientific activities of young researchers and students: theory and practice



31 MARCH

Jizzakh, Uzbekistan

www.d-pressa.com

MINISTRY OF HIGHER EDUCATION, SCIENCE AND INNOVATION OF THE REPUBLIC OF UZBEKISTAN

JIZZAKH BRANCH OF THE NATIONAL UNIVERSITY OF UZBEKISTAN NAMED AFTER MIRZO ULUGBEK

SCIENTIFIC JOURNAL OF SCIENCE TECHNOLOGY & DIGITAL FINANCE

JOURNAL OF INTERNATIONAL SCIENCE NETWORKS

Innovation, integration and modern problems in the scientific activities of young researchers and students: theory and practice collection of materials of the international scientific and practical conference on the topic

(March 31, 2026)

Jizzakh-2026

Innovation, integration and modern problems in the scientific activities of young researchers and students: theory and practice – Jizzakh: Department of economics and tourism of Jizzakh branch of the national university of Uzbekistan named after Mirzo Ulugbek, March 31, 2026, 790 pp.

Editors in charge: Ass.prof. Soy M.P.

In the collection of materials of the conference, the role and role of Science, Education and production in the era of globalization, the pressing problems of the issues of interaction of these processes, feedback on their solutions were presented by mature specialists of the field.

In addition, research on the scientific and practical topic, carried out in the economics, Exact Sciences, Natural Sciences and socio-humanities during the globalization period, information is presented in the scientific and practical fields, which includes the latest innovative technologies in the fields of production.

It can be argued that this collection is one of the specific intersections of current thoughts and innovative ideas of the world of science. This scientific and practical conference was actively attended by professors and scientific researchers engaged in scientific research in Uzbekistan and foreign countries. In increasing the position of the scientific and practical conference, the professors and teachers of domestic and foreign higher educational institutions made a significant contribution.

Professors and teachers of foreign higher educational institutions who actively participated in the work of the conference made a worthy contribution to the high level of interaction with scientists of our country. The processes of international cooperation with foreign countries and exchange with them in the field of Science in the era of globalization have a positive effect on the development of Higher Education, the fields of Science and production. The materials of this conference are special in that they include a wide range of research, from theoretical developments to practical solutions, demonstrating the diversity of approaches and directions in this area.

In conclusion, it should be noted that this scientific and practical conference will be a very useful collection for everyone who is interested in modern research in the fields of further development of Higher Education, Science, Education and production in the era of globalization. The authors are responsible for the content and quality of the articles and abstracts included in the collection.

8. Kamolov D. GLOBALIZATION PHENOMENON AND GLOBALISM //Journal of Contemporary World Studies. – 2023. – Т. 1. – №. 1. – С. 4-9.
9. Цой М., Иброхимов Ш. СОВРЕМЕННАЯ СИСТЕМА ОБРАЗОВАНИЯ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ В УЗБЕКИСТАНЕ //International Journal of scientific and Applied Research. – 2024. – Т. 1. – №. 3. – С. 24-28.
10. Kamolov D. Athenian democracy: individual and collective freedom //Semantic Scholar. – 2021.
11. Kamolov D. Davlat boshqaruviga oid axloqiy qarashlar //Адабиёт учқунлари. – 2021.
12. ЦОЙ М. РОЛЬ ГЕНДЕРНОГО РАВЕНСТВА В ВОПРОСАХ СОКРАЩЕНИЯ БЕДНОСТИ И СОЗДАНИЯ ДОСТОЙНЫХ РАБОЧИХ МЕСТ–МИРОВОЙ ОПЫТ И ПРАКТИКА УЗБЕКИСТАНА //Архив научных исследований. – 2022. – Т. 2. – №. 1.
13. Kamolov D. ON THE WAY TO THE DIGITAL EDUCATION SYSTEM OF UZBEKISTAN. – 2023.
14. Dostonbek K. SPIRITUAL AND MORAL ENVIRONMENT OF SOCIETY //Social science and innovation. – 2023. – Т. 1. – №. 2. – С. 128-133.

POST-KVANT KRIPTOGRAFIYASI: RAQAMLI DUNYONI KVANT TAHDIDIDAN HIMOYA QILISHNING STRATEGIK YO‘NALISHLARI

Nizoyeva Latifaoy Saitmurod qizi
O‘zbekiston Milliy universiteti Jizzax filiali “Axborot tizimlari va texnologiyalari” 2-bosqich talabasi

Annotatsiya. Ushbu maqolada hisoblash texnikasining yangi avlodi — kvant kompyuterlarining zamonaviy kiberxavfsizlik tizimlariga ko‘rsatadigan tahdidlari tahlil qilinadi. An’anaviy asimmetrik shifrlash algoritmlarining (RSA, ECC) zaifliklari va ularning o‘rnini bosuvchi post-kvant kriptografiyasi (PQC) turlari, xususan, panjaraga asoslangan va ko‘p o‘zgaruvchanli tizimlar batafsil yoritilgan. Shuningdek, maqolada global standartlashtirish jarayonlari va ma’lumotlarni himoya qilishning kelajakdagi istiqbollari haqida so‘z yuritiladi.

Kalit so‘zlar: Post-kvant kriptografiyasi, Kvant kompyuteri, Shor algoritmi, Panjaraga asoslangan kriptografiya, NIST standartlari, Kiberxavfsizlik, Kripto-egiluvchanlik, ML-KEM, Raqamli imzo.

Axborot texnologiyalari rivojlanishi bilan ma’lumotlar maxfiyligini ta’minlash har qachongidan ham muhimroq ahamiyat kasb etmoqda. Hozirgi kunda dunyo bo‘ylab tranzaksiyalar, davlat sirlari va shaxsiy yozishmalar asosan RSA va Elliptik egri chiziqlar (ECC) kabi kriptografik algoritmlar bilan himoyalangan. Biroq, kvant mexanikasi qonuniyatlari asosida ishlaydigan kvant kompyuterlarining yaratilishi ushbu tizimlar uchun “ekzistensial xavf” tug‘dirmoqda. Klassik

kompyuterlar uchun yechish imkonsiz bo‘lgan matematik masalalar kvant tizimlari tomonidan bir necha soniyada hal qilinishi mumkin. Shu sababli, butun dunyo IT-hamjamiyati bugungi kunda “Post-kvant kriptografiyasi” (PQC) deb nomlanuvchi yangi himoya qatlamiga o‘tish ustida ishlamoqda.

Kvant kompyuterlari bitlar o‘rniga kubitlar (quantum bits) bilan ishlaydi. Bu ularga bir vaqtning o‘zida millionlab holatlarni tahlil qilish imkonini beradi. 1994-yilda Piter Shor tomonidan ishlab chiqilgan algoritm shuni isbotladiki, yetarli quvvatga ega kvant kompyuteri hozirgi kriptografiyaning asosi bo‘lgan “katta sonlarni ko‘paytuvchilarga ajratish” muammosini darhol yechadi. Bu esa biz hozirda xavfsiz deb hisoblayotgan HTTPS, VPN va elektron raqamli imzolar kelajakda osonlikcha buzilishini anglatadi.

PQC kvant kompyuterlari ham yecha olmaydigan o‘ta murakkab matematik strukturaga tayanadi. Ilmiy hamjamiyat hozirda quyidagi to‘rtta asosiy yo‘nalishni eng xavfsiz deb tan olmoqda:

1. Panjaraga asoslangan kriptografiya (Lattice-based Cryptography): Bu usul n-o‘lchamli panjaradagi eng yaqin nuqtani topish (Shortest Vector Problem) muammosiga asoslanadi. Bu vazifa hatto kvant kompyuterlari uchun ham geometrik jihatdan o‘ta murakkab hisoblanadi.
2. NIST tomonidan standartlashtirilgan Kyber va Dilithium algoritmlari aynan shu yo‘nalishga tegishli.
3. Ko‘p o‘zgaruvchanli kvadratik tenglamalar: Bu yerda xavfsizlik o‘nlab va yuzlab noma’lumli kvadratik tenglamalar tizimini yechish qiyinligiga asoslangan. Bu tizimlar ayniqsa elektron raqamli imzolarni yaratishda yuqori samaradorlik ko‘rsatadi.
4. Kodlarga asoslangan kriptografiya (Code-based Cryptography): Xatolarni tuzatuvchi kodlar (Error-correcting codes) nazariyasiga tayanadi. Uning eng mashhur vakili — McEliece algoritmi bo‘lib, u 1978-yildan beri buzilmasdan kelayotgan eng ishonchli usullardan biridir.

AQShning Milliy Standartlar va Texnologiyalar Instituti (NIST) 2016-yildan buyon dunyo olimlari o‘rtasida tanlov o‘tkazib kelmoqda. 2024-yil avgust oyida NIST birinchi marta 3 ta asosiy post-kvant standartini e’lon qildi:

1. ML-KEM (asl nomi Kyber): Ma’lumotlarni umumiy shifrlash uchun.
2. ML-DSA (asl nomi Dilithium): Raqamli imzolar uchun.
3. SLH-DSA (Sphincs+): Muqobil, hash-asosli raqamli imzo.

Ushbu standartlar yaqin 5 yil ichida dunyodagi barcha bank, moliya va davlat tizimlariga majburiy tartibda joriy etilishi kutilmoqda.

Ko‘pchilik kvant kompyuterlari hali to‘liq ishga tushmadi-ku, nega hozir xavotir olishimiz kerak, degan savolni beradi. Biroq, kiberjinoyatchilar bugun shifrlangan ma’lumotlarni o‘g‘irlab, ularni saqlab qo‘yishmoqda. Maqsad — kelajakda kvant kompyuteri paydo bo‘lishi bilan bu ma’lumotlarni ochish. Bu ayniqsa davlat sirlari, sog‘liqni saqlash ma’lumotlari va intellektual mulk uchun o‘ta xavflidir.

Maqolaning muhim qismlaridan biri bu — yangi tizimlarga o‘tish jarayonidir. Kripto-egiluvchanlik bu — tashkilotning o‘z infratuzilmasini buzmagan holda, bir

shifrlash algoritmidan ikkinchisiga tezkorlik bilan o‘ta olish qobiliyatidir. Kelajakda algoritmlardan birida zaiflik topilsa, tizim to‘xtab qolmasligi uchun dasturiy ta’minot shunga mos tarzda modulyar bo‘lishi shart.

Post-kvant kriptografiyasi shunchaki nazariy fan emas, balki raqamli suverenitetni saqlab qolishning asosiy omilidir. Kvant davriga tayyorgarlik ko‘rish faqat texnologik emas, balki strategik xavfsizlik masalasidir. O‘zbekistonda ham milliy kriptografik standartlarni post-kvant talablariga moslashtirish, bu sohada yuqori malakali matematik-dasturchilarni tayyorlash bugungi kunning kechiktirib bo‘lmas vazifasi hisoblanadi.

Foydalanilgan adabiyotlar:

1. NIST (2024). “Federal Information Processing Standards (FIPS) for Post-Quantum Cryptography”.
2. Shor, P. W. (1994). “Algorithms for quantum computation: discrete logarithms and factoring”.
3. Bernstein, D. J., & Buchmann, J. (2017). “Post-Quantum Cryptography”. Springer.
4. Cloudflare, Google & Apple Technical Reports on PQ3 and Post-Quantum Integration (2023-2024).
5. Абдуназаров С. А., Цой М. П. Реформирование системы образования Республики Узбекистан //Актуальные научные исследования в современном мире. – 2016. – №. 10-6. – С. 14-17.
6. Цой М. П., Ибрагимов З. Т. ЗАКОНОДАТЕЛЬНЫЕ ОСНОВЫ ЦИФРОВОГО ОБРАЗОВАНИЯ //International Journal of Contemporary Scientific and Technical Research. – 2022. – Т. 1. – №. 2. – С. 339-342.
7. Салохитдинов Ш. ОЛИЙ ТАЪЛИМ ХИЗМАТЛАРИ СИФАТИНИ БАҲОЛАШ ТИЗИМИНИНГ ИЖТИМОИЙ-ИҚТИСОДИЙ МОҲИЯТИ, МАЗМУНИ ВА НАЗАРИЙ ЁНДАШУВЛАР //МАЗМУНИ ВА НАЗАРИЙ ЁНДАШУВЛАР.–2023. – 2023.
8. Saloxitdinov S. Oliy ta’lim xizmatlari sifatini baholashning zamonaviy konsepsiyalari va innovatsion mexanizmlari: milliy va xalqaro tajribani taqqoslamali tahlil qilish asosida takomillashtirish yo ‘nalishlari //Academic literature. – 2025. – Т. 1. – №. 1. – С. 1-128.
9. Kamolov D. ON THE WAY TO THE DIGITAL EDUCATION SYSTEM OF UZBEKISTAN. – 2023.
10. Цой М., Камолов Д. ЗНАЧЕНИЕ И РОЛЬ ДЕЯТЕЛЬНОСТИ СУБЪЕКТОВ МАЛОГО ПРЕДПРИНИМАТЕЛЬСТВА В ЭКОНОМИКЕ: МИРОВОЙ ОПЫТ И ПРАКТИКА УЗБЕКИСТАНА //Academic literature. – 2025. – Т. 1. – №. 1. – С. 1-105.
11. Салохитдинов Ш. Ф., Ўғли Н. А. Д. ОЛИЙ ТАЪЛИМ МУАССАСАЛАРИДА ТАЪЛИМ ХИЗМАТЛАРИ СИФАТИ ОМИЛЛАРИНИ БАҲОЛАШ //Science and innovation. – 2024. – Т. 3. – №. Special Issue 18. – С. 983-987.