

KIBERMAKONDA XAVFSIZ MUHITNI TA'MINLASH: DAVLATLAR TAJRIBASI

ISBN 978-9910-618-10-9



9 789910 618109

MONOGRAFIYA

**O'ZBEKISTON RESPUBLIKASI
MAKTABGACHA VA MAKTAB TA'LIMI VAZIRLIGI
CHIRCHIQ DAVLAT PEDAGOGIKA UNIVERSITETI**

BERKINOV OYBEK TOXIR O'G'LI

**KIBERMAKONDA XAVFSIZ
MUHITNI TA'MINLASH:
DAVLATLAR TAJRIBASI**

Monografiya

**«ZEBO PRINTS»
Toshkent – 2025**

UO'K 004.056;004.86

KBK 32.816;87.60

B-57

Berkinov O.T.

Kibermakonda xavfsiz muhitni ta'minlash: davlatlar tajribasi
/ Monografiya. - T.: «ZEBO PRINTS», 2025. – 184 bet.

Ushbu monografiya kibermakon xavfsizligini ta'minlashning nazariy, huquqiy va amaliy jihatlarini o'rganishga bag'ishlangan. Asarda kibermakon tushunchasining falsafiy-huquqiy talqini, sun'iy intellekt va raqamli texnologiyalar bilan bog'liq yangi xavf-xatarlar, inson huquqlari va axborot etikasi masalalari tahlil qilingan.

AQSh, Yevropa Ittifoqi, Rossiya, Xitoy, Yaponiya va Koreya kabi davlatlarning tajribasi qiyosiy o'rganilib, Markaziy Osiyo mamlakatlari va O'zbekiston sharoitida kibermakon xavfsizligini ta'minlashning huquqiy asoslari hamda milliy strategiyalari ko'rib chiqilgan. Shuningdek, BMT, NATO va SHHT kabi xalqaro tashkilotlarning kibermakon xavfsizligidagi roli ham yoritilgan.

Monografiyada kiberxavfsizlik faqat texnik masala emas, balki ijtimoiy-falsafiy hodisa sifatida baholanib, ta'lim, ilmiy tadqiqotlar va fuqarolik jamiyati ishtirokining dolzarbligi asoslangan. Tadqiqot natijalari O'zbekiston uchun milliy manfaatlarni xalqaro tamoyillar bilan uyg'unlashtirishda nazariy va amaliy ahamiyatga ega.

Monografiya faylasuf olimlar, tadqiqotchilar va oliy ta'lim muassasalari Gumanitar fanlar fakultetlari talabalari uchun mo'ljallangan. Ushbu monografiya ChDPU Gumanitar fanlar fakulteti Milliy g'oya, ma'naviyat asoslari va huquq ta'limi kafedrasida tayyorlangan.

Taqrizchilar:

Gulchehra GAFFAROVA – falsafa fanlari doktori, professor

Ilyos SIDDIQOV – falsafa fanlari doktori, professor

Monografiya Chirchiq davlat pedagogika universiteti Ilmiy texnik kengashi tomonidan nashrga tavsiya etilgan (... son bayonnoma, 2025 yil ...

ISBN 978-9910-618-10-9

KIRISH

XXI asr taraqqiyoti insoniyat oldiga mutlaqo yangi voqelikni – kibermakonni taqdim etdi. Bu tushuncha dastlab fantastik adabiyotlarda metafora sifatida paydo bo'lgan bo'lsa-da, bugungi kunda siyosat, iqtisodiyot, huquq, falsafa va ijtimoiy munosabatlarning markaziga aylandi. Kibermakon – bu faqat texnologik infratuzilma emas, balki inson faoliyatining barcha sohalarini qamrab oluvchi yangi ijtimoiy-madaniy muhitdir. Shu sababli unda xavfsiz muhitni ta'minlash masalasi dolzarb bo'lib, har bir davlat, mintaqa va butun insoniyat uchun strategik vazifaga aylandi.

Bugungi davrning o'ziga xosligi shundaki, kibermakonning transmilliy tabiati mavjud xavf-xatarlarni yanada kuchaytirib yubordi. Bir davlat hududida sodir bo'lgan kiberhujum boshqa mamlakatlarning iqtisodiy va siyosiy hayotiga bevosita zarar yetkazmoqda. Masalan, 2017-yilda sodir bo'lgan "WannaCry" virusi 150 dan ortiq davlatlarda millionlab kompyuterlarga zarar yetkazdi va bu voqea kiberxavfsizlik masalasini xalqaro siyosatning eng muhim kun tartibiga olib chiqdi¹. Shunday global xatarlar insoniyatni kibermakon xavfsizligini davlatlararo hamkorlik asosida hal qilishga majbur etmoqda.

Kibermakon xavfsizligining dolzarbligi, avvalo, kiberjinoyatlarning ko'payishida namoyon bo'lmoqda. Xalqaro statistika ma'lumotlariga ko'ra, 2023-yilda dunyo bo'yicha kiberjinoyatlar oqibatida yetkazilgan zarar 8 trillion AQSh dollaridan oshdi². Bu nafaqat iqtisodiy yo'qotish, balki ijtimoiy barqarorlikka ham tahdid bo'ldi. Moliyaviy firibgarlik, shaxsiy ma'lumotlarning o'g'irlanishi, davlat organlariga qarshi hujumlar jamiyat ishonchini zaiflashtirmoqda.

Shuningdek, kiberterrorizm va kiberpropaganda xavflari ham ortib bormoqda. Terroristik guruhlar internet orqali o'z

¹ Europol. Internet Organised Crime Threat Assessment 2018. – The Hague: Europol, 2018. – P. 11–17

² Cybersecurity Ventures. 2023 Cybercrime Report. – New York: Cybersecurity Ventures, 2023. – P. 5–10.

mafkurasini yoymoqda, yoshlarni radikallikka undamoqda. Davlatlararo axborot urushlari va dezinformatsiya kampaniyalari xalqaro munosabatlarga salbiy ta'sir ko'rsatmoqda. Shu bois, kibermakon nafaqat texnologik, balki falsafiy-huquqiy muammo sifatida ham o'rganilishi lozim.

Mavzuning dolzarbligi yana shundan iboratki, kibermakonda inson huquqlari va erkinliklari masalasi yangi bosqichga chiqdi. Bir tomondan, internet insonlarga so'z erkinligi, axborot olish, ijtimoiy tarmoqlar orqali o'z fikrini erkin ifoda etish imkonini berdi. Boshqa tomondan, shaxsiy hayot daxlsizligi va ma'lumotlarni himoya qilish masalalari jiddiy muammoga aylandi. Yirik IT-kompaniyalar (Google, Meta, Amazon, Microsoft) milliardlab foydalanuvchilarning shaxsiy ma'lumotlarini yig'imoqda va qayta ishlamoqda. Bu esa inson huquqlarining buzilishi, "raqamli qullik" xavfini yuzaga keltirmoqda¹.

Yana bir muhim jihat – raqamli suverenitet muammosidir. Davlatlar o'z hududida internet tarmoqlarini, axborot oqimlarini va shaxsiy ma'lumotlarni nazorat qilishga intilmoqda. Masalan, Xitoy "Buyuk xavfsizlik devori" orqali internetni qattiq nazorat qilsa, Yevropa Ittifoqi GDPR qonunlari orqali shaxsiy ma'lumotlarni himoya qilmoqda. Bu esa global boshqaruv mexanizmlari va milliy siyosatlar o'rtasida ziddiyatlarni keltirib chiqarmoqda.

Shu bilan birga, kibermakonda xavfsiz muhitni ta'minlash masalasi O'zbekiston uchun ham dolzarbdir. Mamlakatda "Raqamli O'zbekiston – 2030" dasturi qabul qilingan, "Shaxsiy ma'lumotlar to'g'risida" va "Axborot xavfsizligi to'g'risida"gi qonunlar qabul qilinib, amaliyotga tatbiq qilinmoqda². Bu tashabbuslar O'zbekistonning global jarayonda faol ishtirok etishini ko'rsatadi. Biroq xalqaro kiberxavf-xatarlarning kuchay-

¹ Floridi, L. The Ethics of Information. – Oxford: Oxford University Press, 2013. – P. 44–53.

² O'zbekiston Respublikasi Prezidentining PQ-6079-son qarori, 05.10.2020-y. "Raqamli O'zbekiston – 2030" davlat dasturi. – Toshkent: Prezident Administratsiyasi, 2020. – URL: <https://lex.uz/docs/5031048>

ishi shuni anglatadiki, milliy siyosatni global tamoyillar bilan uyg'unlashtirish talab etiladi.

Kibermakonda xavfsiz muhitni ta'minlash bugungi kunda falsafiy, huquqiy, siyosiy va amaliy jihatdan dolzarb ilmiy muammo sifatida qaralishi lozim. Bu nafaqat davlat siyosati, balki insoniyatning umumiy barqarorligi uchun ham muhim ahamiyat kasb etadi.

Kibermakon xavfsizligining dolzarbligi, shuningdek, uning geosiyosiy ahamiyatida ham yaqqol namoyon bo'lmoqda. XXI asrda davlatlar o'rtasidagi raqobat tobora axborot texnologiyalari maydoniga ko'chib bormoqda. Internet infratuzilmasi, sun'iy intellekt, kvant hisoblash, kosmik texnologiyalar kibergeosiyosatning markaziy elementlariga aylanmoqda. Natijada, "kiberqurollanish poygasi" kuchayib, davlatlar o'z milliy xavfsizlik strategiyalarini yangilashga majbur bo'lmoqda¹.

Kibermakonda kechayotgan kurashning asosiy sababi — axborot resurslari ustidan nazoratdir. Bugungi kunda axborot iqtisodiy boylik va siyosiy qudratning eng muhim omiliga aylangan. Shu bois yirik davlatlar kiberxavfsizlikni nafaqat mudofaa chorasiga, balki global hukmronlik vositasiga aylantirishga intilmoqda. Masalan, AQSh Milliy xavfsizlik agentligi (NSA) o'zining texnologik ustunligi orqali global axborot oqimlarini kuzatish imkoniyatiga ega. Xitoy esa o'zining "Kibersuverenitet konsepsiyasi" orqali internet ustidan qat'iy nazorat o'rnatib, milliy manfaatlarni ustuvor qo'ymoqda².

Shunday qilib, kibermakon xavfsizligi nafaqat huquqiy va axloqiy masala, balki xalqaro siyosiy kuchlar muvozanatida hal qiluvchi rol o'ynayotgan hodisaga aylandi. Bu esa uning dolzarbligini yanada oshirmoqda.

Kibermakon xavfsizligining yana bir dolzarb jihati — bu ijtimoiy ong va madaniyatga ta'siridir. Internet va ijtimoiy tarmoqlar insonlarning dunyoqarashini shakllantiruvchi asosiy vositaga aylandi. Dezinformatsiya, yolg'on xabarlar va manip-

¹ Nye, J. *Cyber Power*. – Harvard Kennedy School, 2010. – P. 7–12.

² Deibert, R. *Black Code: Inside the Battle for Cyberspace*. – Toronto: Signal, 2013. – P. 65–73.

ulyativ kontent jamiyatdagi ijtimoiy barqarorlikka bevosita xavf tug'diradi. Masalan, 2016-yilgi AQSh prezidentlik saylovi-da kiberpropaganda va "feyk news" muammosi demokratik jarayonlarga bevosita aralashuv sifatida baholangan¹. Shu kabi holatlar kibermakon xavfsizligini nafaqat texnik masala, balki siyosiy-falsafiy muammo sifatida ham ko'rib chiqishga majbur qiladi.

Axborot etikasi masalasi ham dolzarbdir. Insoniyat yangi texnologiyalardan foydalanar ekan, ularni axloqiy me'yorlar asosida boshqarishi zarur. L. Floridi, T. Moor, J. Weckert kabi olimlarning tadqiqotlari shuni ko'rsatadiki, axborot etikasi — bu faqat falsafiy tushuncha emas, balki global xavfsizlik siyosatining ajralmas qismidir². Axborotning haqqoniyligi, shaffofligi, shaxsiy hayot daxlsizligi kabi tamoyillar buzilsa, kibermakon xavfsizligini ta'minlash imkonsiz bo'ladi.

O'zbekiston uchun bu masalaning dolzarbligi ikki yo'nalishda ko'rinadi:

1. Milliy xavfsizlik nuqtai nazaridan. Kiberjinoyatlar, moliyaviy firibgarliklar, davlat ma'lumotlariga hujumlar mamlakat iqtisodiy va siyosiy barqarorligiga xavf tug'diradi.

2. Falsafiy-huquqiy nuqtai nazardan. Raqamli davrda inson qadr-qimmati, shaxsiy hayot daxlsizligi va huquqlarning kafolatlanishi O'zbekiston jamiyatida ham markaziy masalaga aylangan.

Shu bilan birga, kibermakonda xavfsiz muhitni ta'minlash bo'yicha xalqaro hamkorlikning dolzarbligi ham ortmoqda. BMT, NATO, SHHT, OSCE, ITU kabi tashkilotlar davlatlararo kelishuvlar orqali umumiy tamoyillarni shakllantirishga intilmoqda. Ammo amaliyotda milliy manfaatlar bilan global qadriyatlar o'rtasidagi qarama-qarshiliklar hanuz kuchli. Shu sababli, O'zbekiston kabi rivojlanayotgan davlatlar uchun eng muhim

¹ Allcott, H., Gentzkow, M. Social Media and Fake News in the 2016 Election. – Journal of Economic Perspectives, Vol. 31, No. 2, 2017. – P. 211–236.

² Floridi, L., Moor, J. H., Weckert, J. Information Ethics: On the Philosophical Foundations of Computer Ethics. – Ethics and Information Technology, Vol. 1, 1999. – P. 37–56.

masala — milliy siyosatni xalqaro tamoyillar bilan uyg'unlashtirishdir.

Kibermakon xavfsizligining dolzarbligi yana shundan iboratki, kelajakda yuzaga keladigan yangi texnologiyalar (masalan, sun'iy intellekt, kvant kompyuterlari) hozirgi xavfsizlik paradigmasini tubdan o'zgartirib yuborishi mumkin. Bugungi kunda qo'llanilayotgan kriptografik tizimlar kvant hisoblash imkoniyatlari oldida zaif bo'lib qolishi ehtimoldan xoli emas¹. Shu bois, texnologik rivojlanish bilan bir qatorda falsafiy va huquqiy asoslarni ham yangilab borish zaruriyati tug'ilmoqda.

Kibermakon xavfsizligining dolzarbligini belgilovchi yana bir muhim omil — bu xalqaro huquqiy me'yorlar va ularning yetarli darajada samarali ishlamayotganidir. Bugungi kunda kiberjinoyatlarga qarshi kurash bo'yicha yagona universal hujjat mavjud emas. 2001-yilda qabul qilingan Budapest konvensiyasi muhim bosqich bo'lsa-da, uni barcha davlatlar imzolamagan. Masalan, Rossiya, Xitoy, Braziliya kabi davlatlar konvensiyaga qo'shilmagan. Shu bois xalqaro maydonda turli yondashuvlar va manfaatlar to'qnashuvi mavjud bo'lib, bu jarayon global xavfsizlikni zaiflashtirmoqda².

Bundan tashqari, xalqaro tashkilotlarning tashabbuslari ham ko'pincha tavsiyaviy xarakterga ega. BMTning "Governmental Group of Experts" (GGE) va "Open-Ended Working Group" (OEWG) faoliyatlari muhim bo'lsa-da, ular davlatlar uchun majburiy huquqiy kuchga ega emas. Bu esa kibermakon xavfsizligini ta'minlashda huquqiy bo'shliqni keltirib chiqarmoqda³. Shu sababli yangi universal konvensiyalar ishlab chiqish zarurati tobora kuchaymoqda.

¹ Mosca, M. Cybersecurity in an Era with Quantum Computers: Will We Be Ready? – IEEE Security & Privacy, Vol. 16, No. 5, 2018. – P. 38–41.

² Council of Europe. Convention on Cybercrime (Budapest Convention). – Budapest: CoE, 2001. – URL: <https://www.coe.int/en/web/conventions/full-list>

³ United Nations General Assembly. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. – New York: UN, 2015. – A/70/174.

Kibermakonda xavfsizlik masalasining dolzarbligini oshiruvchi omillardan yana biri — kiberhujumlarning tanqidiy infratuzilmalarga tahdididir. Energetika, transport, moliya, sog'liqni saqlash kabi sohalar tobora ko'proq raqamlashtirilmoqda. Bu esa ularni kiberhujumlar uchun nishonga aylantiradi. Masalan, 2021-yilda AQShdagi Colonial Pipeline kompaniyasiga qilingan kiberhujum butun mamlakat bo'ylab yoqilg'i ta'minotida jiddiy uzilishlarga olib keldi¹. Bunday voqealar kibermakonda xavfsiz muhitni ta'minlash faqatgina texnik masala emas, balki milliy xavfsizlik strategiyalarining ajralmas qismi ekanini ko'rsatmoqda.

Kibermakon xavfsizligi dolzarbligining yana bir jihati — inson kapitali va ta'lim bilan bog'liqdir. Kiberhujumlarning aksariyati inson xatolari yoki yetarli bilimlarning yo'qligi sababli amalga oshiriladi. Shu bois davlatlar kiberxavfsizlik bo'yicha ta'lim dasturlarini kuchaytirishga alohida e'tibor qaratmoqda. UNESCOning ma'lumotlariga ko'ra, 2030-yilgacha kiberxavfsizlik sohasida 3,5 million mutaxassis yetishmasligi prognoz qilinmoqda². Bu esa kiberxavfsizlikni faqat texnologik emas, balki ijtimoiy-ta'limiy muammo sifatida ham ko'rib chiqishga asos bo'ladi.

O'zbekiston uchun bu masalaning dolzarbligi ayniqsa ahamiyatlidir. Mamlakatda raqamli transformatsiya jarayonlari jadal kechmoqda, biroq bu bilan birga yangi xavf-xatarlar ham paydo bo'lmoqda. Masalan, davlat xizmatlarining onlayn shaklga o'tishi, elektron hukumat tizimining kengayishi, moliyaviy xizmatlarning raqamlashtirilishi kiberhujumlar xavfini kuchaytiradi. Shu sababli, O'zbekistonda kibermakon xavfsizligini ta'minlash nafaqat texnologik siyosat, balki milliy ri

¹ Perlroth, N. How a Cyberattack on Colonial Pipeline Led to Fuel Shortages. – The New York Times, May 2021.

² UNESCO. Cybersecurity Skills Gap Report 2022. – Paris: UNESCO Publishing, 2022. – P. 19–26.

vojlantirish strategiyasining markaziy yo'nalishlaridan biri sifatida qaralmoqda¹.

Falsafiy nuqtai nazardan, kibermakon xavfsizligi dolzarbligi insoniyat oldida yangi savollarni tug'diradi: erkinlik va xavfsizlikning chegarasi qayerda? Shaxsiy hayot daxlsizligi davlat xavfsizligidan ustun qo'yilishi mumkinmi? Yangi texnologiyalar inson qadr-qimmatini mustahkamlashmi yoki uni zaiflashtirishmi? Shu kabi savollar kiberfalsafa va huquqiy tahlillarni birlashtirishni talab etmoqda.

Demak, mavzuning dolzarbligi quyidagi jihatlar orqali ifodalanadi:

1. Kiberjinoyatlar va kiberterrorizmning global ko'lamda ortib borishi.
2. Xalqaro huquqiy mexanizmlarning yetarli emasligi va yangi konvensiyalar zarurati.
3. Tanqidiy infratuzilmalarga tahdidlarning kuchayishi.
4. Inson huquqlari, shaxsiy hayot daxlsizligi va axborot etikasi muammolari.
5. Yangi texnologiyalar (SI, kvant hisoblash)ning xavfsizlik paradigmasiga ta'siri.
6. Kiberxavfsizlikda inson kapitali va ta'limning yetishmasligi.
7. O'zbekiston uchun milliy xavfsizlik va global hamkorlik nuqtai nazaridan dolzarblilik.

Shu asosda, kibermakonda xavfsiz muhitni ta'minlash masalasi dolzarb falsafiy-huquqiy muammo sifatida ko'rilishi va keng qamrovli ilmiy izlanishlarni talab qilishi isbotlanadi.

Kibermakon xavfsizligi va u bilan bog'liq falsafiy-huquqiy muammolar global miqyosda nisbatan yangi, ammo jadal rivojlanayotgan tadqiqot yo'nalishidir. Ushbu mavzuning o'rganilish darajasini tahlil qilar ekanmiz, uni uch bosqichda ko'rib chiqish mumkin: nazariy asoschilar, xalqaro ilmiy maktablar va O'zbekiston olimlari tadqiqotlari.

¹ O'zbekiston Respublikasi Prezidentining PQ-6079-son qarori, 05.10.2020-y. "Raqqamli O'zbekiston - 2030" davlat dasturi. - Toshkent: Prezident Administratsiyasi, 2020. - URL: <https://lex.uz/docs/5031048>

Kibermakon tushunchasi va uni o'rganishning dastlabki nazariy asoslari XX asr o'rtalaridan boshlangan. Birinchi navbatda A. Turingning "Computing Machinery and Intelligence" (1950) maqolasi alohida ahamiyatga ega¹. Unda u mashinalarning "aql"ga ega bo'lishi mumkinligi haqidagi savolni qo'yadi. Bu yondashuv keyinchalik sun'iy intellekt va kibermakon tushunchalarini falsafiy tahlil qilishga asos yaratdi.

N.Viner esa o'zining "Cybernetics: Or Control and Communication in the Animal and the Machine" (1948) asarida kibermakonning ilmiy paradigmasini shakllantirdi². Uning "kibernetika" tushunchasi texnologik jarayonlarni boshqarish va aloqa nazariyasini falsafiy darajaga ko'tardi. Aynan Vinerning ishlari zamonaviy axborot jamiyatining falsafiy asoslarini belgilab berdi.

Keyinchalik J.fon Neymanning "The Computer and the Brain" (1958) asari hisoblash jarayonlarini inson miyasi faoliyati bilan qiyoslab, kibermakonni ilmiy asosda anglashga xizmat qildi. Shu tariqa, ushbu olimlarning ishlari kibermakonni ontologik va gnoseologik talqin qilishga ilmiy zamin yaratdi.

XXI asr boshidan kibermakon xavfsizligi masalasi alohida ilmiy yo'nalish sifatida shakllandi. Bu borada bir necha xalqaro ilmiy maktablarni ajratib ko'rsatish mumkin:

- "Network Society" maktabi (M. Castells). Ispaniyalik sotsiolog Manuel Kastels o'zining "The Rise of the Network Society" (1996) asarida internet va tarmoqlashgan jamiyatning ijtimoiy tuzilishini tahlil qildi³. Unga ko'ra, kibermakon zamonaviy ijtimoiy tizimlarning asosiy maydoniga aylangan.

- Axborot etikasi maktabi (L. Floridi). Italiyalik olim Luciano Floridi "The Ethics of Information" (2013) asarida axborot

¹ Turing, A. *Computing Machinery and Intelligence*. – Mind, Vol. LIX, No. 236, 1950. – P. 433–460.

² Wiener, N. *Cybernetics: Or Control and Communication in the Animal and the Machine*. – Cambridge: MIT Press, 1948. – P. 11–25.

³ Castells, M. *The Rise of the Network Society*. – Oxford: Blackwell, 1996. – P. 1–35.

etikasi konsepsiyasini ishlab chiqdi¹. U kibermakon xavfsizligini axloqiy tamoyillar bilan uyg'unlashtirish zarurligini ta'kidladi.

- Kiberqudrat nazariyasi (J. Nye). Amerikalik siyosatshunos Joseph Nye "Cyber Power" (2010) asarida kibermakonni xalqaro siyosiy kuchning yangi manbai sifatida baholadi². Unga ko'ra, axborot resurslari harbiy kuch kabi strategik ahamiyatga ega.

- Kiberxavfsizlik siyosati maktabi (R. Deibert). Kanadalik olim Ronald Deibert "Black Code" (2013) asarida davlatlarning axborot ustidan nazorat o'rnatish siyosatini tahlil qildi³. U "internetni militarizatsiya qilish" xavfini ko'rsatib berdi.

- Huquqiy maktablar. "Tallinn Manual" (2013, 2017) xalqaro huquqda kiberurush masalalarini tartibga solishga qaratilgan eng muhim ilmiy ish sifatida e'tirof etilgan⁴. Bu hujjat NATO tomonidan qo'llab-quvvatlangan va kibermakonni xalqaro huquq kontekstida tahlil qilishga xizmat qilmoqda.

Shu asosda aytish mumkinki, xalqaro ilmiy maktablar kibermakon xavfsizligini turli yondashuvlardan – sotsiologik, falsafiy, siyosiy, huquqiy va texnologik jihatdan tadqiq etgan.

Kibermakon xavfsizligi masalalari Rossiya va Yevropa ilmiy maktablarida ham keng o'rganilgan. Ularning yondashuvlari ko'pincha xalqaro xavfsizlik, huquqiy me'yorlar, geopolitik manfaatlar va ijtimoiy-falsafiy talqinlar asosida shakllangan.

Rossiya ilmiy maktabi kibermakon xavfsizligini asosan geo-siyosiy va harbiy xavfsizlik nuqtai nazaridan tadqiq etgan. Bu yo'nalishda bir necha olimlarning ishlari alohida o'rin tutadi:

- A.V.Bartosh–uo'zining "Kiberugrozyimezhdunarodnaya bezopasnost'" (2012) asarida kiberxavfsizlikni xalqaro harbiy

¹ Floridi, L. The Ethics of Information. – Oxford: Oxford University Press, 2013. – P. 44–53.

² Nye, J. Cyber Power. – Harvard Kennedy School, 2010. – P. 7–12.

³ Deibert, R. Black Code: Inside the Battle for Cyberspace. – Toronto: Signal, 2013. – P. 65–73.

⁴ Schmitt, M. (ed.). Tallinn Manual on the International Law Applicable to Cyber Warfare. – Cambridge: Cambridge University Press, 2013. – P. 4–19.

xavfsizlikning ajralmas qismi sifatida talqin qiladi¹. Bartosh kiberhujumlarni yangi turdagi "gibrid urush" vositasi sifatida baholab, ularni xalqaro huquqda tartibga solish zarurligini ta'kidlaydi.

- I. O. Voynova – "Kiberprostranstvo kak novaya sotsial'naya real'nost'" (2018) asarida kibermakonni sotsiologik va falsafiy nuqtai nazardan tahlil qiladi². Unga ko'ra, kibermakon insoniyat hayotining yangi "ontologik maydoni" bo'lib, unda ijtimoiy munosabatlarning tubdan yangilanishi sodir bo'lmoqda.

- V. A. Knyazev – "Informatsionnaya bezopasnost' gosudarstva" (2015) kitobida Rossiya davlatining axborot suverenitetini ta'minlash mexanizmlarini o'rgangan³. Uning yondashuvida milliy manfaatlar ustuvorligi, shaxsiy huquqlar esa ko'proq ikkinchi planga tushib qolgan.

- G. L. Smolyan – "Tsifrovaya transformatsiya obshchestva i bezopasnost'" (2019) kitobida raqamlashtirish jarayonlarining xavf-xatarlarini tahlil qilib, kibermakonni nazorat qilmaslik jamiyat uchun jiddiy tahdid ekanini ko'rsatadi⁴.

Rossiya olimlari tadqiqotlari shuni ko'rsatadiki, bu maktabda kibermakon ko'proq davlat suvereniteti va milliy xavfsizlik bilan bog'liq masala sifatida talqin qilinadi. Shu bois ularning yondashuvlari xalqaro huquqiy kelishuvlardan ko'ra milliy siyosat va geosiyosiy manfaatlarga tayanadi.

Yevropa ilmiy maktabida kibermakon xavfsizligi asosan huquqiy va etik tamoyillar asosida o'rganilgan. Bu yerda bir necha muhim olim va institutlarning ishlari ajralib turadi:

- Jens David Ohlin – "The Ethics of Cybersecurity" (2019) kitobida kiberxavfsizlik masalalarini falsafiy-axloqiy nuqtai

¹ Bartosh, A. V. Kiberugrozy i mezhdunarodnaya bezopasnost'. – Moskva: Aspekt Press, 2012. – P. 14–28.

² Voynova, I. O. Kiberprostranstvo kak novaya sotsial'naya real'nost'. – Moskva: Nauka, 2018. – P. 33–49.

³ Knyazev, V. A. Informatsionnaya bezopasnost' gosudarstva. – Moskva: Yurayt, 2015. – P. 57–68.

⁴ Smolyan, G. L. Tsifrovaya transformatsiya obshchestva i bezopasnost'. – Moskva: ROSSPEN, 2019. – P. 41–52.

nazardan tahlil qiladi¹. U kibermakonda inson huquqlari va xavfsizlik o'rtasidagi muvozanatni topish zarurligini ta'kidlaydi.

- Michael Schmitt – NATO homiyligida tayyorlangan "Tallinn Manual" (2013, 2017) nashrlariga bosh muharrir sifatida katta hissa qo'shgan². Ushbu qo'llanma kiberurushni xalqaro huquq normalariga bog'lash bo'yicha eng muhim manba hisoblanadi.

- ENISA (European Union Agency for Cybersecurity) – bu tashkilot muntazam ravishda Yevropa Ittifoqi hududidagi kiberxavfsizlik holati haqida hisobotlar chiqaradi. Masalan, "ENISA Threat Landscape Report 2021"da asosiy kiberxavflar va ularning oqibatlarini tizimli tarzda yoritilgan³.

- Thomas Rid – "Rise of the Machines: A Cybernetic History" (2016) asarida kibernetika tarixini va kibermakon xavfsizligining geosiyosiy ildizlarini o'rganadi⁴.

- Eckersley, P. – Yevropalik huquqshunos sifatida "Digital Rights" bo'yicha olib borgan ishlari shaxsiy hayot daxlsizligi va ma'lumotlarni himoya qilish masalalarini keng qamrab oladi. Bu yondashuv ayniqsa Yevropa Ittifoqining GDPR (General Data Protection Regulation) hujjatida o'z ifodasini topgan.

Yevropa olimlari tadqiqotlarida kibermakon xavfsizligi ko'p-roq inson huquqlari, axborotetikasi va huquqiy standartlar bilan bog'liq masala sifatida talqin qilinadi. Bu Rossiya maktabidan farqli ravishda shaxsiy erkinlik va global tamoyillarni ustuvor qo'yadi.

Kibermakon xavfsizligi masalalari O'zbekistonda ham so'nggi yillarda dolzarb ilmiy tadqiqot yo'nalishlaridan biriga aylandi. Bu borada milliy olimlar tomonidan olib borilgan ilmiy izlanishlar, davlat siyosati va mintaqaviy hamkorlik tajribalari alohida e'tiborga loyiqdir.

¹ Ohlin, J. D. The Ethics of Cybersecurity. – Oxford: Oxford University Press, 2019. – P. 88–102.

² Schmitt, M. (ed.). Tallinn Manual on the International Law Applicable to Cyber Warfare. – Cambridge: Cambridge University Press, 2013. – P. 4–19.

³ ENISA. Threat Landscape Report 2021. – Athens: European Union Agency for Cybersecurity, 2021. – P. 12–27.

⁴ Rid, T. Rise of the Machines: A Cybernetic History. – New York: W. W. Norton & Company, 2016. – P. 63–78.

So'nggi o'n yillikda O'zbekistonda raqamli transformatsiya va kibermakon xavfsizligi mavzulariga bag'ishlangan ilmiy maqola, monografiya va dissertatsiyalar soni ortib bormoqda. Bu jarayonning uch asosiy yo'nalishini ko'rsatish mumkin:

1. Falsafiy-nazariy izlanishlar.

o A. Nurmatov o'zining "Kiberxavfsizlik falsafasi: ijtimoiy va huquqiy muammolar" (2022) asarida kibermakonni falsafiy jihatdan tahlil qilib, inson huquqlari va texnologik taraqqiyot o'rtasidagi muvozanat masalasini yoritgan¹. Unga ko'ra, kibermakon xavfsizligini faqat texnologik choralar bilan emas, balki axloqiy va falsafiy tamoyillar bilan uyg'unlashtirish lozim.

o Sh. Pirimova "Kiber makonda OAV so'z erkinligini ta'minlashning xavfsizlik tizimi" (2024) nomli maqolasida internetda axborot erkinligi va xavfsizlik o'rtasidagi qarama-qarshilikni o'rgangan². U axborot siyosatini demokratik qadriyatlar bilan uyg'unlashtirish zarurligini ta'kidlaydi.

2. Huquqiy tadqiqotlar.

o N. Qarshiyeva "O'zbekistonda kiberoxavfsizlik: raqamli iqtisodiyotni himoya qilish" (2024) maqolasida kiberji-noyatlarga qarshi huquqiy mexanizmlar va ularning milliy iqtisodiyotdagi o'rni haqida yozgan³. Uning tadqiqotida xalqaro konvensiyalar bilan uyg'unlik masalalari ham ko'tarilgan.

o I. Abdurahmonov "Raqamli iqtisodiyotda huquqiy muhofaza" (2021)⁴ kitobida shaxsiy ma'lumotlarni himoya qilish va raqamli iqtisodiy faoliyatda kiberoxavfsizlik masalalarini keng qamrab olgan.

¹ Nurmatov, A. Kiberxavfsizlik falsafasi: ijtimoiy va huquqiy muammolar. – Toshkent: Iqtisodiyot, 2022. – P. 21–36.

² Pirimova, Sh. Kiber makonda OAV so'z erkinligini ta'minlashning xavfsizlik tizimi. – Yangi O'zbekiston ilmiy-amaliy to'plami, №4(21), 2024. – P. 471–476.

³ Qarshiyeva, N. T. O'zbekistonda kiberoxavfsizlik: raqamli iqtisodiyotni himoya qilish. – Iqtisodiy integratsiya va mintaqaviy raqobatbardoshlik xalqaro jurnali, Vol. 1, №6, 2024. – P. 53–61.

⁴ Abdurahmonov, I. Raqamli iqtisodiyotda huquqiy muhofaza. – Toshkent: TDYUI nashriyoti, 2021. – P. 15–29.

3. Amaliy-texnik izlanishlar.

o Toshkent axborot texnologiyalari universiteti va Inha universiteti olimlari tomonidan kibermakon xavfsizligini ta'minlash bo'yicha texnik yechimlar, algoritmlar va dasturiy mahsulotlar ishlab chiqilmoqda. Masalan, kriptografiya, autentifikatsiya tizimlari, ma'lumotlarni himoya qilish protokollari bo'yicha bir qator ilmiy ishlar amalga oshirilgan.

Markaziy Osiyo mamlakatlari ham kibermakon xavfsizligini ta'minlash masalasini ilmiy tadqiqot darajasida o'rganib kelmoqda:

- Qozog'iston olimlari (masalan, A. Beisenov, "Informatsionnaya bezopasnost' Kazakhstana"¹, 2020) milliy axborot tizimlarini himoya qilish va xalqaro hamkorlik masalalariga e'tibor qaratmoqda.

- Qirg'izistonda "Kiberxavfsizlik konsepsiyasi – 2025" qabul qilingan va unga ilmiy doiralar faol hissa qo'shmoqda.

- Tojikiston va Turkmanistonda esa bu boradagi tadqiqotlar hali dastlabki bosqichda, asosan davlat siyosati va xalqaro tashkilotlar tavsiyalariga asoslangan.

Markaziy Osiyo davlatlari olimlarining umumiy xulosasi shundan iboratki, mintaqada kiberxavfsizlik masalalari bir-biriga chambarchas bog'liq va umumiy xavfsizlik tizimi yaratish dolzarbdir. Shu jihatdan, SHHT va MDH doirasidagi hamkorlik ilmiy va siyosiy jihatdan katta ahamiyat kasb etadi.

O'zbekiston va mintaqa olimlarining tadqiqotlari, garchi hali xalqaro miqyosdagi ishlardan ko'ra kamroq miqyosda bo'lsa-da, milliy tajriba va sharoitlarga moslashgan yechimlar ishlab chiqishga xizmat qilmoqda. Ularning ishlari asosan quyidagi yo'nalishlarda to'plangan:

- kiberxavfsizlikning falsafiy va axloqiy asoslari;
- huquqiy tartibga solish mexanizmlari;
- texnik yechimlar va amaliy qo'llanmalar;
- mintaqaviy xavfsizlik hamkorligi.

Demak, O'zbekistonda va Markaziy Osiyoda olib borilgan

¹ Beisenov, A. Informatsionnaya bezopasnost' Kazakhstana. – Almaty: KazNU, 2020. – P. 44–58.

tadqiqotlar kibermakon xavfsizligi muammosining dolzarbligini tasdiqlaydi va uni o'rganish bo'yicha ilmiy salohiyat shakllanayotganini ko'rsatadi.

Kibermakon xavfsizligi masalalari XX asr o'rtalaridan buyon jahon ilm-fanida keng o'rganib kelinmoqda. Ushbu tadqiqotlarning tahlili shuni ko'rsatadiki, mazkur mavzuning o'rganilganlik darajasini uch asosiy bosqichga ajratish mumkin: nazariy asoschilar, xalqaro ilmiy maktablar, hamda O'zbekiston va mintaqaviy izlanishlar.

Birinchi bosqichda, kibermakon tushunchasining nazariy poydevori asosan A. Turing, N. Viner va J. fon Neyman kabi olimlarning asarlarida shakllandi. Ularning ishlari mashina aqli, kibernetika va hisoblash jarayonlarini falsafiy talqin qilish orqali bugungi kunda kibermakon xavfsizligi bilan bog'liq tadqiqotlarga zamin yaratdi.

Ikkinchi bosqichda, xalqaro ilmiy maktablar shakllandi. M. Castells kibermakonni global tarmoqlar jamiyati sifatida tahlil qildi. L. Floridi axborot etikasi tamoyillarini ishlab chiqib, kiberxavfsizlikni axloqiy me'yorlar bilan bog'ladi. J.Nye kiberqudrat konsepsiyasini ilgari surdi va axborot resurslarini xalqaro siyosiy kuch sifatida baholadi. R. Deibert esa kibermakonni davlatlar tomonidan militarizatsiya qilinish jarayonini ko'rsatib berdi. Huquqiy maktablar doirasida yaratilgan "Tallinn qo'llanmasi" (2013, 2017) esa kiberurushni xalqaro huquq doirasida tartibga solishga uringan eng muhim ilmiy tashabbus sifatida qadrlanadi.

Rossiya olimlari orasida A. Bartosh kiberxavf-xatarlarni gibrid urush vositasi sifatida ko'rib chiqib, xalqaro huquqiy tartibga solish zarurligini ta'kidladi. I. Voynova kibermakonni ijtimoiy-falsafiy kategoriya sifatida tahlil qildi. V. Knyazev axborot xavfsizligida davlat manfaatlari ustuvorligini ilgari surdi, G. Smolyan esa raqamli transformatsiya xavflarini ko'rsatib berdi.

Yevropa maktabi esa inson huquqlari va axborot etikasi masalalariga ko'proq urg'u berdi. J. D. Ohlin kiberxavfsizlikni falsafiy-axloqiy nuqtai nazardan tadqiq etdi. M. Schmitt bosh

muharrirligida tayyorlangan "Tallinn qo'llanmasi" xalqaro huquqda katta ahamiyat kasb etdi. ENISA muntazam ravishda xavf-xatarlar bo'yicha tahliliy hisobotlar chiqarib, amaliy siyosiy tavsiyalar berdi. T. Rid esa kibernetikaning tarixiy ildizlarini o'rganib, zamonaviy kibermakon xavfsizligining geosiyosiy omillarini ochib berdi.

Uchinchi bosqichda, O'zbekiston va Markaziy Osiyo olimlarining tadqiqotlari shakllanmoqda. A. Nurmatov kibermakonni falsafiy jihatdan tahlil qilib, inson huquqlari va texnologiya o'rtasidagi muvozanat masalasini ko'tardi. Sh. Pirimova so'z erkinligi va xavfsizlik o'rtasidagi dialektikani o'rgandi. N. Qarshiyeva raqamli iqtisodiyot kontekstida kiberoxavfsizlikni huquqiy muammolar bilan bog'ladi. I. Abdurahmonov esa shaxsiy ma'lumotlar himoyasi va iqtisodiy faoliyat xavfsizligini tadqiq etdi. Markaziy Osiyo davlatlari, xususan Qozog'iston, Qirg'iziston va Tojikiston olimlari ham milliy kiberoxavfsizlik konsepsiyalari va xalqaro hamkorlik masalalariga hissa qo'shmoqda.

Umuman olganda, mazkur tadqiqotlarning tahlili shuni ko'rsatadiki:

- Nazariy asoschilar kibermakonni ilmiy va falsafiy tushuncha sifatida shakllantirgan.
- Xalqaro ilmiy maktablar uni siyosiy, huquqiy va axloqiy kontekstda keng qamrovli tahlil qilgan.
- Rossiya olimlari asosan davlat suvereniteti va milliy xavfsizlikka urg'u bergan bo'lsa, Yevropa tadqiqotchilari inson huquqlari va etik tamoyillarni markazga qo'ygan.
- O'zbekiston va mintaqaviy olimlarning ishlari esa milliy sharoitga mos ravishda falsafiy, huquqiy va texnik yechimlarni ishlab chiqishga qaratilgan.

Shunday qilib, kibermakon xavfsizligi masalasi xalqaro miqyosda keng o'rganilgan bo'lsa-da, u doimiy ravishda yangi ilmiy izlanishlarni talab qiladi. Xususan, O'zbekiston va Markaziy Osiyo sharoitida kibermakon xavfsizligini falsafiy-huquqiy nuqtai nazardan yanada chuqurroq o'rganish, xalqaro tamoyillar bilan uyg'unlashtirish dolzarb vazifa bo'lib qolmoqda.

Mazkur monografiyaning asosiy maqsadi – kibermakon xavfsizligini falsafiy-huquqiy tahlil qilish, turli davlatlar tajribalarini o'rganish va O'zbekiston uchun amaliy saboqlar chiqarishdan iboratdir. Bu maqsad kiberxavfsizlikni nafaqat texnologik, balki falsafiy, huquqiy va ijtimoiy nuqtai nazardan ham chuqur o'rganishni talab qiladi.

Monografiyaning umumiy maqsadi – kibermakonni insoniyat taraqqiyotining yangi ontologik maydoni sifatida talqin qilish, undagi xavfsizlik muammolarini tizimli tahlil qilish hamda davlatlar tajribasini qiyosiy asosda o'rganish orqali ilmiy xulosalar ishlab chiqishdir. Ushbu yondashuv kibermakon xavfsizligini faqat texnik muammo sifatida emas, balki global falsafiy-huquqiy muammo sifatida ko'rib chiqishni nazarda tutadi va quyidagi aniq maqsadlarni o'z oldiga qo'yadi:

1. Kibermakon tushunchasini falsafiy-huquqiy nuqtai nazardan tahlil qilish.

2. Kibermakon xavfsizligining global dolzarbligini ko'rsatish.

3. Rivojlangan davlatlar (AQSh, Yevropa Ittifoqi, Rossiya, Xitoy, Yaponiya, Janubiy Koreya)ning kiberxavfsizlik tajribasini o'rganish.

4. Markaziy Osiyo davlatlarida kibermakon xavfsizligi muammolarini tahlil qilish.

5. O'zbekistonning milliy strategiyasi va qonunchilik asoslarini chuqur o'rganish.

6. Xalqaro tashkilotlarning roli va global konvensiyalar zaruriyatini yoritish.

7. Kibermakon xavfsizligini ta'minlashda ta'lim va ilmiy tadqiqotlarning ahamiyatini asoslash.

8. Falsafiy-huquqiy umumlashtirish asosida O'zbekiston uchun amaliy tavsiyalar ishlab chiqish.

Mazkur maqsadlarni amalga oshirish uchun quyidagi vazifalar belgilangan:

1. Tarixiy-vazifaviy yo'nalish. Kibermakon tushunchasining tarixiy shakllanishini, kibernetika va informatikaning rivojlanishini, A. Turing, N. Viner va boshqa olimlarning hissasini ko'rsatish.

2. Huquqiy-vazifaviy yo'nalish. Xalqaro huquqiy hujjatlarni (Budapest konvensiyasi, Tallinn qo'llanmasi) o'rganib, ularning afzallik va kamchiliklarini tahlil qilish, O'zbekiston qonunchiligi bilan taqqoslash.

3. Siyosiy-vazifaviy yo'nalish. Kibermakon xavfsizligining xalqaro siyosiy jarayonlardagi o'rnini tahlil qilish, davlatlararo ziddiyatlar va hamkorlik imkoniyatlarini ko'rsatish.

4. Falsafiy-vazifaviy yo'nalish. Erkinlik va xavfsizlik dialektikasini falsafiy nuqtai nazardan asoslash, inson huquqlari va axborot etikasi masalalarini kiberxavfsizlik kontekstida qayta talqin qilish.

5. Amaliy-vazifaviy yo'nalish. O'zbekiston uchun milliy strategik chora-tadbirlar ishlab chiqish, "Raqamli O'zbekiston – 2030" dasturi doirasida kibermakon xavfsizligini mustahkamlash yo'llarini ko'rsatish.

Monografiyaning maqsadi va vazifalari kibermakon xavfsizligini kompleks yondashuv asosida o'rganishni ko'zda tutadi. Ya'ni:

- falsafiy nuqtai nazar kibermakonning mohiyatini ochib berishga xizmat qiladi;
- huquqiy tahlil xalqaro va milliy me'yorlarni taqqoslash imkonini beradi;
- amaliy vazifalar esa davlat siyosati va xalqaro hamkorlik uchun ilmiy asoslangan tavsiyalar ishlab chiqishga yordam beradi.

Bu yondashuv orqali tadqiqot kibermakon xavfsizligini ta'minlashga oid ilmiy, huquqiy va amaliy yo'nalishlarda bir vaqtning o'zida nazariy asos va amaliy yechimlarni ishlab chiqishga xizmat qiladi.

Monografiyaning ilmiy yangiligi. Kibermakon xavfsizligi masalalari bugungi kunda jahon miqyosida turli fanlar kesishmasida o'rganilmoqda. Ammo bu mavzuning falsafiy-huquqiy tahlili hali yetarli darajada chuqurlashmagan. Mazkur monografiyaning ilmiy yangiligi ham shundan iboratki, unda kibermakon xavfsizligi nafaqat texnologik va huquqiy muammo sifatida, balki falsafiy, ijtimoiy va axloqiy kontekstda

ham kompleks tarzda o'rganiladi.

Birinchidan, ushbu tadqiqot kibermakonni texnologik infratuzilma sifatida emas, balki yangi ontologik maydon sifatida talqin qiladi. Bu yondashuv I.Voynova, M.Castells va L.Floridi kabi olimlarning ishlari asosida yanada kengaytirilib, kibermakonning jamiyatdagi mohiyati, uning ijtimoiy ongga va madaniyatga ta'siri falsafiy-huquqiy nuqtai nazardan yoritiladi.

Kibermakon xavfsizligi shu bilan birga erkinlik va xavfsizlik dialektikasida ko'riladi. Mazkur tadqiqot inson huquqlari, shaxsiy hayot daxlsizligi va davlat suvereniteti o'rtasidagi qarama-qarshiliklarni falsafiy jihatdan asoslab beradi. Bu jihat ilmiy adabiyotlarda hali keng o'rganilmagan.

Ikkinchidan, AQSh, Yevropa Ittifoqi, Rossiya, Xitoy, Yaponiya va Janubiy Koreyaning milliy kiberxavfsizlik strategiyalari tahlil qilinib, ularning o'xshash va farqli jihatlari ko'rsatib beriladi.

Masalan:

- AQSh tajribasida milliy xavfsizlik va harbiy ustunlik birinchi o'ringa qo'yilgan.

- Yevropa Ittifoqi inson huquqlari va ma'lumotlarni himoya qilishga ustuvor ahamiyat bergan.

- Rossiya va Xitoy milliy suverenitet va davlat nazoratini markaziy nuqta sifatida belgilagan.

- Yaponiya va Koreya esa innovatsion texnologiyalar orqali kibermakon xavfsizligini ta'minlashga intilgan.

Ushbu qiyosiy tahlil yordamida O'zbekiston uchun qanday model samaraliroq bo'lishi mumkinligi yuzasidan ilmiy xulosalar chiqarilgan.

Uchinchidan, kibermakon xavfsizligini inson huquqlari bilan uyg'unlashtirish konsepsiyasini ishlab chiqishdir. Ko'plab tadqiqotlarda xavfsizlik texnik yoki huquqiy masala sifatida ko'riladi, inson huquqlari esa ikkinchi darajaga tushib qoladi. Mazkur monografiyada esa aksincha, inson huquqlari – shaxsiy hayot daxlsizligi, so'z erkinligi, axborot olish huquqi – kiberxavfsizlik siyosatining markaziy elementi sifatida qaraladi.

Bu jihat nafaqat falsafiy, balki amaliy ahamiyatga ham ega.

Chunki global miqyosda ham (masalan, Yevropa Ittifoqining GDPR hujjati), ham O'zbekiston qonunchiligida inson huquqlari va ma'lumotlarni himoya qilish masalalari tobora muhim bo'lib bormoqda.

Mazkur monografiyaning muhim ilmiy yangiliklaridan yana biri – kibermakon xavfsizligini O'zbekiston sharoitiga moslashtirilgan konseptual model asosida tahlil qilishdir. Raqamli iqtisodiyot, elektron hukumat, onlayn ta'lim va elektron tijoratning rivojlanishi bilan mamlakatda yangi turdagi xavf-xatarlar paydo bo'ldi. Shu bois tadqiqotda milliy qonunchilik (masalan, "Shaxsiy ma'lumotlar to'g'risida" va "Axborot xavfsizligi to'g'risida"gi qonunlar) xalqaro standartlar bilan qiyoslanib, bo'shliqlar va ehtiyojlar aniqlangan.

Bu yondashuvning yangiligi shundaki, kibermakon xavfsizligi masalalari milliy kontekstda – O'zbekistonning siyosiy, iqtisodiy va madaniy sharoitlarini hisobga olgan holda tahlil qilingan. Natijada, "Raqamli O'zbekiston – 2030" dasturining samarali amalga oshirilishi uchun ilmiy asoslangan tavsiyalar ishlab chiqilgan.

Ilmiy yangiliklardan yana biri kibermakon xavfsizligini dialektik yondashuv asosida tahlil qilishdir. Unda quyidagi qarama-qarshiliklar falsafiy nuqtai nazardan o'rganilgan:

- erkinlik ↔ xavfsizlik,
- global tamoyillar ↔ milliy manfaatlar,
- texnologik taraqqiyot ↔ axloqiy me'yorlar.

Mazkur dialektik yondashuv kibermakon xavfsizligini ko'p qirrali jarayon sifatida talqin etish imkonini beradi. Shu orqali inson huquqlarini cheklamagan holda xavfsizlikni ta'minlash mexanizmlari ishlab chiqiladi.

Monografiyada yana bir yangi ilmiy yondashuv sifatida kiberxavfsizlik madaniyatini shakllantirish masalasi ilgari surilgan. O'zbekiston sharoitida kiberxavfsizlikni ta'minlash faqat texnik yoki huquqiy choralar bilan cheklanmasligi, balki jamiyatda axborot madaniyatini rivojlantirish orqali amalga oshirilishi zarurligi asoslangan.

Shu nuqtai nazardan, ta'lim tizimiga kiberxavfsizlikka

oid fanlarni kiritish, ilmiy-tadqiqot muassasalarida axborot xavfsizligi bo'yicha alohida yo'nalishlar ochish taklif qilingan. Bu yondashuvning ilmiy yangiligi shundaki, u kibermakon xavfsizligini jamiyat ongining ajralmas qismi sifatida ko'radi.

Monografiyada kibermakon xavfsizligi masalalariga kompleks yondashuv asoslangan. U quyidagi uch darajani o'z ichiga oladi:

- texnik daraja (kriptografiya, dasturiy himoya, tarmoqlar xavfsizligi),
- huquqiy daraja (milliy qonunchilik, xalqaro konvensiyalar, tashkilotlar roli),
- falsafiy-ijtimoiy daraja (inson huquqlari, axborot etikasi, madaniy kontekst).

Mazkur yondashuvning ilmiy yangiligi shundaki, u kibermakon xavfsizligini faqat bitta yo'nalishda emas, balki tizimli ravishda, barcha omillar uyg'unligida tahlil qiladi. Bu esa O'zbekiston uchun universal, barqaror va amaliy asoslangan yechimlarni ishlab chiqishga imkon beradi.

Ushbu monografiya natijalari amaliy jihatdan bir necha yo'nalishda qo'llanishi mumkin.

Birinchidan, monografiyada ilgari surilgan nazariy va qiyosiy tahlillar O'zbekiston davlat siyosatini ishlab chiqishda qo'llanishi mumkin. Xususan:

- "Raqamli O'zbekiston – 2030" dasturini amalga oshirishda kibermakon xavfsizligini alohida ustuvor yo'nalish sifatida belgilash;
- milliy qonunchilikni xalqaro standartlarga (Budapest konvensiyasi, GDPR, Tallinn qo'llanmasi) uyg'unlashtirish;
- davlat organlari o'rtasida kiberxavfsizlikni muvofiq-lashtirish mexanizmlarini kuchaytirish.

Bu amaliy ahamiyat shundan iboratki, tadqiqot natijalari asosida ishlab chiqilgan tavsiyalar milliy xavfsizlik strategiyasini takomillashtirishga xizmat qiladi.

Ikkinchidan, kibermakon xavfsizligini huquqiy jihatdan tartibga solish hozirgi davrning eng dolzarb vazifalaridan biridir. Monografiya natijalari asosida quyidagi yo'nalishlarda

amaliy xulosalar chiqarish mumkin:

- "Axborot xavfsizligi to'g'risida"gi Qonun va "Shaxsiy ma'lumotlar to'g'risida"gi Qonunlarni xalqaro tajribaga mos holda yanada takomillashtirish;

- kiberjinoyatlarga qarshi maxsus qonunchilik asoslarini ishlab chiqish;

- sud-huquq amaliyotida kibermakon bilan bog'liq jinoyatlarni ko'rib chiqish mexanizmlarini kuchaytirish.

Bu yondashuv huquqiy tizimning amaliy samaradorligini oshirishga yordam beradi.

Uchinchidan, kibermakon xavfsizligini ta'minlash faqat texnologik yoki huquqiy chora-tadbirlar bilan cheklanmaydi. Bu jarayonda ta'lim tizimi muhim rol o'ynaydi. Monografiya natijalari ta'lim jarayonida quyidagi amaliy vazifalarni bajarishga xizmat qiladi:

- oliy ta'lim muassasalarida "Kiberxavfsizlik falsafasi", "Axborot etikasi", "Raqamli jamiyat xavfsizligi" kabi maxsus fanlarni joriy etish;

- talabalarni milliy va xalqaro tajribalar bilan tanishtirish;

- kiberxavfsizlik madaniyatini yoshlar ongida shakllantirish.

Ta'lim sohasidagi bunday amaliy yondashuv O'zbekistonning uzoq muddatli rivojlanish strategiyasida barqaror kiberxavfsizlik muhitini yaratishga zamin bo'ladi.

To'rtinchidan, monografiya natijalari xalqaro miqyosdagi hamkorlik uchun ham amaliy ahamiyatga ega. Chunki kibermakon xavfsizligini ta'minlashda biror davlat yolg'iz harakat qila olmaydi. Shu bois:

- BMT, NATO, SHHT, OSCE va ENISA doirasidagi hamkorlikni kengaytirish;

- qo'shni davlatlar bilan mintaqaviy kiberxavfsizlik tizimini shakllantirish;

- xalqaro konvensiyalar va kelishuvlarda faol ishtirok etish kabi vazifalar dolzarbdir.

Mazkur monografiyada berilgan tavsiyalar O'zbekistonning xalqaro miqyosdagi pozitsiyasini mustahkamlashga yordam beradi.