UDK: 32.019,5

KVANT KOMPYUTERLARINING HUQUQIY SOHAGA TA'SIRI: IMKONIYATLAR VA MUAMMOLAR

Abdixakimov Islombek Bahodir o'g'li
Toshkent davlat yuridik universiteti Kiber huquq kafedrasi o'qituvchisi

islombekabduhakimov@gmail.com
https://orcid.org/0000-0002-3682-2810

ВЛИЯНИЕ КВАНТОВЫХ КОМПЬЮТЕРОВ НА ПРАВОВУЮ СФЕРУ: ВОЗМОЖНОСТИ И ПРОБЛЕМЫ

Абдихакимов Исламбек Баходир угли
Преподаватель кафедры киберправа Ташкентского государственного юридического университета

THE IMPACT OF QUANTUM COMPUTERS ON THE LEGAL SPHERE: OPPORTUNITIES AND CHALLENGES

Abdikhakimov Islombek Bahodir o'g'li
Lecturer at the Department of Cyber Law, Tashkent State University of Law

Annotatsiya: *Kvant kompyuterlari zamonav iy texnologiyaning eng muhim yutuqlaridan biri bo'lib, turli sohalar, xususan, huquqiy soha uchun ham katta imkoniyatlar va muammolar tug'dirmoqda. Ushbu tadqiqot kvant kompyuterlari texnologiyasining huquqiy sohaga ta'sirini, uning keltirib chiqaradigan asosiy huquqiy muammolarni va imkoniyatlarni IMRAD metodi asosida o'rganadi. Tadqiqot davomida intellektual mulk huquqlari, ma'lumotlar xavfsizligi, shifrlash tizimlari, huquqiy tartibga solish va axloqiy masalalar kabi asosiy yo'nalishlar tahlil qilindi. Natijalar shuni ko'rsatadiki, kvant kompyuterlari hozirgi shifrlash tizimlarini buzish qobiliyatiga ega bo'lib, bu esa ma'lumotlar xavfsizligi va shaxsiy hayot daxlsizligi sohasida jiddiy xavflar tug'diradi. NIST tomonidan 2024-yil avgust oyida e'lon qilingan post-kvant kriptografiya standartlari ushbu muammolarga javob sifatida ishlab chiqilgan bo'lsa-da, ularning amaliy joriy etilishi ko'p vaqt va resurs talab qiladi. Tadqiqot natijalari huquqshunoslar, siyosatchilar va texnologiya sohasidagi mutaxassislar uchun kvant texnologiyalarining huquqiy oqibatlarini tushunish va ularga tayyorgarlik ko'rish zarurligini ko'rsatadi.*

Аннотация: *Квантовые компьютеры являются одним из важнейших достижений современной технологии и открывают как большие возможности, так и серьезные вызовы для различных сфер, в том числе для юридической. Данное исследование, основанное на методе IMRAD, изучает влияние технологий квантовых вычислений на правовую сферу, а также основные правовые проблемы и возможности, возникающие в этом контексте. В ходе исследования были проанализированы такие ключевые направления, как права интеллектуальной*

собственности, безопасность данных, системы шифрования, правовое регулирование и этические вопросы. Результаты показывают, что квантовые компьютеры обладают способностью взламывать существующие системы шифрования, что создает серьезные риски для безопасности данных и неприкосновенности частной жизни. Стандарты постквантовой криптографии, опубликованные NIST в августе 2024 года, были разработаны в ответ на эти проблемы, однако их практическое внедрение требует значительных времени и ресурсов. Полученные результаты указывают на необходимость для юристов, политиков и специалистов в области технологий понимать правовые последствия квантовых технологий и заблаговременно готовиться к ним.

Abstract: *Quantum computers are among the most significant achievements of modern technology, offering both great opportunities and serious challenges for various fields, including the legal sector. This study, based on the IMRAD method, explores the impact of quantum computing technologies on the legal sphere, as well as the main legal issues and opportunities they create. The research analyzes key areas such as intellectual property rights, data security, encryption systems, legal regulation, and ethical considerations. The results show that quantum computers have the ability to break current encryption systems, posing serious risks to data security and privacy. The post-quantum cryptography standards published by NIST in August 2024 were developed in response to these issues, though their practical implementation will require significant time and resources. The findings highlight the need for lawyers, policymakers, and technology professionals to understand the legal implications of quantum technologies and to prepare for their potential impact.*

Kalit so‘zlar: *kvant kompyuterlari, huquqiy soha, intellektual mulk, kiberxavfsizlik, post-kvant kriptografiya, ma'lumotlar xavfsizligi, NIST standartlari, huquqiy tartibga solish.*

Ключевые слова: *квантовые компьютеры, правовая сфера, интеллектуальная собственность, кибербезопасность, постквантовая криптография, безопасность данных, стандарты NIST, правовое регулирование.*

Keywords: *quantum computers, legal sphere, intellectual property, cybersecurity, post-quantum cryptography, data security, NIST standards, legal regulation.*

1. KIRISH

Kvant kompyuterlari zamonaviy texnologiyaning eng inqilobiy yutuqlaridan biri bo'lib, klassik kompyuterlar hal qila olmaydigan murakkab masalalarni hal qilish imkoniyatini beradi. Kvant mexanikasi qonunlaridan foydalangan holda ishlaydigan bu qurilmalar klassik bitlar o'rniga kvantli bitlar yoki qubitlardan foydalanadi va bu ularga bir vaqtning o'zida ko'plab holatlarni ifodalash imkonini beradi [1]. Ushbu xususiyat kvant kompyuterlariga klassik kompyuterlarga nisbatan eksponensial tezlik ustunligi beradi.

Jahon iqtisodiyotining raqamlashtirish darajasi ortib borar ekan, ma'lumotlar xavfsizligi va shifrlash tizimlari muhim ahamiyat kasb etmoqda. Hozirgi paytda internet va raqamli aloqalarning xavfsizligi asosan RSA va elliptik egri chizig'iga asoslangan shifrlash algoritmlariga tayanadi. Biroq, kvant kompyuterlari, xususan, Shor algoritmi orqali, ushbu shifrlash tizimlarini buzish qobiliyatiga ega [2]. Bu esa huquqiy jihatdan jiddiy muammolar tug'diradi, chunki moliyaviy operatsiyalar, tibbiy ma'lumotlar, davlat sirlari va shaxsiy ma'lumotlar xavf ostida qoladi.

Kvant kompyuterlarining huquqiy sohaga ta'siri ko'p qirrali bo'lib, bir necha asosiy yo'nalishlarni o'z ichiga oladi. Birinchidan, intellektual mulk huquqlari sohasida yangi muammolar paydo

UDK: 32.019,5

bo'lmoqda, chunki kvant algoritmlarini va apparat ta'minotini patentlash an'anaviy patent tizimining chegaralarini sinaydi [3]. Ikkinchidan, ma'lumotlar xavfsizligi va maxfiylik sohasida kvant kompyuterlari hozirgi shifrlash standartlarini noto'g'ri qilish xavfini tug'diradi. Uchinchidan, huquqiy tartibga solish sohasida hukumatlar va xalqaro tashkilotlar kvant texnologiyalarini qanday boshqarish masalasida yangi yondashuvlarni ishlab chiqishi kerak.

Jahon Iqtisodiy Forumi tomonidan 2024-yilda e'lon qilingan ma'lumotlarga ko'ra, kvant kompyuterlari kelajakdagi texnologik taraqqiyotning asosiy yo'nalishlaridan biri hisoblanadi [4]. Biroq, ushbu texnologiyaning potentsial xavflari ham e'tiborga olinishi kerak. Xususan, "hozir to'pla, keyinroq shifrlash" hujumlari allaqachon amalga oshirilmoqda, ya'ni jinoyatchilar hozirgi shifrlangan ma'lumotlarni saqlab qo'yib, kelajakda kvant kompyuterlari orqali ularni ochishni rejalashtirmoqda [5].

Amerika Qo'shma Shtatlarining Milliy Standartlar va Texnologiya Instituti (NIST) ushbu muammolarni hal qilish maqsadida 2024-yil avgust oyida birinchi post-kvant kriptografiya standartlarini e'lon qildi [6]. FIPS 203, FIPS 204 va FIPS 205 standartlari kvant kompyuterlariga qarshi himoya qilish uchun yangi shifrlash algoritmlarini taqdim etadi. Biroq, ushbu standartlarni amaliy joriy etish jarayoni murakkab va ko'p vaqt talab qiladi.

Ushbu tadqiqotning maqsadi kvant kompyuterlarining huquqiy sohaga ta'sirini tizimli tahlil qilish, asosiy imkoniyatlar va muammolarni aniqlash hamda kelajakda yuzaga kelishi mumkin bo'lgan huquqiy masalalar uchun tavsiyalar ishlab chiqishdir. Tadqiqot quyidagi asosiy savollarga javob berishga qaratilgan: kvant kompyuterlari intellektual mulk huquqlariga qanday ta'sir qiladi, ma'lumotlar xavfsizligi va maxfiylik qonunchiligida qanday o'zgarishlar zarur, kvant texnologiyalarini huquqiy jihatdan qanday tartibga solish mumkin va huquqshunoslar ushbu yangi texnologiyaga qanday tayyorgarlik ko'rishlari kerak.

2. METODLAR

Ushbu tadqiqot asosiy manbalar, akademik adabiyotlar va xalqaro tashkilotlarning rasmiy hujjatlariga asoslangan keng qamrovli adabiyotlar tahlili metodidan foydalanadi. Tadqiqot jarayonida quyidagi metodologik yondashuvlar qo'llanildi.

Adabiyotlarni to'plash bosqichida 2022-2025-yillar oralig'ida nashr etilgan akademik maqolalar, huquqiy tahlillar, texnologiya kompaniyalarining hisobotlari va xalqaro tashkilotlarning rasmiy hujjatlari o'rganildi. Asosiy ma'lumotlar manbalari qatoriga Cambridge University Press, Oxford Academic, Amerika Advokatlar Assotsiatsiyasi nashrlari, NIST rasmiy hujjatlari va nufuzli yuridik firmalarning tahlillari kiradi. Ma'lumotlar to'plashda maxsus e'tibor kvant kompyuterlari, huquqiy ta'sirlar, intellektual mulk va kiberxavfsizlik kabi kalit so'zlar kombinatsiyasiga berildi.

Tadqiqotda faqat tekshirilgan va ishonchli manbalar qo'llanildi. Barcha ma'lumotlar manbalarining haqiqiyligini tekshirish uchun nufuzli akademik bazalar, rasmiy hukumat veb-saytlari va ekspert xulosalari tasdiqidan foydalanildi. Tadqiqotda sun'iy ma'lumotlar yoki noaniq manbalardan foydalanilmadi.

Tadqiqot tahlili ikki asosiy bosqichdan iborat bo'ldi. Birinchi bosqichda kvant kompyuterlarining huquqiy sohaga ta'siri to'rtta asosiy yo'nalish bo'yicha tahlil qilindi: intellektual mulk huquqlari, ma'lumotlar xavfsizligi va shifrlash, huquqiy tartibga solish va axloqiy masalalar. Ikkinchi bosqichda har bir yo'nalish bo'yicha mavjud muammolar va potentsial yechimlar aniqlanib, xalqaro amaliyot va standartlar bilan qiyoslandi.

Tadqiqotda qiyosiy huquqiy tahlil metodi qo'llanildi, bunda turli davlatlarning kvant texnologiyalariga yondashuvlari

taqqoslandi. Amerika Qo'shma Shtatlari, Yevropa Ittifoqi, Xitoy va boshqa rivojlangan davlatlarning kvant siyosati va huquqiy chora-tadbirlari o'rganildi. Bu qiyosiy tahlil O'zbekiston uchun eng maqbul huquqiy yondashuvlarni aniqlashga yordam berdi.

Tadqiqotda interdissiplinar yondashuv qo'llanildi, ya'ni huquqshunoslik, texnologiya va axloq sohalari kesishmasida tahlil amalga oshirildi. Bu yondashuv kvant kompyuterlarining murakkab tabiatini to'liq tushunish va huquqiy ta'sirlarni ko'p qirrali baholash imkonini berdi.

Tadqiqot jarayonida eng so'nggi ma'lumotlarni olish uchun maxsus e'tibor NIST tomonidan 2024-yil avgust oyida e'lon qilingan yangi post-kvant kriptografiya standartlariga berildi. Shuningdek, Patent va Tovar Belgilari Apellyatsiya Kengashi (PTAB) qarorlari va eng so'nggi sud amaliyotlari tahlil qilindi.

Tadqiqot natijalarini tizimlashtirish va taqdim etishda IMRAD (Introduction, Methods, Results, Discussion) metodidan foydalanildi. Bu standart akademik yondashuv tadqiqot natijalarini tizimli va tushunarli tarzda taqdim etish imkonini beradi.

3. NATIJALAR

Tadqiqot natijalari kvant kompyuterlarining huquqiy sohaga ko'p qirrali ta'sirini ko'rsatadi. Quyida har bir asosiy yo'nalish bo'yicha aniqlangan asosiy natijalar keltirilgan.

3.1. Intellektual Mulk Huquqlari va Patentlash Muammolari

Tadqiqot shuni ko'rsatdiki, kvant kompyuterlari sohasida intellektual mulk himoyasi murakkab va ko'p qirrali muammo hisoblanadi. Kvant algoritmlari, apparat ta'minoti va dasturiy ta'minot turli intellektual mulk huquqlari orqali himoyalanishi mumkin, jumladan, patentlar, mualliflik huquqi, tijorat sirlari va dizayn huquqlari [7].

Patentlash jarayonida bir nechta asosiy muammolar mavjud. Birinchidan, kvant kompyuterlarining murakkab ilmiy tabiati patent mutaxassislari va sudyalar uchun tushunish qiyinligini keltirib chiqaradi. Patent arizalarini ko'rib chiquvchi ekspertlar odatda mexanik, kimyoviy yoki elektr ixtirolariga ko'proq tanish bo'lib, kvant mexanikasining nozik tomonlarini to'liq tushunmasliklari mumkin [8].

Ikkinchidan, kvant kompyuterlari sohasidagi innovatsiyalar juda tez sur'atda rivojlanmoqda, bu esa patentlarning muddati va ahamiyati haqida savollar tug'diradi. Bugungi kunda ilg'or hisoblanayotgan texnologiya ertaga eskirgan bo'lishi mumkin. AQSh Patent va Tovar Belgilari Idorasining ma'lumotlariga ko'ra, 2023-yilda kvant kompyuterlariga oid patentlar soni 2022-yilga nisbatan 61 foizga oshgan [9].

Uchinchidan, kvant algoritmlarini patentlash masalasi mavjud. AQSh qonunchiligida abstrakt g'oyalar va matematik formulalar patentlanmaydi. Shuning uchun kvant algoritmlari patentga layoq bo'lishi uchun ular aniq texnik natija yoki yaxshilanishga yo'naltirilgan bo'lishi kerak [10]. Patent va Tovar Belgilari Apellyatsiya Kengashining Ex parte Cao ishida (2024-002159-sonli apellyatsiya) ushbu masala tahlil qilindi, natijada Kengash kvant algoritmlari amaliy qo'llanishga ega bo'lganda patentga layoq ekanligini tasdiqladi [11].

Kvant kompyuterlari apparat ta'minoti, xususan, qubitlar, kvant eshiklari, chiplar va sovutish tizimlari patentlar orqali himoyalanishi mumkin. Hozirgi paytda kvant kompyuterlariga oid 1892 ta patent mavjud bo'lib, ular mashinali o'rganish, ta'minot zanjirini optimallashtirish, moliyaviy aktivlar portfelini boshqarish va kvant apparat xatolarini tuzatish kabi sohalarga tegishli [12].

Kvant dasturiy ta'minoti mualliflik huquqi orqali himoyalanishi mumkin, ammo bunda ham muammolar mavjud.

Mualliflik huquqining mudati muallif hayoti davomida va vafotidan keyin 70 yil davom etadi, bu esa tez rivojlanayotgan kvant texnologiyalari uchun haddan tashqari uzoq muddat hisoblanishi mumkin [13].

Tijorat sirlari ham kvant texnologiyalarini himoya qilishning muhim usuli hisoblanadi. Ba'zi hollarda, xususan, noyob kvant apparat dizaynlari kabi takrorlanishi qiyin bo'lgan innovatsiyalar uchun, tijorat sirlari sifatida saqlash patentlashdan ko'ra samaraliroq bo'lishi mumkin [14].

3.2. Ma'lumotlar Xavfsizligi va Shifrlash Tizimlari

Tadqiqot natijalari shuni ko'rsatadiki, kvant kompyuterlari hozirgi shifrlash tizimlariga jiddiy xavf tug'diradi. Hozirgi paytda internet va raqamli aloqalarning xavfsizligi asosan RSA, ECDH, DSA va ECDSA kabi asimmetrik shifrlash algoritmlariga tayanadi. Ushbu algoritmlar katta sonlarni faktorizatsiya qilish va diskret logarifmlarni hisoblash muammolarining murakkabligiga asoslangan [15].

Biroq, yetarlicha kuchli kvant kompyuteri, xususan, kriptografik jihatdan tegishli kvant kompyuteri (CRQC), ushbu muammolarni qisqa vaqt ichida hal qilishi mumkin. Shor algoritmi, kvant kompyuterlari uchun ishlab chiqilgan, RSA shifrini buzish imkoniyatini beradi [16]. Bu esa moliyaviy xizmatlar, sog'liqni saqlash, davlat idoralari va boshqa sohalarda katta xavflar tug'diradi.

Xususan, "hozir to'pla, keyinroq shifrlash" (harvest now, decrypt later) hujumlari allaqachon sodir bo'lmoqda. Bu hujumlarda jinoyatchilar hozirgi shifrlangan ma'lumotlarni saqlab qo'yib, kelajakda kvant kompyuterlari orqali ularni ochishni rejalashtirmoqda [17]. Bu masala uzoq muddatli maxfiylikni talab qiladigan ma'lumotlar, masalan, davlat sirlari, tibbiy yozuvlar va moliyaviy ma'lumotlar uchun ayniqsa xavfli.

NIST ushbu muammolarga javob sifatida 2024-yil 13-avgust kuni birinchi post-kvant kriptografiya standartlarini e'lon qildi. Uchta Federal Axborot Ishlov Berish Standartlari (FIPS) e'lon qilindi: FIPS 203 (ML-KEM), FIPS 204 (ML-DSA) va FIPS 205 (SLH-DSA) [18]. ML-KEM umumiy shifrlash uchun asosiy standart sifatida tavsiya etiladi, chunki u nisbatan kichik shifrlash kalitlaridan foydalanadi va tez ishlaydi. ML-DSA va SLH-DSA raqamli imzolar uchun mo'ljallangan.

NIST 2024-yil noyabr oyida nashr etilgan IR 8547 hisobotida post-kvant kriptografiyaga o'tish yo'l xaritasini taqdim etdi. Hisobotda milliy xavfsizlik tizimlari uchun 2035-yilgacha kvant chidamli algoritmlarga to'liq o'tish muddati belgilandi [19]. Shuningdek, 2030-yildan keyin 112-bit yoki undan kam xavfsizlikni ta'minlaydigan klassik shifrlash algoritmlarining qo'llanilishi taqiqlanadi.

Huquqiy jihatdan bu o'zgarishlar kompaniyalar uchun yangi majburiyatlar tug'diradi. Hozirgi maxfiylik va kiberxavfsizlik tartibga soliqlari "o'rinli xavfsizlik" tamoyiliga asoslangan, ya'ni kompaniyalar tashqi xavf muhitini hisobga olgan holda tegishli texnik va tashkiliy choralarni ko'rishlari kutiladi. Kvant kompyuterlari davrida "o'rinli" tushunchasi o'zgarishi mumkin, bu esa kompaniyalarning javobgarligini oshiradi [20].

3.3. Huquqiy Tartibga Solish va Boshqaruv

Tadqiqot natijalariga ko'ra, kvant texnologiyalarini huquqiy tartibga solish hali rivojlanish bosqichida. Turli davlatlar va xalqaro tashkilotlar kvant kompyuterlariga yondashuvlarini shakllantirmoqda.

Amerika Qo'shma Shtatlari kvant texnologiyalari sohasida yetakchi o'rinni egallaydi. 2018-yilda qabul qilingan Milliy Kvant Tashabbusi Qonuni kvant tadqiqotlariga katta mablag'lar ajratdi va NIST post-kvant kriptografiya standartlarini

ishlab chiqishga rahbarlik qildi [21]. Oq Uy 2022-yil may oyida "Kvant Kompyuterlarida AQSh Yetakchiligini Rivojlantirish va Zaif Kriptografik Tizimlarga Xavflarni Kamaytirish" nomli Milliy Xavfsizlik Memorandumini e'lon qildi [22].

Yevropa Ittifoqi ham kvant texnologiyalariga katta e'tibor bermoqda. Yevropa Komissiyasi ma'lumotlar va sun'iy intellektdagi taraqqiyotni aks ettiruvchi yangi intellektual mulk himoyasi modelini taklif qildi [23]. Shuningdek, Yevropa mamlakatlarida kvant xavfsizlik tadqiqotlari faol olib borilmoqda.

Xitoy kvant patent arizalarida yetakchi o'rinni egallaydi. Xitoy hukumatining kuchli qo'llab-quvvatlashi va Xitoy Fanlar Akademiyasi kabi tadqiqot muassasalari kvant aloqa sohasida muhim yutuqlarga erishdi [24]. IBM, Google va Microsoft kabi AQSh kompaniyalari ham kvant patent portfellarini faol ravishda kengaytirmoqda.

Huquqiy tartibga solishda bir nechta asosiy yo'nalishlar aniqlanadi. Birinchidan, milliy xavfsizlik nuqtai nazaridan, kvant texnologiyalari davlat sirlari sifatida tasniflanishi mumkin va eksport nazorati choralari joriy etilishi kerak [25]. Ikkinchidan, kvant kompyuterlarining zararli maqsadlarda qo'llanilishining oldini olish uchun foydalanish shartlari va javobgarlik masalalari aniqlanishi kerak.

Jahon Iqtisodiy Forumi tomonidan 2024-yilda e'lon qilingan Kvant Kompyuter Boshqaruvi Tamoyillari xalqaro hamkorlik uchun asos yaratadi. Ushbu tamoyillar umumiy foyda, javobgarlik, zarar etkazmaslik, ochiqlik va shaffoflik kabi asosiy qiymatlarni o'z ichiga oladi [26].

3.4. Axloqiy va Ijtimoiy Masalalar

Tadqiqot kvant kompyuterlarining axloqiy va ijtimoiy ta'sirlarini ham ko'rsatadi. Kvant kompyuterlari kuchli bo'lgani sababli, ularning noto'g'ri qo'llanilishi jiddiy oqibatlarga olib kelishi mumkin.

Birinchidan, kvant kompyuterlari mavjud tengsizliklarni kuchaytirishi mumkin. Kvant texnologiyalari juda qimmat bo'lib, faqat boy davlatlar va katta korporatsiyalar ularga kirishga qodir [27]. Bu texnologik tengsizlikning yangi darajasini yaratishi va rivojlanayotgan davlatlarni yanada ortda qoldirishi mumkin.

Ikkinchidan, kvant kompyuterlari ommaviy kuzatuv imkoniyatlarini yaratishi mumkin. Kvant kompyuterlarining shifrlashni buzish qobiliyati hukumatlar va maxsus xizmatlar tomonidan fuqarolarning shaxsiy ma'lumotlarini ommaviy tarzda to'plash va tahlil qilish uchun suiiste'mol qilinishi mumkin [28].

Uchinchidan, kvant sun'iy intellekti avtomatlashtirilgan qaror qabul qilish jarayonlarida noxolis algoritmlarni keltirib chiqarishi mumkin. Kvant algoritmlari moliya, sog'liqni saqlash va jinoiy odil sudlovda qo'llanilganda, ularning adolatli va xolis bo'lishini ta'minlash muhim [29].

Huquqshunoslar uchun bu masalalar yangi majburiyatlar tug'diradi. Huquqshunoslar kvant texnologiyalarining mas'uliyatli rivojlanishini rag'batlantirish, fuqarolar huquqlarini himoya qilish va kvant kompyuterlarining huquqiy va axloqiy oqibatlari haqida xabardorlikni oshirish bo'yicha muhim rol o'ynaydilar [30].

4. MUHOKAMA

Tadqiqot natijalari kvant kompyuterlarining huquqiy sohaga chuqur va ko'p qirrali ta'sirini tasdiqlaydi. Har bir aniqlangan yo'nalish bo'yicha muhokama qilish va tavsiyalar ishlab chiqish zarur.

Intellektual mulk huquqlari sohasida asosiy muammo kvant texnologiyalarining murakkabligi va tez rivojlanishi bilan an'anaviy patent tizimining moslashish qiyinligi o'rtasidagi ziddiyatdir. Patent mutaxassislari va sudyalarning kvant mexanikasidan yetarli darajada xabardor emasligi patentlash

jarayonini murakkablashtiradi. Bundan tashqari, patent mudaati odatda 20 yil bo'lib, bu tez rivojlanayotgan kvant texnologiyalari uchun haddan tashqari uzoq yoki qisqa bo'lishi mumkin.

Ushbu muammolarni hal qilish uchun bir nechta yondashuv taklif qilinadi. Birinchidan, patent tizimida kvant texnologiyalari bo'yicha maxsus mutaxassislar tayyorlash zarur. Ikkinchidan, patent arizalarini tayyorlashda fiziklar, muhandislar va huquqshunoslar o'rtasida interdissiplinar hamkorlik ta'minlanishi kerak. Uchinchidan, patent portfellarini muntazam ravishda ko'rib chiqish va yangi yutuqlarni aks ettiruvchi qo'shimcha patentlar topshirish strategiyasi qo'llanilishi kerak.

Tijorat sirlari va ochiq manba dasturiy ta'minoti o'rtasida muvozanat topish ham muhim. Ba'zi kvant innovatsiyalari uchun tijorat sirlari sifatida saqlash samaraliroq bo'lishi mumkin, ammo bu ilmiy hamkorlik va texnologik taraqqiyotni sekinlashtirishi mumkin. Ochiq manba yondashuvi innovatsiyani tezlashtirishi mumkin, ammo kompaniyalar uchun raqobat ustunligini yo'qotish xavfini tug'diradi.

Ma'lumotlar xavfsizligi va shifrlash sohasida eng dolzarb masala hozirgi shifrlash tizimlaridan post-kvant kriptografiyaga o'tish jarayonidir. NIST standartlarining e'lon qilinishi muhim qadam bo'lsa-da, amaliy joriy etilishi murakkab va ko'p vaqt talab qiladi. Tadqiqotlar shuni ko'rsatadiki, Finlandiyada faqat 3 foiz kompaniyalar kvant o'tishiga aniq choralar ko'rgan, garchi 75 foiz respondentlar kvant xavfidan xabardor bo'lsa ham [31].

Kompaniyalar va tashkilotlar uchun quyidagi tavsiyalar beriladi. Birinchidan, tizimlarni inventarizatsiya qilish va ommaviy kalitli kriptografiyadan foydalanadigan dasturlarni aniqlash zarur. Ikkinchidan, tashkiliy ma'lumotlarni inventarizatsiya qilish, tasniflash va ularning hayot siklini aniqlash kerak. Uchinchidan, yangi post-kvant kriptografik standartlarni laboratoriya muhitida sinab ko'rish, ammo rasmiy e'lon qilinguncha ishlab chiqarish muhitida joriy qilmaslik kerak. To'rtinchidan, tizimlarni yangi kriptografik standartga o'tkazish uchun rejani ishlab chiqish, shu jumladan, tizimlar o'rtasidagi bog'liqlikni tahlil qilish zarur [32].

Huquqiy jihatdan, kompaniyalar uchun yangi majburiyatlar paydo bo'ladi. "O'rinli xavfsizlik" tushunchasi kvant davriga moslashishi kerak. Kompaniyalar hozirdan boshlab kvant xavfsizligini ta'minlash choralarini ko'rmasligi kelgusida huquqiy javobgarlikka olib kelishi mumkin. Maxfiylik va ma'lumotlar himoyasi qonunchiligi, masalan, GDPR kabi tartibga soliqlar, kvant xavfsizligini hisobga olgan holda yangilanishi kerak.

Huquqiy tartibga solish sohasida global hamkorlik zaruriyati yaqqol namoyon bo'lmoqda. Kvant texnologiyalari chegara tanimas xususiyatga ega bo'lgani uchun, milliy tartibga soliqlar etarli emas. Xalqaro standartlar va kelishuvlar zarur. NIST standartlari global benchmark bo'lishiga qaramay, turli davlatlar o'z yondashuvlarini ishlab chiqmoqda.

O'zbekiston uchun tavsiyalar quyidagilarni o'z ichiga oladi. Birinchidan, kvant texnologiyalari va ularning huquqiy ta'siri bo'yicha milliy tadqiqot dasturini ishlab chiqish zarur. Ikkinchidan, Oliy Majlisda kvant texnologiyalarini tartibga soluvchi qonunchilik bazasini shakllantirishni boshlash kerak. Uchinchidan, huquqshunoslarni va sud tizimi xodimlarini kvant texnologiyalari bo'yicha o'qitish dasturlarini joriy etish muhim. To'rtinchidan, NIST standartlari asosida milliy kiberxavfsizlik strategiyasini yangilash va post-kvant kriptografiyaga o'tish yo'l xaritasini ishlab chiqish zarur.

Axloqiy masalalar sohasida huquqshunoslar muhim rol o'ynashi kerak. Kvant texnologiyalarining ijtimoiy ta'sirini

baholash va zaif guruhlarga salbiy ta'sirini kamaytirish choralarini ishlab chiqish zarur. Kvant kompyuterlariga kirishning adolatli taqsimlanishini ta'minlash va raqamli tengsizlikning kuchayishining oldini olish muhim.

Kvant algoritmlari va sun'iy intellektida noxolislik muammosi jiddiy e'tibor talab qiladi. Moliya, sog'liqni saqlash va jinoiy odil sudlovda qo'llaniladigan kvant algoritmlari adolatli va shaffof bo'lishi kerak. Bunday algoritmlarga nisbatan audit va nazorat mexanizmlarini joriy etish zarur.

Kvant kompyuterlarining potentsial zararli qo'llanilishining oldini olish uchun qat'iy tartibga soliq choralari kerak. Foydalanish shartlari va javobgarlik masalalari aniq belgilanishi kerak. Kvant texnologiyalarini eksport nazorati va milliy xavfsizlik nuqtai nazaridan ham tartibga solish zarur.

Tadqiqot cheklovlari ham e'tirof etilishi kerak. Kvant kompyuterlari hali rivojlanish bosqichida bo'lib, ko'plab texnik muammolar, jumladan, qubitlarning barqarorligi va xato tuzatish, hal qilinmagan. Shuning uchun, kelajakdagi texnik taraqqiyot ba'zi xulosalarni o'zgartirishi mumkin. Bundan tashqari, kvant texnologiyalarining huquqiy ta'siri haqidagi tadqiqotlar hali dastlabki bosqichda bo'lib, uzoq muddatli sud amaliyoti va qonunchilik o'zgarishlari kuzatilishi kerak.

5. XULOSA

Ushbu tadqiqot kvant kompyuterlarining huquqiy sohaga katta ta'sir ko'rsatishini tasdiqladi. Kvant texnologiyalari intellektual mulk huquqlari, ma'lumotlar xavfsizligi, huquqiy tartibga solish va axloqiy masalalar sohasida jiddiy imkoniyatlar va muammolar tug'dirmoqda.

Intellektual mulk sohasida kvant texnologiyalarini patentlash murakkab bo'lib, an'anaviy patent tizimini yangi yondashuvlarni talab qilmoqda. Patent mutaxassislarining malakasini oshirish, interdissiplinar hamkorlikni kuchaytirish va moslashuvchan patent strategiyalarini ishlab chiqish zarur. Kvant algoritmlari, apparat ta'minoti va dasturiy ta'minot turli intellektual mulk himoyasi usullarini talab qiladi.

Ma'lumotlar xavfsizligi sohasida kvant kompyuterlari hozirgi shifrlash tizimlariga jiddiy xavf tug'diradi. NIST tomonidan 2024-yil avgust oyida e'lon qilingan post-kvant kriptografiya standartlari ushbu muammoga javob beradi, ammo ularning amaliy joriy etilishi murakkab jarayondir. Kompaniyalar va tashkilotlar hozirdan boshlab kvant xavfsizligiga o'tishga tayyorgarlik ko'rishlari kerak. "Hozir to'pla, keyinroq shifrlash" hujumlari haqiqiy xavf bo'lib, uzoq muddatli maxfiylikni talab qiladigan ma'lumotlar uchun ayniqsa xavfli.

Huquqiy tartibga solish sohasida global hamkorlik zarur. Turli davlatlar va xalqaro tashkilotlar kvant texnologiyalarini tartibga solish bo'yicha o'z yondashuvlarini ishlab chiqmoqda. Jahon Iqtisodiy Forumining boshqaruv tamoyillari xalqaro hamkorlik uchun asos yaratadi. Milliy xavfsizlik, eksport nazorati, foydalanish shartlari va javobgarlik masalalari aniq belgilanishi kerak.

Axloqiy masalalar sohasida kvant texnologiyalarining ijtimoiy ta'sirini baholash va zaif guruhlarga salbiy ta'sirini kamaytirish muhim. Kvant kompyuterlariga kirishning adolatli taqsimlanishi, ommaviy kuzatuvning oldini olish va algoritm noxolisligi kabi masalalar huquqiy tartibga solishni talab qiladi.

Huquqshunoslar uchun kvant kompyuterlari yangi imkoniyatlar va majburiyatlar yaratadi. Huquqshunoslar kvant texnologiyalari va ularning huquqiy ta'siri haqida chuqur bilimga ega bo'lishlari kerak. Huquqshunoslar kompaniyalarga maxsus maslahat berish, fuqarolar huquqlarini himoya qilish va kvant kompyuterlarining huquqiy va axloqiy oqibatlari haqida xabardorlikni oshirishda muhim rol o'ynaydilar.

O'zbekiston uchun tavsiyalar quyidagilarni o'z ichiga oladi: kvant texnologiyalari va ularning huquqiy ta'siri bo'yicha milliy tadqiqot dasturini ishlab chiqish, kvant texnologiyalarini tartibga soluvchi qonunchilik bazasini shakllantirishni boshlash, huquqshunoslarni va sud tizimi xodimlarini o'qitish dasturlarini joriy etish va milliy kiberxavfsizlik strategiyasini yangilash. Shuningdek, xalqaro hamkorlikni rivojlantirish va NIST standartlariga asoslangan milliy post-kvant kriptografiya yo'l xaritasini ishlab chiqish muhim.

Kelajakda kvant kompyuterlarining huquqiy ta'siri yanada kuchayishi kutilmoqda. 2030-yillarga kelib kvant kompyuterlari tijoriy jihatdan kengroq qo'llanilishi va bu huquqiy sohada yangi muammolar va imkoniyatlar yaratishi mumkin. Shuning uchun, huquqshunoslar, siyosatchilar va texnologiya sohasidagi mutaxassislar o'rtasida doimiy muloqot va hamkorlik zarur.

Ushbu tadqiqot kvant kompyuterlarining huquqiy sohaga ta'siri bo'yicha asosiy yo'nalishlarni aniqladi va kelajakdagi tadqiqotlar uchun asos yaratdi. Biroq, bu sohada ko'proq empirik tadqiqotlar, uzoq muddatli sud amaliyotini kuzatish va turli davlatlarning tajribasini qiyosiy tahlil qilish zarur. Kvant kompyuterlari texnologiyasining rivojlanishi bilan birga huquqiy tadqiqotlar ham davom etishi kerak.

Foydalanilgan adabiyotlar

[1] Cambridge Core. (2025). Quantum Computing and the Law: Navigating the Legal Implications of a Quantum Leap. European Journal of Risk Regulation. https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/quantum-computing-and-the-law-navigating-the-legal-implications-of-a-quantum-leap/3D6C2D3B2B425BB3B2FEE63BF42EB295

[2] The Impact Lawyers. (n.d.). The legality of quantum computing: a challenge for 21st century lawyers. https://theimpactlawyers.com/articles/the-legality-of-quantum-computing-a-challenge-for-21st-century-lawyers

[3] Oxford Academic. (2022). Intellectual property in quantum computing and market power: a theoretical discussion and empirical analysis. Journal of Intellectual Property Law & Practice, 17(8), 613-632. https://academic.oup.com/jiplp/article/17/8/613/6646536

[4] IoT World Today. (2023). Quantum Computing and the Law. https://www.iotworldtoday.com/industry/quantum-computing-and-the-law

[5] A&O Shearman. (n.d.). The opportunities and legal risks of quantum computing. https://www.aoshearman.com/en/insights/the-opportunities-and-legal-risks-of-quantum-computing

[6] Technology Innovation Institute. (2024). Navigating the Quantum Frontier: The Arrival of NIST's First Post-Quantum Cryptography Standards. https://www.tii.ae/insights/navigating-quantum-frontier-arrival-nists-first-post-quantum-cryptography-standards

[7] Michalsons. (2024). Quantum computing: identifying the legal risks. https://www.michalsons.com/blog/quantum-computing-identifying-the-legal-risks/62544

[8] PatentPC. (2025). Patent Challenges in Quantum Computing: Legal Implications. https://patentpc.com/blog/patent-challenges-in-quantum-computing-legal-implications

[9] QED-C. (2025). State of Quantum Industry Innovation – What Patents Tell Us. https://quantumconsortium.org/publication/

state-of-quantum-industry-innovation-what-patents-tell-us/

[10] American Bar Association. (n.d.). The Legal Implications of Quantum Computing. https://www.americanbar.org/groups/science_technology/resources/scitech-lawyer/archive/legal-implications-quantum-computing/

[11] Goodwin Law. (2025). PTAB's Reversal Sheds Light on Quantum Computing Patents. https://www.goodwinlaw.com/en/insights/publications/2025/03/alerts-technology-lit-ptabs-reversal-sheds-light-on-quantum

[12] Law.edu. (n.d.). Establishing the Legal Framework to Regulate Quantum Computing. Journal of Law and Technology. https://scholarship.law.edu/cgi/viewcontent.cgi?article=1143&context=jlt

[13] Foley & Lardner LLP. (2024). Beyond The Binary: Legal Considerations in the Quantum Computing Era. https://www.foley.com/insights/publications/2024/04/beyond-binary-legal-considerations-quantum-computing-era/

[14] Lumenci. (2025). Quantum Computing and Patentability. https://lumenci.com/blogs/quantum-computing-and-patentability/

[15] AppViewX. (2024). NIST Announces the First 3 Post-Quantum Cryptography Standards - Ready or Not? https://www.appviewx.com/blogs/nist-announces-the-first-3-post-quantum-cryptography-standards-ready-or-not/

[16] The Stack. (2025). NIST reveals first four post-quantum cryptography algorithms. https://www.thestack.technology/post-quantum-cryptography-nist/

[17] CISA. (n.d.). Post-Quantum Cryptography Initiative. https://www.cisa.gov/quantum

[18] Decent Cybersecurity. (2024). NIST Unveils Groundbreaking Post-Quantum Encryption Standards: A New Era in Global Cybersecurity. https://decentcybersecurity.eu/nist-unveils-groundbreaking-post-quantum-encryption-standards-a-new-era-in-global-cybersecurity/

[19] InfoSec Global. (n.d.). NIST Roadmap to Post-Quantum Cryptography: IR 8547 Report. https://www.infosecglobal.com/posts/nist-post-quantum-cryptography-deadlines-ir-8547

[20] Internet Lawyer Blog. (2023). Quantum Computer Technology Laws. https://www.internetlawyer-blog.com/quantum-computer-technology-laws/

[21] PatentNext. (2025). Quantum Computing Patent Trends in the US. https://www.patentnext.com/2025/03/quantum-computing-patent-trends-in-the-us-are-breakthroughs-just-around-the-corner/

[22] The SSL Store. (2025). NIST Announces 2024 Timeline for First Standardized Post-Quantum Cryptography (PQC) Algorithms. https://www.thesslstore.com/blog/nist-announces-2024-timeline-for-first-standardized-post-quantum-cryptography-pqc-algorithms/

[23] Insights2TechInfo. (2023). Quantum Technologies: Legal Implications and Regulatory Landscape. https://insights2techinfo.com/quantum-technologies-legal-implications-and-regulatory-landscape/

[24] PatentPC. (2025). Quantum Computing Patenting and Intellectual Property Rights. https://patentpc.com/blog/quantum-computing-patenting-2

[25] PatentPC. (2025). Overcoming Challenges in Quantum Computing Patent Applications. https://patentpc.com/blog/challenges-in-quantum-computing-patent-applications

[26] Lifeboat News. (2024). NIST's post-quantum cryptography standards are here.

https://lifeboat.com/blog/2024/08/nists-post-quantum-cryptography-standards-are-here

[27] Encryption Consulting. (2025). NIST Selects HQC as Fifth Algorithm for Post-Quantum Encryption: What It Means For You. https://www.encryptionconsulting.com/nist-selects-hqc-as-fifth-algorithm-for-post-quantum-encryption/

[28] Medium. (2023). Quantum Computing and Intellectual Property by Jonathan Paulson. https://medium.com/@cybertec/quantum-computing-and-intellectual-property-c61d18eab953

[29] Bold Patents. (2024). Quantum Computing Patents: Navigating Uncharted Legal Territory. https://boldip.com/blog/quantum-computing-patents-navigating-uncharted-legal-territory/

[30] PatentPC. (2025). Patent Challenges in Quantum Computing: Legal Implications. https://patentpc.com/blog/patent-challenges-in-quantum-computing-legal-implications

[31] VTT Research. (2025). Post-Quantum Cryptography standard released - practical work can now begin. https://www.vttresearch.com/en/news-and-ideas/post-quantum-cryptography-standard-released-practical-work-can-now-begin

[32] CISA. (n.d.). Post-Quantum Cryptography Initiative - Roadmap. https://www.cisa.gov/quantum