TOSHKENT DAVLAT YURIDIK UNIVERSITETI

YURISPRUDENSIYA

HUQUQIY ILMIY-AMALIY JURNALI

2024-yil 2-son

VOLUME 4 / ISSUE 2 / 2024

DOI: 10.51788/tsul.jurisprudence.4.2.

Crossref Content Registration

ISSN: 2181-1938

DOI: 10.51788/tsul.jurisprudence

MUNDARIJA

12.00.01 – DAVLAT VA HUQUQ NAZARIYASI VA TARIXI. HUQUQIY TA'LIMOTLAR TARIXI

12.00.02 – KONSTITUTSIYAVIY HUQUQ. MA'MURIY HUQUQ. MOLIYA VA BOJXONA HUQUQI

12.00.03 – FUQAROLIK HUQUQI. TADBIRKORLIK HUQUQI. OILA HUQUQI. XALQARO XUSUSIY HUQUQ

12.00.06 – TABIIY RESURSLAR HUQUQI. AGRAR HUQUQ. EKOLOGIK HUQUQ

12.00.09 – JINOYAT PROTSESSI. KRIMINALISTIKA, TEZKOR-QIDIRUV HUQUQ VA SUD EKSPERTIZASI

12.00.10 – XALQARO HUQUQ

DOI: https://dx.doi.org/10.51788/tsul.jurisprudence.4.2./XOTJ9919
UDC: 340.13:004.7(045)(575.1)

KVANT TAHDIDI: KVANT HISOBLASHNING XALQARO KIBERXAVFSIZLIKKA TA'SIRINI VA YANGI HUQUQIY BAZALARGA SHOSHILINCH EHTIYOJNI O'RGANISH

Gulyamov Said Saidaxrorovich,
Toshkent davlat yuridik universiteti
Kiber huquq kafedrasi mudiri,
professor, yuridik fanlar doktori
ORCID: 0000-0002-2299-2122
e-mail: said.gulyamov1976@gmail.com

Abdixakimov Islombek Bahodir o'g'li,
Toshkent davlat yuridik universiteti
Kiber huquq kafedrasi o'qituvchisi
ORCID: 0000-0002-3682-2810
e-mail: islombekabduhakimov@gmail.com

Annotatsiya. *Kvant hisoblashning jadal rivojlanishi tobora raqamlashtirilayotgan dunyomizning kiberxavfsizligiga jiddiy tahdid solmoqda. Kvant kompyuterlari yanada kuchliroq bo'lgani va foydalanish imkoni ortgani sari ularda ayni paytda nozik ma'lumotlarimiz, moliyaviy operatsiyalarimiz va muhim infratuzilmani himoya qiladigan ko'plab kriptografik algoritmlarni buzish potensiali paydo bo'lmoqda. Yaqinlashib kelayotgan ushbu "kvant tahdidi" shaxslar, tashkilotlar va davlatlar uchun keng qamrovli oqibatlarga olib boradi, chunki bu ma'lumotlarning keng tarqalishiga, iqtisodiy buzilishlarga va milliy xavfsizlikka putur yetkazishi mumkin. Ushbu xavf tobora ortib borayotgani e'tirof etilishiga qaramay, mavjud huquqiy va me'yoriy bazalar kvant kibertahdidlari keltirib chiqaradigan o'ziga xos muammolarini hal qilish uchun aytarli darajada tayyor emas. Bundan tashqari, kvant inqilobining geosiyosiy oqibatlari murakkab va serqirra bo'lib, global kuchlar muvozanatini o'zgartirib yuborish hamda texnologik tengsizliklarni kuchaytirish qobiliyatiga ega. Ushbu xatarlarni yumshatish va kvant tayyorgarligini oshirish uchun xalqaro hamjamiyat zudlik bilan texnik, iqtisodiy, huquqiy va siyosiy sohalarni qamrab oluvchi yangi qonunchilik asoslari hamda hamkorlik mexanizmlarini ishlab chiqishga ehtiyoj sezmoqda. Ushbu maqola kiberxavfsizlikka kvant tahdidining fanlararo tahlilini taqdim etadi, uning turli sektorlar va xalqaro munosabatlardagi potensial ta'sirini o'rganadi hamda keng qamrovli global boshqaruv tizimini ishlab chiqish uchun siyosat bo'yicha tavsiyalar beradi. Ko'p manfaatdor tomonlarning hamkorligi va kvantga chidamli yechimlar yordamida ushbu muammoni faol hal qilish orqali biz mazkur transformatsion texnologiya oldida yanada xavfsizroq va mustahkam raqamli kelajak sari harakat qilishimiz mumkin.*

Kalit so'zlar: *kvant hisoblash, kiberxavfsizlik, kriptografiya, xalqaro huquq, global boshqaruv, geosiyosat, rivojlanayotgan texnologiyalar, raqamli xavfsizlik, kvant tahdidi, kvantdan keyingi kriptografiya.*

КВАНТОВАЯ УГРОЗА: ИЗУЧЕНИЕ ВЛИЯНИЯ КВАНТОВЫХ ВЫЧИСЛЕНИЙ НА МЕЖДУНАРОДНУЮ КИБЕРБЕЗОПАСНОСТЬ И ОСТРАЯ НЕОБХОДИМОСТЬ В НОВЫХ ПРАВОВЫХ РАМКАХ

Гулямов Саид Саидахрарович,
доктор юридических наук, профессор,
заведующий кафедрой «Киберправо»
Ташкентского государственного
юридического университета

Абдихакимов Исломбек Баходир угли,
преподаватель кафедры «Киберправо»
Ташкентского государственного
юридического университета

Аннотация. *Быстрое развитие квантовых вычислений представляет собой серьёзную угрозу кибербезопасности нашего всё более оцифрованного мира. По мере того как квантовые компьютеры становятся более мощными и доступными, у них появляется потенциал взлома многих криптографических алгоритмов, которые в настоящее время защищают наши конфиденциальные данные, финансовые транзакции и критически важную инфраструктуру. Эта надвигающаяся «квантовая угроза» имеет далеко идущие последствия для отдельных лиц, организаций и национальных государств, поскольку может привести к широкомасштабным утечкам данных, экономическим потрясениям и угрозе национальной безопасности. Несмотря на растущее признание этого риска, существующие правовые и нормативные базы в значительной степени не готовы к решению уникальных проблем, связанных с квантовыми киберугрозами. Более того, геополитические последствия квантовой революции сложны, многогранны и потенциально способны изменить глобальный баланс сил и усугубить технологическое неравенство. Чтобы смягчить эти риски и повысить квантовую готовность, международному сообществу необходимо срочно разработать новые правовые рамки и механизмы сотрудничества, которые охватывают техническую, экономическую, правовую и политическую области. В этой статье представлен междисциплинарный анализ квантовой угрозы кибербезопасности, рассмотрено её потенциальное влияние на различные сектора и международные отношения, а также предложены политические рекомендации для разработки комплексной структуры глобального управления. Активно решая эту проблему посредством сотрудничества с участием многих заинтересованных сторон и квантовоустойчивых решений, мы можем работать над созданием более безопасного и устойчивого цифрового будущего перед лицом этой преобразующей технологии.*

Ключевые слова: *квантовые вычисления, кибербезопасность, криптография, международное право, глобальное управление, геополитика, новые технологии, цифровая безопасность, квантовая угроза, постквантовая криптография.*

THE QUANTUM THREAT: EXAMINING THE IMPACT OF QUANTUM COMPUTING ON INTERNATIONAL CYBERSECURITY AND THE URGENT NEED FOR NEW LEGAL FRAMEWORKS

Gulyamov Said Saidakhrarovich
Tashkent State University of Law,
Head of the Department of Cyber Law,
Professor, Doctor of Law

Abdikhakimov Islombek Bakhodir ugli
Lecturer of the Department of Cyber Law

Abstract. *The rapid advancement of quantum computing poses a significant threat to the cybersecurity of our increasingly digitized world. As quantum computers become more powerful and accessible, they have the potential to break many of the cryptographic algorithms that currently secure our sensitive data, financial transactions, and critical infrastructure. This looming "quantum threat" has far-reaching implications for individuals, organizations, and nation-states, as it could lead to widespread data breaches, economic disruption, and compromised national security. Despite the growing recognition of this risk, existing legal and regulatory frameworks are largely unprepared to address the unique challenges of quantum-enabled cyber threats. Moreover, the geopolitical implications of the quantum revolution are complex and multifaceted, with the potential to reshape the global balance of power and exacerbate technological inequalities. To mitigate these risks and promote quantum readiness, there is an urgent need for the international community to develop new legal frameworks and cooperative mechanisms that span technical, economic, legal, and political domains. This article provides an interdisciplinary analysis of the quantum threat to cybersecurity, examines its potential impacts across various sectors and international relations, and offers policy recommendations for developing a comprehensive global governance framework. By proactively addressing this challenge through multi-stakeholder collaboration and quantum-resistant solutions, we can work towards a more secure and resilient digital future in the face of this transformative technology.*

Keywords: *quantum computing, cybersecurity, cryptography, international law, global governance, geopolitics, emerging technologies, digital security, quantum threat, post-quantum cryptography*

Kirish

Kvant hisoblash texnologiyasining jadal rivojlanishi kiberxavfsizlik sohasi uchun jiddiy muammolarni keltirib chiqaradi. Kvant kompyuterlari yanada kuchliroq bo‘lib, foydalanish imkoni kengaygan sari ularda raqamli infratuzilmamizni muhofazalovchi, jumladan, nozik ma’lumotlarni, moliyaviy operatsiyalarni va milliy xavfsizlik sirlarini himoya qilish uchun foydalaniladigan ko‘plab kriptografik algoritmlarni buzish potensiali yuzaga kelmoqda [1, 2]. Yaqinlashib kelayotgan “kvant tahdidi” butun dunyo bo‘ylab shaxslar, tashkilotlar va milliy davlatlar uchun keng qamrovli oqibatlarni keltirib chiqaradi. Hozirgi shifrlash standartlarini buzishga qodir kvant kompyuterlarini ishlab chiqish endi uzoq faraz emas – keyingi o‘n yoki yigirma yil ichida bu juda real imkoniyatdir [3]. Aslida razvedka agentliklari va texnologiya kompaniyalari ushbu kelajakni kutish uchun kvant hisoblashlari bo‘yicha tadqiqotlar va ishlanmalarga allaqachon katta miqdorda sarmoya kiritmoqdalar [4]. Kvant kompyuterlari yetarli quvvat va barqarorlik darajasiga erishgandan so‘ng ular hatto eng ilg‘or klassik superkompyuterlarga qaraganda ma’lum turdagi hisob-kitoblarni o‘ta yuqori darajada tezroq bajarishga qodir bo‘ladi. Bunga RSA [5] kabi keng qo‘llanadigan ochiq kalitli kriptografiya tizimlarining asosi bo‘lgan katta raqamlarni tezkor faktor qilish qobiliyati kiradi.

Ushbu kvant hisoblash “kripto-apokalipsis”ining oqibatlari halokatli bo‘lishi mumkin. Ilgari xavfsiz shifrlangan deb hisoblangan moliyaviy ma’lumotlar, tibbiy tarixlar, tijorat sirlari va maxfiy hukumat ma’lumotlari to‘satdan kvant hisoblash resurslariga kirish huquqiga ega bo‘lgan zararli shaxslarning shifrni ochishiga zaiflik qilishi ehtimoldan xoli emas [6]. Bu ma’lumotlarning keng ko‘lamli buzilishiga, iqtisodiy tanazzulga, sanoat josusligiga va hatto davlat sirlarining oshkor etilishiga olib kelishi mumkin. Raqamli axborot tobora o‘zaro bog‘langan va jamiyatning barcha jabhalari uchun muhim bo‘lgan dunyoda kiberxavfsizlikka kvant tahdidi yuqori xavfni ifodalaydi.

Xalqaro hamjamiyat ushbu dolzarb muammoni hal qilish uchun kvant hisob-kitoblaridan kelib chiqadigan kiberxavfsizlik xatarlarini boshqarish maqsadida zudlik bilan yangi qonunchilik asoslari va ham-

korlik kelishuvlarini ishlab chiqishga ehtiyoj sezmoqda. Ma'lumotlarni himoya qilish, maxfiylik, intellektual mulk va kompyuter jinoyati bilan bog'liq amaldagi qonunlar hamda qoidalar kvantga chidamli kriptografiyani hisobga olgan holda ishlab chiqilmagan [7]. Raqamli xavfsizlik infratuzilmamizning kvant xavfsizligini ta'minlash uchun hukumatlar, sanoat, ilmiy doiralar va fuqarolik jamiyati o'rtasida global miqyosdagi keng ko'lamli, ko'p tomonlama hamkorlik talab etiladi.

Material va metodlar

Kvant hisoblashning kiberxavfsizlik va xalqaro munosabatlarga ko'p qirrali ta'sirini har tomonlama o'rganish uchun ushbu tadqiqotda fanlararo yondashuvdan foydalanildi. Kompyuter fanlari, kriptografiya, iqtisodiyot, huquq, siyosatshunoslik va xavfsizlikni o'rganish kabi turli sohalardan manbalar ko'rib chiqildi. Kvant hisoblash, kvantdan keyingi kriptografiya va kvant xavfsizligi bo'yicha ilmiy maqolalar, kitoblar, davlat idoralari, tahlil markazlari va sanoat guruhlarining texnik hisobotlari, konferensiya materiallari, huquqiy va siyosiy hujjatlar kabi birlamchi hamda ikkilamchi manbalarga murojaat qilindi. Shuningdek, yangi maqolalar, bloglardagi postlar va ommaviy axborot vositalaridagi kvant texnologiyalariga oid materiallardan ham foydalanildi. Ushbu manbalar xalqaro huquqiy va siyosiy asoslar orqali kiberxavfsizlikka kvant tahdidi bilan bog'liq asosiy muammolar, mavzular va imkoniyatlarni aniqlash maqsadida tizimli ravishda ko'rib chiqilib, tahlil qilindi.

Tadqiqot natijalari

Fanlararo tahlil natijalari shuni ko'rsatadiki, kiberxavfsizlikka kvant tahdidi murakkab, ko'p o'lchovli muammo bo'lib, texnik, iqtisodiy, huquqiy va siyosiy sohalarda muvofiqlashtirilgan global javobni talab qiladi.

Texnik imkoniyatlar va vaqt jadvali

Texnik nuqtayi nazardan ekspertlar o'rtasida joriy ochiq kalitli kriptografiya standartlarini buzishga qodir kvant kompyuterlari kelgusi 10-20 yil ichida ishlab chiqilishi mumkinligi haqida o'sib borayotgan konsensus mavjud [8]. Keng miqyosli, xatolari tuzatilgan kvant kompyuterlarini yaratishda hanuz muhim muhandislik to'siqlari mavjud bo'lsa-da, butun dunyo bo'ylab ham akademik, ham sanoat laboratoriyalarida jadal taraqqiyot kuzatilmoqda. Oxirgi bosqichlar orasida "Google"ning 53 kubitli protsessorda "kvant ustunligi" namoyishi [9] va IBMning 127 kubitli "Eagle" protsessorini [10] ishga tushirishini sanab o'tish mumkin. Shu bilan birga, tadqiqotchilar klassik va kvant kompyuterlarining hujumlariga qarshi tura oladigan yangi post-kvant kriptografik algoritmlarni ishlab chiqish ustida ishlamoqda [11]. 2016-yilda AQSh Milliy standartlar va texnologiyalar instituti (NIST) 2024-yilgacha bir yoki bir nechta kvantga chidamli ochiq kalit algoritmlarini aniqlash va standartlashtirishni maqsad qilgan post-kvant kriptografiyasi uchun standartlashtirish jarayonini boshladi [12]. Biroq ushbu yangi standartlar o'rnatilgandan keyin ham ularni ochiq kalitli kriptografiyaga tayanadigan barcha apparat, dasturiy ta'minot va aloqa protokollarida to'liq joylashtirish uchun ko'p yillar kerak bo'ladi [13].

Mutaxassislar ushbu vaqt jadvallarini hisobga olgan holda yaqin kelajakda kvant kompyuterlari post-kvant alternativlari keng qo'llanishidan oldin joriy shifrlash usullarini buzishga qodir bo'ladigan tanqidiy "o'tish davri"ga duch kelishimizdan ogohlantirmoqda [14]. Ushbu zaiflik oynasida bugungi kunda o'g'irlangan nozik ma'lumotlar kvant hisoblashlari yetarli darajada rivojlanganidan keyin saqlanishi va shifrlanishi mumkin – bu "Hozir yig'ib oling, keyinroq shifrini hal qiling" degan tahdiddir [15].

Iqtisodiy va ijtimoiy ta'sirlar

Kvantga asoslangan kibertahdidlarning potensial iqtisodiy va ijtimoiy ta'siri juda keng qamrovlidir. "Rand" korporatsiyasining 2019-yilgi hisobotida kiberjinoyatchilikning yillik global qiymati allaqachon yuzlab mlrd dollarni tashkil etishi va har yili ortib borishi

taxmin qilingan [16]. Kvant hisoblashlari ushbu tendensiyani keskin tezlashtirishi mumkin, bu esa ko‘plab kiberxavfsizlik himoyalarimizni bir kechada eskirtiradi.

Masalan, onlayn moliyaviy operatsiyalar, elektron tijorat va kriptovalyutalarni himoya qiluvchi ochiq kalitli kriptografiya kvant hujumlariga, ayniqsa, chidamsizdir [17]. Agar kuchli kvant kompyuteriga ega bo‘lgan zararli aktyor banklar, kredit karta kompaniyalari va raqamli valyuta birjalari qo‘llaydigan shifrlashni buzishi mumkin bo‘lsa, u trillionlab dollar qiymatidagi aktivlarni o‘g‘irlashi va butun jahon moliyaviy tizimini buzishi mumkin. Xuddi shunday, kvant kompyuterlari maxfiy biznes ma’lumotlari, tijorat sirlari va intellektual mulk xavfsizligini buzish uchun ishlatilishi mumkin, bu esa sanoat josusligi va insofsiz raqobatdan katta iqtisodiy yo‘qotishlarga olib boradi [18].

To‘g‘ridan to‘g‘ri moliyaviy xarajatlardan tashqari, kvant kiber tahdidlar zamonaviy jamiyatni ta’minlovchi raqamli infratuzilmaga bo‘lgan ishonchni ham buzishi mumkin [19]. Kvant hisoblash orqali amalga oshirilgan keng ko‘lamli ma’lumotlarning buzilishi milliardlab odamlarning shaxsiy ma’lumotlari, jumladan, nozik tibbiy yozuvlar, shaxsiy aloqalar va biometrik ma’lumotlarni fosh qilishi ehtimoldan xoli emas. Bu sizib chiqqan ma’lumotlar shantaj, shaxsiy ma’lumotlarni o‘g‘irlash yoki maqsadli zo‘ravonlik uchun ishlatilgan hollarda shaxsiy daxlsizlik, fuqarolik erkinliklari va hatto jismoniy xavfsizlik uchun jiddiy xavf tug‘diradi.

Bundan tashqari, shifrlashni buzish uchun kvant kompyuterlaridan foydalanish milliy xavfsizlik va xalqaro barqarorlik uchun jiddiy oqibatlarni keltirib chiqarishi mumkin [20]. Mamlakat mudofaasi va strategik manfaatlari uchun muhim bo‘lgan maxfiy hukumat va harbiy ma’lumotlar kvant imkoniyatlariga ega bo‘lgan xorijiy dushmanlar tomonidan qo‘lga kiritilishi va shifrlanishiga qarshi himoyasiz bo‘lib qolishi mumkin. Eng yomon ssenariyda bu yangi qurollanish poygasiga olib borishi mumkin, chunki mamlakatlar kvant texnologiyalarni hujum va mudofaa maqsadlarida ishlab chiqishga intiladi, bu esa mojarolar va noto‘g‘ri hisoblash xavfini oshiradi.

Huquqiy va tartibga soluvchi bo‘shliqlar

Kiberxavfsizlikka kvant tahdidining tobora ortib borayotgani e’tirof etilishiga qaramay, mavjud qonunlar va qoidalar ushbu rivojlanayotgan texnologiya keltirib chiqaradigan muammolarni hal qilishga deyarli tayyor emas [21]. Ma’lumotlarni himoya qilish, shaxsiy daxlsizlik, intellektual mulk va kompyuter jinoyatlariga oid ko‘pgina huquqiy bazalar kvantdan oldingi davrda ishlab chiqilgan va kvant bilan bog‘liq hujumlar xavfini yetarli darajada bartaraf etmaydi.

Misol uchun, Yevropa Ittifoqining Umumiy ma’lumotlarni himoya qilish to‘g‘risidagi reglamenti (GDPR) kompaniyalardan shaxsiy ma’lumotlar xavfsizligini ta’minlash uchun “tegishli texnik va tashkiliy chora-tadbirlar”ni amalga oshirishni talab qiladi [22]. Biroq GDPR kvant hisoblash yoki post-kvant kriptografiyasi haqida alohida eslatib o‘tmaydi, qonunga rioya qilish uchun kvant tayyorligining qaysi darajasini aniqlashni alohida tashkilotlarga topshiradi. Xuddi shunday, 60 dan ortiq mamlakatlar tomonidan ratifikatsiya qilingan Kiberjinoyatlar to‘g‘risidagi Budapesht konvensiyasi kvant kompyuterlaridan xakerlik va ma’lumotlarni o‘g‘irlash kabi jinoiy harakatlar uchun foydalanish imkoniyatlarini ko‘rib chiqmaydi [23].

Qo‘shma Shtatlarda 2018-yilgi Milliy Kvant tashabbusi to‘g‘risidagi qonun kvant tadqiqotlari va ishlanmalarini jadallashtirish bo‘yicha federal dasturni yaratdi, ammo u kvant kiberxavfsizlik standartlari yoki qoidalari bilan bog‘liq hech qanday qoidalarni o‘z ichiga olmaydi [24]. AQSh Milliy standartlar va texnologiyalar instituti (NIST) post-kvant kriptografik standartlarni ishlab chiqish bo‘yicha sa’y-harakatlar olib bormoqda, ammo

bular qonuniy majburiy talablar emas, balki ixtiyoriy ko‘rsatmalardir [12].

Boshqa mamlakatlar ham kvantga xos kiberxavfsizlik siyosatiga ehtiyoj seza boshladi, biroq taraqqiyot notekis va qisman bo‘ldi. Misol uchun, Xitoyning 2020-yilda kuchga kirgan Kriptografiya qonuni kvant kriptografiyasini ishlab chiqish va ishlatish qoidalarini o‘z ichiga oladi, ammo u kvantdan keyingi xavfsizlikning kengroq muammolarini hal qilmaydi [25]. Yaponiyaning kiberxavfsizlik strategiyasi kvant hisoblash xatarlariga tayyorgarlik ko‘rish zarurligini eslatib o‘tadi, biroq u hech qanday aniq harakatlar yoki muddatlarni taqdim etmaydi [26].

Umuman olganda, tez rivojlanayotgan kvant tahdidi manzarasi hamda milliy va xalqaro darajadagi huquqiy, tartibga soluvchi javoblarning sekin sur’ati o‘rtasida aniq tafovut mavjud. Izchil hamda muvofiqlashtirilgan siyosat asoslarining yo‘qligi kvant o‘tishini boshqarishga harakat qilayotgan shaxslar, tashkilotlar va davlatlar uchun sezilarli noaniqlik va xavf tug‘diradi.

Geosiyosiy oqibatlar

Kvant inqilobining geosiyosiy oqibatlari murakkab va ko‘p qirrali bo‘lib, kelgusi o‘n yilliklarda global kuchlar muvozanatini qayta o‘zgartirish imkoniyati mavjud [20]. Mamlakatlar iqtisodiy, harbiy va razvedka maqsadlarida kvant texnologiyalarini ishlab chiqish va ulardan foydalanish uchun bellashar ekan, kvant hisoblash xalqaro raqobat hamda hamkorlikning tobora muhim sohasiga aylanib boradi.

Milliy xavfsizlik nuqtayi nazaridan, Qo‘shma Shtatlar kvant axborot ilm-fanini strategik ustuvorlik sifatida belgilagan, tadqiqot va ishlanmalarga katta miqdorda sarmoya kiritgan Xitoy kabi kuchayib borayotgan kuchlarga nisbatan texnologik ustunligini yo‘qotishi mumkinligidan xavotirlar mavjud [27]. Ba’zi ekspertlarning ogohlantirishicha, agar Xitoy kvant hisoblash va kripto-tahlil sohasida sezilarli yetakchilikka erishsa, harbiy hamda razvedka operatsiyalarida, masalan, AQSh kodlarini buzish, nozik aloqalarni tutib olishda hal qiluvchi ustunlikka ega bo‘lishi mumkin [28]. Bu federal moliyalashtirishni ko‘paytirish va AQShda kvant tadqiqotlarini muvofiqlashtirish, shuningdek, kvant texnologiyalarining xorijiy dushmanlarga o‘tkazilishining oldini olish uchun qat’iy eksport nazorati hamda investitsiya skriningi talablarini keltirib chiqardi [29].

Bir vaqtning o‘zida kvant hisob-kitoblari bilan bog‘liq global muammolarni hal qilish uchun xalqaro hamkorlik va homiylik zarurati tobora ortib bormoqda, masalan, kvantdan keyingi kriptografik standartlarni ishlab chiqish va kvant sohasida mas’uliyatli davlat xatti-harakatlari uchun norma va qoidalarni o‘rnatish [30] bunga misol bo‘la oladi. Ba’zi ekspertlarning ta’kidlashicha, kvant texnologiyalari Sovuq urush davridagi yadroviy qurollarni nazorat qilish kabi buyuk kuchlar hamkorligining asosiy yo‘nalishi bo‘lishi mumkin, chunki AQSh ham, Xitoy ham kvant kiberhujumining halokatli oqibatlarini oldini olishdan umumiy manfaatdordir [31].

Boshqa davlatlar ham so‘nggi yillarda Yevropa Ittifoqi, Yaponiya, Avstraliya, Kanada va Buyuk Britaniya kvant poygasida o‘z o‘rinlarini egallashga intilmoqda [32]. Ba’zi kichikroq shtatlar Shveysariyaning kvant zondlash va metrologiyaga e’tibor qaratishi kabi kvant tajribasining o‘ziga xos sohalarini o‘rganmoqda [33]. Shuningdek, kvant hamkorlik uchun ko‘p tomonlama platformalarni yaratish bo‘yicha sa’y-harakatlar mavjud, masalan, Yevropa kvant flagmani dasturi [34] va NATOga a’zo davlatlar o‘rtasida taklif etilayotgan Kvant alyansi.

Biroq kvant hisoblashning geopolitikasi nafaqat buyuk kuchlar raqobati va hamkorligi, shuningdek, global tengsizlik, raqamli suverenitet hamda texnologik boshqaruvning kengroq muammolari bilan kesishadi. Kvant inqilobi rivojlangan va rivojlanayotgan mamlakatlar o‘rtasidagi mavjud tafovutni kuchaytirishi mumkin, degan xavotirlar mavjud, chunki hozirda bir nechta davlatlar

ilg‘or kvant tadqiqotlarini olib borish uchun resurslarga hamda tajribaga ega [35]. Bu kvant texnologiyalaridan adolatli foydalanish va ularning afzalliklarini ta’minlash, shuningdek, davlat yoki nodavlat subyektlari tomonidan kvant imkoniyatlaridan noto‘g‘ri foydalanishning oldini olish bilan bog‘liq savollarni yuzaga keltiradi.

Kiberxavfsizlikka kvant tahdidi global texnologiyalarni boshqarishga nafaqat davlatlar va hukumatlararo tashkilotlar, balki inklyuziv va ko‘p manfaatli tomonlarni ko‘proq jalb etish zarurligini ta’kidlaydi [36]. Kvant kompyuterlari yanada kuchliroq bo‘lib, foydalanish imloni kengaygani sari xususiy sektor, fuqarolik jamiyati hamda texnik hamjamiyatning mas’uliyatli kvant innovatsiyalari, ulardan foydalanish normalari va standartlarini shakllantirishdagi roli ortib boradi. Bu Jahon iqtisodiy forumining kvant hisoblash boshqaruvi tarmog‘i kabi davlat-xususiy sheriklikning yangi shakllarini, shuningdek, akademik doiralar va ochiq manbalar hamjamiyatini ko‘proq jalb etishdan iborat bo‘lishi mumkin [37].

Umuman olganda, kvant inqilobining geosiyosiy oqibatlari XXI asrda xalqaro xavfsizlik va barqarorlikka yanada yaxlit hamda integratsiyalashgan yondashuv zarurligiga e’tiborni qaratadi. Bu esa global tartibni shakllantirishda texnologiya, iqtisod, huquq va siyosatning murakkab o‘zaro ta’sirini tan olishga majbur qiladi. Kvant kiberxavfsizlik uchun samarali xalqaro huquqiy bazani ishlab chiqish nafaqat texnik yechimlarni, balki ushbu transformatsion texnologiya qo‘zg‘atadigan ijtimoiy, axloqiy va boshqaruv muammolarini chuqurroq tushunishni ham talab qiladi.

Tadqiqot natijalari tahlili

Ushbu fanlararo tahlil natijalari shuni ko‘rsatadiki, kiberxavfsizlikka kvant tahdidi murakkab, shoshilinch va global muammo bo‘lib, bir nechta sohalarda muvofiqlashtirilgan xalqaro javobni talab qiladi. Mavjud ochiq kalitli kriptografiya standartlarini buzishga qodir kvant kompyuterlarini ishlab chiqish savol emas, balki mutaxassislar bu muhim chegaraga keyingi o‘n yoki yigirma yillik ichida erishishi mumkinligi haqida ogohlantirmoqda. Ushbu kvant kripto-apokalipsisining potensial oqibatlari keng ko‘lamli ma’lumotlarning buzilishi va moliyaviy yo‘qotishlardan milliy xavfsizlik sirlarini buzish hamda raqamli tizimlarga jamoatchilik ishonchini yo‘qotishgacha bo‘lgan keng qamrovli muammolarga sabab bo‘lishi mumkin.

Ushbu tahdid tobora ortib borayotgani e’tirof etilishiga qaramay, mavjud huquqiy va me’yoriy bazalar kvant hisoblashlari bilan bog‘liq noyob muammolarni hal qilish uchun deyarli tayyor emas. Kiberxavfsizlik, ma’lumotlarni himoya qilish va intellektual mulk bilan bog‘liq ko‘plab qonunlar va siyosatlar kvantdan oldingi davrda ishlab chiqilgan bo‘lib, kvantni qo‘llab-quvvatlaydigan hujumlar xavfini yetarli darajada bartaraf etmaydi. Butun dunyo tizimlari kvantga tayyor bo‘lishi hamda ushbu tez rivojlanayotgan texnologiya ustidan samarali boshqaruv va nazoratni ta’minlashi uchun ularni yangilash zarur.

Kvant inqilobining geosiyosiy oqibatlari murakkab va ko‘p qirrali bo‘lib, kelgusi o‘n yilliklarda global kuchlar muvozanatini qayta shakllantirish imkoniyati bor. Mamlakatlar iqtisodiy, harbiy va razvedka maqsadlarida kvant texnologiyalarini ishlab chiqish, ishlatish uchun kimo‘zar o‘ynar ekan, yangi texnologik qurollanish poygasi hamda mavjud global tengsizliklarning kuchayishi xavfi haqida xavotirlar uyg‘onadi. Ushbu muammolarni hal qilish nafaqat xalqaro hamkorlik va hamjihatlikni kuchaytirishni, balki xususiy sektor, fuqarolik jamiyati hamda texnik hamjamiyatni jalb etadigan global texnologiya boshqaruviga yanada inklyuziv va ko‘p manfaatli yondashuvni talab qiladi.

Ushbu topilmalarga asoslanib, kvant tayyorligini oshirish va kvant bilan bog‘liq kibertahdidlar xavfini yumshatish uchun xalqaro huquqiy bazani ishlab chiqish bo‘yicha bir nechta siyosiy tavsiyalar taqdim etiladi:

– post-kvant kriptografiyasini rivojlantirish va standartlashtirishni jadallashtirish: hukumatlar va xalqaro standartlar organlari zaif ochiq kalit tizimlarini almashtirish uchun kvantga chidamli kriptografik algoritmlarni tadqiq qilish, sinovdan o‘tkazish va joylashtirishga ustuvor ahamiyat berishlari kerak. Bu ilmiy-tadqiqot va ishlanmalarga katta sarmoya kiritishni, shuningdek, o‘zaro hamkorlik va keng miqyosda qabul qilinishini ta’minlash uchun akademiya, sanoat hamda hukumat o‘rtasida muvofiqlashtirishni, hamkorlikni talab qiladi;

– kiberxavfsizlik va ma’lumotlarni himoya qilish bilan bog‘liq milliy va xalqaro qonunlar hamda qoidalarni mustahkamlash; siyosatchilar kvant hisoblashlari xavfini aniq ko‘rib chiqish uchun mavjud huquqiy bazalarni yangilashlari va ular kelajakda rivojlanayotgan tahdidlarga qarshi tura olishi isbotlanganligini ta’minlashlari kerak. Bunga moliya, sog‘liqni saqlash va milliy xavfsizlik kabi ayrim muhim sohalarda post-kvant kriptografiyasidan foydalanish majburiyati, shuningdek, kvant bilan bog‘liq hodisalar uchun aniq javobgarlik va jazo mexanizmlarini o‘rnatish kiradi;

– kvant texnologiyalari bo‘yicha xalqaro hamkorlik va muloqotni rag‘batlantirish. Davlatlar kibermakonda va fazodagi mavjud sa’y-harakatlarga o‘xshash kvant sohasidagi mas’uliyatli davlat xatti-harakati uchun normalar, qoidalar hamda tamoyillarni o‘rnatish uchun birgalikda ishlashi kerak. Bu yangi ko‘p tomonlama forumlarni yaratish yoki mavjudlarini kengaytirishni o‘z ichiga olishi mumkin, masalan, kvant muammolarini hal qilish uchun Birlashgan Millatlar Tashkilotining Xalqaro xavfsizlik kontekstida kibermakonda mas’uliyatli davlat xatti-harakatlarini rivojlantirish bo‘yicha hukumat ekspertlari guruhi tuzilishi kerak;

– ko‘p manfaatdor tomonlarning ishtiroki va hamkorligini rag‘batlantirish. Hukumatlar kvant texnologiyalarini boshqarishda yanada inklyuziv va ishtirokchi yondashuvlarni ishlab chiqish uchun xususiy sektor, fuqarolik jamiyati, akademik doiralar va texnik hamjamiyat bilan faol hamkorlik qilishi zarur. Bu kvant tadqiqotlari va ishlanmalari bo‘yicha davlat-xususiy sheriklikni qo‘llab-quvvatlash, ochiq manba va ochiq fan tashabbuslarini ilgari surish hamda kvant siyosati masalalari bo‘yicha taklif va yo‘l-yo‘riq ko‘rsatish uchun ko‘p manfaatli maslahat organlarini tashkil etishni o‘z ichiga olishi mumkin;

– kvant hisoblashning axloqiy va ijtimoiy oqibatlarini ko‘rib chiqish. Kvant texnologiyalari kuchliroq va keng tarqalgan bo‘lib, ularning jamiyatga kengroq ta’sirini, shu jumladan, shaxsiy hayot, tenglik va inson huquqlari masalalarini hisobga olish muhim bo‘ladi. Siyosatchilar kvant innovatsiyasining axloqiy va ijtimoiy jihatlari bo‘yicha tadqiqot va muloqotni qo‘llab-quvvatlashi hamda ushbu texnologiyalarning afzalliklari turli jamoalar va mintaqalarda adolatli va insofli taqsimlanishini ta’minlashga harakat qilishi kerak;

– kvant savodxonligi va ishchi kuchini rivojlantirishga sarmoya kiritish. Kvantga tayyorlik uchun mustahkam poydevor yaratish maqsadida mamlakatlar malakali kvant ishchi kuchini rivojlantirishi va kvant texnologiyalari haqida jamoatchilikda tushuncha hosil qilishni rag‘batlantirish uchun ta’lim va o‘qitish dasturlariga ustuvor ahamiyat berishlari kerak. Bunga kvant tushunchalarini maktab o‘quv dasturlariga integratsiya qilish, kvant axborot fanlari bo‘yicha oliy ta’lim markazlarini tashkil etish va kvant bilan bog‘liq sohalarda ishchilarning malakasini oshirish hamda qayta malakasini oshirish imkoniyatlarini taqdim etish kiradi.

Ushbu siyosiy tavsiyalarni amalga oshirish butun dunyo hukumatlari, sanoat, ilmiy doiralar va fuqarolik jamiyatidan barqaror harakat va yetakchilikni talab qiladi. Bundan tashqari, kvant landshafti o‘zgarishi, yangi muammolar va imkoniyatlar paydo bo‘lishi bilan moslashish hamda rivojlanishni talab etadi. Biroq kvant kiberxavfsizlik bo‘yicha

keng qamrovli xalqaro huquqiy bazani ishlab chiqish borasida faol qadam qo‘yish orqali xavflarni kamaytirishga va ushbu transformatsion texnologiyaning afzalliklarini yuzaga chiqarishga yordam berishimiz mumkin. Bu butun insoniyat farovonligi uchun ham zarurdir.

Xulosalar

Xulosa qilib aytadigan bo‘lsak, kiberxavfsizlikka kvant tahdidi xalqaro hamjamiyatdan shoshilinch e’tibor va choralar ko‘rishni talab qiladigan aniq va mavjud xavfdir. Kvant kompyuterlari bilan bog‘liq halokatli oqibatlarning oldini olish, muammoni hal qilish uchun barcha sohalarni qamrab oluvchi va keng doiradagi manfaatdor tomonlarni jalb qiluvchi muvofiqlashtirilgan va ko‘p qirrali yondashuvlar zarur.

Ushbu mavjud tahdidga mustahkam xalqaro huquqiy bazani yaratishda birgalikda ishlash orqali yordam bera olamiz. Bu oson ish bo‘lmaydi, lekin kvant texnologiyalarining to‘liq imkoniyatlaridan foydalanmoqchi bo‘lsak, ularning xavf va qiyinchiliklarini yumshatish zaruratini ham tan olishimiz kerak. Daromadlar katta, lekin imkoniyatlar ham katta. Demak, hamma uchun xavfsizroq, adolatli hamda farovon dunyoni birgalikdagi sa’y-harakatlar va hamkorlik bilan qurishimiz mumkin.

REFERENCES

1. Bernstein D.J., Heninger N., Lou P., Valenta L. Post-quantum cryptography. *Nature*, 2017, vol. 549 (7671), pp. 188–194. DOI: 10.1038/nature23461

2. National Academies of Sciences, Engineering, and Medicine. Quantum computing: Progress and prospects. The National Academies Press, 2019. DOI: 10.17226/25196

3. Mohseni M., Read P., Neven H., Boixo S., Denchev V., Babbush R., Fowler A., Smelyanskiy V., Martinis J. Commercialize quantum technologies in five years. *Nature*, 2017, vol. 543 (7644), pp. 171–174. DOI: 10.1038/543171a

4. Herman M., Horowitz M., Shukla S., Stanton B., Wright G. How will the advent of quantum computing affect the cyber security landscape? *Georgetown Journal of International Affair*s, 2017, vol. 18 (3), pp. 118–127. Available at: https://www.jstor.org/stable/26395934

5. Shor P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Review*, 1999, vol. 41 (2), pp. 303–332. DOI: 10.1137/S0036144598347011

6. Buchanan B. The cybersecurity dilemma: Hacking, trust, and fear between nations. Oxford University Press, 2017.

7. Vermeer M., Peet E.D. Securing communications in the quantum computing age: Managing the risks to encryption. No. RR-3102-RC. RAND Corporation, 2021. DOI: 7249/RR3102

9. Arute F., Arya K., Babbush R., Bacon D., Bardin J.C., Barends R., Biswas R., Boixo S., Brandao F.G., Buell D.A., Burkett B., Chen Y., Chen Z., Chiaro B., Collins R., Courtney W., Dunsworth A., Farhi E., Foxen B., Martinis J.M. Quantum supremacy using a programmable superconducting processor. *Nature*, 2019, vol. 574 (7779), pp. 505–510. DOI: 10.1038/s41586-019-1666-5

10. IBM. IBM unveils breakthrough 127-qubit quantum processor. 2021. Available at: https://newsroom.ibm.com/2021-11-16-IBM-Unveils-Breakthrough-127-Qubit-Quantum-Processor

12. NIST. Post-quantum cryptography: Round 3 submissions. 2020. Available at: https://csrc.nist.gov/Projects/post-quantum-cryptography/round-3-submissions

13. Cloud Security Alliance. Quantum-safe security: Preparing for the post-quantum world. 2019. Available at: https://cloudsecurityalliance.org/artifacts/quantum-safe-security-preparing-for-the-post-quantum-world/

14. Dyakonov M. When will useful quantum computers be constructed? Not in the foreseeable future, this physicist argues. Here's why: The case against: Quantum computing. *IEEE Spectrum*, 2018, vol. 5 (3), pp. 24–29. DOI: 10.1109/MSPEC.2018.8278134

16. White J., Saunders D.L., Dreibelbis J. The economic impact of cybercrime: No slowing down. No. PE-614.1. RAND Corporation, 2019. Available at: https://www.rand.org/pubs/external_publications/PE614-1.html

17. Lewis J.A. Cryptography after the quantum revolution. Eds. L. Gyongyosi, S. Imre. IntechOpen. *Advanced quantum technologies*, 2020, pp. 35–47. DOI: 10.5772/intechopen.90471

20. Kemp J., Vedral V., Stevens T. Quantum technologies in international relations. *Journal of International Relations and Development*, 2021, no. 24, pp. 671–680. DOI: 10.1057/s41268-021-00229-9

22. European Parliament and Council. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. General Data Protection Regulation. *Official Journal of the European Union*, 2016, L119, pp. 1–88. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

23. Council of Europe. Convention on Cybercrime. *European Treaty Series*, 2001, no. 185. Available at: https://rm.coe.int/1680081561

24. U.S. Congress. National Quantum Initiative Act. Public Law No: 115-368. 2018, 21 December. Available at: https://www.congress.gov/bill/115th-congress/house-bill/6227

25. Standing Committee of the National People's Congress. Cryptography Law of the People's Republic of China. 2019. Available at: http://www.npc.gov.cn/npc/c30834/201910/6f7be7dd5ae5459a8de8baf36296bc74.shtml

26. Government of Japan. *Cybersecurity strategy*, 2021. Available at: https://www.nisc.go.jp/eng/pdf/cs-senryaku2021-en.pdf

27. Kania E.B. China's quantum future. Foreign Affairs, 2018. Available at: https://www.foreignaffairs.com/articles/china/2018-09-26/chinas-quantum-future

28. Harrell P., Malkin E., Hoffman S. China's efforts in quantum information science: Drivers, milestones, and strategic implications. No. IDA Document D-10709. Institute for Defense Analyses. 2018.

29. Monteleone C., Puccio L., Madiega T., Szczepanski M. European Parliament Briefing: Quantum technologies: What are they about and why are they important? 2021. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/696188/EPRS_BRI(2021)696188_EN.pdf

30. United Nations Institute for Disarmament Research. The impact of quantum technologies on the future of cybersecurity. 2019. Available at: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/UNIDIR-Impact-QT-CyberSecurity.pdf

31. Fischer S. Quantum technology and nuclear stability: A critical assessment. Bulletin of the Atomic Scientists, 2019, vol. 75 (5), pp. 214–219. DOI: 10.1080/00963402.2019.1654272

32. Loft P., Bellis K., Butcher S. Quantum technologies. UK Parliamentary Office of Science and Technology. 2021. Available at: https://researchbriefings.files.parliament.uk/documents/POST-PN-0552/POST-PN-0552.pdf

33. Federal Department of Foreign Affairs. Switzerland's foreign policy strategy 2020–2023: Digital foreign policy strategy 2021–2024. Available at: https://www.eda.admin.ch/dam/eda/en/documents/publications/SchweizerischeAussenpolitik/Digistrat-2024_EN.pdf

34. European Commission. Quantum Flagship, 2021. Available at: https://qt.eu/

35. Lee H.M., Becket R., Bromley T.R., Howe P.D., Vieu C. Global governance of quantum technologies: Opportunities and challenges. Eds. R. Vohra, C. Wulf, M. Eichhammer. *Quantum technology and optimization problems*, Springer International Publishing, 2020, pp. 1–12. DOI: 10.1007/978-3-030-42019-9_1

36. Reddy S., Sharma R., Ballakur A. Multistakeholder approaches to governing quantum technologies. Ed. N. Datta. *Disruptive quantum technologies*, Springer Singapore, 2021, pp. 57–88. DOI: 10.1007/978-981-16-3138-6_3

37. World Economic Forum. Quantum Computing Governance Network. 2021. Available at: https://www.weforum.org/platforms/shaping-the-future-of-digital-economy-and-new-value-creation/quantum-computing-governance-principles

YURISPRUDENSIYA

HUQUQIY ILMIY-AMALIY JURNALI

2024-YIL 2-SON

VOLUME 4 / ISSUE 2 / 2024

DOI: 10.51788/tsul.jurisprudence.4.2.

Texnik muharrirlar: U. Sapayev, D. Rajapov
Tahririyat manzili:
100047. Toshkent shahar, Sayilgoh ko‘chasi, 35.
Tel.: (0371) 233-66-36, 233-41-09.
Faks: (0371) 233-37-48.

Veb-sayt: www.tsul.uz
E-mail: lawjournal@tsul.uz
Obuna indeksi: 1387.

Jurnal 23.04.2024-yilda tipografiyaga topshirildi.
Qog‘oz bichimi: A4. Shartli bosma tabog‘i 13,5.
Adadi: 100. Buyurtma raqami: 50.
TDYU tipografiyasida chop etildi.