KIBERXAVFSIZLIKDA KVANT KRIPTOGRAFIYA: YANGI IMKONIYATLAR VA TAHDIDLAR

Boymirzayeva Sitora Otabek qizi
Qarshi davlat universiteti talabasi,
setoraboymirzayeva1@gmail.com

Annotatsiya*. Axborot texnologiyalarining jadal rivojlanishi natijasida axborot xavfsizligini ta'minlash masalalari tobora muhim ahamiyat kasb etmoqda. Ayniqsa, kvant hisoblash texnologiyalarining paydo bo'lishi an'anaviy kriptografik algoritmlar xavfsizligiga yangi tahdidlarni yuzaga keltirmoqda. Mazkur maqolada kvant kriptografiyaning kiberxavfsizlik tizimlaridagi o'rni, uning imkoniyatlari va mavjud xavf-xatarlar tahlil qilinadi. Tadqiqotda kvant kalit taqsimoti texnologiyalari, kvant xavfsizlik mexanizmlari va kvant hisoblashning zamonaviy kriptografiya tizimlariga ta'siri ilmiy jihatdan ko'rib chiqiladi.*

Kalit so'zlar: *Kvant kriptografiyasi, kiberxavfsizlik, kvant kalitlarini taqsimlash (QKD), kvantdan keyingi kriptografiya, Shor algoritmi, ma'lumotlarni shifrlash, kvant tahdidlari, tarmoq xavfsizligi, axborot maxfiyligi, kvant xavfsizligi algoritmlari.*

Annotation. *As a result of the rapid development of information technologies, the issues of ensuring information security are becoming increasingly important. In particular, the emergence of quantum computing technologies poses new threats to the security of traditional cryptographic algorithms. This article analyzes the role of quantum cryptography in cybersecurity systems, its capabilities and existing risks. The study scientifically examines quantum key distribution technologies, quantum security mechanisms and the impact of quantum computing on modern cryptographic systems.*

Keywords: *Quantum cryptography, cybersecurity, Quantum Key Distribution (QKD), post-quantum cryptography, Shor's algorithm, data encryption, quantum threats, network security, information privacy, quantum-safe algorithms.*

Аннотация. *В результате стремительного развития информационных технологий вопросы обеспечения информационной безопасности приобретают все большее значение. В частности, появление технологий квантовых вычислений создает новые угрозы для безопасности традиционных криптографических алгоритмов. В данной статье анализируется роль квантовой криптографии в системах кибербезопасности, ее возможности и существующие риски. В исследовании научно рассматриваются технологии квантового распределения ключей, механизмы квантовой безопасности и влияние квантовых вычислений на современные криптографические системы.*

Ключевые слова: *Квантовая криптография, кибербезопасность, квантовое распределение ключей (QKD), постквантовая криптография, алгоритм Шора, шифрование данных, квантовые угрозы, сетевая безопасность, конфиденциальность информации, квантово-устойчивые алгоритмы.*

Axborot texnologiyalarining rivojlanishi zamonaviy jamiyatning barcha sohalarida tub o’zgarishlarga olib kelmoqda. Raqamli iqtisodiyotning shakllanishi, elektron hukumat tizimlarining joriy etilishi hamda global internet tarmoqlarining kengayishi natijasida axborot resurslari strategik ahamiyat kasb eta boshladi. Bunday sharoitda axborot xavfsizligini ta’minlash muhim masalalardan biri hisoblanadi .

Kiberxavfsizlik bugungi kunda davlatlar, tashkilotlar va foydalanuvchilar uchun ustuvor yo’nalishlardan biriga aylangan. Internet tarmoqlarining rivojlanishi bilan bir qatorda kiberhujumlar soni ham ortib bormoqda. Bu esa ma’lumotlarni himoyalash uchun yanada samarali kriptografik usullarni ishlab chiqishni talab qiladi.

Hozirgi kunda ma’lumotlarni himoyalash uchun keng qo’llanilayotgan kriptografik algoritmlar matematik muammolarning murakkabligiga asoslangan. Masalan, RSA algoritmi katta sonlarni faktorlarga ajratish muammosiga asoslanadi. Elliptik egri chiziqlar kriptografiyasi esa murakkab matematik hisoblashlarga tayangan holda ishlaydi . Biroq kvant hisoblash texnologiyalarining rivojlanishi

ushbu algoritmlarning xavfsizligini shubha ostiga qo’ymoqda. Kvant kompyuterlari ayrim matematik muammolarni an’anaviy kompyuterlarga nisbatan ancha tez yecha oladi. Bu esa kelajakda an’anaviy kriptografik tizimlar zaiflashishiga olib kelishi mumkin .

Shu sababli kvant kriptografiya so’nggi yillarda kiberxavfsizlik sohasida eng istiqbolli yo’nalishlardan biriga aylandi. Kvant kriptografiya kvant mexanikasi qonunlariga asoslangan bo’lib, ma’lumotlarni himoyalashning mutlaqo yangi usullarini taklif etadi.

Kvant hisoblashning jadal rivojlanishi axborot texnologiyalari tarixidagi eng muhim siljishlardan biridir. Klassik kompyuterlar ma’lumotni ikkilik bitlarda (0 yoki 1) qayta ishlaganda, kvant kompyuterlari superpozitsiya va chalkashlik tamoyillaridan foydalanadigan kubitlardan foydalanadi. Ushbu asosiy farq kvant mashinalariga ma’lum hisob-kitoblarni bugungi kunda mavjud bo’lgan eng kuchli superkompyuterlarga qaraganda tezroq bajarishga imkon beradi.

Kiberxavfsizlik nuqtai nazaridan, bu taraqqiyot ikki qirrali qilichdir. Asosiy tashvish joriy ochiq kalitlar infratuzilmasi (PKI) zaifligi bilan bog’liq. Ko’pgina zamonaviy shifrlash standartlari, jumladan RSA (Rivest-Shamir-Adleman) va ECC (Elliptik Curve Cryptography) katta butun sonlarni faktoringlash yoki diskret logarifm masalalarini hal qilishning o’ta qiyinligiga tayanadi.

Strategik oqibatlar va o’tish davri muammolari. “Kvant xavfsizligi” davriga o’tish nafaqat texnik yangilanish, balki strategik zaruratdir. Bu joriy ma’lumotlar aktivlarini tekshirish, zaif tizimlarni aniqlash va klassik xavfsizlikni kvantga chidamli qatlamlar bilan birlashtirgan gibrid kriptografik modellarni amalga oshirishni o’z ichiga oladi.

Xulosa qilib aytganda, kvant kalitlarini taqsimlash (QKD) va post-kvant kriptografiyasi (PQC) integratsiyasi keng qamrovli mudofaa strategiyasini taklif qiladi. QKD fizikaning o’zgarmas qonunlariga, xususan Heisenberg noaniqlik printsipiga asoslangan apparatga asoslangan yechimni taqdim etsa-da, PQC murakkab matematik panjaralar va ko’p o’lchovli tenglamalar orqali dasturiy ta’minotga asoslangan, kengaytiriladigan yondashuvni taklif qiladi. Bu ikki soha

o’rtasidagi sinergiya, ehtimol, xavfsizlik nafaqat xususiyat, balki tarmoqning o’ziga xos xususiyati bo’lgan kelajakdagi “Kvant Internet” ning asosini tashkil qiladi.

Oldinga intilish, raqamli suverenitetni muvaffaqiyatli himoya qilish xalqaro hamkorlik va kriptografik protokollarni standartlashtirishga bog’liq bo’ladi. NIST kabi tashkilotlarning kvantga chidamli algoritmlarni tekshirish va amalga oshirish bo’yicha olib borayotgan sa’y-harakatlari bu yo’lda hal qiluvchi qadamdir. Biroq, bizning global raqamli iqtisodiyotimizning yakuniy barqarorligi gibrid yondashuvga tayanadi - kvant mexanikasining jismoniy aniqligini post-kvant matematikasining algoritmik mustahkamligi bilan birlashtiradi.

FOYDALANILGAN ADABIYOTLAR

1. Alagic, G., et al. (2022). Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process. NIST IR 8413. National Institute of Standards and Technology.
2. Ibragimov, A. A. The Role of Quantum Entanglement in Secure Communication Channels. Uzbekistan Journal of Physics, 23(2), (2021), 45-52.
3. Kabulov, A. V., & Normatov, I. H. Algorithmic methods of data protection in the era of quantum computing. Uzbek Mathematical Journal, 4, (2019), 12-21.
4. Otamuratov, B. S. Kvant hisoblashlarining klassik shifrlash standartlariga ta’siri. Amaliy fizika va matematika konferensiyasi materiallari, Toshkent, (2023), 112-115-betlar.
5. Raximov, N. O., & Yo’ldoshev, A. A. Xavfsiz tarmoqlarda kvant kalitlarini taqsimlash protokollari tahlili. TATU xabarlari, 3(59), (2021), 24-33.
6. Xurramov, A. M. Zamonaviy axborot tizimlarida post-kvant kriptografiyasini joriy etish muammolari. Scientific Progress, 3(4), (2022), 567-574.
7. Saidova D. Teaching Programming Collaboratively Through Google Colab AND Github Integration //Green Economy and Development. – Т. 3. – №. 11. – С. 667884.
8. Saidova D. E. Analysis of the problems of the teaching object-oriented programming to students //International Journal of Social Science Research and Review. – 2022. – Т. 5. – №. 6. – С. 229-234.