International Journal of Science and Technology

International Journal of Science and Technology, 2026, 3–8

doi: 10.70728/tech.v3.i01.001
Volume 03, Issue 01
ISSN: 3030-3443
Paper

PAPER

KIBER MAKONDA HUQUQNI MUHOFAZA QILISH: MUAMMO VA YECHIMLAR

Turdimatov Mamirjon Mirzayevich[1,*] and Sobirov Sherzodbek Sohibjon o'g'li[2]

[1]Farg'ona davlat texnika universiteti, "Dasturiy injiniring va kiberxavfsizlik" kafedrasi dotsenti, t.f.n.
[2]"Axborot xavfsizligi" yo'nalishi 1-bosqich magistranti

* turdimatovmamir1958@gmail.com, sherzodbeksobirov470@gmail.com

Abstract

Ushbu ilmiy maqolada kiber makonda huquqni muhofaza qilish tizimining dolzarb muammolari va ularni bartaraf etish yo'llari kompleks tarzda tahlil qilingan. So'nggi o'n yillikda raqamli texnologiyalarning jadal rivojlanishi natijasida kiberjinoyatlar soni va murakkabligi sezilarli darajada oshdi. Internet, bulutli hisoblash, sun'iy intellekt va IoT texnologiyalarining keng qo'llanilishi jinoyatchilikning virtual muhitga ko'chishiga sabab bo'ldi.. Tadqiqot jarayonida normativ-huquqiy hujjatlar, xalqaro konvensiyalar, ilmiy adabiyotlar va xorijiy tajribalar tahlil qilindi. Natijalar shuni ko'rsatadiki, kiber makonda huquqni muhofaza qilish samaradorligini oshirish uchun qonunchilikni modernizatsiya qilish, raqamli kriminalistika imkoniyatlarini kengaytirish, kadrlar salohiyatini mustahkamlash va xalqaro hamkorlikni rivojlantirish zarur. Mazkur maqola magistratura darajasidagi ilmiy tadqiqotlar uchun nazariy va amaliy ahamiyatga ega.

Key words: kiber makon, huquqni muhofaza qilish, kiberjinoyat, raqamli kriminalistika, kiberxavfsizlik, xalqaro hamkorlik.

Introduction

So'nggi o'n yillikda raqamli texnologiyalarning jadal rivojlanishi natijasida kiber makon jamiyat hayotining ajralmas qismiga aylandi. Internet, mobil aloqa, bulutli hisoblash texnologiyalari, sun'iy intellekt va IoT1 qurilmalarining keng joriy etilishi ijtimoiy-iqtisodiy jarayonlarni soddalashtirish va tezlashtirishga xizmat qilmoqda. Shu bilan birga, ushbu jarayonlar xavfsizlik masalalarini yangi bosqichga olib chiqdi[9]. Endilikda jinoyatchilik faqat jismoniy makon bilan cheklanib qolmay, virtual muhitda ham faol namoyon bo'lmoqda [13].

Kiberjinoyatlar shaxsiy ma'lumotlarni noqonuniy qo'lga kiritish, moliyaviy firibgarlik[1], intellektual mulk huquqlarini buzish[2], davlat

Compiled on: January 16, 2026.

va muhim infratuzilmalarga qarshi hujumlar ko‘rinishida namoyon bo‘ladi[10]. Bunday jinoyatlar yuqori darajadagi anonimlik, tezkorlik va transchegaraviylik xususiyatiga ega[3] bo‘lgani sababli ularni aniqlash va isbotlash an’anaviy huquqni muhofaza qilish mexanizmlari uchun mur akkab vazifaga aylanmoqda[9]. Huquqni muhofaza qiluvchi organlar tarixan jinoyatchilikka qarshi kurashda jismoniy dalillar, guvohlarning ko‘rsatmalari va hududiy yurisdiksiya doirasida faoliyat yuritib kelgan. Kiber makonda esa jinoyat sodir etilgan joyni aniqlash, jinoyatchining shaxsini tasdiqlash va raqamli dalillarni saqlab qolish masalalari murakkab tus oladi. Bundan tashqari, texnologik rivojlanish sur’atlari huquqiy tartibga solish mexanizmlaridan tezroq kechmoqda, bu esa normativ-huquqiy bo‘shliqlarni yuzaga keltiradi. Mazkur ilmiy maqolaning asosiy maqsadi — kiber makonda huquqni muhofaza qilish tizimida mavjud muammolarni tizimli ravishda aniqlash, ularning huquqiy, tashkiliy va texnik jihatlarini tahlil qilish hamda zamonaviy raqamli kriminalistika, institutsional islohotlar va xalqaro hamkorlik asosida samarali yechimlar ishlab chiqishdan iborat.

Kiber makonda huquqni muhofaza qilish masalalari so‘nggi o‘n yillikda ko‘plab xorijiy va mahalliy olimlar tomonidan faol o‘rganib kelinmoqda[1][2][9]. Ushbu yo‘nalishdagi tadqiqotlar, asosan, kiberjinoyatchilikning kriminologik xususiyatlari, huquqiy tartibga solish mexanizmlari, raqamli kriminalistika va xalqaro hamkorlik masalalariga qaratilgan.

Masalan, M. Goodman va T. Holt tadqiqotlarida kiberjinoyatchilikning transmilliy xarakteri va uning an’anaviy jinoyatchilikdan farqli jihatlari chuqur tahlil qilinadi. Ularning fikricha, kiberjinoyatlar hududiy chegaralarni inkor etgani sababli, davlatlarning alohida harakatlari yetarli bo‘lmay, xalqaro hamkorlik muhim ahamiyat kasb etadi. Shu bilan birga, R. Brenner kiberjinoyatlar uchun javobgarlik masalasida huquqiy aniqlik va yagona terminologiyaning yetishmasligi muammosiga alohida e’tibor qaratadi. Axborot huquqi sohasidagi tadqiqotlarda esa kiber makonda shaxsiy hayot daxlsizligi va xavfsizlik o‘rtasidagi muvozanat masalasi muhim o‘rin tutadi.

L. Lessig va D. Solove ishlarida raqamli muhitda huquqni muhofaza qilish jarayonida inson huquqlari va erkinliklarini cheklash xavfi mavjudligi ta’kidlanadi. Mualliflar davlat aralashuvi qonuniy, proporsional va shaffof bo‘lishi zarurligini asoslab beradi.

Xalqaro hamkorlikning asosiy shakllari qatoriga axborot almashinuvi, qo‘shma tergov guruhlari, ekstraditsiya2 va huquqiy yordam mexanizmlari kiradi. Biroq, davlatlar o‘rtasidagi huquqiy tizimlar va siyosiy manfaatlardagi farqlar bu jarayonlarni murakkablashtiradi.

Shu jumladan, mintaqaviy va global darajadagi hamkorlik platformalarini rivojlantirish, yagona standartlar va protseduralarni joriy etish kiberjinoyatlarga qarshi kurashda muhim ahamiyat kasb etadi.

MDH va Markaziy Osiyo olimlari tadqiqotlarida esa kiber makonda huquqni muhofaza qilishning institutsional jihatlari, xususan, maxsus bo‘linmalar tashkil etish va kadrlar tayyorlash muammolari ko‘tariladi. Ushbu ishlar milliy huquq tizimlarining rivojlanayotgan texnologiyalarga moslashish zaruratini ko‘rsatib beradi.

Kiberjinoyatlar ko‘pincha bir nechta davlat hududida sodir etiladi yoki ularning oqibatlari transmilliy xarakterga ega bo‘ladi. Shu sababli, kiber makonda huquqni muhofaza qilish xalqaro hamkorliksiz samarali bo‘lishi mumkin emas.

Methods

Mazkur tadqiqot kompleks metodologik yondashuv asosida olib borildi. Tadqiqotda sifat va miqdoriy tahlil usullari uyg‘unlashtirildi, bu esa kiber makonda huquqni muhofaza qilish muammolarini ko‘p qirrali tarzda o‘rganish imkonini berdi.

Birinchi bosqichda normativ-huquqiy tahlil amalga oshirildi. Unda kiberjinoyatlarga oid milliy qonunchilik, xalqaro konvensiyalar va mintaqaviy hujjat lar solishtirma usulda o‘rganildi. Bu orqali mavjud huquqiy mexanizmlarning kuchli va zaif tomonlari aniqlanib, ularni takomillashtirish zarurati asoslandi. Bunda esa, aynan kiber makonda huquqni muhofaza qilishning samaradorligi, avvalo, mustahkam va moslashuvchan huquqiy asoslarning mavjudligiga bog‘liq. Zamonaviy sharoitda kiberjinoyatlar tezkor rivojlanib borayotgan texnologiyalar bilan uzviy bog‘liq bo‘lgani sababli, an’anaviy jinoyat huquqi normalari ko‘pincha yetarli bo‘lmay qolmoqda. Shu bois, ko‘plab davlatlar kiberjinoyatlarga

qarshi kurashish maqsadida maxsus qonunlar, kodekslarga qo'shimchalar va normativ-huquqiy hujjatlarni ishlab chiqmoqda.

Kiberjinoyat tushunchasining huquqiy talqini turli mamlakatlarda farqlanadi. Ayrim davlatlarda kiberjinoyat mustaqil jinoyat turi sifatida e'tirof etilsa, boshqalarda u an'anaviy jinoyatlarning virtual shakli sifatida qaraladi. Ushbu farqlilik esa xalqaro hamkorlik jarayonlarida muayyan muammolarni yuzaga keltiradi. Chunki jinoyat tarkibini turlicha talqin qilish ekstraditsiya, tergov va sud jarayonlarini murakkablashtiradi. Shu jumladan, Budapesht konvensiyasi (Kiberjinoyatlar to'g'risidagi konvensiya) kiber makonda huquqni muhofaza qilishning muhim xalqaro huquqiy asosi hisoblanadi. Ushbu hujjat kiberjinoyatlarni tasniflash, protsessual vakolatlarni belgilash va davlatlar o'rtasida hamkorlikni kuchaytirishga qaratilgan. Biroq, barcha davlatlar ushbu konvensiyaga qo'shilmaganligi sababli, global miqyosda yagona huquqiy makon hali to'liq shakllanmagan. Milliy darajada esa kiber makonda huquqni muhofaza qilish qonunchilikni doimiy ravishda modernizatsiya qilishni talab etadi. Axborot xavfsizligi, shaxsiy ma'lumotlarni himoya qilish, elektron tijorat va raqamli dalillar bilan ishlashga oid normalar bir-biri bilan uzviy bog'liq holda rivojlanishi zarur. Aks holda, huquqiy bo'shliqlar kiberjinoyatchilar tomonidan faol foydalaniladi.

Ikkinchi bosqichda ilmiy adabiyotlar tahlili o'tkazildi. Kiberxavfsizlik, raqamli kriminalistika, axborot huquqi va kriminologiya sohasidagi zamonaviy ilmiy ishlar o'rganilib, asosiy nazariy yondashuvlar umumlashtirildi. Ushbu bosqich tadqiqotning konseptual asoslarini shakllantirishga xizmat qildi. Raqamli kriminalistika kiber makonda huquqni muhofaza qilishning markaziy elementlaridan biri hisoblanadi. U raqamli dalillarni aniqlash[13], yig'ish, saqlash, tahlil qilish[3]va sudda isbot sifatida taqdim etish jarayonlarini o'z ichiga oladi[14]. Zamonaviy kiberjinoyatlar murakkab texnik mexanizmlarga asoslangan bo'lgani sababli, raqamli kriminalistika vositalarisiz samarali tergov olib borish deyarli imkonsizdir.

Raqamli dalillar o'ziga xos xususiyatlarga ega: ular oson o'chirilishi, o'zgartirilishi yoki shifrlanishi mumkin. Shu bois, dalillarni yig'ish jarayonida ularning yaxlitligini (integrity) saqlash muhim ahamiyatga ega. Xalqaro amaliyotda bu borada "chain of custody"tamoyili keng qo'llaniladi, ya'ni dalilning qayerdan, qachon va kim tomonidan olingani aniq hujjatlashtiriladi.

Texnik jihatdan raqamli kriminalistika bir nechta yo'nalishlarni qamrab oladi: disk forensikasi, tarmoq forensikasi, xotira (RAM) tahlili, mobil qurilmalar forensikasi va bulutli muhit forensikasi. Har bir yo'nalish o'ziga xos bilim va vositalarni talab etadi. Masalan, tarmoq forensikasi kiberhujumlarning manbasini aniqlashda muhim bo'lsa, mobil qurilmalar forensikasi shaxsiy ma'lumotlar bilan bog'liq jinoyatlarni fosh etishda keng qo'llaniladi.

Shu qatorda, sun'iy intellekt va mashinaviy o'rganish texnologiyalarining rivojlanishi raqamli kriminalistika sohasiga ham kirib kelmoqda. Katta hajmdagi log-fayllarni avtomatik tahlil qilish, anomaliyalarni aniqlash va kiberhujumlarni prognozlash ushbu texnologiyalar yordamida yanada samarali amalga oshirilmoqda.

Uchinchi bosqichda texnik tahlil qo'llanildi. Raqamli dalillarni yig'ish, saqlash va tahlil qilishda foydalaniladigan raqamli kriminalistika vositalari va metodlari (log-fayllar tahlili, tarmoq trafikini monitoring qilish, disk forensikasi va xotira tahlili) o'rganildi. Bu jarayon huquqni muhofaza qilish organlarining amaliy faoliyatida texnik imkoniyatlarning ahamiyatini baholashga yordam berdi. Kiber makonda huquqni muhofaza qilishning samaradorligi nafaqat huquqiy va texnik omillarga, balki institutsional va inson kapitaliga ham bevosita bog'liq. Huquqni muhofaza qiluvchi organlar tarkibida kiberjinoyatlarga ixtisoslashgan bo'linmalar tashkil etilishi zamonaviy davr talabi hisoblanadi.

Biroq, amaliyot shuni ko'rsatadiki, ko'plab davlatlarda kiberxavfsizlik bo'yicha yetarli malakaga ega mutaxassislar yetishmaydi. Bu holat, avvalo, ta'lim tizimida raqamli kriminalistika va kiberhuquq yo'nalishlarining yetarli darajada rivojlanmaganligi bilan izohlanadi. Shu sababli, oliy ta'lim muassasalarida ushbu yo'nalishlar bo'yicha maxsus magistratura va doktorantura dasturlarini joriy etish muhim ahamiyatga ega.

Shuningdek, huquqni muhofaza qiluvchi organlar xodimlari uchun doimiy malaka oshirish va qayta tayyorlash tizimini yo'lga qo'yish zarur.

Chunki texnologiyalar tez o‘zgarib borar ekan, bir marta olingan bilimlar qisqa muddat ichida eskirishi mumkin.

To‘rtinchi bosqichda tizimli va institutsional yondashuv asosida huquqni muhofaza qilish organlari, texnologik infratuzilma va jamiyat o‘rtasidagi o‘zaro aloqalar tahlil qilindi. Ushbu yondashuv kiber makonda xavfsizlikni ta’minlash faqat davlat organlarining vazifasi emas, balki xususiy sektor va fuqarolik jamiyati bilan hamkorlikni talab etishini ko‘rsatdi.

Results and Discussions

Tadqiqot natijalari kiber makonda huquqni muhofaza qilish tizimida bir qator muhim muammolar mavjudligini aniqladi[9].

Avvalo, huquqiy bazaning texnologik rivojlanish sur’atlariga moslashishida kechikishlar kuzatilmoqda[11]. Bu holat yangi turdagi kiberjinoyatlarni huquqiy jihatdan to‘g‘ri kvalifikatsiya qilishda qiyinchiliklar yaratadi[12].

Ikkinchidan, huquqni muhofaza qiluvchi organlarda raqamli kriminalistika sohasida yuqori malakali kadrlar yetishmasligi muhim muammo sifatida namoyon bo‘ldi. Kiberjinoyatlar murakkab texnik bilimlarni talab qilgani sababli, an’anaviy tergov usullari ko‘plab holatlarda samarasiz bo‘lib qolmoqda. Natijada jinoyatlarni fosh etish darajasi pasayib, jinoyatchilar uchun jazosizlik muhiti yuzaga keladi.

Uchinchidan, texnik infratuzilmaning yetarli darajada rivojlanmaganligi raqamli dalillarni tezkor va ishonchli tahlil qilishga to‘sqinlik qilmoqda[5]. Xususan, shifrlangan ma’lumotlar[6], bulutli muhitda saqlanayotgan axborotlar va IoT qurilmalaridan olinadigan dalillar bilan ishlashda amaliy muammolar mavjud[15].

Shu bilan birga, tadqiqot ijobiy tendensiyalarni ham aniqladi. Xalqaro hamkorlikning kuchayishi, kiberxavfsizlik bo‘yicha maxsus bo‘linmalar tashkil etilishi va raqamli kriminalistika standartlarining joriy etilishi kiberjinoyatlarga qarshi kurash samaradorligini oshirmoqda. Olingan natijalar shuni ko‘rsatadiki, kiber makonda huquqni muhofaza qilish masalasi kompleks va ko‘p qatlamli yondashuvni talab qiladi. Muammolarni faqat texnik vositalar yordamida hal etish yetarli emas; huquqiy islohotlar, institutsional salohiyatni oshirish va xalqaro hamkorlikni mustahkamlash zarur.

Birinchidan, kiberjinoyatlarga oid qonunchilikni muntazam yangilab borish va uni xalqaro standartlarga moslashtirish lozim.

Ikkinchidan, huquqni muhofaza qiluvchi organlar xodimlarini raqamli kriminalistika va kiberxavfsizlik bo‘yicha doimiy qayta tayyorlash muhim ahamiyatga ega.

Uchinchidan, zamonaviy texnik infratuzilma va laboratoriyalar tashkil etish kiberjinoyatlarni fosh etishda hal qiluvchi rol o‘ynaydi. Kiber makonda huquqni muhofaza qilishning amaliy jihatlarini yoritishda milliy va xorijiy tajribani solishtirma tahlil qilish muhim ahamiyatga ega[11]. O‘zbekiston Respublikasida so‘nggi yillarda axborot xavfsizligini ta’minlash va kiberjinoyatlarga qarshi kurashish borasida qator islohotlar amalga oshirilmoqda[16].

Xususan, axborotlashtirish va kiberxavfsizlik sohasidagi normativ-huquqiy hujjatlar takomillashtirildi, huquqni muhofaza qiluvchi organlar tarkibida axborot texnologiyalari bilan bog‘liq jinoyatlarga ixtisoslashgan bo‘linmalar faoliyati yo‘lga qo‘yildi. Bu esa kiberjinoyatlarni aniqlash va tergov qilish samaradorligini oshirishga xizmat qilmoqda.

Shu bilan birga, rivojlangan davlatlar tajribasi bilan solishtirganda, ayrim muammolar saqlanib qolmoqda. Masalan, AQSh va Yevropa Ittifoqi mamlakatlarida raqamli kriminalistika laboratoriyalari zamonaviy texnik vositalar bilan to‘liq jihozlangan bo‘lib, sun’iy intellekt asosidagi tahlil tizimlari keng qo‘llaniladi. Bundan tashqari, ushbu davlatlarda xususiy sektor bilan hamkorlik mexanizmlari yuqori darajada rivojlangan.

O‘zbekiston sharoitida esa kadrlar salohiyatini oshirish, texnik infratuzilmani modernizatsiya qilish va xalqaro axborot almashinuvi mexanizmlarini kengaytirish dolzarb vazifa bo‘lib qolmoqda. Shu nuqtayi nazardan, xorijiy tajribani to‘g‘ridan-to‘g‘ri ko‘chirish emas, balki uni milliy huquqiy va institutsional sharoitlarga moslashtirish muhim ahamiyat kasb etadi.

Conclusion

Tadqiqot natijalari kiberjinoyatchilikning murakkab va tez o‘zgaruvchan xususiyatga ega ekanligini, unga qarshi kurashishda an’anaviy yondashuvlar yetarli emasligini ko‘rsatdi.

Xulosa sifatida, kiber makonda huquqni

muhofaza qilish samaradorligini oshirish quyidagi omillarga bog'liq: zamonaviy va moslashuvchan qonunchilik bazasini shakllantirish, raqamli kriminalistika imkoniyatlarini kengaytirish, yuqori malakali kadrlar tayyorlash va xalqaro hamkorlikni mustahkamlash.

Ushbu yo'nalishlarda amalga oshiriladigan tizimli chora-tadbirlar kiber makonda xavfsizlikni ta'minlash, fuqarolar va davlat manfaatlarini himoya qilishda muhim ahamiyat kasb etadi. Mazkur maqola magistrlik dissertatsiyasi va ilmiy jurnallar uchun nazariy hamda amaliy ahamiyatga ega bo'lgan tadqiqot sifatida xizmat qilishi mumkin.

Adabiyotlar

1. Narasimhan, P., & Kala, N. (2025). Emerging trends in digital forensics: Investigating cybercrime. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 11(1), 3645–3652. https://ijsrcseit.com/index.php
2. James, J. W. (2024). Integrating data mining techniques in computer forensics for enhanced cybercrime investigation and incident response. International Journal of Intelligent Systems and Applications in Engineering, 12(4), 4117–4125. https://ijisae.org/index.php/IJISAE/article/view/7007
3. Mohanan, S. C. V. (2020). Digital forensic in cyber security. International Journal of Engineering Research & Technology, 8(4). https://www.ijert.org/digital-forensic-in-cyber-security
4. Uppalapu, V. K., & Agarwal, A. (2024). Digital forensics investigation framework based on the blockchain, IoT, and social networks. International Journal of Intelligent Systems and Applications in Engineering, 12(21s), 1179–1182. https://ijisae.org/index.php/IJISAE/article/view
5. Malik, A. W., Bhatti, D. S., Park, T.-J., Ishtiaq, H. U., Ryou, J.-C., & Kim, K.-I. (2024). Cloud digital forensics: Beyond tools, techniques, and challenges. Sensors, 24(2), 433. https://doi.org/10.3390/s24020433
6. Fairbanks, J., Arifin, M. M., Afreen, S., & Curtis, A. (2024). Survey and analysis of IoT operating systems: A comparative study on the effectiveness and acquisition time of open source digital forensics tools. arXiv. https://arxiv.org/abs/2407.01474
7. Hassan, M. A., Samara, G., & Abu Fadda, M. (2022). IoT forensic frameworks (DFIF, IoTDOTS, FSAIoT): A comprehensive study. arXiv. https://arxiv.org/abs/2203.15705
8. Tok, Y. C., Wang, C., & Chattopadhyay, S. (2020). STITCHER: Correlating digital forensic evidence on Internet-of-Things devices. arXiv. https://arxiv.org/abs/2003.07242
9. Khan, A. A., & Laghari, A. A. (2021). Digital forensics and cyber forensics investigation: Security challenges, limitations, open issues and future direction. International Journal of Electronic Security and Digital Forensics. https://www.researchgate.net/publication/355183549
10. FORSEC Journal. (2025). Cloud and IoT forensics for strengthening cybercrime investigation: Acquisition challenges and analytical frameworks. https://journal.ekantara.com/forsec/article/view/2
11. New Century Innovations Journal. (2024). Problems of cybercrime investigation in Uzbekistan. 17(3), 81–90. https://newjournal.org/new/article/view/1036
12. E Conference Zone. (2024). Digital cybercrime investigation: Methods, tools and technologies. https://econferencezone.org/index.php
13. IJSRED. (2025). Digital forensics: Trends and challenges. International Journal of Scientific Research and Engineering Development, 7(3). https://ijsred.com/volume7/issue3/IJSRED-V7I3P225.pdf
14. JISEM. (2024). Digital forensics and evidence recovery in modern cybersecurity. Journal of Information Systems Engineering and Management, 10(43s). https://jisem-journal.com
15. Forensic Science International: Digital Investigation. (2024). Comparative study of IoT forensic frameworks. 49, 301748. https://doi.org/10.1016/j.fsidi.2024.301748

16. Turdimatov M.M., Sobirov, S. Kiberfizik tizimlarda energiya boshqaruvi va xavfsizlik tahdidlariga qarshi innovatsion yechimlar. Research and Implementation, 3(10), 598–602. https://rai-journal.uz